Estrategia Nacional de Ciberseguridad (ENCS)

I. Antecedentes: (2017). Proceso Colaborativo "Hacia Una Estrategia Nacional de Ciberseguridad":

1. **Primer Documento** de trabajo ENCS,
2. **Comentarios** de la **Consulta** pública sobre Ciberseguridad,
3. **Recomendaciones** expertos OEA y comunidad nacional a la ENCS,
4. **Documento:** Estrategia Nacional de Ciberseguridad.

II. Resumen ejecutivo de la ENCS

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

Para lograr su cometido, la ENCS se plantea **cinco objetivos estratégicos, en razón de Proteger:**

1. La **Sociedad y sus derechos**, con el fin de generar las condiciones para que la población realice sus actividades y ejerza sus derechos de manera responsable, libre y confiable en el ciberespacio.
2. La **Economía e innovación**, 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.
3. Las **Instituciones Públicas**, para proteger la información y los sistemas informáticos de las instituciones públicas del país, propiciando el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población.
4. La **Seguridad Pública**, orientado a incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio y mantener el orden y la paz pública.
5. La **Seguridad Nacional**, dirigido al desarrollo de capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan atentar contra la independencia, integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales.

Para lograr una protección adecuada a cada uno de los cinco objetivos estratégicos, la ENCS plantea **ocho ejes transversales**:

1) **"Cultura de la ciberseguridad"**, referente al conjunto de valores, principios y acciones en materia de concientización, educación y formación, los cuales inciden en la forma de interactuar en el ciberespacio de una manera armónica, confiable y como factor de desarrollo sostenible.
2) **"Desarrollo de capacidades"**, busca la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad.
3) **"Coordinación y colaboración"**, encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad.

4) **“Investigación, desarrollo e innovación en TIC”** refiere al fomento de la investigación, desarrollo e innovación en el uso y aprovechamiento de las tecnologías en materia de ciberseguridad.
5) **“Estándares y criterios técnicos”**, refiere al desarrollo, adopción y fortalecimiento de los estándares, criterios técnicos, mejores prácticas y de normalización en materia de ciberseguridad.
6) **“Infraestructuras Críticas”**, para minimizar la probabilidad de riesgos y vulnerabilidades en el uso de las TIC para la identificación, monitoreo y gestión de infraestructuras críticas.
7) **“Marco jurídico y autorregulación”**, busca adecuar el marco jurídico nacional vinculado a la ciberseguridad y promover mejores prácticas de autorregulación.
8) **“Medición y seguimiento”**, encaminado al fomento y desarrollo de mecanismos homologados de medición que permitan dar seguimiento a los resultados obtenidos de la implementación de la ENCS, así como proporcionar métricas de uso general.

Todas las acciones de la ENCS se han de desarrollar sobre **tres principios rectores**:

1. Perspectiva de derechos humanos;
2. Enfoque basado en gestión de riesgos, y
3. Colaboración multidisciplinaria y de múltiples actores.

Proceso **colaborativo.**

Acciones Relevantes

Eventos del proceso

- 19 y 20 de abril: Taller de múltiples partes interesadas (colaboración con OEA).
- 16 y 17 de mayo: Reuniones de seguimiento con las partes interesadas.
- 1 y 2 de junio: Taller de múltiples partes interesadas.
- 11 de julio: Foro de discusión en el Senado de la República.
- 12 y 13 de julio: Taller de múltiples partes interesadas (colaboración con OEA)
- 15 de agosto: Foro de discusión.
- 11 de octubre: Creación de la Subcomisión de Ciberseguridad de la CIDGE.
- 16 de octubre: Primera sesión de la Subcomisión de Ciberseguridad de la CIDGE.
- 26 de octubre: Segunda sesión de la Subcomisión de Ciberseguridad de la CIDGE.
- Semana Nacional de Ciberseguridad
- Otros eventos Académicos.

Participación ciudadana

- El documento de trabajo "*Hacia una Estrategia Nacional de Ciberseguridad*" se sometió a consulta pública.[1]
- Las opiniones de la comunidad se recolectaron por medio de una encuesta.[2]

Taller de múltiples partes interesadas
19 y 20 de abril de 2017, Secretaría de Relaciones Exteriores, Ciudad de México.[3]

- Primera actividad del proceso. Contó con el acompañamiento del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (CICTE-OEA).
- Asistieron integrantes de las diversos sectores de la comunidad (gobierno, sociedad civil, comunidad técnica, sector privado y academia).
- Contó con la participación de consultores internacionales y expertos de organizaciones internacionales, cuya participación fue facilitada por el CICTE-OEA.

Reuniones de seguimiento
16 y 17 de mayo de 2017, Oficinas de Presidencia de la República.

- Se llevaron a cabo reuniones por cada una de las partes interesadas de la comunidad.
- Se invitó a los asistentes a enviar comentarios generales en materia de ciberseguridad para la construcción de un documento de trabajo.

---

[1] Gob.mx, *Documento de trabajo Hacia una Estrategia Nacional de Ciberseguridad*, disponible en: https://www.gob.mx/participa/consultas/documento-ciberseguridad
[2] Gob.mx, Consulta, *Hacia una Estrategia Nacional de Ciberseguridad*, disponible en: https://www.gob.mx/mexicopropone
[3] Gob.mx, *Hacía la Estrategia Nacional de Ciberseguridad*, disponible en: https://www.gob.mx/mexicodigital/articulos/hacia-la-estrategia-nacional-de-ciberseguridad?idiom=es

Taller de múltiples partes interesadas
1 y 2 de junio de 2017, Tecnológico de Monterrey, Campus Ciudad de México.

- El taller llevó como título "Cuestiones sociales y económicas asociadas a la ciberseguridad".
- Participaron representantes de las partes interesadas de la comunidad.
- Al finalizar el taller, fueron identificados los temas de mayor interés para los asistentes:
    - Educación, cultura y concientización.
    - Formación de recursos humanos especializados.
    - Armonización legislativa.
    - Coordinación de esfuerzos de prevención.

47º Asamblea General de la OEA
19 al 21 de junio de 2017, Cancún, Quintana Roo.

La Organización de los Estados Americanos (OEA) entregó al gobierno de México una serie de recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad, con el objetivo de mejorar las capacidades de seguridad en el ciberespacio del país, en un evento realizado en el marco de la Asamblea General de la OEA realizado en Cancún, México.[4]

Foro de discusión
11 de julio de 2017, Senado de la República.

- Contó con la participación de múltiples actores de la comunidad.
- Sirvió como preámbulo del siguiente taller de múltiples partes interesadas con invitados internacionales.
- Se tomaron en cuenta los avances del proceso y se discutieron los próximos pasos.
- Señaló la relevancia de la incorporación del sector legislativo en el desarrollo de la estrategia.

Taller de múltiples partes interesadas
12 y 13 de julio de 2017, Holiday Inn Reforma, Ciudad de México.

- Tercer taller del proceso, segundo con la participación de expertos internacionales en colaboración con el CICTE-OEA.
- Publicación del primer documento de trabajo colaborativo del proceso "*Hacia una Estrategia Nacional de Ciberseguridad*".
    - El documento fue publicado en línea para consulta pública abierta en gob.mx/participa

[4] Organización de los Estados Americanos (OEA), *Recomendaciones para el Desarrollo de la Estrategia Nacional de Ciberseguridad*, disponible en: http://www.oas.org/documents/spa/press/Recomendaciones-para-el-Desarrollo-de-la-Estrategia-Nacional-de-Ciberseguridad.pdf

Foro de discusión
15 de agosto de 2017, Museo Memoria y Tolerancia, Ciudad de México.

- Foro de discusión orientado a la colaboración entre las partes interesadas, incluyendo las perspectivas de las organizaciones de la sociedad civil.
- Durante el evento, CICTE-OEA entregó comentarios al documento de trabajo *"Hacia una Estrategia Nacional de Ciberseguridad"*[5], sujeto a consulta pública.

Creación de la Subcomisión de Ciberseguridad de la CIDGE
11 de octubre de 2017, Secretaría de la Función Pública, Ciudad de México.

- Durante la XVIII sesión ordinaria de la CIDGE fue aprobada por unanimidad la creación de la Subcomisión de Ciberseguridad.
- La presidencia de la Subcomisión es ocupada por la División Científica de la Policía Federal.
- Sus integrantes iniciales son la Unidad de Innovación y Estrategia Tecnológica de la OPR, la Unidad de Gobierno Digital de la SFP, SEGOB, SE, SEP, SHCP, y PGR.

Primera sesión de la Subcomisión de Ciberseguridad de la CIDGE
16 de octubre de 2017, Presidencia de la República.

- Los integrantes de la Subcomisión aprobaron la lista de dependencias invitadas a la Subcomisión:
  - SEDENA, SEMAR, SAT, CNBV, PROFECO, CONDUSEF, IPN, CONACYT y CENACE
- Los integrantes e invitados acordaron revisar el documento de trabajo "*Hacia una Estrategia Nacional de Ciberseguridad*" y remitir comentarios.
- Fue aprobada la creación del Grupo de Trabajo de Comunicación en materia de Ciberseguridad.

Segunda sesión de la Subcomisión de Ciberseguridad de la CIDGE
26 de octubre de 2017, CONACYT, Ciudad de México.

- Los integrantes de la Subcomisión aprobaron añadir a 4 dependencias invitadas a la Subcomisión:
  - SRE, SSA, SIPINNA y la Secretaría Técnica del Consejo de Seguridad Nacional.
- Fue aprobada la Estrategia Nacional de Ciberseguridad en lo general.
- Presentación de la ENCS en el marco de la Tercera Semana Nacional de Ciberseguridad.[6] [7]

[5] https://www.gob.mx/cidge/es/articulos/estrategia-nacional-de-ciberseguridad-con-perspectiva-de-derechos-humanos?idiom=es https://www.gob.mx/cidge/es/articulos/estrategia-nacional-de-ciberseguridad-con-perspectiva-de-derechos-humanos?idiom=es

[6] Gob.mx, Programa de actividades "Tercera Semana Nacional de Ciberseguridad", disponible en: https://www.gob.mx/policiafederal/articulos/programa-de-actividades-tercera-semana-nacional-de-la-ciberseguridad

[7] Estrategia Nacional de Ciberseguridad, 13 de noviembre 2017, YouTube, disponible en: https://www.youtube.com/watch?v=vYqqvh04nYU

III. IMPLEMENTACIÓN. 2018.

La implementación de la ENCS está a cargo de la Subcomisión de Ciberseguridad de la **Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico** (CIDGE), fomentando la participación de actores de sociedad civil, academia, sector privado y otras instituciones públicas en los diversos Grupos de Trabajo.

Para la implementación se crearon Grupos de Trabajo por cada uno de los cinco objetivos estratégicos y ocho ejes transversales. Los grupos han tenido reuniones periódicas con sus equipos de trabajo, desde febrero de 2018.

Acciones y recomendaciones de los Grupos de trabajo

1. Protección de la Sociedad y Derechos

Líder: SIPINNA / IFT [8]
Integrantes: Autoridades del Gobierno Federal, actores de academia, sociedad civil, sector privado, expertos nacionales o internacionales.[9]

Acciones realizadas:

1) Mesas de trabajo

El 19 de mayo de 2018, se llevaron a cabo en las instalaciones del IFT cuatro (4) mesas de trabajo cuyo objetivo era diseñar la ruta crítica (actividades, fechas y responsables), plan de trabajo, análisis de riesgos y detección de sinergias de cada uno de los temas que conforman el objetivo estratégico mencionado, dichas mesas estuvieron conformadas y lideradas por representantes de los sectores público, privado, academia y la sociedad civil.

Las mesas se integraron de acuerdo al perfil de las cuatro mesas, cada organismo participante en el grupo tuvo la libertad de seleccionar el o los grupos que le interesan más o tuviera afinidad temática para participar como actor.

[8] Por SIPINNA, Valeria Berumen. Por IFT, Nimbe Leonor Ewald Arostegui.
[9] Autoridades del orden federal, organizaciones de la sociedad civil y académicas relacionadas.

Mesa 1: Fortalecimiento de políticas públicas **Líder**: UNAM-Fac de Ciencias Políticas y Sociales **Objetivo**: Identificar áreas de oportunidad y mejores prácticas en materia de ciberseguridad en el uso y aprovechamiento de las TIC para el fortalecimiento de políticas públicas con perspectiva de derechos humanos y no discriminación. **Participantes**[10]:
Mesa 2: Gestión de riesgos **Líder**: Asociación de Internet MX **Objetivo**: Indicar los ejes de una estrategia relativa a la gestión de riesgos en materia de ciberseguridad que permita concientizar e incentivar a la población en el uso responsable de las TIC. **Participantes**:[11]
Mesa 3: Marco jurídico **Líder**: UNAM **Objetivo**: Recomendar los mecanismos y ruta crítica para la actualización y armonización del marco jurídico en el ámbito de ciberseguridad con perspectiva de derechos humanos y no discriminación. **Participantes**: [12]
Mesa 4: Niñas, niños y adolescentes; accesibilidad, lenguas indígenas **Líder**: CNDH

No. .	Recomendación	Plazo
1.	Se detectó la falta de un marco legal que proporcione un nivel regulatorio óptimo, el cual contemple como punto de partida la ENCS y que asegure, proteja y resguarde el desarrollo de la ciberseguridad en México; principalmente para los grupos en situación de vulnerabilidad y que garantice los derechos vinculados con las tecnologías de la información y comunicación; impulse la coordinación y	**Corto**

[10] CÁMARA DE SENADORES (Comisión de Ciencia y Tecnología), UNAM, SCT, Asoc. de Internet MX. (Entuizer), ANATEL, PROFECO, SRE, Secretaría de Economía, Coordinación de Estrategia Digital Nacional, CONACYT, SIPINNA, IFT.

[11] Asoc. de Internet MX, ANATEL, INAI, INEGI, CNBV, IPN, Coordinación de Estrategia Digital Nacional, PGR – FEVIMTRA – Procuraduría de Derechos Humanos, PROFECO, CONDUSEF, CESI, CNDH, SIPINNA, IFT.

[12] SCJN, PGR - Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, Coordinación de Estrategia Digital Nacional, SFP – Unidad de Gobierno Digital, Asociación de Internet (Entuizer), R3D, CNDH, Subsecretaría de Derechos Humanos – SEGOB, CÁMARA DE SENADORES (Comisión de Ciencia y Tecnología), CÁMARA DE SENADORES (Comisión de Seguridad Pública), UNAM, INMUJERES, SIPINNA, IFT.

	colaboración entre dependencias y sectores involucrados; así como también contemple el manejo apropiado de los desechos informáticos.	
2.	Se requiere de desarrollo, formación y capacitación continua para el poder judicial, con el fin de que consolide sus conocimientos en este ámbito y con ello pueda afrontar los nuevos retos en la impartición de justicia. Aunado a lo anterior, también es indispensable educar a la sociedad a través de campañas que se ajusten a las necesidades de cada grupo, de conformidad con sus diferencias en lenguaje, edad y desarrollo, para el manejo de su exposición a contenidos en medios digitales e Internet.	**corto**
3.	El establecimiento de vínculos con organismos internacionales y con países que tengan implementadas estrategias de ciberseguridad, permitirá el intercambio de conocimiento y experiencias sobre las mejores prácticas, así como también sobre las amenazas y vulnerabilidades a las que se han enfrentado y cómo lo han logrado resolver o mitigar. Lo anterior, busca incluir, principalmente, el manejo que se le ha dado a los grupos en situación de vulnerabilidad.	**corto**
4	Dar seguimiento a los trabajos realizados, así como una activa participación de cada dependencia e integrante de las mesas de trabajo, con el fin de centralizar esfuerzos y no duplicar resultados.	**corto**
5	Es indispensable el compromiso de los proveedores de redes sociales y las instituciones públicas para dar atención enfocada a grupos en situación de vulnerabilidad y la garantía de sus derechos de cara a la Estrategia Nacional de Ciberseguridad, ya que esto no puede dejarse sólo en manos de los usuarios de las TIC e Internet.	**corto**
6	Es necesario incluir las mejores prácticas en materia de ciberseguridad en el uso y aprovechamiento de las TIC para el fortalecimiento de políticas públicas con perspectiva de derechos humanos.	**corto**
7	Se requiere la coordinación de todos los actores involucrados para establecer una estrategia de gestión de riesgos en materia de ciberseguridad que permita gestionar las principales amenazas a las que se encuentra expuesta la población, con la finalidad de concientizar e incentivar un uso responsable de las TIC.	**corto**
8	La actualización y armonización del marco jurídico en el ámbito de ciberseguridad con perspectiva de derechos humanos y no discriminación es requerida.	**mediano**
9	Se considera que la Estrategia Nacional de Ciberseguridad es un documento que requiere de actualizaciones constantes, y la implementación de la misma, cada vez debe incluir mayores actores y debe evolucionar a la par de las tecnologías, se debe considerar la protección de datos personales, la protección de la identidad, el patrimonio digital, así como la pérdida de la libertad de expresión.	**Corto y mediano**

2. Protección de la Economía e Innovación

Líder: Secretaría de Economía / CANIETI[13]

Integrante: Autoridades del Gobierno Federal, actores de academia, sociedad civil, sector privado, expertos nacionales o internacionales.

Acciones realizadas:

1. Se llevaron a cabo reuniones entre la Secretaría de Economía y la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), a fin de analizar tanto el objetivo como las líneas de acción propuestas en el documento de la ENCS.

2. Se llevó a cabo la reunión del grupo de trabajo, en la cual se revisó el objetivo del grupo, se definieron las líneas de acción y se analizaron las sinergias.

3. Se realizó artículo sobre la ENCS en la revista de negocios de ProMéxico. [14]

No.	Recomendación	Plazo
10	Difundir la Estrategia Nacional de Ciberseguridad y el Grupo de Economía e Innovación, a través de publicaciones en medios impresos o digitales. Con ello se busca que las empresas, industrias, así como el sector académico y la sociedad en general conozcan la ENCS.	**Corto**
11	Impulsar la vinculación de las mesas de trabajo de la Plataforma de Industria 4.0 MX de la Secretaría de Economía (eje rector de la política pública), en específico su mesa de ciberseguridad industrial, con el Grupo de Economía e Innovación de la ENCS.	**Corto**

[13] Por Secretaría de Economía, Raúl Rendón; por CANIETI. Mario de la Cruz.
[14] A publicarse en la edición de noviembre de 2018 de la revista Negocios de ProMéxico.

	Lo anterior en aras de poder contar con un análisis y seguimiento a los objetivos planteados, por parte de todos los miembros del ecosistema de economía digital e innovación.	
12	Identificación de las áreas de oportunidad en materia de economía e innovación en el uso y aprovechamiento de las TIC.	**Corto**
13	Fomentar la cultura digital y la formación en materia de ciberseguridad en los sectores productivos.	**Corto**
14	Impulsar acciones que fomenten el desarrollo del comercio electrónico y los servicios a través de las TIC.	**Corto**
15	Abrir el diálogo de las autoridades involucradas en la implementación de la ENCS y la industria.	**Corto**

Acciones realizadas y Recomendaciones de la CNBV

Acciones realizadas:

1. **Foro de Ciberseguridad "*Fortaleciendo la ciberseguridad para estabilidad del sistema financiero mexicano*"**

Celebrado en octubre de 2017, este Foro tuvo el objetivo de resaltar la importancia de procurar y fortalecer la seguridad de los sistemas e infraestructuras tecnológicas para hacer frente a ataques cibernéticos en protección de la información y patrimonio de los usuarios y entidades financieras, de la continuidad de los servicios, y de la estabilidad del sistema financiero en su conjunto.
A partir de este Foro, se construyó y firmó la "Declaración de principios para el fortalecimiento de la ciberseguridad para la estabilidad del sistema financiero mexicano" por parte de la Secretaría de Hacienda y Crédito Público (SHCP), la Comisión Nacional Bancaria y de Valores (CNBV), el Banco de México (Banxico) y los participantes del Sistema Financiero Mexicano.[15]

2. **Firma de las "Bases de Coordinación en materia de seguridad de la información"**

Como consecuencia de la atención y seguimiento a la "Declaración de principios para el fortalecimiento de la ciberseguridad para la estabilidad del sistema financiero mexicano", el día 24 de mayo de 2018, se firmaron las "Bases de Coordinación en materia de seguridad de la información" por

[15] Gob.mx, Foro de Ciberseguridad, disponible en: https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad?idiom=es

parte de los representantes de 6 autoridades del sector financiero, la Procuraduría General de la República (PGR), diversas asociaciones gremiales del sector financiero mexicano y entidades financieras particulares. Estas Bases fortalecen la forma en que las entidades y las autoridades del sector responderán y se coordinarán cuando ocurran eventos que puedan vulnerar la seguridad de la información en el sistema financiero mexicano.[16]

No.	Recomendaciones de la CNBV	Plazo
16	Fortalecimiento de Regulación de Ciberseguridad (CUB). Se están proponiendo modificaciones a las Disposiciones de Carácter General aplicables a las Instituciones de Crédito en materia de Seguridad de la Información, incluyendo una nueva sección (Octava Bis) denominada "De la seguridad de la información", que recopila las disposiciones en la materia, en las que se están plasmando, a efectos de homogeneizar los términos, los siguientes conceptos: Plan Director de Seguridad, Infraestructura Tecnológica, Usuario de la Infraestructura Tecnológica, Ciberataque y Riesgo de Ciberseguridad.	**Corto**
17	Fortalecer regulación. en todos los sectores financieros en los mismos términos que la regulación de Instituciones de Crédito, incluyendo los sectores supervisados por otras Autoridades Financieras.	**Corto-Mediano**
18	Llevar a cabo la creación de comités y grupos especializados que, entre otras cosas, se encarguen de efectuar el seguimiento y medición de las acciones que se desplieguen en el Sistema Financiero Mexicano, cuyo propósito esté enfocado en la atención de la "Declaración de principios para el fortalecimiento de la ciberseguridad para la estabilidad del sistema financiero mexicano" y de las "Bases de Coordinación en materia de seguridad de la información", así como de aquellas iniciativas que surjan en el sector para la protección de la información y patrimonio de los usuarios y entidades financieras.	**Corto-Mediano**
19	Brindar apertura e incentivar la creación de nuevas propuestas y medidas de ciberseguridad a ser adoptadas en el sector financiero, para crear un entorno seguro, en donde la población no sólo tenga cada vez un mayor acceso a servicios y productos financieros, sino que tenga una mayor confianza en su uso a través de medios digitales, fortaleciendo así la economía del país a través de la inclusión financiera.	**Corto-Mediano**

[16] Gob.mx, Firma de las bases de Coordinación en materia de Ciberseguridad, disponible en: https://www.gob.mx/cnbv/articulos/firma-de-las-bases-de-coordinacion-en-materia-de-seguridad-de-la-informacion?idiom=es

20	Concluir la definición e implementación de los Protocolos de Actuación del Grupo de Respuesta a Incidentes de Seguridad de la Información (GRI) que actualmente se encuentran en desarrollo, incluyendo la emisión de un Marco de Referencia en materia de seguridad de la información y Mecanismos de reporte e intercambio seguro de información entre autoridades, entidades y asociaciones del Sistema Financiero Mexicano.	**Mediano**

3. Protección de las Instituciones Públicas

Líder: SFP[17].

Integrantes: Autoridades del Gobierno Federal, actores de academia, sociedad civil, sector privado, expertos nacionales o internacionales.[18]

Acciones realizadas:

El 23 de febrero de 2018, se reunieron los integrantes del Grupo de Trabajo "Instituciones Públicas" (SFP; SHCP; SEGOB -DGTIC/CNS/PF-); SAT, y SE), con el objeto de definir su objetivo y líneas de acción.

Cómo objetivo se determinó "promover acciones que permitan fortalecer los mecanismos de protección en materia de ciberseguridad con los servidores públicos de la Administración Pública Federal y las Entidades Federativas, fomentar el uso de mecanismos de identidad digital, así como coordinar el análisis de vulnerabilidades en servicios digitales en beneficio de la población.

Como líneas de acción, el Grupo de Trabajo de Instituciones Públicas en materia de Ciberseguridad determinó las siguientes:

A. Medir el cumplimiento en las acciones de identificación, detección y reacción ante incidentes en materia de ciberseguridad;
B. Establecer un programa de capacitación para servidores públicos de los diferentes niveles de conocimiento del tema;
C. Fomentar el uso de mecanismos de identidad digital en la Administración Pública Federal y las Entidades Federativas, y
D. Extender la implementación de la Estrategia Nacional de Ciberseguridad a través de la Comisión Nacional de Gobernadores CONAGO.

En este contexto, en el marco del Grupo de Trabajo de "Instituciones Públicas", en materia de ciberseguridad, se llevaron a cabo las siguientes acciones:

1. En el marco del convenio de colaboración suscrito el 24 de noviembre de 2017, entre la Secretaría de la Función Pública y la Secretaría de Gobernación, a través de su Órgano Administrativo Desconcentrados Policía Federal, el cual tiene por objeto establecer las bases y los mecanismos de colaboración para el desarrollo de programas, planes de estudio, cursos y otros eventos académicos que tengan como propósito la capacitación, formación y actualización de servidores públicos de ambas instituciones, en materia de gobierno digital y, datos abiertos, así como prevención de delitos cometidos a través de medios electrónicos, que les permitan fortalecer las atribuciones que tienen encomendadas por disposición legal, se llevaron a cabo actividades de capacitación a servidores públicos en los tres niveles de gobierno.

[17] SFP. Tania Cruz Romero. Titular de la Unidad de Gobierno Digital.

[18] Lista de instituciones que conformaron el Grupo de Trabajo o colaboraron con los líderes para la obtención de las Recomendaciones y realización de esfuerzos.

Del citado Convenio de colaboración, en materia de ciberseguridad, se han logrado los siguiente:

- Se facilitaron **5 talleres presenciales**, dirigidos para servidores públicos federales con sede en Auditorio "Elvia Carrillo Puerto" de la Secretaría de la Función Pública, ubicado en la Ciudad de México:

Fecha	Tema	Número de Asistentes
23 marzo	Focus Group: Curso básico de ciberseguridad	10
20 de abril	Medidas básicas de ciberseguridad	240
25 de mayo	Ciberseguridad infantil	207
22 de junio	Ciberseguridad financiera	115
20 de julio	Ciberseguridad ciudadana	91

- Se facilitaron **4 talleres virtuales**, dirigidos para servidores públicos federales mediante la plataforma digital denominada Zoom:

Fecha	Tema	Número de Asistentes
30 de mayo	Ciberseguridad infantil	58
21 de junio	Ciberseguridad infantil	29
28 de junio	Ciberseguridad financiera	48
5 de julio	Ciberseguridad ciudadana	49

- Se facilitaron **4 talleres virtuales,** dirigidos para servidores públicos estatales y municipales mediante la plataforma Zoom:

Fecha	Tema	Número de Asistentes
25 de abril	Medidas básicas de ciberseguridad	45
27 de junio	Ciberseguridad financiera	28
11 de julio	Ciberseguridad infantil	29
2 de agosto	Prevención de delitos y abusos en línea	50

- En el marco de la iniciativa Academia Digital, a través de la cual se busca que las y los servidores públicos aprendan y refuercen los conocimientos y habilidades digitales, la Secretaría de la Función Pública y la Comisión Nacional de Seguridad, a través de la Policía Federal, pusieron a disposición el **"Curso básico de ciberseguridad"**[19].

[19] https://www.gob.mx/academiadigital/articulos/curso-basico-de-ciberseguridad

- La Secretaría de la Función Pública apoyó a la Unidad de Ciberseguridad, de la División Científica de la Policía Federal, para la revisión de la estructura de una nueva versión del Curso Básico de Ciberseguridad, mediante la realización de un Focus Group realizado el 23 de marzo del 2018. Además, se definió la dinámica de implementación y difusión del curso a nivel de servidores públicos de la Administración Pública Federal.

- La Policía Federal puso a disposición de las servidoras y servidores públicos este curso en línea de ocho horas, el cual se distribuyó en cuatro etapas. El único requisito para tomarlo fue tener acceso a una computadora con internet:

Etapa	Fecha de curso	Número de Participantes
Etapa 1	Del 2 al 13 de julio	114
Etapa 2	Del 16 al 31 de julio	641
Etapa 3	Del 06 al 17 de agosto	1,546
Etapa 4	Del 20 al 31 de agosto	1,360

2. El 10 de mayo de 2018, se publicaron en el Diario Oficial de la Federación, las *Disposiciones Generales que establecen los mecanismos de identificación digital y control de acceso que deberán observar las dependencias y entidades de la Administración Pública Federal y empresas productivas del Estado*[20], los cuales tienen por objeto establecer los mecanismos de identificación digital que deberán observar las instituciones, que servirán como parte del mecanismo de control para los servicios digitales y/o aplicativos electrónicos de las instituciones, así como los medios que otorguen seguridad técnica y certeza jurídica en la ejecución de dichos mecanismos.

3. El 23 de julio de 2018, se publicó en el Diario Oficial de la Federación, el *Acuerdo por 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*[21], en la cual contempla el uso de tecnologías emergentes como el Internet de las Cosas (IoT), la Inteligencia Artificial (IA), la robótica, el uso de tecnologías criptográficas basadas en redes de bloques distribuidos (blockchain), el poder de análisis de la computación cuántica.

Igualmente, en materia de identidad digital, en la Regla General 20 del citado Manual, se establece que el titular de la UTIC deberá asegurarse, conjuntamente con las áreas solicitantes de los aplicativos de

[20] *Cfr.* http://dof.gob.mx/nota_to_doc.php?codnota=5522133
[21] *Cfr.* http://dof.gob.mx/nota_detalle.php?codigo=5532585&fecha=23/07/2018

cómputo o servicios de TIC, que se incluyan en éstos, como campo llave para la interoperabilidad entre éstos, la Clave Única de Registro de Población (CURP) y, en su caso, otros atributos que permitan verificar la identidad digital correspondiente.

4. Por último, el Grupo de Trabajo de "Instituciones Públicas" en materia de ciberseguridad, en el marco del *Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias*, se determinó que es necesario contar con mecanismos de medición y fortalecer los procesos de seguridad de la información.

No.	Recomendación	Plazo
21	**Desarrollo de Capacidades.** Instrumentar un programa de capacitación para funcionarios públicos de los tres órdenes de gobierno en materia de ciberseguridad, conformado por una oferta de cursos en la materia, que pueda ser un modelo mixto, es decir, que combine tanto la capacitación presencial tradicional con la capacitación a distancia basada en las nuevas tecnologías de la información y comunicaciones, según corresponda, para que sean capaces de prevenir, identificar y manejar las amenazas inherentes del ciberespacio, con la finalidad de proteger los activos informáticos de la nación, generando de esta forma mayor certeza dentro de la población. Dicho programa deberá considerar los diferentes marcos jurídicos que correspondan.	**Corto**
22	**Mecanismos de Medición** Diseñar e implementar un mecanismo de medición soportado por tecnologías de la información y comunicaciones que permita, por un lado, generar un diagnóstico basado en información y datos duros sobre el estado en materia de ciberseguridad que guardan las diferentes Instituciones que conforman la Administración Pública Federal, y, por otro lado, desarrollar un plan de acción integral que pueda ser instrumentado por fases, con el propósito de cubrir áreas de oportunidad identificadas en el diagnóstico de referencia, considerando riesgos y amenazas existentes en las instituciones públicas federales y sus posibles impactos en caso de no tomar acciones inmediatas.	**Corto**
23	**Procesos en materia de seguridad de la información** Las instituciones públicas deberán establecer, ejecutar al interior, medir y mejorar de forma periódica, un proceso en materia de seguridad de la información, considerando al menos lo siguiente:	**Mediano**

1. Establecer, operar y mantener un modelo de gobierno de seguridad de la información, definiendo un responsable institucional a cargo del proceso del más alto nivel.
2. Efectuar la identificación de Infraestructuras de información esenciales y, en su caso, críticas, así como de activos clave de la Institución, y elaborar el catálogo respectivo.
3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.
4. Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.
5. Establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.
6. Vigilar los mecanismos establecidos y el desempeño del SGSI, a fin de prever desviaciones y mantener una mejora continua.
7. Fomentar una cultura de seguridad de la información en la Institución.
8. Instaurar un Comité de Control de Cambios, el cual sea el único ente autorizado para autorizar cambios dentro de la Infraestructura Tecnológica y de esa forma evitar que se apliquen cambios que no estén debidamente analizados y probados.
9. Instaurar un procedimiento de Control de Cambios de Emergencia, para aquellos casos en los que el pasar por un Comité de Control de Cambios no sea posible, dada la premura de la necesidad de aplicar un cambio.
10. Establecer un equipo de respuesta a incidentes de seguridad de TIC (ERISC) y definir los roles y responsabilidades de sus integrantes, así como asegurarse de que éstos conozcan las reglas de operación del mismo y la guía técnica de atención a incidentes.
11. El responsable de la seguridad de la información de las Instituciones que tengan el carácter de instancia de Seguridad Nacional, deberá coordinarse con las diversas instancias de Seguridad Nacional involucradas cuando se presente un incidente de seguridad que supere su capacidad de respuesta, utilizando los mecanismos que para el efecto establezca el Comité Especializado de Seguridad de la Información CESI.
12. El responsable de este proceso deberá coordinarse con los responsables de la administración de los servicios de TIC y con aquellos responsables de la operación de los mismos, a fin de que los acuerdos de nivel de servicio SLA y los acuerdos de nivel operacional OLA sean determinados y considerados en función de los programas de continuidad y de contingencia de la Unidad de TIC y del proceso.
13. Establecer, conjuntamente con los responsables de los procesos de la UTIC, así como en su caso con los servidores públicos que corresponda, los mecanismos para garantizar la protección de las infraestructuras de información esenciales y/o críticas que éstos tengan bajo su

	responsabilidad. 14. Asegurar que se integre al SGSI un control de seguridad para evitar intrusiones a la infraestructura de TIC, incluyendo ataques externos vía Internet, Intranet o Extranet. 15. Asegurarse de que se integren al SGSI, controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades.	
24	**Desarrollo de sistemas de información y aplicaciones informáticas.** En el desarrollo y operación de sistemas de información y aplicaciones informáticas, las instituciones públicas deberán considerar al menos lo siguiente, según corresponda, en concordancia con la normatividad vigente que aplique: 1. Requerimientos técnicos en materia de seguridad de información, de privacidad y protección de datos personales; 2. Uso de identidad digital; 3. Previo a la puesta en operación de la aplicación, realizar el o los análisis de vulnerabilidades que correspondan, los cuales, preferentemente deberán ser realizados por un tercero distinto a quien desarrolló la aplicación. 4. Prever que la transferencia de datos o información se realice sobre canales seguros en donde se favorezca el cifrado y la integridad de datos críticos y/o sensibles. 5. Integración de controles de seguridad de la información, así como de mecanismos de protección de ataques de denegación de servicios; 6. Considerar que su hospedaje se encuentre protegido bajo estándares nacionales, y en los casos que aplique, estándares internacionales de seguridad; asimismo, que sea provisto mediante enlaces de internet con protección ante amenazas y ataques, que permita mantener los niveles de servicio; 7. Mantener evidencia auditable del proceso de borrado seguro; 8. Utilizar mecanismos de autenticación y cifrado de acuerdo a estándares internacionales, con un grado no menor a 256 bits para la protección de la comunicación inalámbrica; 9. Implementar medidas y procedimientos para el respaldo de información; 10. Establecer herramientas de filtrado de contenido, que incluya búsquedas e imágenes en Internet, y permitan la segmentación en distintas categorías, reportes y soporte de sitios de nueva generación y/o micro-aplicaciones;	**Mediano**
25	**Fomentar el uso de los medios de identidad digital en servicios digitales,** con base en las *Disposiciones Generales que establecen los mecanismos de identificación digital y control de acceso que deberán observar las dependencias y*	**Corto**

	entidades de la Administración Pública Federal y las empresas productivas del Estado y el *Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias.*	
26	**Difundir la Estrategia Nacional de Ciberseguridad en las Entidades Federativas** 1. Una vez que se cuente con los documento finales de la Estrategia Nacional de Ciberseguridad, se sugiere fomentarla y difundirla a través de la CONAGO y la Subcomisión de Vinculación de Estados y Municipios. 2. Fomentar los cursos de capacitación de los servidores públicos en las Entidades Federativas y los Municipios. 3. Fomentar los mecanismos de identificación digital en servicios digitales.	**Mediano**

4. Protección de la Seguridad Pública

Líder: **CNS-PF-DC[22].**

Integrantes:[23] Autoridades del Gobierno Federal, actores de academia, sociedad civil, sector privado, expertos nacionales o internacionales.

Acciones realizadas:

La Policía Federal trabajó en dos vertientes:

1. En apoyo a los Ejes Transversales con el fin de desarrollar acciones o iniciativas que impacten en los propósitos del Objetivo Estratégico de Seguridad Pública se desarrollaron tres sesiones de trabajo, producto de estas sesiones:
    - Se evaluó la Cadena de Custodia Digital.
    - Se presentó la Propuesta del Modelo de Madurez de Ciberseguridad para evaluar a las Instituciones Públicas
    - Se presentó el primer borrador de la Estrategia de Infraestructuras Críticas (PF)
2. A través del Comité Especializado en Ciberseguridad, se llevaron a cabo dos sesiones con el apoyo de las 43 Unidades de Policías Cibernéticas Estatales a través de las cuales se fomentaron acciones de alcance nacional orientadas a la prevención e investigación de delitos e incidentes cibernéticos así como el impulso de políticas públicas conforme a la Estrategia Nacional de Ciberseguridad propuesta por parte del Gobierno de la República.

Las acciones realizadas son las siguientes:

- A través de la campaña “Un Cibernauta con Estrella” se logró impactar a 20 millones de ciudadanos de manera presencial y en línea.
- Creación del Comité Especializado en Ciberseguridad derivado del II acuerdo de las 2das Reuniones Regionales de la Conferencia Nacional de Secretarios de Seguridad Pública 2017.
- Conformación de 43 Unidades de Policía Cibernética Estatales, 24 dentro de las Secretarías de Seguridad Pública de las Entidades y 19 en Procuración de Justicia (en algunos casos una entidad federativa tiene dos Unidades Cibernéticas).
- Aprobación del Modelo Homologado de Unidades de Policías Cibernéticas que deberá ser implementado a partir de 2017, para lo cual las entidades federativas se comprometen a asignar recursos del Fondo de Aportaciones para la Seguridad Pública de los Estados (FASP).
- Implementación del Formato Homologado sobre Incidentes Cibernéticos a nivel Nacional que permitirá generar indicadores, estadísticas y tendencias de conductas delictivas en materia de ciberseguridad que coadyuven a la elaboración de políticas de prevención e investigación, mejorando los canales de coordinación entre las Unidades de Policías Cibernéticas Estatales, Policía Federal y autoridades competentes.

---

[22] CNS. Radames Hernández-

[23] Colaboradores: SEP-@prende, SFP, otros actores de gobierno federal, ANUIES, INFOTEC y otros actores de Academia.

No.	Recomendación	Plazo
27	**Cultura de Ciberseguridad (líder SEP-Coordinación @prende)** **Campaña Nacional de Concientización en Ciberseguridad "Ciberseguridad México 2018", Cibernauta con Estrella.** Promover acciones coordinadas entre los diversos involucrados para incrementar la resiliencia en los diferentes sectores de la sociedad, con la finalidad de: 1. Realizar campañas de concientización con alcance nacional. 2. Incorporar a los programas de educación básica, media y superior, los contenidos de civismo digital y ciberseguridad. 3. Capacitar a servidores públicos de seguridad pública, de procuración y administración de justicia de los tres niveles de gobierno en materia de ciberseguridad a fin de homologar criterios técnicos y procedimientos administrativos y penales. 4. Generar contenidos en diversos formatos para difusión impresa y digital, considerando la diversidad del público objetivo, a fin de impactar a un mayor número de personas, organizaciones e instituciones. 5. Promover la colaboración entre los diferentes actores estratégicos del país, para ampliar la difusión en múltiples medios de comunicación masiva con el objetivo de potenciar una agenda permanente de concientización. 6. Ampliar el número de eventos de concientización con enfoques específicos como el *ciberbullying, grooming*, privacidad y protección de datos personales, retos virales, seguridad de la información, entre otros. 7. Impulsar un programa de replicadores en todo el país con el fin de multiplicar esfuerzos con los distintos actores claves en el tema de concientización cibernética. 8. Generar guías de implementación de medidas de seguridad y orientación ciudadana con la comunidad.	**Mediano**
28	**Desarrollo de Capacidades.** **Modelo Homologado de Policías Cibernéticas.** 1. Dar continuidad a la implementación del Modelo Homologado de Unidades de Policía Cibernética para las Entidades Federativas, con la finalidad de fortalecer las capacidades de atención ciudadana, investigación y colaboración interinstitucional en los tres niveles de gobierno. 2. Establecer las acciones de mejora continua que permitan adaptar las	**Mediano**

	estrategias y las acciones sobre seguridad pública en materia cibernética, para responder ante los nuevos retos del entorno de ciberseguridad. 3. Establecer los mecanismos que permitan fortalecer la colaboración público-privada, y la coordinación y cooperación entre los distintos órdenes de gobierno incrementando la confianza ciudadana. 4. Establecer medios de contacto automatizados para la ciudadanía con autoridades policiales que fortalezcan la atención inmediata de cualquier delito cibernético.	
29	**Coordinación y Colaboración** **COMITÉ DE CIBERSEGURIDAD** **1.** Impulsar acuerdos en el marco del Comité de Ciberseguridad, a fin de impulsar estrategias y realizar acciones coordinadas de forma local, regional e internacional. 2. Llevar a cabo las gestiones correspondientes que permitan adecuar la normatividad actual a efecto de que el Comité sea un órgano colegiado que reporte directamente al Consejo Nacional de Seguridad Pública. **Intercambio de información** 1. Establecer plataformas tecnológicas para el intercambio de información entre instituciones de seguridad pública encargadas de ciberseguridad y cibercrimen tanto a nivel nacional como internacional.	**Mediano**

30	**Medición y seguimiento.** 1. Impulsar la implementación del Modelo de Madurez de Ciberseguridad para instituciones de seguridad pública del país a fin de identificar los niveles óptimos de seguridad de la información en los tres órdenes de gobierno que permitan su certificación en estándares nacionales e internacionales.	**Mediano**
31	**Marco jurídico y autorregulación.** 1. Implementar el Formato Homologado de Cadena de Custodia de Evidencia Digital que el registro y trazabilidad del manejo de los indicios digitales durante los procedimientos de investigación que realicen las autoridades competentes, a fin de establecer un instrumento de uso generalizado en el país que aporte además información para el impulso de políticas públicas.	**Mediano**

5. Protección de la Seguridad Nacional

Líder: CESI

Acciones realizadas:

1. **Concientización para funcionarios de alto nivel en materia de ciberseguridad:**

    a. Elaboración de un dossier en el que se contemplan notas de interés sobre ciberseguridad. [24]

    b. Implementación del curso básico de ciberseguridad para funcionarios de la APF. [25]

    c. Campañas de concientización sobre ciberseguridad.[26]

2. **Actualización del Manual Administrativo de Aplicación general en Materia de Tecnologías de la Información y comunicaciones (MAAGTICSI).**

    a. Se llevaron a cabo tres reuniones en las que participaron expertos en la materia. Durante los trabajos se analizaron los controles de la norma ISO 27002:2013, el COBIT y las estrategias implementadas en varios países.[27]

No.	Recomendación	Plazo
30	Es necesario crear un organismo con atribuciones legales y autonomía presupuestal para el desarrollo y aplicación de políticas públicas y coordinar los esfuerzos en materia de seguridad de la información.	**Corto**
31	Crear un Centro Nacional de Protección de Infraestructuras Críticas de Información para coordinar de forma adecuada las acciones de protección de los servicios vitales para el bienestar de la población y el funcionamiento de las instituciones del Estado mexicano.	**Mediano**

[24] Dossier de Ciberseguridad, disponible en: https://drive.google.com/file/d/1ji375G3hn1tMtBXQBvJ6pGDEypV0xsBQ/view

[25] Excelsior, CNS y SFP firman acuerdo para combatir los delitos cibernéticos, 25 de noviembre de 2018, disponible en: https://www.excelsior.com.mx/nacional/2017/11/25/1203556

[26] Gob.mx, La Comisión Nacional de Seguridad inaugura campaña de concientización, disponible en: https://www.gob.mx/segob/prensa/la-comision-nacional-de-seguridad-inaugura-campana-de-concientizacion-ciberseguridad-mexico-2018?idiom=es

[27] Propuesta de modificación para MAAGTICSI, disponible en: https://drive.google.com/file/d/10TvM4eiPpXles1QIqJ3gII1f586-v2pi/view

32	Impulsar el mejoramiento de las leyes y armonización legislativa para el castigo de delitos cibernéticos y la cooperación internacional para la detención de cibercriminales que atenten contra del Estado.	**Mediano**
33	Integrar un Catálogo Nacional de Infraestructuras Críticas de Información.	**Mediano**
34	Mejorar los protocolos de colaboración entre dependencias de la Administración Pública y la iniciativa privada para atender incidentes en contra de la Seguridad Nacional.	**Mediano**
35	Fortalecer las capacidades de monitoreo de las infraestructuras críticas de información para desarrollar acciones de defensa en el ciberespacio.	**Mediano**
36	Desarrollar cursos especializados para el personal del sector público y privado que se encuentre involucrado en la protección de infraestructuras críticas de información.	**Corto**
37	Continuar con la distribución de un documento diario con las principales notas de interés de ciberseguridad para los altos funcionarios de la APF.	**Corto**
38	Dar continuidad a la Campaña de Concientización “Ciberseguridad México 2018: #CibernautaConEstrella” y que se realice, como cada año, la Semana Nacional de Ciberseguridad en el mes de octubre.	**Corto**
39	Consolidar la implementación del curso básico de ciberseguridad, diseñado por la CNS, y destinado a todos servidores públicos de Gobierno Federal.	**Mediano**
40	Realizar la actualización del MAAGTICSI en temas de seguridad de la información y tecnologías de la información, a fin de actualizarla en los temas de riesgo y amenaza previstos en cada una de las dependencias que integran el Comité Especializado en Seguridad de la Información.	**Corto**

6. Comunicación Digital

Líder: Coordinación de la Estrategia Digital Nacional - Presidencia de la República

Integrantes: Enlaces de comunicación de las dependencias y entidades: CNS, CONDUSEF, CNBV, SEP-@prende.

Acciones realizadas:

Se realizaron reuniones con diferentes dependencias y entidades de la APF (Policía Federal, CONDUSEF, CNBV, Secretaría de Educación Pública - @prende) en las que se acordó el nombre la campaña, imagen y etiqueta #InternetSeguro[28]

No.	Recomendación	Plazo
41	Reuniones periódicas del grupo de trabajo para compartir nuevas estrategias y campañas de cada dependencia.	**Mediano**
42	Establecer la imagen de #InternetSeguro para toda la APF, de manera que exista una identidad gráfica homologada.	**Mediano**
43	Mantener el tópico "Internet Seguro" dentro de la Ventanilla Única Nacional para que todas las dependencias del grupo de trabajo puedan cargar el contenido relacionado.	**Corto**
44	Sensibilizar a las dependencias de la APF sobre le existencia de la campaña #InternetSeguro para que todas compartan material relacionado con el hashtag y la imagen correspondiente.	**Corto**
45	Activar una campaña transversal en toda la APF - y con más fuerza las dependencias pertenecientes al grupo de trabajo - cuando la coyuntura lo amerite. Por ejemplo: noticias sobre *fishing,* campaña en medios sobre trata de personas, alerta de nuevos *malwares*, etc.	**Mediano**

Recomendaciones de los Ejes transversales

Eje Transversal 1: Cultura y Seguridad

Líder: SEP-Coordinación General @prende.mx[29]

[28] Cfr. gob.mx, Internet seguro, disponible en: https://www.gob.mx/internetseguro

[29] SEP-Coordinación General @prende.mx, Cristina Cárdenas, Coordinadora General @prende.mx, , Carlos Anaya, Director de Estrategia Operativa y Aida Montiel Araujo, Subdirectora de Iniciativas Estratégicas.

Colaboradores[30]

Acciones realizadas:

1. **Talleres de Ciberseguridad**:

Con el fin de promover una concientización sobre el uso seguro y responsable de Internet, la CG@ y la División Científica de la Policía Federal implementaron una serie de Talleres de Ciberseguridad[31] de manera presencial. El objetivo de los talleres es ofrecer información que concientice a alumnas/os de educación básica, para conocer la manera más segura de navegar en la Red e identificar los riesgos que pueden llegar a enfrentar durante su uso. Desde noviembre de 2017, hasta agosto de 2018, se han beneficiado 15 entidades federativas, impactando en más de 23,500 alumnas/os.

2. **Contenidos de concientización en la Plataforma @prende 2.0:**

Con el propósito de promover y difundir ante la comunidad educativa (alumnos/as, docentes, padres de familia) y público en general, el uso seguro y responsable de Internet, la CG@ puso a disposición **recursos multimedia gratuitos**, a través del canal de Ciberseguridad de la Plataforma @prende 2.0.[32]

No.	Recomendación	Plazo
46	Dar seguimiento puntual a los compromisos derivados de las **Bases de Colaboración** entre la Secretaría de Educación Pública (SEP), a través de la Coordinación General @prende.mx (CG@) y la Policía Federal, mediante la División Científica, los cuales contribuyen con el eje Transversal 1 de la Estrategia Nacional de Ciberseguridad.	**Corto**
47	Continuar beneficiando a un **mayor número de alumnas y alumnos en las entidades federativas**, a través de la implementación de talleres presenciales sobre el uso seguro y responsable de Internet.	

[30] División Científica de la Policía Federal, SIPINNA, ANUIES, IPN.
[31] https://www.gob.mx/aprendemx/articulos/taller-la-ciberseguridad-es-materia-de-tod-s
[32] @prende 2.0, Canal de Ciberseguridad, disponible en: https://www.aprende.edu.mx/Canal/Ciberseguridad/index.html

48	Promover la participación de los actores que componen los grupos y ejes de la Estrategia Nacional de Ciberseguridad, de manera recurrente en la **Comunidad de Aprendizaje: Docentes @prende 2.0**, grupo en Facebook que cuenta con **más de 28 mil docentes de México,** a efecto de promover una cultura de uso seguro y responsable de Internet.	
49	Promover **campañas de concientización** sobre el uso seguro y responsable de Internet, a fin de que pueda ser replicado y escalado en más estados. Para ello, se podrá contar con el apoyo de los responsables del Programa de Inclusión Digital y a los SIPINNA en los 32 estados de la República.	**Media**
50	Alentar la implementación de más talleres de concientización sobre el uso seguro y responsable de Internet, a través de los **enlaces de prevención** de las coordinaciones regionales de la Policía Federal, con el apoyo de la Coordinación General @prende.mx, a fin de que puedan apoyar a las escuelas a visitar para las actividades.	
51	Ampliar el nivel educativo de beneficiarios, e impactar a **sectores de educación media superior y superior**, con el apoyo de aliados estratégicos, como lo es el Instituto Politécnico Nacional (IPN) y la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), con quienes se pueden crear importantes alianzas para llegar a un mayor número de beneficiarios.	
52	Continuar apoyando en los trabajos para contribuir con la homologación de términos, los cuales serán clave para contar con una difusión de información clara y concisa en la materia, apoyando al Eje Transversal 7.	

Eje Transversal 2: Desarrollo de Capacidades

Líder: [33]ANUIES
Colaboradores:[34]

Acciones realizadas:

[33] ANUIES. Mtro. José Luis Ponce López, Director de Tecnologías de Información y Comunicación, y Coordinador de Comité de Tecnologías de Información y Comunicación de la ANUIES (ANUIES-TIC).
[34] Universidades que participan en ANUIES-TIC. Grupo de Seguridad de la Información hacia el interior del Comité ANUIES-TIC: *http://anuies-tic.anuies.mx/web/seguridad-la-informacion/*

1. **Presentación de la implementación de la Estrategia Nacional de Ciberseguridad.**

2. **Presentación de la Subcomisión de Ciberseguridad.**

3. **Propuesta desde la perspectiva de las Instituciones de Educación Superior a través de una Comisión Especial del Comité ANUIES-TIC para la Captación de talentos, formación de capital humano y promoción del trabajo colaborativo entre Gobierno, Empresa y la Academia.**

4. **Identificación de capacidades en ciberseguridad.**

    a. Identificar proyectos implementados o en curso que apoyen los objetivos finales del eje transversal: Desarrollo de Capacidades

    b. Identificar nuevas iniciativas o áreas de mejora que apoyen los objetivos finales del eje transversal: Desarrollo de Capacidades.

5. **Propuesta de objetivos y líneas de acción para el eje transversal: desarrollo de capacidades.**

6. **Memorias y recomendaciones del eje transversal: Desarrollo de Capacidades.**

Respecto a las metas establecidas en las líneas de acción propuestas, se realizó lo siguiente:

- **Meta 1. Generar redes (comunidades digitales), nacional y regionales de desarrollo de capacidades en el ámbito de la Ciberseguridad**:

1. Propuesta de Curso Sello Universidad de Guadalajara
2. Propuesta de Módulo de Posgrado de TIC (Centro Universitario Tonalá de la UdeG)
3. Certificación de nuevas capacidades CONOCER: “Aplicación de habilidades para ciberseguridad en el ámbito laboral”

- **Meta 1.2. Convenios marco**

1. Firma de Convenio ANUIES-MNEMO
2. Proceso de firma de Convenio ANUIES – RENIC (Red de Excelencia Nacional de Investigación de Ciberseguridad en España)

- **Meta 1.3. Conformación de Redes**

1. Restablecimiento del contacto de la Red de Seguridad en Cómputo Región Centro-Sur de ANUIES

- **Meta 2.1. Encuesta Nacional del "Estado Actual de las TIC 2018" (sección: indicadores de seguridad de la información).[35]**

1. Lanzamiento de la convocatoria de la Encuesta "Estado actual de las TIC en las IES 2018" .
2. Apoyo a la encuesta de la OEA sobre Ciberseguridad (Policía Federal).

    a. Dimensión 3: Formación, Capacitación y Habilidades de Ciberseguridad

- **Meta 3.1. Potencial captación de talentos en Gestión/Operación de Ciberseguridad**

1. Existe la intención de conformar una iniciativa de captación de talento:

    a. RENIC
    b. MNEMO
    c. Talent Network
    d. Policía federal
    e. Instituto Politécnico Nacional - ESIME Culhuacán (Capture the Flag)

2. Generación de Webinars en colaboración con MNEMO- CERT para nivel licenciatura, posgrado y extensión universitaria.

    a. Retos de la seguridad en el sector financiera
    b. Mejores prácticas para el uso de dispositivos móviles
    c. Simulación de un ataque de malware mediante correo electrónico
    d. Actividad de Malware en México
    e. El forense y la teoría del árbol de los frutos envenenados
    f. Gestión riesgos e incidentes, preámbulo para la Continuidad de Negocio
    g. Técnicas de intrusión en las redes IP
    h. Explotación de vulnerabilidades con Metasploit
    i. Desastres físicos en infraestructuras de telecomunicaciones en IES.

3. Se destaca la temática de CIBERSEGURIDAD para el 3er. Encuentro ANUIES-TIC 2018[36]
4. El Comité ANUIES-TIC generó el Kit de Concientización en materia de Ciberseguridad con la colaboración de INCIBE.[37]
5. Diplomado de Seguridad Informática 2018, Modalidad Virtual.[38]
6. Participación con grupos de trabajo de los objetivos estratégicos:

---

[35] Cfr. ANUIES, Encuesta Nacional del "Estado Actual de las TIC 2016, disponible en: 2016: http://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2016_v2.pdf , y ANUIES, Encuesta Nacional del "Estado Actual de las TIC 2017", disponible en: 2017: http://estudio-tic.anuies.mx/ESTUDIO_2017_ANUIES-TIC_v2_2.pdf
[36] Cfr. ANUIES, Encuentro ANUIES-TIC 2018, disponible en:*https://encuentro-tic.anuies.mx/*
[37] ANUIES-TIC, Kit de Concientización, disponible en: http://anuies-tic.anuies.mx/web/kit/
[38] UACH, ANUIES, Diplomado en Seguridad Informática 2018, disponible en: http://diplomadoanuies.uach.mx/

a. Seguridad Pública
b. Sociedad y Derechos
c. Economía e Innovación

Y ejes transversales:

a. Estándares y criterios técnicos
b. Medición y seguimiento

No	Recomendación	Plazo
53	Generar redes (comunidades digitales), nacional y regionales de desarrollo de capacidades en el ámbito de la Ciberseguridad mediante la promoción de la colaboración con instancias nacionales e internacionales.	**Corto**
54	Realizar un Estudio Nacional sobre Desarrollo de Capacidades en Ciberseguridad mediante un Diagnóstico colaborativo entre los distintos actores de los grupos de trabajo y ejes transversales.	**Corto**
55	Promover la captación de talento académico, de especialistas e investigadores de las universidades e instituciones de educación superior e instancias afines mediante programas y eventos especializados.	**Corto**
56	Promover los programas académicos de las Instituciones de Educación Superior mediante la conformación de un sistema que oferte la Ciberseguridad.	**Corto**
57	Realizar programas especializados que atiendan necesidades específicas orientadas a la certificación de conocimientos en Ciberseguridad mediante el diseño de la currícula que requieran los actores de los grupos de trabajo y ejes transversales de la ENCS.	**Mediano**
58	La Ciberseguridad debe ser un proceso en las organizaciones y debe formar parte de la visión estratégica en la agenda directiva de las instituciones académicas, gobierno y empresas. 1. Se debe “vincular al sector académico, la industria y el gobierno” para la innovación y creación de proyectos de las áreas tecnológicas. 2. Se debe potencializar el trabajo de redes de colaboración mediante el uso de tecnologías de información y comunicaciones. Se deben establecer esquemas de cooperación interinstitucional con las IES que	**Mediano**

	cuentan con experiencia y disposición en el desarrollo tecnológico. 3. El capital humano especializado en seguridad en cómputo debe ser factor crítico en las áreas de tecnologías de información y comunicaciones de las organizaciones. 4. Se debe contar con programas de capacitación especializada en tecnologías de Ciberseguridad. 5. Se deben impulsar la Estrategia Nacional de Ciberseguridad mediante la conformación de grupos de trabajo especializado de la Academia los cuales deben vincularse e inter-operar con los sectores de la industria y gobierno. 6. Se deben de adoptar acciones que permitan la normatividad basada en estándares internacionales adecuados a las necesidades de cada organización. La aplicación de políticas de seguridad Informática, debe ser un elemento importante para este proceso. 7. Debe prevalecer el intercambio de experiencias y la cooperación interinstitucional de los sectores académico, de gobierno e industria, a través de la generación de los proyectos y de la realización de reuniones periódicas (presenciales o virtuales), las cuales deben incentivar y motivar el “espíritu de innovación” y “generación de conocimiento” entre las diversos sectores productivos del país. 8. Se debe promover la Cultura de la Ciberseguridad mediante campañas de concientización.	

Eje Transversal 3: Coordinación y Colaboración

Líder: Unidad de Innovación y Estrategia Tecnológica de Presidencia de la República de México.

Acciones realizadas:

1. Por las propias características de la ENCS el esfuerzo de implementación es muy amplio y complejo, por ello se tomó la decisión de ejecutar una estrategia incremental para su implementación, es decir, una implementación por fases.

   Se ejecutó la reunión de inicio de trabajos de implementación en febrero, en donde expresamente los líderes propuestos para cada Objetivo Estratégico y Eje Transversal manifestó su aceptación como líder y con ellos dar inicio a una participación *multistakeholders* con representación de gobierno, academia, industria y sociedad civil.

   Se definió que la primer fase de implementación sería un documento que integra los esfuerzos ya realizados y en ejecución dentro de los diferentes sectores representados en cada grupos de trabajo.

   Lo anterior fue uno de los principales insumos para transmitir un conocimiento transversal en la materia y estar en posibilidades de formular recomendaciones de cada grupo en su ámbito de competencia.Para ello, se diseñaron 4 entregables y un calendario de entrega de información y de reuniones.

   En cumplimiento a dicho calendario se ejecutaron 7 reuniones de líderes en las instalaciones de la Presidencia de la República con la finalidad de compartir trabajos realizados en cada grupo y tener el mismo nivel de conocimiento de las actividades realizadas, no obstante a estas reuniones de líderes, se participó en 23 mesas de trabajo organizadas en lo individual por cada grupo de trabajo, es decir, al menos una reunión de trabajo semanal.[39]

No.	Recomendación	Plazo
59	Mantener la ECNS como documento vivo. Mantener y fortalecer la participación multistakeholder en los diversos grupos de trabajo de la ENCS. Evaluar la ENCS cada 2 años para realizar ajustes en las acciones a desarrollar en cada Grupo de Trabajo. Establecer y fortalecer el marco institucional para una gestión integral de la ciberseguridad. Crear un ente público especializado en Ciberseguridad de alto nivel, incluyendo un modelo organizacional y de gobernanza de la ciberseguridad, que incluya la colaboración constante de múltiples partes interesada de los diverso sectores y órdenes de gobierno y poderes.	**Corto**

[39] Las reuniones realizadas desde 2017 a la fecha son evidencia de esta acción.

60	Invitar como integrantes a un Consejo Consultivo que acompañe y asesore al ente público especializado en Ciberseguridad. Con representación de: • Cada uno de los Organismos Constitucionales Autónomos • CONAGO • Poder Judicial • Poder Legislativo • Industria • Academia • Sociedad Civil Organizada • Comunidad Técnica	**Mediano**
61	Crear un ente público especializado en Ciberseguridad con enfoque ciudadano. Que sea el vínculo con los múltiples actores y fomente la cultura de ciberseguridad a toda la población y sectores.	**Corto**
62	Impulsar la participación de los otros órdenes de gobierno y coadyuvar a que formulen sus estrategias de Ciberseguridad, así como Estrategias especializadas por sector: Energía, Telecomunicaciones, Financiero,	**Mediano**

Eje Transversal 4: Investigación, Desarrollo e Innovación en TIC

Líder: CONACYT

Colaboradores: Autoridades del Gobierno Federal, Actores de la Academia, Sociedad Civil, Sector Privado, Expertos Nacionales o Internacionales.

Acciones realizadas:

1. Se asistió a la reunión mensual de líderes de grupos de trabajo y ejes transversales en donde se abordan los siguientes temas:

    a. Avances tanto de los líderes de los objetivos estratégicos, así como también de los objetivos transversales.
    b. Las acciones que se están llevando a cabo, o en su defecto, acciones propuestas para avanzar en el cumplimiento de los objetivos.

    En específico en una de las reuniones se abordaron los siguientes temas:

    La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) manifestó que hay una iniciativa muy fuerte de incluir alternativas de alto nivel en diversas instituciones para formar profesionales de alto nivel interesados en temas relacionados con ciberseguridad.

2. Se participó en la mesa de trabajo convocada por la "Asociación de Internet MX", lo anterior para tratar temas relacionados al eje transversal de "Estándares y Criterios Técnicos", en la cual se estableció la propuesta de realizar un diagnóstico en las instituciones para hacer de conocimiento del grupo, la existencia de estándares ya operando en estas; y de igual manera se estableció la propuesta de la generación de una regulaciones técnica (NMX o NOM) en la cual se considere cuestiones ciberseguridad, de cifrado de información, cadena de custodia, entre otras.

3. Se participó en las mesas de trabajo convocadas por el Instituto Federal de Telecomunicaciones, en específico en la mesa de "Fortalecimiento de políticas públicas" la cual fue liderada por la UNAM y cuyo objetivo era el de identificar las áreas de oportunidad existentes, así como también las mejores prácticas en materia de ciberseguridad en el uso y aprovechamiento de las TIC.
    De igual manera participaron en esta mesa la "Comisión de Ciencia y Tecnología de la Cámara de Senadores", "La Asociación de Internet MX", "PROFECO", "Secretaría de Relaciones Exteriores", "Secretaría de Economía".

4. Se participó en la mesa de trabajo convocada por "Policía Federal", lo anterior para tratar y se generó la propuesta de integración de una plataforma de colaboración para incidentes relacionados con "STIX, TAXII y CyBOX" con investigadores especializados en materia de ciberseguridad.

No.	Recomendación	Plazo
63	Crear un marco de desarrollo profesional en materia de ciberseguridad, a fin de que, los perfiles interesados en estos temas encuentren alternativas de alto nivel para el desarrollo de sus capacidades en el país y con ello evitar la fuga de talento al extranjero.	Mediano
64	Implementar una estrategia de difusión y colaboración institucional que permita que la investigación y los conocimientos en materia de ciberseguridad se traduzca en acciones concretas para evolucionar a una investigación aplicada y con ello convertir a la ciencia, la tecnología y la innovación en elementos fundamentales de la cultura general de la sociedad	Mediano
65	Impulsar la cultura de la ciberseguridad a través de la asignación de recursos institucionales, que permitan la implementación de líneas de acción específicas en el tema.	Mediano

Eje Transversal 5: Estándares y Criterios Técnicos

Líder: Asociación de internet Mx

Colaboradores: NYCE, INFOTEC, PF y otros socios Asociación de Internet Mx

Acciones realizadas:

1. Identificar los estándares y criterios técnicos Nacionales e internacionales existentes, aplicables a las ECSN. Estos estándares y criterios técnicos se han documentado en un documento que sirva como un marco de referencia en materia de ciberseguridad.

2. Coadyuvar con los Grupos de Trabajo para identificar la necesidad de aplicación de estándares y criterios técnicos.

3. Desarrollo, adaptación o modificación de estándares y criterios técnicos necesario para los grupos de trabajo y el cumplimiento de los objetivos de la ECSN. Para este esfuerzo se identificaron los siguientes proyectos de norma mexicana:

    a. Norma mexicana de comercio electrónica
    b. Norma mexicana escuelas seguras en el uso de internet
    c. Norma mexicana Metodología de análisis forense de datos y guías de ejecución

No.	Recomendación	Plazo
66	Desarrollar o adoptar normatividad en materia de monitoreo y respuesta ante incidentes de ciberseguridad, aplicable a los CERT y CSIRT	**Mediano**
67	Creación y mantenimiento de un marco de referencia que permita identificar las distintas normas existentes en el entornos nacional e internacional, que establezcan requisitos o brinden lineamientos para actividades relacionadas con la ciberseguridad, un ejemplo de este documento es el Ciber Security Framework Publicado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América, disponible en: https://www.nist.gov/cyberframework	**Mediano**
68	Adopción de estándares en materia de ciberseguridad de parte de la APF (incluyéndose al MAAGTICSI) y de la iNiciativa Privada (por medio de la certificación), incluyendo las prácticas establecidas en normas como ISO/IEC	**Mediano**

	27001, ISO/IEC 27001, ISO/IEC 271017, ISO/IEC 27018, ISO/IEC 27032	
69	Retomar al análisis para la adopción e implementación de la regulación y criterios necesarios para la firma y ratificación de México en el convenio de Budapest	
70	Desarrollar un marco de referencia de leyes, regulaciones y otra normativa aplicable en materia de ciberseguridad, en particular que identifique: - La tipificación de los delitos cibernéticos - Las obligaciones que deben cumplir los sujetos obligados	**Mediano**

Eje Transversal 6: Infraestructuras Críticas

Líder: SENER

Colaboradores: CESI

Acciones realizadas:

- Se llevó a cabo la reunión de trabajo con personal de la CFE para identificar los avances realizados por éstos, para el establecimiento del Eje Transversal 6 “Protección de Infraestructuras Críticas”.
- Adicionalmente, se le hizo la invitación a formar parte del grupo piloto del Sector Energético a fin de establecer las líneas de acción básicas para la protección de las infraestructuras de información consideradas estratégicas
- Se realizó una reunión de trabajo con personal de PEMEX para conocer sus avances en el tema de “Protección de Infraestructuras Críticas”.
- Adicionalmente, también se le hizo la invitación a formar parte del grupo piloto del Sector Energético a fin de establecer las líneas de acción básicas para la protección de las infraestructuras de información consideradas estratégicas.
- Se realizó una reunión con personal de la Oficina Comercial de Finlandia para revisar su estrategia de Ciberseguridad a fin de complementar el desarrollo del Eje Transversal 6. Derivado de dicha reunión, se obtuvieron los documentos “Cyber Security in Finland” así como “Finland´s Cyber security Strategy”, mismos que se encuentran en análisis de la Dirección General de Tecnologías de Información y Comunicaciones.
- Se convocó a una reunión con los representantes de seguridad de todas las dependencias, organismos desconcentrados y empresas productivas del Sector Energía, misma que se celebró en las instalaciones de la Secretaría de Energía el pasado viernes 24 de junio de 2018.

No.	Recomendación	Plazo
71	Una vez que se haya establecido, y se encuentre trabajado con el grupo del sector energético, el cual tendrá la función de establecer las bases y líneas de acción para la identificación, monitoreo y protección de sus infraestructuras críticas, se procederá a establecer grupos de trabajo con las cabezas de los sectores productivos de la Nación, a fin de enriquecer y homologar las acciones antes mencionadas.	**Corto**
72	Identificar las Infraestructuras Críticas y las Infraestructuras Críticas de Información para impulsar el plan de protección por parte de los sectores productivos de la Nación.	**Corto**
73	Explorando actualmente la posibilidad de organizar un evento para octubre de	**Corto**

	2018, de Protección de Infraestructuras Críticas de Información, donde se planea invitar a representantes de los diversos sectores del país, así como contar con oradores del sector público y privado que aporten sus experiencias y recomendaciones.	
74	Coordinar las actividades realizadas tanto por el CISEN, el CIDGE y el CESI para con ello trabajar en un solo contexto ya que se ha detectado que, en dichas instancias, se está trabajando en el tema de Infraestructuras Críticas de manera aislada.	**Corto y Mediano**
75	Seguir la Guía de Buenas Prácticas en Protección de Infraestructuras Críticas de Información (Meridian), para que el documento y procedimientos subsecuentes que surjan del mismos, estén orientados en mejores prácticas internacionales.	**Corto**
76	Establecer un documento rector, tomando como referencia la guía mencionada, en el cual se establezcan y homologuen de manera general los pasos que debería seguir cualquier organización para la identificación de sus infraestructuras críticas, sus infraestructuras críticas de información y el plan de protección de las mismas. Este documento se pretende sea cabildeado con los grupos mencionados en el punto 4, esto con el fin de obtener retroalimentación que permita eficientar el proceso de detección, monitoreo y atención de Infraestructuras Críticas.	**Corto**

Eje Transversal 7: Marco Jurídico y Autorregulación

Líder: Anahiby Becerril (INFOTEC-AMDETIC)

Colaboradores: SEP-@aprende, Policía Federal, otras autoridades del gobierno federal, Academia, NYCE, ANUIES, CONACYT, SE, expertos nacionales, sector privado y sociedad civil

Acciones realizadas:

1. **Asistencia a la segunda reunión del Grupo de Trabajo de Seguridad Pública, donde se propuso:**

    a. Revisión del proyecto de cadena de custodia evidencia digital
    b. Propuesta de la realización de talleres de práctica jurídica en materia de delitos electrónicos, por parte de PF en colaboración con las Procuradurías Estatales.
    c. Envío de sugerencias del Proyecto de NMX-I-319-NYCE-2017 Tecnologías de la Información-Técnicas de Seguridad- Escuelas responsables en el uso de Internet.

2. **Asistencia a la primera reunión del Grupo de Trabajo Economía e Innovación, donde se señalaron áreas de oportunidad:**

    a. Conformación de documento de buenas prácticas en materia de ciberseguridad, enfocado a MiPyMES, desarrollado por el Grupo de Trabajo Secretaría de Economía.
    b. Revisar la regulación y estándares en materia de seguridad de la información, que sean aplicables a las empresas.
    c. Se envió documento de sinergias a SE.

3. **Asistencia a la reunión mensual de líderes de grupos de trabajo y ejes transversales:**

    a. Presentación de los objetivos del ET7.
    b. Realización de propuestas de trabajo a otros líderes, detectar áreas de oportunidad:
        i. Propuesta a SEP para la elaboración de un protocolo de Actuación de Instituciones de educación básica en casos de violencia a través de medios electrónicos (redes sociales):
        ii. Propuesta ANUIES para impulsar un documento de recomendaciones a Instituciones de educación superior, para incorporar en sus planes de estudio materias que involucren las siguientes temáticas: Derecho Informático o TIC, informática forense, comercio electrónico/economía digital, Protección de datos personales (para empresas y sujetos obligados), derecho de la ciberseguridad, entre otros.

4. **Primera reunión del Eje Transversal 7 "Marco Jurídico y autorregulación":**

a. Se llevó a cabo la 1ª reunión del ET7.
b. Se realizó la invitación a diversos *stakeholders*
c. Presentación de los objetivos a trabajar, y detección de áreas de interés.
d. Solicitud de propuestas de contenidos y temas por abordar.

5. **Reunión mensual de Líderes de grupo:**

a. Asistencia y presentación de avances.

6. **Asistencia a la primera reunión del Eje Tranversal 6 "Estándares y Criterios técnicos:**

a. Propuesta de NMX y NOM, a saber: en cifrado, ciberseguridad (NIST Cybersecurity Framework- NIS UE), cadena de custodia y levantamiento de evidencia digital, entre otras.

7. **Participación en las mesas de trabajo relativas al objetivo estratégico "Sociedad y Derechos":**

a. Se presentó la sugerencia para una reforma legislativa en materia de protección de datos personales de niñas, niños y adolescentes.

8. **Segunda reunión del eje transversal 7 "Marco Jurídico y autorregulación":**

a. En específico se abordó el tema del documento de levantamiento de evidencia digital y cadena de custodia, a partir de la experiencia de Policía Federal. A partir de aquí se conformará una propuesta.

9. **Participación en la reunión del eje transversal "Estándares y criterios técnicos"**
10. **Asistencia a la primera reunión del eje transversal 8. "Medición y seguimiento" de la ENCS. Derivado de la reunión se llevaron a cabo las siguientes acciones:**

a. Envío de propuestas para conformar el índice de medición y seguimiento de la ENCS.
b. Propuesta para un foro en materia de derecho internacional y la postura del Estado mexicano en respuesta a ciberataques y la colaboración internacional de un ciberespacio seguro.

11. **Tercera reunión ET "Marco Jurídico y autorregulación":**

a. Presentación de la propuesta final del documento de evidencia digital y cadena de custodia.
b. Análisis de la propuesta para la medición e indicadores del índice de medición de la ENCS presentado por el ET8.

12. **Asistencia a la tercera reunión Objetivo Estratégico "Seguridad Pública":**

a. Se asistió a la reunión.

b. Presentación del documento final de levantamiento de evidencia digital mismo que deberá ser aprobado por la CNS y propuesta para la conformación de un manual para operadores de justicia y una NOM en la materia.

13. **Reunión con ProMéxico para establecer lineamientos de participación para artículo en PROMEXICO, respecto al marco legal de ciberseguridad, derivado de la ENCS:**

a. El artículo fue enviado en versión español e inglés, el 20 de agosto de 2018.

No.	Recomendación	Plazo
77	Con el empleo de las TIC y el ciberespacio para la comisión de delitos, la situación se torna diferente a los métodos tradicionales. Lo anterior consecuencia de su accesibilidad, costo, además de tener un mayor impacto en poco tiempo. Para establecer la responsabilidad, la evidencia es crítica. Sin embargo, la naturaleza del ciberespacio, y en particular el hecho de que es un dominio virtual, el anonimato y la velocidad de las actividades que en él se desarrollan, la posibilidad de "suplantación" y el potencial de la acción en múltiples etapas, plantea serios desafíos para la colección, el análisis, autenticación y evaluación de evidencia. Ahí la importancia de *contar con un marco jurídico adecuado* que sea aplicable a los delitos que diariamente se cometen en este ambiente virtual.	**Largo**
78	*Impulsar los trabajos para la adhesión de México al Convenio de Budapest*. No debemos olvidar que, gracias a su transnacionalidad, las amenazas no sólo provienen de actores locales, sino que pueden provenir de cualquier lugar del mundo. En los últimos años los ciberataques transnacionales han ido en incremento, y esta tendencia irá en aumento. Hemos sido testigos de la exposición de nuestras vulnerabilidades, hemos presenciado daños a gran escala, a miles de personas e infraestructuras, veloz y sin fronteras. Destaca así la necesidad de contar con un marco jurídico que nos provea de cooperación internacional, para la colaboración a los delitos transnacionales, en específico los que se llevan a cabo a través de esta tecnología. De ahí la importancia de continuar con los trabajos para el análisis de la adhesión a México del Convenio de Budapest. Estamos ante la gran oportunidad de lograr un consenso internacional que ayude al combate contra el cibercrimen.	**Corto**
79	Conformación de un un marco regulatorio que nos provea de herramientas necesarias para prevenir, proteger, responder y ser resilientes ante los actos delictivos que se comenten en el ciberespacio. Lo anterior debe desarrollarse respetando siempre la arquitectura de Internet, por lo que ***el marco regulatorio debe evitar la fragmentación de Internet o cualquier consecuencia nociva para***	**Mediano**

	su funcionamiento técnico. Nuestro interés debe enfocarse en construir un Internet seguro y resiliente, en el cual los usuarios puedan ejercer sus Derechos Humanos, de forma responsable, sin censura, vigilancia masiva o intromisiones arbitrarias. En este sentido, se debe procurar que la regulación de ciberseguridad no se convierta en una barrera al comercio electrónico, economía digital e inversión extranjera. Estos marcos regulatorios no pueden imponer barreras que eviten el desarrollo y crecimiento económico, que trae aparejado este tipo de comercio.	
80	Adecuar y reformar la legislación, en materia de protección de datos personales y privacidad de niñas, niños y adolescentes, atendiendo a los recientes adiciones a la Ley General de Niñas, Niños y Adolescentes, en materia de acceso a las TIC y uso seguro de Internet. Lo anterior en colaboración con SIPINNA y SEP.	**Mediano**
81	Colaborar en el desarrollo de estándares y normas nacionales en materia de ciberseguridad. Hace falta el crear estándares en la materia, las NOM o NMX que coadyuven a fortalecer el marco jurídico, por ejemplo: • Cifrado (estándares mínimos sobre algoritmos de cifrado a emplear), • NOM o NMX en materia de ciberseguridad, que se encuentre armonizada con el marco jurídico; • *NMX-I-27032-NYCE- 2018 Tecnologías de la información – Técnicas de seguridad – Lineamientos para la ciberseguridad,* trabajar para que la NMX-I-27037-NYCE-2015, IDENTIFICACIÓN, RECOPILACIÓN, ADQUISICIÓN Y PRESERVACIÓN DE LA EVIDENCIA DIGITAL, de convierta en NOM, entre otras. Así como la detección de otros estándares técnicos que fortalezcan al marco jurídico. Labor que debe realizarse desde un esfuerzo de participación conjunta. Estos estándares técnicos vendrán a reforzar la legislación.	**Mediano**
82	Coadyuvar en el desarrollo de un *Manual de levantamiento de evidencia digital y cadena de custodia*, para Policía Cibernética y primeros respondientes, que permita fortalecer su labor al contar con lineamientos técnicos y de trazabilidad en el tratamiento de dichos indicios y su presentación como evidencia en el proceso.	**Mediano**
83	Desarrollo de una terminología homologada que permita una mayor eficacia en la aplicación de la legislación. Esto servirá para encausar los esfuerzos a las modificaciones necesarias al marco jurídico.	**Corto**
84	Enfocar esfuerzos para apoyar al sector MiPymes, generando buenas prácticas	**Mediano**

	para que puedan cumplir con el marco regulatorio, ayudando al desarrollo e innovación de la economía digital.	
85	Desarrollar acciones en la capacitación de operadores de justicia, en materia de ciberseguridad: fiscales, peritos, jueces, abogados. Realizar talleres de prácticas jurídicas en ciberseguridad, ayudará a fortalecer habilidades y fomentar la cooperación entre estos actores. Para lo cual se necesita la colaboración de Policía Federal, así como el Poder Judicial y las Procuradurías de los estados.	**Mediano**
86	Garantizar la continuidad de los esfuerzos logrados en conjunto. En este sentido, destaca la importancia de reunirse con el equipo de transición gubernamental, para buscar un seguimiento de las acciones a realizar.	**Largo**
87	Garantizar la implementación del enfoque *multistakeholder* para la implementación de las acciones derivadas de la ENCS.	**Largo**
88	Se detectaron necesidades y áreas de oportunidad que requieren de un procedimiento más largo para su realización. Por ejemplo, en el ámbito internacional, teniendo en cuenta la falta de consenso dentro del Grupo de Expertos de las Naciones Unidas (2016-2017), se solicitó a la comunidad internacional que buscará un espacio alternativo de debate sobre la aplicación del derecho internacional a las actividades cibernéticas y el desarrollo de normas de comportamiento responsable. Por ello es importante que nuestro país realice un análisis sobre nuestra política internacional en torno a las cuestiones relativas a las respuestas y manejo ante los ataques cibernéticos contra las capacidades -terroristas o de otro índole-, en línea, fuera del conflicto armado según el derecho internacional. Considerando que tales ataques no constituyen ataques armados, uso de la fuerza o actos coercitivos que violan el principio de no intervención.	**Mediano**
89	Impulsar la adecuación y actualización de los planes de estudio que fomenten el desarrollo de habilidades y capacidades de los estudiantes de nivel superior y posgrado, que nos permita contar con profesionistas especializados en la materia. Este trabajo se realiza conjunto con ANUIES y resultará importante la participación de CONACYT.	**Corto**

Eje Transversal 8: Medición y Seguimiento

Líder: SRE

Colaboradores: INEGI, Presidencia de la República, Policía Federal, SEP-@prende, otras autoridades del gobierno federal, ANUIES, INFOTEC, IPN.

Acciones realizadas:

1. Se llevaron a cabo un par de reuniones con la finalidad de desarrollar una propuesta de índice para medir la efectividad de la ENCS. Los indicadores propuestos han resultado útiles para hacer un diagnóstico inicial sobre la existencia de elementos legales, recursos, infraestructura y nivel de institucionalización de la política de ciberseguridad nacional. [40]

No.	Recomendación	Plazo
90	Proponemos como instrumento de diagnóstico de capacidades cibernéticas nacionales el instrumento de medición de la Estrategia Nacional de Ciberseguridad del anexo ÚNICO, que serviría para consolidar de manera sistemática la información que se proporciona o debe estar disponible para los índices internacionales y que se conforma por: • 7 categorías que engloban de manera concisa los siguientes rubros: 1. Indicadores generales de ciberseguridad nacional. 2. Indicadores de medidas organizativas. 3. Indicadores técnicos y de infraestructura. 4. Indicadores de educación en ciberseguridad. 5. Indicadores básicos de ciberseguridad. 6. Indicadores de manejo de crisis e incidentes. 7. Indicadores internacionales. • 18 puntos clave: Se encuentran dentro de las categorías, de esta forma profundiza un poco más sobre los temas en materia de ciberseguridad. Los puntos clave son: 1. Políticas de ciberseguridad. 2. Análisis e información de amenazas cibernéticas. 3. Estrategia nacional de ciberseguridad.	**Corto**

[40] Documento anexo

4. Organismos gubernamentales y privados de ciberseguridad.
5. Desarrollo de medidas técnicas.
6. Desarrollo de tecnologías de información y comunicación.
7. Desarrollo de infraestructura.
8. Desarrollo educacional y profesional.
9. Protección de servicios digitales.
10. Identificación electrónica y servicios de confianza.
11. Marco jurídico y autorregulación
12. Protección de datos personales y acceso a la información
13. Gobierno electrónico
14. Lucha contra el crimen cibernético
15. Respuesta a incidentes cibernéticos.
16. Gestión de crisis cibernética.
17. Concientización en ciberseguridad.
18. Contribución a la ciberseguridad global.

- 63 indicadores:

  Desarrollan de manera individual un tópico, dando como resultado estar al tanto sobre con cuáles acciones cumple y con cuáles no. A modo de ejemplo, se presentan ejemplos de algunos indicadores de cada punto clave:

  1.1 Estrategia de ciberseguridad
  1.2 Políticas y disposiciones en materia de tecnologías digitales, tecnologías de la información y comunicaciones, tecnologías de seguridad de la información de la estrategia
  2.1 Capacidad de análisis contra amenazas cibernéticas
  2.2 Publicación de reportes de amenazas cibernéticas
  3.1 Organismo, comisión o agencia
  3.2 Grupos de trabajo, comisiones, comités asesores y consejos.
  4.1 Agencias u organismos gubernamentales
  4.2 Agencias u organismos privados
  5.1 CERT
  5.2 CSIRT
  6.1 Investigación y Desarrollo
  6.2 Programas innovación tecnológica
  7.1 Infraestructuras fiables y de calidad
  7.2 Innovación en infraestructura
  8.1 Programas de ciberseguridad escolares
  8.2. Programas de ciberseguridad profesionales
  8.3 Participación de asociaciones civiles en materia de ciberseguridad
  9.1 Estándar de ciberseguridad en el sector público y privado

	9.2 Estándar de ciberseguridad en el sector financiero 10.1 Identificación electrónica 10.2 Firma electrónica 11.1 Marco jurídico en materia de ciberseguridad 11.2 Implementación de justicia 12.1 Legislación de protección de datos personales 12.2 Legislación de protección a menores de edad 13.1 Unidad de gobierno electrónico 13.2 Estrategia de gobierno electrónico 14.1Unidad de crimen cibernético 14.2 Modelo homologado de policía cibernética 15.1 Unidad de respuesta a incidentes cibernéticos 15.2 Responsabilidad de registro de incidentes cibernéticos 16.1 Plan de gestión de crisis cibernética 16.2 Prácticas de gestión de crisis cibernética 17.1 Campañas de concientización de ciberseguridad 17.2 Programa de concientización de ciberseguridad 18.1 Cooperación internacional 18.2 Legislaciones internacionales Lo anterior en conjunto conforma de manera holística una visión sobre temas en materia de ciberseguridad vitales, para la creación de espacios cibernéticos seguros, libres de actores maliciosos y protegiendo los derechos de los cibernautas, es por esto mismo, que se sugiere que el instrumento de medición, sea actualizado y evaluado, por lo menos cada 2 años, con el fin de cumplir de manera efectiva los objetivos de la Estrategia Nacional de Ciberseguridad (ENCS).	
91	Como parte del instrumento de medición, se propone utilizar el modelo "*Capability Maturity Model",* con la finalidad de conocer cuál es nivel de madurez en el que se encuentra la ENCS, de este modo, según sea el avance que se tenga, se verá reflejado en alguno de los cinco rubros que componen este modelo. De igual forma se propone la utilización de la "Teoría del cambio" con perspectiva de "Ciclo de política", la cual se sugiere sea implementada para la medición de cada estrategia que sea implementada, con el fin de conocer cuál es el impacto que tiene en la sociedad, y a partir del análisis de este, se realice el seguimiento adecuado, para un mejor resultado.	**Corto Mediano**
92	Seguir trabajando en el desarrollo de un índice para medir la efectividad de la ENCS en el mediano plazo para lo cual será necesario coordinar a los 14 grupos	**Corto**

	de trabajo encargados de la implementación para poder trasladar los objetivos y ejes transversales en actividades y acciones concretas que permitan identificar la gestión y monitoreo de la implementación de la estrategia y el resultado de la efectividad de la misma en colaboración con especialistas del INEGI y otras agencias o entidades capaces de desarrollar indicadores de gestión o monitoreo e indicadores de resultado o efectividad. Esto permitirá también alinear y mapear las categorías, puntos clave e indicadores del instrumento de diagnóstico con los objetivos estratégicos y ejes transversales de la estrategia y medir efectivamente la efectividad de ésta.	

Anexo I
PROPUESTA
ÍNDICE CIBERSEGURIDAD-MX

METODOLOGÍA
PROPUESTA Y DESARROLLO

El Índice para medir la implementación y efectividad de la Estrategia Nacional de Ciberseguridad (ENCS), tiene como principal objetivo medir la preparación de México en materia de ciberseguridad para hacer frente a los riesgos, amenazas y ataques informáticos sofisticados, así como conocer nuestro grado de aprovechamiento de las Tecnologías de la Información y Comunicación; para esto consideramos:

- Los objetivos. Protección de:
  1. Sociedad y derechos;
  2. Economía e innovación;
  3. Instituciones públicas;
  4. Seguridad pública;
  5. Seguridad nacional.
- Ejes transversales.
  1. Cultura de ciberseguridad;
  2. Desarrollo de capacidades;
  3. Coordinación y colaboración;
  4. Investigación, desarrollo e innovación en tic;
  5. Estándares y criterios técnicos;
  6. Infraestructuras críticas;
  7. Marco jurídico y autorregulación;
  8. Medición y seguimiento.
- Principios rectores.
  1. Enfoque basado en gestión de riesgos;
  2. Perspectiva de derechos humanos; y
  3. Colaboración multidisciplinaria y de múltiples actores.

El índice se enfoca en aspectos medibles de ciberseguridad implementados efectivamente por el Gobierno Mexicano.

VISIÓN.

Desarrollar una herramienta eficiente para la medición de la ciberseguridad Nacional, que brinde información precisa y actualizada que nos permitan identificar las áreas de oportunidad en la materia.

ESTRUCTURA.

7 categorías:

1. Indicadores generales de ciberseguridad nacional.
2. Indicadores de medidas organizativas.
3. Indicadores técnicos y de infraestructura.
4. Indicadores de educación en ciberseguridad.
5. Indicadores básicos de ciberseguridad.
6. Indicadores de manejo de crisis e incidentes.
7. Indicadores internacionales.

ÍNDICADORES.

I. INDICADORES GENERALES DE CIBERSEGURIDAD NACIONAL

1. Políticas de ciberseguridad.

1.1 Estrategia de ciberseguridad

- Criterio: El Gobierno de México cuenta con una Estrategia Nacional de Ciberseguridad.
- Referencia: Documento oficial
- Evidencia: *https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf*

1.2 Políticas y disposiciones en materia de tecnologías digitales, tecnologías de la información y comunicaciones, tecnologías de seguridad de la información

- Criterio: El Gobierno de México cuenta con instrumentos para el desarrollo, revisión, ajuste y mejora de políticas de ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
    - Evidencia:*https://www.gob.mx/cidge/acciones-y-programas/politica-tic-maagticsi-2017*
        - *http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014*
        - *http://www.dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016*
- En el marco jurídico del Gobierno Mexicano existen diversas disposiciones contenidas en diferentes ordenamientos jurídicos que regulan aspectos relacionados con la seguridad de la información y la ciberdelincuencia, a saber:
    - Constitución Política de los Estados Unidos Mexicanos (CPEUM):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf*
    - Código Penal Federal (CPF):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/9_090318.pdf*
    - Código Nacional de Procedimientos Penales (CNPP):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf*
    - Ley Federal de Telecomunicaciones y Radiodifusión (LFTR):

        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_311017.pdf*
    - Ley General del Sistema Nacional de Seguridad Pública (LGSNSP):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP_260617.pdf*
    - Ley General de Transparencia y Acceso a la Información Pública (LGTAIP):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf*
    - Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf*
    - Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*
    - Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*
    - Ley de Instituciones de Crédito (LIC):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/43_090318.pdf*
    - Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo (LRASCAP):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LRASCAP_280414.pdf*
    - Ley del Mercado de Valores (LMV):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LMV_090318.pdf*
    - Ley Federal del Derecho de Autor (LFDA):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/122_130116.pdf*
    - Ley Federal contra la Delincuencia Organizada (LFDO):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/101_070417.pdf*
    - Ley de Firma Electrónica Avanzada (LFIEL):
        - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf*
    - Ley para Regular las Instituciones de Tecnología Financiera (FINTECH):
        - *http://www.dof.gob.mx/nota_detalle.php?codigo=5515623&fecha=09/03/2018*

1.3 Programas nacionales o locales de ciberseguridad

- Criterio: El Gobierno de México cuenta con un mecanismo para el desarrollo de programas o proyectos de apoyo a la industria de las TIC, la investigación y desarrollo o centros de excelencia en materia de ciberseguridad y de capacitación de recursos humanos
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

1.4 Plan de acción para la implementación de la estrategia

- Criterio: Existen parámetros para medir la implementación en la colaboración multidisciplinaria y de múltiples actores dentro de la implementación de la estrategia.
- Referencia: Sitio web o documento oficial.
- Evidencia: N/A

2. Análisis e información de amenazas cibernéticas.

2.1 Capacidad de análisis contra amenazas cibernéticas

- Criterio: El Gobierno Mexicano cuenta un equipo de análisis especializada contra amenazas ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.gob.mx/policiafederal/estructuras/division-cientifica*

2.2 Publicación de reportes de amenazas cibernéticas

- Criterio: Se realiza una publicación parcial sobre el análisis de amenazas cibernéticas.
- Referencia: Documento oficial.
- Evidencia: N/A

2.3 Seguridad en espacios cibernéticos

- Criterio: El Gobierno Mexicano cuenta con al menos una página web que proporcione información sobre ciberseguridad.
- Referencia: Sitio web oficial.
- Evidencia: *https://www.gob.mx/ciberseguridad*

3. Estrategia Nacional de Ciberseguridad.

3.1 Organismo, comisión o agencia

- Criterio: Existe algún organismo, comisión o agencia encargada de la implementación de la Estrategia Nacional de Ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.gob.mx/cidge*

3.2 Grupos de trabajo, comisiones, comités asesores y consejos.

- Criterio: Existe algún parámetro para medir la implicación de los grupos de trabajo, comisiones, comités asesores y consejos.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

3.3 Prácticas en materia de ciberseguridad

- Criterio: Logros y avances a partir de la Estrategia Nacional de Ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

3.4 Alianzas en materia de ciberseguridad

- Criterio: Existen acuerdos públicos-privados con el fin de avanzar en materia de ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

II. INDICADORES DE MEDIDAS ORGANIZATIVAS.

4. Organismos gubernamentales y privados de ciberseguridad.

4.1 Agencias u organismos gubernamentales

- Criterio: Existen agencias u organismos gubernamentales que se encarguen de la ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *http://www.cns.gob.mx/portalWebApp/wlp.c?__c=f7124*

4.2 Agencias u organismos privados

- Criterio: Existen agencias u organismos Privados que se encarguen de la Ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia:
    - *http://telmex.com/web/empresas/servicios-de-ciberseguridad?gclid=EAIaIQobChMIh7-12Ma22wIVS77ACh04UwqYEAAYAyAAEgKJ9_D_BwE&dclid=COntst_GttsCFUR1AQodoqoIcg;*
    - *https://www.gnp.com.mx/empresas/corporativos/danos/otros-seguros/cyber-seguridad?gclid=EAIaIQobChMIh7-12Ma22wIVS77ACh04UwqYEAAYAiAAEgJ--vD_BwE;* *https://cert.mnemo.com/*

4.3 Evaluación de riesgo

- Criterio: Se realizan periódicamente evaluaciones de riesgo o auditorias en materia de ciberseguridad a nivel gubernamental o privado.
- Referencia: Matrices de riesgos institucionales
- Evidencia: N/A

III. INDICADORES TÉCNICOS Y DE INFRAESTRUCTURA.

5. Desarrollo de medidas técnicas.

5.1 CERT

- Criterio: El Gobierno Mexicano/Institución Privada cuenta con un CERT nacional y/o sectorial.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia:
    - *https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es;*
    - *https://www.first.org/members/teams/cert-mx;*
    - *https://www.cert.org.mx/historico_cert/index.html;*
    - *https://www.scitum.com.mx/ScitumCert;*
    - *https://www.mnemo.com/cert/*

5.2 CSIRT

- Criterio: El Gobierno Mexicano/Institución Privada cuenta con un CSIRT nacional y/o sectorial.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *http://www.iqsec.com.mx/es/#&panel1-1*

5.3 CIRT

- Criterio: El Gobierno Mexicano/Institución Privada cuenta con un CIRT nacional y/o sectorial.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

6. Desarrollo de tecnologías de información y comunicación.

6.1 Investigación y Desarrollo

- Criterio: El Gobierno Mexicano cuenta con personal especializado en la investigación y desarrollo de las TIC.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.conacyt.gob.mx/*

6.2 Programa de Investigación, desarrollo e innovación tecnológica

- Criterio: Existen indicadores para medir la investigación y desarrollo de las TIC, así como un programa de investigación y desarrollo que promueva la innovación de las TIC (actualización cada 5 años).
- Referencia: Documento oficial o sitio web oficial.
- Evidencia: (Indicador)
    - *http://www3.inegi.org.mx/sistemas/cni/infometadato.aspx?idOrden=1.1&ind=6200011869&porDetalle=no&gen=636&d=n*
    - *http://www3.inegi.org.mx/sistemas/cni/infometadato.aspx?idOrden=1.1&ind=6200011866&porDetalle=no&gen=635&d=n*

7. Desarrollo de infraestructura.

7.1 Infraestructuras fiables y de calidad

- Criterio: Existen parámetros nacionales para el desarrollo de las infraestructuras de telecomunicaciones.
- Referencia: Documento oficial o sitio web oficial.
- Evidencia: N/A

7.2 Innovación en infraestructura

- Criterio: Existen parámetros y/o proyectos nacionales para modernizar las infraestructuras de telecomunicaciones.
- Referencia: Documento oficial o sitio web oficial.
- Evidencia: N/A

IV. INDICADORES DE EDUCACIÓN EN CIBERSEGURIDAD

8. Desarrollo educacional y profesional.

8.1 Programas de ciberseguridad profesionales

- Criterio: Existen cursos o programas educativos profesionales para formar a las nuevas generaciones en conocimientos y profesiones relacionadas con la ciberseguridad.
- Referencia: Programa o curso acreditado.
- Evidencia:
  - *https://www.lasalle.mx/oferta-educativa/especialidades/facultad-de-ingenieria/ciberseguridad/; https://redtech.lpages.co/hacking-y-ciberseguridad-sede-monterrey-junio/; http://cesnav.edu.mx/cesnav/links_acc_progr/seginfor_site/seginfor_index.html; http://www.posgrados.esimecu.ipn.mx/index.php?option=com_content&view=category&layout=blog&id=26&Itemid=144;*
  - *https://www.ameci.org/index.php/conferencias-talleres-cursos;*
  - *http://docencia.tic.unam.mx/info/SI.pdf;*
  - *http://www.matematicas.uady.mx/unidad-de-extension/diplomados/seguridad-informatica;*
  - *http://diplomadoanuies.uach.mx/;*
  - *https://posgrados.esimecu.ipn.mx/index.php?option=com_content&view=category&layout=blog&id=29&Itemid=248;*
  - *http://www.posgrados.esimecu.ipn.mx/index.php?option=com_content&view=category&layout=blog&id=26&Itemid=144;*
  - *http://www.lasalle.mx/oferta-educativa/especialidades/facultad-de-ingenieria/ciberseguridad/;*
  - *http://www.lasalle.mx/oferta-educativa/maestria/facultad-de-ingenieria/maestria-ciberseguridad/;*
  - *http://www.uanl.mx/content/licenciado-en-seguridad-en-tecnologias-de-informacion;*
  - *http://posgrado.uanl.mx/maestria-ingenieria-en-seguridad-de-la-informacion/;*
  - *https://posgrados.inaoep.mx/ts/index.php?movil=0;*
  - *https://posgrados.inaoep.mx/archivos/convocatorias/ConvocatoriaTecSeguridad/Gob_Convocatoria_Maestria_Tecnologias_Seguridad_Otono_2018.pdf;*
  - *https://www.unitec.mx/maestria-en-seguridad-de-tecnologia-de-informacion/;*
  - *https://cesnav.uninav.edu.mx/cesnav/estudios.html*

8.2 Participación de asociaciones civiles en materia de ciberseguridad

- Criterio: Existen asociaciones profesionales de ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia:*www.amdetic.org* *http://www.amdetic.org/cuarto-encuentro-latinoamericano/* *https://www.ameci.org*

8.3 Conformación de equipos de respuesta a incidentes cibernéticos

- Criterio: Existen equipos de respuesta creados por instituciones educativas.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.seguridad.unam.mx/; https://cert.uach.mx/?view=home*

8.4 Publicación de reportes

- Criterio: Se realiza una publicación parcial sobre incidentes cibernéticos.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.seguridad.unam.mx/incidentes*

V. INDICADORES BÁSICOS DE CIBERSEGURIDAD.

9. Protección de servicios digitales.

9.1 Estándar de ciberseguridad en el sector público y privado

- Criterio: La ley demanda a los proveedores del sector público y privado implementen requisitos de ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: Sector privado
    - *http://www.dof.gob.mx/nota_detalle.php?codigo=5495124&fecha=25/08/2017*
- Sector publico

9.2 Estándar de ciberseguridad en el sector financiero

- Criterio: La ley demanda a los proveedores del sector financiero implementan requisitos de ciberseguridad.
- Referencia: Documento legal.
- Evidencia: *https://www.gob.mx/shcp/es/articulos/conoce-los-5-principios-para-el-fortalecimiento-de-la-ciberseguridad-para-la-estabilidad-del-sistema-financiero-mexicano*

9.3 Autoridades competentes para supervisar

- Criterio: El Gobierno Mexicano cuenta con una autoridad en Ciberseguridad que se encargue de verificar que los proveedores cumplan con la lo que la ley les demanda a los proveedores.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.gob.mx/cidge/estructuras/comision-intersecretarial-para-el-desarrollo-del-gobierno-electronico*

10. Identidad digital y servicios de confianza.

10.1 Identidad digital

- Criterio: La identidad digital está regulada.
- Referencia: Documento legal.
- Evidencia: N/A

10.2 Firma electrónica

- Criterio: La firma electrónica está regulada.
- Referencia: Documento legal.
- Evidencia: *https://eservicios.impi.gob.mx/seimpi/ayudaSEIMPI/LFEA.pdf; https://www.gob.mx/efirma*

10.3 Requerimientos para criptosistemas

- Criterio: Los requerimientos para criptosistemas están regulados.
- Referencia: Documento legal.
- Evidencia: N/A

10.4 Transacciones electrónicas

- Criterio: Las transacciones electrónicas están reguladas.
- Referencia: Documento legal.
- Evidencia:
    - *https://www.cnbv.gob.mx/Normatividad/Ley%20de%20Instituciones%20de%20Cr%C3%A9dito.pdf*
    - *https://www.gob.mx/shcp/es/articulos/conoce-los-5-principios-para-el-fortalecimiento-de-la-ciberseguridad-para-la-estabilidad-del-sistema-financiero-mexicano*

10.5 Confianza en el comercio electrónico

- Criterio: Las empresas de e-commerce cuentan con un sello de confianza que garantice el bienestar del consumidor.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *http://sellosdeconfianza.org.mx/*

10.6 Seguridad en el comercio electrónico

- Criterio: Existen leyes que protejan al consumidor ante un actor malicioso en una compra electrónica.
- Referencia: Documento legal
- Evidencia: *http://www.ordenjuridico.gob.mx/Congreso/pdf/105.pdf*

11. Marco jurídico y autorregulación

11.1 Marco jurídico en materia de ciberseguridad

- Criterio: Existen legislaciones que promuevan la seguridad de las tecnologías de información y comunicación, garantizando los derechos humanos tanto en el ciberespacio, como a los niñas, niños y adolescentes.
- Referencia: Documento legal u otra
- Evidencia: (Niñas, niños y adolescentes)
- Ley General de Niñas, Niños y Adolescentes: Artículo 101 Bis 2, refiere: ”Niñas, niños y adolescentes tienen derecho al acceso y uso seguro del Internet como medio efectivo para ejercer los derechos a la información, comunicación, educación, salud, esparcimiento, no discriminación, entre otros, de conformidad con el principio de interdependencia, en términos de las disposiciones aplicables” .Publicada en el DOF el 20 de junio de 2018, *http://www.dof.gob.mx/nota_detalle.php?codigo=5527036&fecha=20/06/2018*

11.2 Implementación de justicia

- Criterio: Existe un sistema de justicia penal en materia de ciberseguridad que regulen las penas y castigos de aquellos que cometan actos fuera de la ley.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

11. 3 Medidas de normalización (estándares) y autorregulación, en materia de ciberseguridad

- Criterio: Existen guías, esquemas o procesos en cuanto a la normalización y autorregulación, en materia de ciberseguridad.
- Referencia: Documento oficial.
- Evidencia: N/A

11.3. Normalización

- Criterio: Adopción, adaptación y aplicación de directrices para realizar, buenas prácticas en materia de ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

11.4 Autorregulación

- Criterio: Reglas o estándares específicos que permitan armonizar los tratamientos y facilitar el ejercicio en materia de ciberseguridad.
- Referencia: Documento oficial.
- Evidencia: N/A

12. Protección de datos personales y acceso a la información

12.1 Legislación de protección de datos personales

- Criterio: Existe alguna legislación de datos personales.
- Referencia: Documento legal.

- Evidencia:
    - *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf; https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf*

12.2 Legislación de protección a menores de edad

- Criterio: Existe una legislación de protección a menores de edad.
- Referencia: Documento legal.
- Evidencia: https://www.gob.mx/segob/articulos/ley-general-de-los-derechos-de-ninas-ninos-y-adolescentes-ya-la-conoces; http://www.salud.gob.mx/unidades/cdi/nom/compi/L290500.html

12.3 Autoridades competentes para supervisar

- Criterio: Existe una autoridad de supervisión pública independiente que es responsable de la protección de datos personales para adultos, niñas, niños y adolescentes.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: (Protección de datos).
    - *http://inicio.ifai.org.mx/SitePages/ifai.aspx*
    - Niñas, niños y adolescentes) *https://www.gob.mx/segob/documentos/sistema-nacional-de-proteccion-integral-de-ninas-ninos-y-adolescentes-sipinna*

13. Gobierno electrónico

13.1 Unidad de gobierno electrónico

- Criterio: El Gobierno de México cuenta con autoridades especializadas en gobierno electrónico.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *https://www.gob.mx/cidge*

13.2 Estrategia de gobierno electrónico

- Criterio: El Gobierno de México cuenta con una estrategia digital.
- Referencia: Documento oficial.
- Evidencia: *https://framework-gb.cdn.gob.mx/data/institutos/edn/Estrategia_Digital_Nacional.pdf*

13.2 Normatividad de gobierno electrónico

- Criterio: Marco normativo del gobierno electrónico en México.
- Referencia: Documento oficial
- Evidencia: *https://www.gob.mx/cms/uploads/attachment/file/273176/Normatividad_Gobierno_Digital__Estados_.pptx.pdf*

13.3 Estandarización y certificación de trámites digitales

- Criterio: Existe una guía de sellos de confianza en cuanto a gobierno digital.
- Referencia: Documento oficial.
- Evidencia: *http://www.dof.gob.mx/nota_detalle.php?codigo=5446678&fecha=03/08/2016*

13.4 Confianza en trámites gubernamentales

- Criterio: Existe un reglamento para los tramites gubernamentales.
- Referencia: Documento legal u oficial.
- Evidencia: *http://www.dof.gob.mx/nota_detalle.php?codigo=5380863&fecha=03/02/2015*

13.5 Principios y criterios técnicos en materia de accesibilidad Web

- Criterio: Existen disposiciones para la accesibilidad a la web entre dependencias y entidades de la administración pública.
- Referencia: Documento legal u oficial.
- Evidencia: *http://dof.gob.mx/nota_detalle.php?codigo=5418749&fecha=03/12/2015*

VI. INDICADORES DE MANEJO DE CRISIS E INCIDENTES.

14. Lucha contra el crimen cibernético

14.1Unidad de crimen cibernético

- Criterio: Existe una unidad que se encarga del crimen cibernético.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia:
    - *http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html*
    - *pgr: http://www.dof.gob.mx/nota_detalle.php?codigo=5496125&fecha=05/09/2017*

14.2 Modelo homologado de policía cibernética

- Criterio: El Gobierno Mexicano cuenta con una estrategia para la implementación de un modelo homologado de policía cibernética.
- Referencia: Documento oficial
- Evidencia:
  https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf

15. Respuesta a incidentes cibernéticos.

15.1 Unidad de respuesta a incidentes cibernéticos

- Criterio: El Gobierno Mexicano cuenta con una unidad de respuesta 24/7.
- Referencia: Sitio web oficial o documento oficial
- Evidencia:
  http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059;
  http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

15.2 Responsabilidad de registro de incidentes cibernéticos

- Criterio: Los proveedores de servicios, tienen la obligación de reportar los incidentes cibernéticos.

- Referencia: Documento legal.
- Evidencia: N/A

15.3 Autoridades competentes para supervisar

- Criterio: Existe una autoridad de supervisión que es responsable de los incidentes cibernéticos.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: *http://www.cns.gob.mx/*

16. Gestión de crisis cibernética.

16.1 Plan de gestión de crisis cibernética

- Criterio: El Gobierno Mexicano tiene un plan de gestión de crisis cibernética.
- Referencia: Documento oficial.
- Evidencia: N/A

16.2 Prácticas de gestión de crisis cibernética

- Criterio: El Gobierno Mexicano ha llevado a cabo un ejercicio de gestión de crisis cibernética a nivel nacional.
- Referencia: Documento de ejercicio (oficial).
- Evidencia: N/A

17. Concientización en ciberseguridad.

17.1 Campañas de concientización de ciberseguridad

- Criterio: Se realizan campañas nacionales sobre ciberseguridad.
- Referencia: Sitio web o documento oficial.
- Evidencia:
  - *https://www.gob.mx/policiafederal/prensa/policia-federal-y-condusef-inauguran-ciclo-de-conferencias-en-materia-de-ciberseguridad;*
  - *https://www.gob.mx/internetseguro;*
  - *https://www.youtube.com/watch?v=wnhSRH30T-A;*
  - *https://www.gob.mx/policiafederal/prensa/la-comision-nacional-de-seguridad-inaugura-campana-de-concientizacion-ciberseguridad-mexico-2018-149497;*
  - *https://www.gob.mx/policiafederal/articulos/cibernauta-con-estrella?idiom=es;*
  - *https://www.gob.mx/policiafederal/articulos/programa-de-actividades-tercera-semana-nacional-de-la-ciberseguridad%20http://anuies-tic.anuies.mx/web/kit/*

17.2 Programa de concientización de ciberseguridad

- Criterio: Existen parámetros para medir el impacto de las campañas sobre ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
  - Evidencia: N/A

VII. INDICADORES INTERNACIONALES

18. Contribución a la ciberseguridad global.

18.1 Cooperación internacional

- Criterio: Existen acuerdos bilaterales o internacionales en materia de Ciberseguridad.
- Referencia: Sitio web oficial, documento oficial u otra.
- Evidencia:
    - Acuerdo trilateral: México ha consolidado un diálogo trilateral sobre seguridad en América del Norte que incluye cuestiones de seguridad cibernética entre México, EUA y Canadá.
    - Organizaciones internacionales: A nivel internacional, México es parte de la Convención contra la Delincuencia Organizada Transnacional (Convención de Palermo), que incluye algunas formas nuevas y emergentes de delincuencia, como los delitos cibernéticos; y el Convenio sobre Delito Cibernético de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB).
    - México reconoce la importancia de la Convención del Consejo de Europa contra la Delincuencia Cibernética (Convenio de Budapest) y promueve activamente las normas voluntarias de comportamiento responsable de los Estados y el desarrollo de medidas prácticas de fomento de la confianza entre los Estados.
    - A nivel regional, somos parte del Grupo de Trabajo sobre Medidas para la Promoción de la Confianza del Comité Interamericano contra el Terrorismo (CICTE) de la OEA.

18.2 Legislaciones internacionales

- Criterio: Existen legislaciones internacionales en Ciberseguridad.
- Referencia: Documento legal.
- Evidencia: N/A

18.3 Organizaciones internacionales de ciberseguridad

- Criterio: Hay organizaciones internacionales encargadas de Ciberseguridad.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

18.4 Participación en foros internacionales

- Criterio: El Gobierno Mexicano participa en foros/eventos/convenciones internacionales.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia:
    - *https://www.thegfce.com/members-and-partners/members/mexico;*
    - *https://www.internetsociety.org/events/gccs-2017/;*
    - *https://www.meridianprocess.org/;*
    - *http://www.oas.org/es/sms/cicte/programas_cibernetica.asp;*
    - *http://www.coe.int/en/web/cybercrime/tcy;*

- *http://www.igf2016.mx/*

18.5 Desarrollo de infraestructura

- Criterio: Existen parámetros internacionales para que el desarrollo de las infraestructuras tecnológicas sea fiable, sostenible y de calidad, así como investigaciones científicas para la innovación es las mismas.
- Referencia: Sitio web oficial o documento oficial.
- Evidencia: N/A

ANEXO II

Modelos de referencia

- Modelo de Madurez de Capacidad de Seguridad Cibernética para las Naciones (CMM), Global Cyber Security Capacity Centre University of Oxford, 3/31/2016
- Modelo Homologado de Unidades de policía cibernética, División científica de la Policía Federal

Normas mexicanas

- NMX-I-289-NYCE-2016, TECNOLOGÍAS DE LA INFORMACIÓN-METODOLOGÍA DE ANÁLISIS FORENSE DE DATOS Y GUÍAS DE EJECUCIÓN (CANCELA A LA NMX-I-289-NYCE-2013) Esta Norma Mexicana establece una metodología para la realización y evaluación de las actividades del cómputo forense en equipos de cómputo incluyendo de forma enunciativa mas no limitativa a todo aquel equipo que procese, almacene y/o transmita información y homogeniza los criterios y actividades relacionadas al proceso forense y análisis de evidencia digital que se desarrolla en nuestro País. El campo de aplicación de esta Norma Mexicana se encuentra en las personas u organizaciones que realicen actividades de cómputo forense en general.
- NMX-I-291-NYCE-2013 TECNOLOGÍAS DE LA INFORMACIÓN-DIGITALIZACIÓN DOCUMENTAL CON VALOR AGREGADO Los presentes requisitos, son de carácter general y tienen como objeto establecer lineamientos, para que cualquier persona pueda proceder a la migración de mensajes de datos de los documentos que conserven en medios físicos que tengan el carácter de originales y que la ley no tenga disposición en contrario, a través de un cotejo del proceso de migración del medio físico al medio electrónico, como se define en el apartado de definiciones de los presentes requisitos, por un tercero certificado, obteniendo como consecuencia que los documentos migrados a mensajes de datos tengan el mismo valor probatorio que los originales en papel que les sirvieron de base. Para valorar la fuerza probatoria de los documentos migrados, se estima primordialmente la fiabilidad del método con que se haya migrado, resguardado y almacenado. La naturaleza probatoria de los documentos digitalizados sigue siendo la misma después de su migración. En ningún momento se entiende que documentos privados al ser migrados mediante un proceso cotejado por un tercero certificado tienen el valor probatorio de un documento público. Por lo que le son aplicables las disposiciones del derecho común
- NMX-I-27001-NYCE-2015 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-REQUISITOS (CANCELA A LA NMX-I-27001-NYCE2009) Esta Norma Mexicana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en el contexto de la organización. Esta Norma Mexicana también incluye requisitos para la valoración y tratamiento de riesgos de seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en Esta Norma Mexicana son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. La exclusión de cualquiera de los requisitos especificados en los capítulos del 4 al 10 no es aceptable cuando una organización pretende la conformidad con Esta Norma Mexicana.
- NMX-I-27002-NYCE-2015 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-CÓDIGO DE BUENAS PRÁCTICAS PARA EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN (CANCELA A LA NMXI-27002-NYCE-2009) Esta Norma Mexicana proporciona lineamientos para las normas de seguridad de la información y prácticas de gestión de seguridad de la información, incluyendo la selección,

implementación y administración de los controles, teniendo en cuenta el(los) entorno(s) de riesgos de seguridad de la información de la organización. Esta Norma Mexicana está diseñada para ser utilizado por las organizaciones que pretenden: a) Seleccionar los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la NMX-I27001-NYCE; b) Implementar controles de seguridad de la información generalmente aceptadas; y c) Desarrollar sus propios lineamientos de gestión seguridad de la información.

· NMX-J-C-I-489-ANCE-ONNCCE-NYCE CENTROS DE DATOS DE ALTO DESEMPEÑO-SUSTENTABLE Y ENERGÉTICO-REQUISITOS Y MÉTODOS DE COMPROBACIÓN Esta norma mexicana es aplicable a las edificaciones especializadas que alberguen CDAD y que se ubiquen en territorio nacional, públicas o privadas; en conjunto de edificios urbanos y sus obras exteriores, nuevas o usadas parcialmente o en la totalidad de su superficie y en cualquier modalidad: en operación, construcción nueva, remodelación, reestructuración y ampliación.

· NMX-I-27037-NYCE-2015 TECNOLOGÍAS DE LA INFORMACIÓN–TÉCNICAS DE SEGURIDAD–DIRECTRICES PARA LA IDENTIFICACIÓN, RECOPILACIÓN, ADQUISICIÓN Y PRESERVACIÓN DE LA EVIDENCIA DIGITAL Esta Norma Mexicana provee las directrices para actividades específicas en el manejo de evidencia digital, que son identificación, recopilación, adquisición y preservación de la evidencia digital que pueda contener un valor como evidencia. Esta Norma Mexicana proporciona orientación a las personas, con respecto a las situaciones comunes encontradas a lo largo de los procesos de manejo de la evidencia digital y asiste a las organizaciones en sus procedimientos disciplinarios y facilita el intercambio de evidencia digital potencial entre jurisdicciones. Esta Norma Mexicana proporciona orientación para los siguientes dispositivos y/o funciones que son usados en diversas circunstancias: -Medios de almacenamiento digital usado en computadoras estándar, como discos duros, disquetes, discos ópticos y magneto-ópticos, dispositivos de datos con funciones similares; -Teléfonos móviles, Asistentes Digitales Personales por sus siglas en inglés (PDAs), Dispositivos Electrónicos Personales por sus siglas en inglés (PEDs), tarjetas de memoria; -Sistemas de navegación móvil; -Cámaras digitales y de video (incluyendo CCTV); -Computadoras estándar con conexiones de red; -Redes basadas en TCP/IP y otros protocolos digitales, y -Dispositivos con alguna función similar a las descritas en esta lista.

· NMX-I-22301-NYCE-2015 TECNOLOGÍAS DE LA INFORMACIÓN-SEGURIDAD SOCIALSISTEMAS DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIOREQUERIMIENTOS Esta Norma Mexicana para la gestión de la continuidad del negocio especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse contra la reducción de la probabilidad de una ocurrencia, prepararse para responder y recuperarse de los incidentes disruptivos perturbadores cuando éstos se presenten. Los requisitos especificados en esta Norma Mexicana son genéricos y se pretende que sean aplicables a todas las organizaciones o partes de las mismas, sin importar su tipo, tamaño y naturaleza de la organización. El alcance de la aplicación de estos requisitos depende del entorno operativo de la organización y la complejidad. El propósito de esta Norma Mexicana es que una organización diseñe un SGCN que sea adecuado a sus necesidades y que cumpla con las necesidades de las partes interesadas. Se debe evitar el uso de esta Norma Mexicana como una plantilla para definir la estructura del Sistema de Gestión de Continuidad del Negocio (SGCN). Estas necesidades están determinadas por los requisitos legales, regulatorios, organizacionales y de la industria, los productos y servicios, los procesos empleados, el tamaño y la estructura de la organización y los requerimientos de las partes interesadas. Esta Norma Mexicana es aplicable a todos los tipos y tamaños de organizaciones que deseen: a) Establecer,

implementar, mantener y mejorar un SGCN; b) Garantizar la conformidad con la política de continuidad del negocio establecida; c) Demostrar conformidad con la norma ante otros; d) Buscar la certificación / registro de su SGCN por un organismo acreditado de certificación de tercera parte, o; e) Hacer una auto-determinación y auto-declaración de conformidad con esta Norma Mexicana. Esta Norma Mexicana puede utilizarse para evaluar la capacidad de una organización para cumplir sus propias necesidades de continuidad y obligaciones con terceros.

· NMX-I-27018-NYCE-2016 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-CÓDIGO DE PRÁCTICA PARA LA PROTECCIÓN DE DATOS PERSONALES (DP) PARA PROVEEDORES DE SERVICIOS DE NUBES PÚBLICAS Esta Norma Mexicana establece objetivos de control y lineamientos comúnmente aceptados para implementar medidas de protección para los datos personales en conformidad con los principios de privacidad de la norma que se indica en el inciso B.4 del apéndice “B” para ambientes públicos de cómputo en la nube. Esta Norma Mexicana específica en particular los lineamientos basados en la NMX-I-27002-NYCE2015, tomando en cuenta los requisitos normativos para la protección de los DP que se aplican dentro del contexto del (de los) ambiente(s) de riesgo de la seguridad de la información de un prestador de servicios de nubes públicas. Esta Norma Mexicana aplica a todos los tipos y tamaños de organizaciones, incluyendo las empresas públicas y privadas, entidades gubernamentales y organizaciones sin ánimo de lucro, que proveen servicios de procesamiento de información como procesadores de DP por medio del cómputo en la nube bajo contrato para otras organizaciones. Los lineamientos en esta Norma Mexicana también pueden resultar relevantes para las organizaciones que actúan como responsables de DP; no obstante, los responsables de DP pueden estar sujetos a legislación, normatividad y obligaciones de protección adicionales, que no apliquen a los proveedores de servicios de nubes públicas. El fin de esta Norma Mexicana no es cubrir tales obligaciones adicionales.

· NMX-I-27032-NYCE-2018 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-LINEAMIENTOS PARA LA CIBERSEGURIDAD Esta Norma Mexicana provee una guía para mejorar el estado de la Ciberseguridad, señalando los aspectos únicos de esta actividad y su dependencia con otros dominios de la seguridad, en particular: • Seguridad de la información; • Seguridad en redes; • Seguridad en Internet, y • Protección de la infraestructura de información crítica (PIIC). Cubre las prácticas básicas de seguridad que deben ser tomadas como referencia por los interesados en el Ciberespacio. Esta Norma Mexicana provee: • Una visión general de la Ciberseguridad; • Una explicación de la relación entre Ciberseguridad y otros tipos de seguridad; • Una definición de las partes interesadas y una descripción de sus roles en la Ciberseguridad; • Una guía para abordar los problemas comunes de Ciberseguridad, y • Un marco para permitir a las partes interesadas colaborar en la resolución de los problemas de Ciberseguridad

· NMX-I-27033-1-NYCE-2018 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-SEGURIDAD DE LA RED-PARTE 1: VISIÓN GENERAL Y CONCEPTOS Esta parte de la familia de normas NMX-I-27033- NYCE proporciona una visión general de la seguridad de la red y las definiciones relacionadas. Define y describe los conceptos relacionados, y proporciona una guía sobre la gestión de la seguridad de la red. (La seguridad de la red se aplica a la seguridad de los dispositivos, a la seguridad de las actividades de gestión relacionadas con los dispositivos, aplicaciones/servicios y los usuarios finales, además de la seguridad de la información que se transfiere a través de los enlaces de comunicación). Es relevante para cualquier persona que posea, opera o utiliza una red. Esto incluye altos directivos y otros gestores no técnicos o usuarios, además de los gerentes y administradores que tienen responsabilidades específicas para la seguridad de la información y/o seguridad de la red, el

funcionamiento de la red o que son responsables de un programa de seguridad general de la organización y el desarrollo de políticas de seguridad. También es relevante para cualquier persona involucrada en la planeación, diseño e implementación de los aspectos arquitectónicos de la seguridad de la red. Esta parte de la familia NMX-I27033-NYCE también: - Proporciona orientación sobre la forma de identificar y analizar riesgos de seguridad de la red y la definición de los requerimientos de seguridad de la red basados en ese análisis. - Proporciona información general de los controles que soportan las arquitecturas técnicas de seguridad de la red y los controles técnicos relacionados, así como los controles técnicos y no técnicos que son aplicables no sólo para redes. - Da una introducción a la forma de lograr arquitecturas técnicas de seguridad de la red de buena calidad, los riesgos, el diseño y aspectos de control asociados con los escenarios típicos de la red y áreas "tecnológicas" de la red (que son tratados a detalle en la familia NMX-I-27033-NYCE), y - Aborda brevemente asuntos relacionados con la implementación y operación de los controles de seguridad de la red, su continuo monitoreo y revisión de su implementación. En general, se ofrece una introducción a la familia NMX-I-27033-NYCE y un "programa de trabajo" a todas las otras partes de esta familia.

- NMX-I-27033-2-NYCE-2018 TECNOLOGÍAS DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-SEGURIDAD DE LA RED-PARTE 2: DIRECTRICES PARA EL DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD DE LA RED Esta parte de la familia de normas NMX-I-27033- NYCE proporciona directrices para las organizaciones para planificar, diseñar, implementar documentos de seguridad de la red.

Las siguientes normas mexicanas se encuentran en desarrollo

- Norma mexicana de comercio electrónico
- Norma mexicana escuelas seguras en el uso de internet
- Norma mexicana Metodología de análisis forense de datos y guías de ejecución

Normas Internacionales

- ISO/IEC 7064:2003 Information technology -- Security techniques -- Check character systems
- ISO/IEC 9796-2:2010 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
- ISO/IEC 9796-3:2006 Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
- ISO/IEC 9797-1:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
- ISO/IEC 9797-2:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
- ISO/IEC 9797-3:2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-function
- ISO/IEC 9798-1:2010 Information technology -- Security techniques -- Entity authentication -- Part 1: General
- ISO/IEC 9798-2:2008 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms
- ISO/IEC 9798-3:1998 Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques
- ISO/IEC 9798-4:1999 Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function

· ISO/IEC 9798-5:2009 Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques
· ISO/IEC 9798-6:2010 Information technology -- Security techniques -- Entity authentication -- Part 6: Mechanisms using manual data transfer
· ISO/IEC 10116:2017 Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
· ISO/IEC 10118-1:2016 Information technology -- Security techniques -- Hash-functions -- Part 1: General
· ISO/IEC 10118-2:2010 Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
· ISO/IEC 10118-3:2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions Dedicated Hash-Function 8 (SHA-224)
· ISO/IEC 10118-4:1998 Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic
· ISO/IEC 11770-1:2010 Information technology -- Security techniques -- Key management -- Part 1: Framework
· ISO/IEC 11770-2:2008 Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
· ISO/IEC 11770-3:2015 Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
· ISO/IEC 11770-4:2017 Information technology -- Security techniques -- Key management -- Part 4: Mechanisms based on weak secrets
· ISO/IEC 11770-5:2011 Information technology -- Security techniques -- Key management -- Part 5: Group key management
· ISO/IEC 11770-6:2016 Information technology -- Security techniques -- Key management -- Part 6: Key derivation
· ISO/IEC 13888-1:2009 Information technology -- Security techniques -- Non-repudiation -- Part 1: General
· ISO/IEC 13888-2:2010 Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques
· ISO/IEC 13888-3:2009 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
· ISO/IEC TR 14516:2002 Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services
· ISO/IEC 14888-1:2008 Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General
· ISO/IEC 14888-2:2008 Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms
· ISO/IEC 14888-3:2016 Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
· ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
· ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components

· ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
· ISO/IEC TR 15443-1:2012 Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts
· ISO/IEC TR 15443-2:2012 Information technology -- Security techniques -- Security assurance framework -- Part 2: Analysis
· ISO/IEC TR 15446:2017 Information technology -- Security techniques -- Guidance for the production of protection profiles and security targets
· ISO/IEC 15816:2002 Information technology -- Security techniques -- Security information objects for access control
· ISO/IEC 15945:2002 Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures
· ISO/IEC 15946-1:2016 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General
· ISO/IEC 15946-5:2017 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation
· ISO/IEC 17825:2016 Information technology -- Security techniques -- Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
· ISO/IEC 17922:2017 Information technology -- Security techniques -- Telebiometric authentication framework using biometric hardware security module
· ISO/IEC 18014-1:2008 Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework
· ISO/IEC 18014-2:2009 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
· ISO/IEC 18014-3:2009 Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens
· ISO/IEC 18014-4:2015 Information technology -- Security techniques -- Time-stamping services -- Part 4: Traceability of time sources
· ISO/IEC 18031:2011 Information technology -- Security techniques -- Random bit generation
· ISO/IEC 18032:2005 Information technology -- Security techniques -- Prime number generation
· ISO/IEC 18033-1:2015 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
· ISO/IEC 18033-2:2006 Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers
· ISO/IEC 18033-3:2010 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
· ISO/IEC 18033-4:2011 Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers
· ISO/IEC 18033-5:2015 Information technology -- Security techniques -- Encryption algorithms -- Part 5: Identity-based ciphers
· ISO/IEC 18045:2008 Information technology -- Security techniques -- Methodology for IT security evaluation
· ISO/IEC 18367:2016 Information technology -- Security techniques -- Cryptographic algorithms and security mechanisms conformance testing

· ISO/IEC 18370-1:2016 Information technology -- Security techniques -- Blind digital signatures -- Part 1: General
· ISO/IEC 18370-2:2016 Information technology -- Security techniques -- Blind digital signatures -- Part 2: Discrete logarithm based mechanisms
· ISO/IEC TS 19249:2017 Information technology -- Security techniques -- Catalogue of architectural and design principles for secure products, systems and applications
· ISO/IEC 19592-1:2016 Information technology -- Security techniques -- Secret sharing -- Part 1: General
· ISO/IEC 19592-2:2017 Information technology -- Security techniques -- Secret sharing -- Part 2: Fundamental mechanisms
· ISO/IEC 19772:2009 Information technology -- Security techniques -- Authenticated encryption
· ISO/IEC 19790:2012 Information technology -- Security techniques -- Security requirements for cryptographic modules
· ISO/IEC TR 19791:2010 Information technology -- Security techniques -- Security assessment of operational systems
· ISO/IEC 19792:2009 Information technology -- Security techniques -- Security evaluation of biometrics
· ISO/IEC 19896-1:2018 IT security techniques -- Competence requirements for information security testers and evaluators -- Part 1: Introduction, concepts and general requirements
· ISO/IEC TR 20004:2015 Information technology -- Security techniques -- Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
· ISO/IEC 20008-1:2013 Information technology -- Security techniques -- Anonymous digital signatures -- Part 1: General
· ISO/IEC 20008-2:2013 Information technology -- Security techniques -- Anonymous digital signatures -- Part 2: Mechanisms using a group public key
· ISO/IEC 20009-1:2013 Information technology -- Security techniques -- Anonymous entity authentication -- Part 1: General
· ISO/IEC 20009-2:2013 Information technology -- Security techniques -- Anonymous entity authentication -- Part 2: Mechanisms based on signatures using a group public key
· ISO/IEC 20009-4:2017 Information technology -- Security techniques -- Anonymous entity authentication -- Part 4: Mechanisms based on weak secrets
· ISO/IEC TS 20540:2018 Information technology -- Security techniques -- Testing cryptographic modules in their operational environment
· ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)
· ISO/IEC 24745:2011 Information technology -- Security techniques -- Biometric information protection
· ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts
· ISO/IEC 24760-3:2016 Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice
· ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Requirements

· ISO/IEC 27002:2013 Information technology -- Security techniques -- Information security management systems -- Guidance
· ISO/IEC 27004:2016 Information technology -- Security techniques -- Information security risk management
· ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
· ISO/IEC 27019:2017 Information technology -- Security techniques -- Information security controls for the energy utility industry
· ISO/IEC 27021:2017 Information technology -- Security techniques -- Competence requirements for information security management systems professionals
· ISO/IEC TR 27023:2015 Information technology -- Security techniques -- Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
· ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
· ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity
· ISO/IEC 27033-1:2015 Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
· ISO/IEC 27033-2:2012 Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
· ISO/IEC 27033-3:2010 Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
· ISO/IEC 27033-4:2014 Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways
· ISO/IEC 27033-5:2013 Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
· ISO/IEC 27033-6:2016 Information technology -- Security techniques -- Network security -- Part 6: Securing wireless IP network access
· ISO/IEC 27034-1:2011 Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts
· ISO/IEC 27034-2:2015 Information technology -- Security techniques -- Application security -- Part 2: Organization normative framework
· ISO/IEC 27034-3:2018 Information technology -- Application security -- Part 3: Application security management process
· ISO/IEC 27034-5:2017 Information technology -- Security techniques -- Application security -- Part 5: Protocols and application security controls data structure
· ISO/IEC 27034-6:2016 Information technology -- Security techniques -- Application security -- Part 6: Case studies
· ISO/IEC 27034-7:2018 Information technology -- Application security -- Part 7: Assurance prediction framework
· ISO/IEC TS 27034-5-1:2018 Information technology -- Application security -- Part 5-1: Protocols and application security controls data structure, XML schemas
· ISO/IEC 27035-1:2016 Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management

· ISO/IEC 27035-2:2016 Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response
· ISO/IEC 27036-1:2014 Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
· ISO/IEC 27036-2:2014 Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Requirements
· ISO/IEC 27036-3:2013 Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security
· ISO/IEC 27036-4:2016 Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
· ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
· ISO/IEC 27038:2014 Information technology -- Security techniques -- Specification for digital redaction
· ISO/IEC 27039:2015 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
· ISO/IEC 27040:2015 Information technology -- Security techniques -- Storage security
· ISO/IEC 27041:2015 Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method
· ISO/IEC 27042:2015 Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence
· ISO/IEC 27043:2015 Information technology -- Security techniques -- Incident investigation principles and processes
· ISO/IEC 27050-1:2016 Information technology -- Security techniques -- Electronic discovery -- Part 1: Overview and concepts
· ISO/IEC 27050-3:2017 Information technology -- Security techniques -- Electronic discovery -- Part 3: Code of practice for electronic discovery
· ISO/IEC TR 27103:2018 Information technology -- Security techniques -- Cybersecurity and ISO and IEC Standards
· ISO/IEC TS 29003:2018 Information technology -- Security techniques -- Identity proofing
· ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework
· ISO/IEC 29101:2013 Information technology -- Security techniques -- Privacy architecture framework
· ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework
· ISO/IEC 29128:2011 Information technology -- Security techniques -- Verification of cryptographic protocols
· ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment
· ISO/IEC 29146:2016 Information technology -- Security techniques -- A framework for access management
· ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure

· ISO/IEC TR 29149:2012 Information technology -- Security techniques -- Best practices for the provision and use of time-stamping services
· ISO/IEC 29150:2011 Information technology -- Security techniques -- Signcryption
· ISO/IEC 29151:2017 Information technology -- Security techniques -- Code of practice for personally identifiable information protection
· ISO/IEC 29190:2015 Information technology -- Security techniques -- Privacy capability assessment model
· ISO/IEC 29191:2012 Information technology -- Security techniques -- Requirements for partially anonymous, partially unlinkable authentication.
· ISO/IEC 29192-1:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 1: General
· ISO/IEC 29192-2:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 2: Block ciphers
· ISO/IEC 29192-3:2012 Information technology -- Security techniques -- Lightweight cryptography -- Part 3: Stream ciphers
· ISO/IEC 29192-4:2013 Information technology -- Security techniques -- Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques
· ISO/IEC 29192-5:2016 Information technology -- Security techniques -- Lightweight cryptography -- Part 5: Hash-functions
· ISO/IEC TS 30104:2015 Information Technology -- Security Techniques -- Physical Security Attacks, Mitigation Techniques and Security Requirements
· ISO/IEC 30111:2013 Information technology -- Security techniques -- Vulnerability handling processes

Normas Internacionales en desarrollo

· ISO/IEC NP 9797-2 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
· ISO/IEC DIS 9798-2 Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using authenticated encryption
· ISO/IEC FDIS 9798-3 Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques
· ISO/IEC CD 9798-5 Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques
· ISO/IEC FDIS 10118-3.2 IT Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
· ISO/IEC FDIS 11770-2 IT Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
· ISO/IEC NP 11770-5 Information technology -- Security techniques -- Key management -- Part 5: Group key management
· ISO/IEC NP 13888-1 Information technology -- Security techniques -- Non-repudiation -- Part 1: General
· ISO/IEC NP 13888-3 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques

· ISO/IEC FDIS 14888-3 IT Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
· ISO/IEC CD 15408-1 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
· ISO/IEC CD 15408-2 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
· ISO/IEC CD 15408-3 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
· ISO/IEC CD 15408-4 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 4: Framework for the specification of evaluation methods and activities
· ISO/IEC CD 15408-5 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 5: Pre-defined packages of security requirements
· ISO/IEC NP 18014-2 Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
· ISO/IEC CD 18032 Information technology -- Security techniques -- Prime number generation
· ISO/IEC NP 18033-1 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
· ISO/IEC DIS 18033-6 Information technology security techniques -- Encryption algorithms -- Part 6: Homomorphic encryption
· ISO/IEC CD 18045 Information technology -- Security techniques -- Methodology for IT security evaluation
· ISO/IEC FDIS 19086-4 Cloud computing -- Service level agreement (SLA) framework -- Part 4: Components of security and of protection of PII
· ISO/IEC PRF TS 19608
· Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
· ISO/IEC 19896-2 IT security techniques -- Competence requirements for information security testers and evaluators -- Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
· ISO/IEC 19896-3 IT security techniques -- Competence requirements for information security testers and evaluators -- Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators
· ISO/IEC CD 19989-1 Information technology -- Security techniques -- Criteria and methodology for security evaluation of biometric systems -- Part 1: Framework
· ISO/IEC NP 19989-2 Information technology -- Security techniques -- Criteria and methodology for security evaluation of biometric systems -- Part 2: Biometric recognition performance
· ISO/IEC NP 19989-3 Information technology -- Security techniques -- Criteria and methodology for security evaluation of biometric systems -- Part 3: Presentation attack detection
· ISO/IEC NP 20008-2 Information technology -- Security techniques -- Anonymous digital signatures -- Part 2: Mechanisms using a group public key
· ISO/IEC CD 20009-3 Information technology -- Security techniques -- Anonymous entity authentication -- Part 3: Mechanisms based on blind signatures concepts
· ISO/IEC DIS 20085-1 Information technology -- Security techniques -- Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules -- Part 1: Test tools and techniques

· ISO/IEC CD 20085-2 Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules -- Part 2: Test calibration methods and apparatus
· ISO/IEC DIS 20543 Information technology -- Security techniques -- Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
· ISO/IEC AWI 20547-4 Information technology -- Big data reference architecture -- Part 4: Security and privacy
· ISO/IEC FDIS 20889 Privacy enhancing data de-identification terminology and classification of techniques
· ISO/IEC CD 20897-1 Security requirements and test methods for physically unclonable functions for generating non-stored security parameters -- Part 1: Security requirements for PUFs
· ISO/IEC NP 20897-2 Security requirements and test methods for physically unclonable functions for generating non-stored security parameters -- Part 2: Test methods of PUFs
· ISO/IEC FDIS 21878 Information technology -- Security techniques -- Security guidelines for design and implementation of virtualized servers
· ISO/IEC AWI TR 22216 Information technology -- Security techniques -- Introductory guidance on evaluation for IT security
· ISO/IEC AWI 23264 Information Technology -- Security Techniques -- Redaction of Authentic Data
· ISO/IEC NP 24745 Information technology -- Security techniques -- Biometric information protection
· ISO/IEC DIS 24761 Information technology -- Security techniques -- Authentication context for biometrics
· ISO/IEC NP 27002 Information technology -- Security techniques -- Code of practice for information security controls
· ISO/IEC PDTS 27008 Information technology -- Security techniques -- Guidelines for the assessment of information security controls
· ISO/IEC CD 27009 Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 -- Requirements
· ISO/IEC NP 27014 Information technology -- Security techniques -- Governance of information security
· ISO/IEC FDIS 27018 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
· ISO/IEC AWI 27030 Information technology -- Security techniques -- Guidelines for security and privacy in Internet of Things (IoT)Title missing
· ISO/IEC CD 27034-4 Information technology -- Security techniques -- Application security -- Part 4: Validation and verification
· ISO/IEC NP 27035-3 Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for incident response operations
· ISO/IEC FDIS 27050-2 Information technology -- Electronic discovery -- Part 2: Guidance for governance and management of electronic discovery
· ISO/IEC NP 27050-4 Information technology -- Security techniques -- Electronic discovery -- Part 4: Technical readiness
· ISO/IEC NP 27070 Information technology -- Security techniques -- Security requirements for establishing virtualized roots of trust

- ISO/IEC AWI TS 27101 Information technology -- Security techniques -- Cybersecurity -- Framework development guidelines
- ISO/IEC CD 27102 Information technology -- Security techniques -- Information security management guidelines for cyber insurance
- ISO/IEC PDTR 27550 Information technology -- Security techniques -- Privacy engineering
- ISO/IEC AWI 27551 Information technology -- Security techniques -- Requirements for attribute-based unlinkable entity authentication
- ISO/IEC CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements
- ISO/IEC AWI TS 27570 Information Technology -- Security Techniques -- Privacy guidelines for Smart Cities
- ISO/IEC FDIS 29101 Information technology -- Security techniques -- Privacy architecture framework
- ISO/IEC NP 29115 Information technology -- Security techniques -- Entity authentication assurance framework
- ISO/IEC FDIS 29147 Information technology -- Security techniques -- Vulnerability disclosure
- ISO/IEC CD 29184 Guidelines for online privacy notices and consent
- ISO/IEC DIS 29192-6 Information technology -- Security techniques -- Lightweight cryptography -- Part 6: Message authentication codes (MACs)
- ISO/IEC DIS 29192-7 Information technology -- Security techniques -- Lightweight cryptography -- Part 7: Broadcast authentication protocols
- ISO/IEC CD 30111 Information technology -- Security techniques -- Vulnerability handling processes

Normas y prácticas Extranjeras y privadas

- NIST SP 800-53 Controles de seguridad y privacidad para organizaciones y sistemas de información federales, National Institute of Standards and Technology
- CIS CSC, Center for Internet Security Critical Security Controls for Effective Cyber Defense. Controles de seguridad para una efectiva ciberdefensa, Centro de seguridad para el Internet
- COBIT 5 Control Objectives for Information and Related Technologies, ISACA
- Familia ISA 62443 Familia de estándares de Ciberseguridad de la International Society of Automation

FUENTES DE INFORMACIÓN

1. Campaña Cibernauta con Estrella *https://www.gob.mx/policiafederal/articulos/cibernauta-con-estrella?idiom=es*
2. ISO/IEC 27002:2013, Information Technology - Security Techniques Code of Practice for Information Security Controls
3. COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.
3. Transforming Cybersecurity: Using COBIT® 5.
4. Framework for Improving Critical Infrastructure Cybersecurity version 1.1, National Institute of Standards and Technology, 2018.
5. Security and Privacy Controls for Information Systems and Organizations, Draft NIST Special Publication 800-53
6. National Cyber Security Index (NCSI), e-Governance Academy Foundation, https://ncsi.ega.ee/ncsi-index/
7. Global Cybersecurity Index, International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
8. "Recomendaciones: Hacia la construcción de la Estrategia Nacional de Ciberseguridad (ENCS) en México" AMDETIC. *https://drive.google.com/file/d/0BwwuPXLVXE44X1pJakFSSVZvWUk/view*
9. Documentos emitidos por el INAI que pueden resultar relevantes para el tema de Ciberseguridad:
    - *Recomendaciones para el manejo de incidentes de seguridad de datos personales.* Disponible en la página web del Instituto, en el apartado de Protección de Datos Personales, o bien en la siguiente dirección electrónica**:** *http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf*
    - Los estándares de protección de datos personales para los estados Iberoamericanos: *http://inicio.ifai.org.mx/nuevo/Estandares/Estandares%20(Espa).pdf*
    - Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (CNTAID) 2016: *http://proyectos.inai.org.mx/cntaid2016/index.php/censo-y-resultados*
    - Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2016: *http://proyectos.inai.org.mx/enaid2016/index.php/encuestas-y-resultados*
    - Guía para prevenir el robo de identidad: *http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf*
    - Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares: *http://inicio.inai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf*
    - Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales: *http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf*
    - Guía para el Borrado Seguro de Datos Personales: *http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf*

- Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas: *http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf*
- Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales: *http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf*
- Recomendaciones para la Designación de la Persona o Departamento de Datos Personales: *http://inicio.inai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf*

10. Defending Politically Vulnerable Organizations Online. Center for Long-Term Cybersecurity (CLTC). *https://cltc.berkeley.edu/defendingpvos/*

11. *www.gob.mx/internetseguro*

Otras acciones de Policía Federal. División Científica en el marco de la Estrategia Nacional de Ciberseguridad

- Tercera Semana Nacional de la Ciberseguridad. https://www.gob.mx/policiafederal/articulos/programa-de-actividades-tercera-semana-nacional-de-la-ciberseguridad
- Segunda Semana Nacional de Ciberseguridad https://www.gob.mx/policiafederal/articulos/segunda-semana-nacional-de-ciberseguridad
- 1er Semana Nacional de la Ciberseguridad https://www.gob.mx/policiafederal/prensa/la-comision-nacional-de-seguridad-organiza-la-semana-nacional-de-la-ciberseguridad
- Impulsa Policía Federal la creación del primer Comité de Ciberseguridad a nivel nacional https://www.gob.mx/policiafederal/prensa/impulsa-policia-federal-la-creacion-del-primer-comite-de-ciberseguridad-a-nivel-nacional
- Reune CNS a las Unidades de Policía Cibernética del país y realiza la primera Sesión del Comité de Ciberseguridad https://www.gob.mx/policiafederal/prensa/reune-cns-a-las-unidades-de-policia-cibernetica-del-pais-y-realiza-la-primera-sesion-del-comite-de-ciberseguridad?idiom=es
- CNS realiza Primer Coloquio de Ciberseguridad para Medios de Comunicación https://www.gob.mx/policiafederal/articulos/cns-realiza-primer-coloquio-de-ciberseguridad-para-medios-de-comunicacion-118212
- Policía Federal y Condusef inauguran ciclo de conferencias en materia de Ciberseguridad https://www.gob.mx/policiafederal/prensa/policia-federal-y-condusef-inauguran-ciclo-de-conferencias-en-materia-de-ciberseguridad?idiom=es
- La Comisión Nacional de Seguridad inaugura campaña de concientización “Ciberseguridad México 2018” https://www.gob.mx/policiafederal/prensa/la-comision-nacional-de-seguridad-inaugura-campana-de-concientizacion-ciberseguridad-mexico-2018-149497
- Glosario de términos en Ciberseguridad https://www.gob.mx/policiafederal/articulos/glosario-de-terminos-en-ciberseguridad?idiom=es

- Recomendaciones de Ciberseguridad para prevenir afectaciones por código malicioso tipo “Ransomware” https://www.gob.mx/policiafederal/prensa/policia-federal-emite-recomendaciones-de-ciberseguridad-para-prevenir-afectaciones-por-codigo-malicioso-tipo-ransomware
- Descarga materiales educativos y preventivos en materia de Ciberseguridad https://www.gob.mx/policiafederal/articulos/descarga-materiales-educativos-y-preventivos-en-materia-de-ciberseguridad?idiom=es