CIBERSEGURIDAD EN MÉXICO Y EN OTROS PAÍSES

Marco normativo

Comité Técnico en materia de Despliegue de 5G en México
Mesa 5. Ciberseguridad

Índice

Ciberseguridad en México y en otros países

I. Introducción

En 2017, México presentó su Estrategia Nacional de Ciberseguridad con el objetivo de identificar y establecer las acciones de seguridad cibernética aplicables a las áreas social, económica y política para permitirles a la población y las organizaciones públicas y privadas el uso de las Tecnologías de la Información y las Comunicaciones (TIC) de manera responsable para el desarrollo sostenible del Estado mexicano.

Actualmente, no hay una actualización de la Estrategia, además, México no cuenta con una ley dedicada de delito cibernético, pero el artículo 211 del Código Penal prevé el delito informático. Sin embargo, de acuerdo con el Reporte de Ciberseguridad 2020 del Banco Interamericano de Desarrollo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen.[1]

De acuerdo con el Código Penal Federal, algunos de los delitos tipificados en México, en los cuales se emplean los sistemas informáticos, electrónicos, Internet, computadoras, programas informáticos como medio o como fin se encuentran: la revelación de secretos, el acceso ilícito a sistemas y equipos informáticos, el acoso sexual, el engaño telefónico, la extorsión telefónica, falsificación de títulos, pornografía, suplantación de identidad, entre otros. Otros delitos en cuya comisión se emplean las TIC son el delito de fraude, el robo, el delito equiparado al fraude, entre otros.

II. Estrategia Nacional de Ciberseguridad (ENC)[2]

Durante 2017 el proceso de desarrollo de la ENC se llevaron a cabo talleres, reuniones de seguimiento y conversatorios con diferentes actores en México: sociedad civil, sector privado, comunidad técnica y académica e instituciones públicas de los tres poderes y de los diferentes órdenes de gobierno.

Como antecedente a tomar en cuenta, la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE) fue creada en 2005 para el desarrollo del Gobierno Electrónico, cuyo fin es promover y consolidar el uso y aprovechamiento de las TIC en la Administración Pública Federal, mediante la adecuada coordinación de las acciones que al efecto proponga la Secretaría de la Función Pública, con las dependencias de la Administración Pública Federal. Asimismo, con la finalidad de una adecuada coordinación entre las Dependencias

[1] Banco Interamericano de Desarrollo (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. http://dx.doi.org/10.18235/0002513

[2] Para mayor detalle se puede consultar:https://intranet.inaes.gob.mx/pdf/CiberSeguridad/Estrategia_Nacional_Ciberseguridad.pdf

y, en su caso, Entidades se fueron constituyendo Subcomisiones para el cumplimiento de su propósito.[3]

En este sentido, durante 2017, se creó la Subcomisión de Ciberseguridad en la XVIII sesión ordinaria de la CIDGE, en sus dos sesiones de 2017 surgió el documento de la ENC.

La ENC establece ocho ejes transversales a fin de fortalecer las acciones en materia de ciberseguridad aplicables:

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

Asimismo, la estrategia establece los siguientes objetivos estratégicos:

1. Sociedad y derechos. Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de expresión, vida privada y protección de datos personales, entre otros.
2. Economía e innovación. Fortalecer los mecanismos en materia de ciberseguridad para proteger la economía de los diferentes sectores productivos del país y propiciar el desarrollo e innovación tecnológica, así como el impulso de la industria nacional en materia de ciberseguridad, a fin de contribuir al desarrollo económico de individuos, organizaciones privadas, instituciones públicas y sociedad en general.
3. Instituciones públicas. Proteger la información y los sistemas informáticos de las instituciones públicas del país para el funcionamiento óptimo de éstas y la continuidad en la prestación de servicios y trámites a la población.
4. Seguridad pública. Incrementar las capacidades para la prevención e investigación de conductas delictivas en el ciberespacio que afectan a las personas y su patrimonio, con la finalidad de mantener el orden y la paz pública.
5. Seguridad nacional. Desarrollar capacidades para prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia,

[3] ACUERDO que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, 9 de diciembre de 2005, México. http://www.dof.gob.mx/nota_detalle.php?codigo=2101617&fecha=09/12/2005

integridad y soberanía nacional, afectando el desarrollo y los intereses nacionales.[4]

En su actuar la ENC planteaba desarrollarse a través de tres principios rectores: 1) perspectiva de derechos humanos; 2) enfoque basado en gestión de riesgos, y 3) colaboración multidisciplinaria y de múltiples actores.

Sobre la implementación de la ENC se diseñó que estuviera a cargo de la Subcomisión de Ciberseguridad de la CIDGE, fomentando la participación de actores de sociedad civil, academia, sector privado y otras instituciones públicas en los diversos Grupos de Trabajo. En este sentido, a partir de 2018 se iniciaron reuniones por cada uno de los cinco objetivos estratégicos y ocho ejes transversales trabajando con los actores interesados.[5] Posterior a 2018, no se han realizado acciones por parte de la Subcomisión ni en el marco del CIDGE, la última sesión de su Consejo Ejecutivo se tiene registrada el primero de abril de 2019.[6]

III. Guardia Nacional y el Centro Especializado en Respuesta Tecnológica

De acuerdo con la Constitución Política de las Estados Unidos Mexicanos (CPEUM) en su artículo 21, la Guardia Nacional es una institución policial de carácter civil, así como un órgano administrativo desconcentrado de la Secretaría de Seguridad y Protección Ciudadana. Asimismo, de acuerdo con las facultades del Presidente, señaladas artículo 89 de la CPEUM, puede disponer de la Guardia Nacional en los términos que la ley señale[7].

El secretario de la Secretaría de Seguridad y Protección Ciudadana tiene entre sus facultades organizar, dirigir y supervisar bajo su adscripción a la Guardia Nacional. Sin embargo, al frente de la Guardia Nacional hay un comandante, quien se apoya de la Comandancia de la Guardia Nacional; Jefatura General de Coordinación Policial; Coordinación de Administración y Finanzas; Unidad de Órganos Especializados por Competencia; Unidad para la Protección de los Derechos Humanos, Disciplina y Desarrollo Profesional; Unidad de Asuntos Internos; Unidad de Asuntos Jurídicos y Transparencia; Coordinación Territorial; Coordinación Estatal; Coordinación de Unidad de Nivel Batallón.[8]

Asimismo, la Guardia Nacional cuenta con una Coordinación Operativa Interinstitucional de carácter permanente y está integrada por representantes de las dependencias de la Secretaría de Seguridad y Protección Ciudadana, la Secretaria de Defensa Nacional y la Secretaría de Marina. Al respecto, la

---

[4] Gobierno de México (2017). Estrategia Nacional de Ciberseguridad. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[5] Gobierno de México (2018). Memoria y Recomendaciones ENCS. https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf

[6] Gobierno de México (2019). 42a Sesión del Consejo Ejecutivo de la CIDGE. https://www.gob.mx/cidge/articulos/42a-sesion-del-consejo-ejecutivo-de-la-cidge?idiom=es

[7] Constitución Política de los Estados Unidos Mexicanos, México. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

[8] Reglamento de la Ley de la Guardia Nacional, México. https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGN_111220.pdf

Coordinación apoya con la coordinación y colaboración estratégica entre las dependencias de la Administración Pública Federal y la Guardia Nacional.

En el caso de la Unidad de Órganos Especializados por Competencia tiene el objetivo de proponer los lineamientos, mecanismos, técnicas generales de investigación y prevención de delitos, y de atención a mandamientos ministeriales y judiciales, mediante la observancia a lo establecido en la normatividad interna, las disposiciones jurídicas aplicables y el respeto a los derechos humanos por sus direcciones generales encargadas de las funciones técnico-especializadas. En este sentido una de sus direcciones adscritas es la Dirección General Científica, la cual busca proponer políticas y procedimientos institucionales en la actuación de los servicios técnico-científicos, mediante la aplicación de estrategias contra la ciberdelincuencia, la investigación criminalística y desarrollo científico-tecnológico para la implementación de las acciones que apoyen las investigaciones en materia de prevención del delito, así como el esclarecimiento de hechos delictivos competencia de la Guardia Nacional. De esta última se destaca entre sus funciones la de implementar las acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet, con la finalidad de prevenir conductas delictivas.[9]

México cuenta con un Centro Especializado en Respuesta Tecnológica, conocido como Centro Nacional de Respuesta a Incidencias Informáticas (CERT MX), previamente parte de la División Científica de la Policía Federal, pero con la promulgación del reglamento de la Ley de la Guardia Nacional paso a manos de esta última como parte de la Dirección General Científica. En este sentido, de acuerdo con el artículo 9 la Ley de la Guardia Nacional está encargada de realizar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet sobre sitios web, con el fin de prevenir conductas delictivas.[10]

El CERT-MX tiene la misión de brindar los servicios de apoyo en la respuesta a incidentes cibernéticos que afectan a las instituciones en el país que cuentan con infraestructura crítica de información, que incluye la identificación de amenazas y modus operandi de la ciberdelincuencia para el alertamiento a la ciudadanía, mediante la gestión de incidentes de seguridad informática, fungiendo como el único punto de contacto y coordinación dentro y fuera del territorio nacional y actuando en la investigación forense digital y el análisis técnico policial en apoyo al Ministerio Público.[11]

El CERT-MX realiza el monitoreo en la red pública de internet a fin de prevenir conductas delictivas, obtiene información de diversas fuentes de agencia nacionales e internacionales y colabora con otros equipos de respuesta que

[9]MANUAL de Organización General de la Guardia Nacional, México. https://dof.gob.mx/nota_detalle.php?codigo=5635311&fecha=16/11/2021
[10] Ley de la Guardia Nacional, Diario Oficial de la Federación, 27 de mayo de 2019, México. https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019
[11] Gobierno de México. ¿Qué es el CERT-MX?. https://www.gob.mx/gncertmx?tab=%C2%BFQu%C3%A9%20es%20CERT-MX?

conforman la comunidad global del Forum for Incident Response and Security Teams (FIRST)[12].

El objetivo de FIRST es reunir a equipos de respuesta a incidentes y seguridad de todos los países del mundo para garantizar una internet segura para todos por medio de plataformas, medios y herramientas para que los equipos encuentren siempre el socio adecuado y colaboren de manera eficiente. [13]

Dentro del FIRST hay otros 11 equipos de México por parte de la industria y otras instituciones como el CERT de la Universidad Nacional Autónoma de México; Centro de Respuesta ante Incidentes Informáticos (CSIRT, por sus siglas en inglés) de AXTEL; BESTEL *Security Operation Center and Indicents Response Teams;* CERT DSI Totalsec; CERT-AT&T México; CSIRT Ikusi México; CSIRT IQsec; Mnemo-CERT; CERT Silent4Business; CERT Scitum; TIC DEFENSE CERT.

IV. Estrategia Digital Nacional

Como antecedente, el 22 de marzo de 2021, como parte del Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica, se plantearon una serie de acciones a desarrollarse por la Coordinación de Estrategia Digital Nacional (CEDN).

Lo anterior fundamentado en el artículo 8 de la Ley Orgánica de la Administración Pública Federal, en la cual se detalla que "el Ejecutivo Federal contará con las unidades de apoyo técnico y estructura que el presidente determine, de acuerdo con el presupuesto asignado a dicha Oficina", así como que las unidades podrán estar adscritas de manera directa a la Presidencia o a través de la Oficina referida y desarrollarán, en otras funciones, las políticas del Gobierno Federal en los temas de informática, tecnologías de la información, comunicación y de gobierno digital, en términos de las disposiciones aplicables.[14]

LA CEDN tiene la misión de promover e impulsar que las y los mexicanos gocen y se beneficien del acceso a las tecnologías información y comunicación, así como de los servicios de banda ancha e internet y su potencial transformador para el desarrollo social cultural y económico.

En este sentido la CEDN en materia de seguridad de la información buscaba realizar evaluaciones de seguridad para detectar amenazas y mejorar la gestión de riesgos; implementar sistemas basados en Software Libre, coordinación entre autoridades para los procesos de prevención y atención de incidencias cibernéticas; e implementar un protocolo de seguridad digital y promoción de buenas prácticas de prevención a través del CERT-MX.

Asimismo, el CIDGE, como órgano de coordinación Ejecutiva en materia de Gobierno Digital, es también un mecanismo para la articulación de las políticas

[12] El FIRST es una organización enfocada en la respuesta a incidentes. https://www.first.org/.
[13] FIRST. *First Teams.* https://www.first.org/about/mission
[14]Ley Orgánica de la Administración Pública Federal, México.

tecnológicas de la CEDN, sin embargo de acuerdo con el Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica, posiblemente se modifique, actualice o sustituya el CIDGE a fin de hacerlo armonizable con el marco normativo actual para mejorar la coordinación operativa en la implementación de las políticas tecnológicas.[15]

En septiembre de 2021 se publicó en el Diario Oficial de la Federación el acuerdo por el que se expide la Estrategia Digital Nacional (EDN) 2021-2024, con el propósito orientar el uso y el desarrollo de las TIC al bienestar social y lograr independencia tecnológica, así como evitar monopolios. Además, detalla que es de observancia obligatoria para las dependencias y entidades de la Administración Pública Federal, las cuales deberán actuar conforme a su misión, visión y sus ejes; así como apegarse a sus principios, objetivos y líneas de acción.

En este sentido la EDN aterriza las capacidades gubernamentales bajo 5 principios: austeridad, combate a la corrupción, eficiencia en los procesos digitales, seguridad de la información y soberanía tecnológica. En el caso de la seguridad de la información se integra el objetivo específico de promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales, al respecto, se plantea una colaboración entre autoridades para mejorar los procesos de prevención y atención de incidencias cibernéticas, así como buenas prácticas de prevención y reacción a través de la colaboración con el CERT-MX.[16]

V. Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos

Sustentado en la EDN, el Protocolo tiene el objetivo de fortalecer la Ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país, con la finalidad de alcanzar los niveles de riesgo aceptables en la materia, contribuyendo al mantenimiento del orden constitucional, la preservación de la democracia, el desarrollo económico, social y político del país, así como al bienestar de las mexicanas y los mexicanos.

Al respecto, han considerado como metodología de aplicación el Marco de Referencia sobre Ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos de América (NIST). Dicho Marco hace referencia a las normas y directrices internacionales existentes, así como a las mejores prácticas de la industria, para promover la protección de las infraestructuras críticas mediante la gestión de riesgos. Representa una colección de normas y mejores prácticas

[15] Gobierno de México (2021). Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica. https://www.gob.mx/cedn/documentos/proceso-de-planeacion-para-el-desarrollo-de-la-estrategia-digital-nacional-y-de-la-politica-tecnologica.

[16] Estrategia Digital Nacional 2021-2024, 6 de septiembre de 2021, México. https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#:~:text=La%20Estrategia%20Digital%20Nacional%20que%20se%20desprende%20del%20Plan%20Nacional,mediante%20su%20incorporaci%C3%B3n%20a%20la.

existentes que han demostrado su eficacia para proteger los sistemas informáticos de las ciber-amenazas, garantizar la confidencialidad de las empresas y proteger la privacidad y las libertades civiles de las personas. En este sentido, el Marco es una metodología cuyo objetivo es reducir y gestionar mejor los riesgos de seguridad cibernética y puede ser usado por las partes interesadas para permitirles identificar y priorizar acciones para reducir el riesgo de seguridad cibernética, así como para alinear los enfoques de políticas, negocios y tecnología para manejar dicho riesgo.[17]

Sobre la coordinación para el Protocolo Nacional de Gestión de Incidentes Cibernéticos, el CERT-MX de la Dirección General Científica de la Guardia Nacional, fungirá como la única instancia de coordinación entre las Instituciones de la Administración Pública Federal, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país involucradas. Asimismo, el Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, detalla que las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, además de que se recomienda que se establezcan y operen un Equipo de Respuesta a Incidentes de seguridad en TIC en las organizaciones.[18]

VI. Policía cibernética

El Sistema Nacional de Seguridad Pública (SNSP) es quien sienta las bases de coordinación y distribución de competencias, en materia de seguridad pública, entre la Federación, los Estados y municipios, bajo la directriz del Consejo Nacional de Seguridad Pública (CNSP).

El CNSP es el órgano superior del SNSP, y es presidido por el presidente de la República, e integrado por los Secretarios de Gobernación, Defensa Nacional, Marina, el Procurador General de la República, los Gobernadores de los Estados, el jefe del Gobierno de la Ciudad de México, el Comisionado Nacional de Seguridad, y el Secretario Ejecutivo del SNSP.[19]

El Programa Nacional de Seguridad Pública 2014-2018 estableció dentro de sus estrategias, la detección y atención oportuna de los delitos cibernéticos, y previó como una de sus líneas de acción el desarrollo de un Modelo de Policía Cibernética

[17] Instituto Nacional de Estándares y Tecnología (2018). Marco de Ciberseguridad. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018es.pdf.
[18] ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, 6 de septiembre de 2021, México. .https://www.dof.gob.mx/nota_detalle.php?codigo=5561285&fecha=27/05/2019.
[19] https://www.gob.mx/sesnsp/acciones-y-programas/que-es-el-consejo-nacional-de-seguridad-publica-cnsp.

para las entidades federativas. En este sentido, en el país, existen Unidades de Policías Cibernéticas en cada uno de los estados de la República Mexicana, las cuales realizan actividades de prevención, vigilancia, identificación, monitoreo y rastreo en la red pública de Internet, con la finalidad de prevenir cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes.

VII. El Centro Nacional de Inteligencia

El Centro Nacional de Inteligencia (CNI) se creó el 30 de noviembre de 2018, en sustitución del Centro de Investigación y Seguridad Nacional (CISEN), pero ahora bajo la supervisión de la Secretaría de Seguridad y Protección Ciudadana (SSCP), y conservando las funciones que se establecen en la Ley de Seguridad Nacional.

De acuerdo con la Ley Orgánica de la Administración Pública Federal el CNI funge como un sistema de investigación e información, que contribuye a preservar la integridad, estabilidad y permanencia del Estado mexicano, así como contribuir, en lo que corresponde al Ejecutivo de la Unión, a dar sustento a la unidad nacional, a preservar la cohesión social y a fortalecer las instituciones de gobierno.

Dentro del artículo 19 de la Ley de Seguridad Nacional se mencionan sus funciones en las que se incluyen[20]:

1. Operar tareas de inteligencia como parte del sistema de seguridad nacional que contribuyan a preservar la integridad, estabilidad y permanencia del Estado Mexicano, a dar sustento a la gobernabilidad y a fortalecer el Estado de Derecho;
2. Procesar la información que generen sus operaciones, determinar su tendencia, valor, significado e interpretación específica y formular las conclusiones que se deriven de las evaluaciones correspondientes, con el propósito de salvaguardar la seguridad del país;
3. Preparar estudios de carácter político, económico, social y demás que se relacionen con sus atribuciones, así como aquellos que sean necesarios para alertar sobre los riesgos y amenazas a la Seguridad Nacional;
4. Elaborar los lineamientos generales del plan estratégico y la Agenda Nacional de Riesgos;
5. Proponer medidas de prevención, disuasión, contención y desactivación de riesgos y amenazas que pretendan vulnerar el territorio, la soberanía, las instituciones nacionales, la gobernabilidad democrática o el Estado de Derecho;
6. Establecer cooperación interinstitucional con las diversas dependencias de la Administración Pública Federal, autoridades federales, de las entidades federativas y municipales o delegacionales, en estricto apego a sus respectivos ámbitos de competencia con la finalidad de coadyuvar en la

[20] Ley de Seguridad Nacional, México. https://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac_200521.pdf.

preservación de la integridad, estabilidad y permanencia del Estado Mexicano;

7. Proponer al Consejo el establecimiento de sistemas de cooperación internacional, con el objeto de identificar posibles riesgos y amenazas a la soberanía y seguridad nacionales;
8. Adquirir, administrar y desarrollar tecnología especializada para la investigación y difusión confiable de las comunicaciones del Gobierno Federal en materia de Seguridad Nacional, así como para la protección de esas comunicaciones y de la información que posea;
9. Operar la tecnología de comunicaciones especializadas, en cumplimiento de las atribuciones que tiene encomendadas o en apoyo de las instancias de gobierno que le solicite el Consejo de Seguridad Nacional;
10. Prestar auxilio técnico a cualquiera de las instancias de gobierno representadas en el Consejo de Seguridad Nacional, conforme a los acuerdos que se adopten en su seno.

También en el Manual de Organización General de la SSCP, en el caso de la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica de la SSPC, tiene la función de establecer mecanismos de coordinación funcional con el Centro Nacional de Inteligencia (CNI), con el propósito de determinar el valor, significado e interpretación de la información sistematizada a favor de los trabajos de inteligencia de la Secretaría.[21]

En este sentido, en el Informe de la Estrategia Nacional de Seguridad Pública de 2019 se menciona que en junio y julio el CNI analizó el Proyecto de Iniciativa de Ley Federal de Ciberseguridad y formuló comentarios desde los ámbitos jurídico y técnico, así como la opción de establecer un grupo y Plan de trabajo para enriquecer el proyecto. También la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica de la SSPC, integró una mesa de trabajo, en la cual participó el CNI y la entonces División Científica de la Policía Federal a fin de elaborar el proyecto legislativo. Dicho proyecto fue presentado a la Consejería Jurídica del Ejecutivo Federal.[22]

También considerando las funciones previas del CNI como CISEN del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información, tiene la atribución de ser comunicado sobre los servidores públicos que designen como responsables de la seguridad de la información; así como de los enlaces responsables de mantener comunicación con los equipos de respuesta a incidentes de seguridad en TIC, para efectos de su registro.[23]

---

[21] Manual de Organización General de la Secretaría de Seguridad y Protección Ciudadana, México. https://www.dof.gob.mx/nota_detalle.php?codigo=5606770&fecha=04/12/2020#gsc.tab=0

[22] SSPC (2019). Informe Anual Estrategia Nacional de Seguridad Pública, México, p. 62. https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2020-07-08-1/assets/documentos/SSyPC_Informe_Estrategia_Nacional_de_Seguridad_Publica.pdf

[23] Centro Nacional de Inteligencia (2018). Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información. https://www.gob.mx/cni/documentos/manual-administrativo-de-aplicacion-general-en-materia-de-tecnologias-de-la-informacion

VIII. Programas Sectoriales

De acuerdo con la Ley de Planeación, los Programas Sectoriales se sujetan a las previsiones contenidas en el Plan Nacional de Desarrollo para el período de gobierno correspondiente. En estos se especifican los objetivos, prioridades y políticas que regirán el desempeño de las actividades del sector administrativo de que se trate.

El pasado 2 de julio de 2020 se presentó el Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024. El objetivo del programa es atender las problemáticas del deterioro de las condiciones de seguridad pública en las regiones del país; deficiente reinserción social de las personas privadas de la libertad; desvinculación de la inteligencia generada para la seguridad nacional con la seguridad pública; coordinación ineficiente de políticas públicas de prevención con participación ciudadana, con estados y regiones; limitada y obsoleta infraestructura en materia de tecnologías de la información y comunicaciones en las instituciones de seguridad, e insuficiencia de un marco legal y de instrumentos para una política de la gestión integral de riesgos.

Al respecto, el programa consta de 5 Objetivos prioritarios que responden al nivel más alto de la planeación nacional del desarrollo, ya que marcan los temas que se consideran prioritarios atender durante la presente administración. Es importante enfatizar en el Objetivo prioritario 4, el cual busca fortalecer las capacidades tecnológicas que permitan a las instituciones de seguridad de los tres órdenes de gobierno el intercambio seguro de la información en la generación de inteligencia, prevención y persecución del delito.

La relevancia de Objetivo 4 viene de la mano del reconocimiento de la obsolescencia de la infraestructura tecnológica de las instituciones de seguridad pública, sobre la que actualmente desarrolla su operación y que se manifiesta en delitos cibernéticos que han abierto nuevos espacios dónde se cometen. En este sentido, se detalla que en los últimos años se atendieron más de 260 mil incidentes y 68 mil reportes ciudadanos; neutralizando alrededor de 26 mil sitios web identificados con actividades ilícitas, y se han realizado 4,500 colaboraciones internacionales, por lo que se requiere de atención prioritaria.[24]

Al respecto, entre los principales problemas en materia tecnológica se destaca que frente a la constante actualización tecnológica se requiere de sistemas de gestión de seguridad de la información más eficientes que incorporen estrategias de ciberseguridad para la prevención, detección y respuesta a incidentes como ataques cibernéticos en las instituciones de seguridad, por lo que es necesario fortalecer la seguridad a fin de evitar las vulnerabilidades lógicas y físicas en las plataformas tecnológicas de las instituciones de seguridad, así como ampliar los

[24] PROGRAMA Sectorial de Seguridad y Protección Ciudadana 2020-2024, 2 de julio de 2020, México. https://dof.gob.mx/nota_detalle.php?codigo=5596028&fecha=02/07/2020

acuerdos de colaboración interinstitucional para fortalecer los mecanismos de seguridad de la información.

Entre las Estrategias Prioritarias y las Acciones Puntuales para alcanzar el objetivo, la que va de la mano con los temas de ciberseguridad es la Estrategia 4.2 que busca implementar procesos de gestión de riesgos para la protección de los sistemas de información y telecomunicaciones de las plataformas tecnológicas que permitan a las instituciones de seguridad de los tres órdenes de gobierno proteger la información ante la presencia de ciberataque.

De este modo se espera que a través de las siguientes Acciones Puntuales se consiga el objetivo deseado:

1. Implementar infraestructura y protocolos de seguridad informática para la prevención de ciberataques en el intercambio de información entre las instituciones de seguridad de los tres órdenes de gobierno.
2. Promover acuerdos en materia de seguridad informática con las instituciones de seguridad de los tres órdenes de gobierno y del sector privado para combatir los delitos cibernéticos.
3. Capacitar en el uso, mantenimiento y actualización de las herramientas tecnológicas en materia de ciberseguridad para prevenir y hacer frente a los diversos ataques cibernéticos.
4. Establecer mecanismos de coordinación en el ámbito nacional e internacional para la prevención, investigación y persecución del delito en materia de ciberseguridad.
5. Diseñar e implementar programas para promover la cultura y concientización sobre seguridad de la información y tecnología, en las instituciones de seguridad de los tres órdenes de gobierno.

Asimismo, una de las Acciones del Objetivo prioritario 1 espera que en el marco de la prevención, investigación y persecución del delito en materia de ciberseguridad se establezcan mecanismos de coordinación en el ámbito nacional e internacional, con perspectiva de género, diferenciada e intercultural. Lo anterior, bajo el Objetivo de mejorar las condiciones de seguridad en las regiones del territorio nacional para construir la paz.

Con el Programa Sectorial, se espera observar un cambio en las condiciones de vida de la población, por lo que, a fin de conocer el avance en el cumplimiento de estos objetivos, se han establecido metas para el bienestar y parámetros. Ambos son expresiones cuantitativas construidas a partir de variables cuantitativas o cualitativas, que proporcionan un medio sencillo y fiable para medir el cumplimiento de las metas establecidas, reflejar los cambios vinculados con las acciones del programa, dar seguimiento y evaluar sus resultados.

Para el caso del Objetivo 4 se espera reconocer estos cambios a través de los siguientes parámetros:

1. Porcentaje promedio de la actualización de la capacidad tecnológica de la Secretaría de Seguridad y Protección Ciudadana: mide el porcentaje de avance en la actualización de la infraestructura tecnológica respecto a la programación del periodo 2020-2024 realizada por Guardia Nacional, el Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica de la SSPC, considerando cuatro rubros: servicios de telecomunicación, sistemas de información, infraestructura de cómputo y equipamiento tecnológico.
2. Porcentaje promedio de la actualización de la capacidad tecnológica de la Secretaría de Seguridad y Protección Ciudadana: mide el porcentaje de minutos promedio de disponibilidad de los aplicativos de los siete Registros Nacionales que son consultados y utilizados por los distintos usuarios de los tres órdenes de gobierno.
3. Promedio de los resultados de la evaluación de las bases de datos criminalísticas y del personal del SNSP: mide el promedio nacional del cumplimiento en el acopio de información de las Bases de Datos criminalísticas y de personal del SNSP sobre los criterios de oportunidad, suministro e integridad. Cada base de datos se evalúa con fundamento en la Nueva Metodología para la Evaluación de las Bases de Datos Criminalísticos y de Personal de Seguridad Pública y se calcula el promedio de los resultados. El promedio tiene una escala de 0 a 100.

En el caso de la Secretaría de Marina el 3 de julio de 2020, se presentó el Programa Sectorial de Marina 2020-2024 con el fin de emplear el Poder Naval de la Federación de forma eficiente y eficaz para preservar la seguridad nacional, fortalecer una Autoridad Marítima Nacional y Guardia Costera, que aseguren la seguridad y protección de los puertos, el mantenimiento del Estado de derecho en las costas y aguas nacionales, la salvaguarda de la vida humana en la mar y la conservación del ambiente marino.

El Programa Sectorial de la Secretaría de Marina plantea la implementación de seis objetivos prioritarios, dónde se destaca el primer objetivo estratégico de preservar la seguridad nacional y coadyuvar en la seguridad interior del país, ya que toma en cuenta la ciberseguridad por medio de su estrategia prioritaria 1.4 "*fortalecer las capacidades de seguridad en el ciberespacio para coadyuvar con la seguridad nacional y seguridad interior*". Entre las acciones puntuales correspondientes a esta estrategia se mencionan:

- Desarrollar y mantener las capacidades humanas y tecnológicas que apoyen las operaciones en el Ciberespacio, fortaleciendo las acciones institucionales en materia de ciberseguridad para el mantenimiento de la integridad y permanencia del Estado mexicano.
- Contribuir con el esfuerzo nacional para reducir la vulnerabilidad cibernética, a través de la coordinación y cooperación con otras Fuerzas

Armadas, sector público, privado y académico, a favor de la seguridad nacional y seguridad interior.
- Planear, conducir y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa, a través de operaciones en el ciberespacio.
- Promover el marco jurídico, la normatividad interna y doctrina adecuada en materia de operaciones en el ciberespacio, a fin de actuar conforme a derecho en materia de ciberseguridad.[25]

En el caso de los parámetros para reconocer los avances y resultados de este objetivo, el Plan Sectorial de la Marina considera medir el porcentaje de fortalecimiento del Sistema de Inteligencia Naval y de Seguridad en el Ciberespacio. Nacional; el cuál mide el avance de las acciones del Sistema de Inteligencia de la Armada de México (SIAM), en apoyo a la toma de decisiones en el desarrollo de las Operaciones Navales; además de la Seguridad en el Ciberespacio para disminuir la vulnerabilidad cibernética institucional y nacional.

Al respecto, con el Acuerdo Secretarial Núm.- 335/2022, el 1 de junio de 2022, la Unidad de Ciberseguridad pasó a ser la Coordinadora General del Ciberespacio (EMCOGCIBER). La EMCOGCIBER tiene la misión de determinar y conducir la gobernanza del ciberespacio para la seguridad de la infraestructura esencial de información de la Secretaría de Marina y coadyuvar al esfuerzo nacional en el mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano, a través de la formación de la fuerza cibernética y las operaciones de ciberdefensa a desarrollar con los Cibercomandos.[26] Entre sus atribuciones se incluye:

- Integrar la innovación tecnológica para la explotación del ciberespacio, a fin de obtener las competencias estratégicas, operacionales y tácticas para el desarrollo de ciberoperaciones.
- Proponer y coordinar con las instancias correspondientes el desarrollo profesional de quienes integran la fuerza cibernética.
- Proponer mecanismos de cooperación con las fuerzas armadas, agencias gubernamentales y el sector privado, tanto nacionales como extranjeras, para fortalecer la seguridad y defensa del ciberespacio.
- Promover la actualización de la estrategia institucional del ciberespacio.
- Proponer la profesionalización del personal de hombres y mujeres que conforma la fuerza cibernética de la Secretaría de Marina Armada de México.
- Determinar y conducir la gobernanza del ciberespacio mediante políticas y estándares de seguridad para el empleo de las tecnologías de la información y comunicaciones de la institución.

[25]PROGRAMA Sectorial de Marina 2020-2024, 3 de julio de 2020, México. https://www.dof.gob.mx/nota_detalle.php?codigo=5596130&fecha=03/07/2020.
[26] Secretaría de Marina. (2022). Coordinadora General del Ciberespacio. Seguridad y Defensa en el Ciberespacio. https://www.gob.mx/semar/es/articulos/unidad-de-ciberseguridad-279197.

- Promover y gestionar los recursos humanos, materiales y tecnológicos para la gobernanza del ciberespacio.[27]

Asimismo, como parte de tomar en cuenta la mejora interna, el objetivo prioritario 3 busca fortalecer la Autoridad Marítima Nacional. A pesar de que no alude a la ciberseguridad, la estrategia 3.2 de dicho objetivo "*fortalecer las capacidades en materia de protección marítima y portuaria para el mantenimiento del Estado de derecho en aguas nacionales y recintos portuarios*" es de relevancia por considerarse como rectora en el documento de la "Estrategia Institucional para el Ciberespacio 2021-2024"[28] que la Unidad de Ciberseguridad de la Secretaría de Marina publicó el 4 de mayo de 2021.[29]

Dicha Estrategia surgió para orientar los esfuerzos institucionales en fortalecer las capacidades de ciberdefensa, ciberseguridad y seguridad de la información, en apego con la estrategia 1.4. De tal forma que permita administrar el riesgo cibernético institucional y marítimo nacional, para ello se establecieron una serie de líneas de acción acorde con cada una de las acciones puntuales mencionadas.

Respecto a la acción puntual de desarrollar y mantener capacidades humanas y tecnológicas se mencionan las siguientes líneas de acción:

- Optimizar el recurso humano a través de la conformación de la fuerza cibernética laboral en la Secretaría de Marina.
- Concientizar en seguridad de la información, ciberseguridad y ciberdefensa; generando una memoria histórica funcional en materia de ciberespacio como entorno de seguridad y desarrollo nacional.
- Generar productos de seguridad en el ciberespacio para gestionar el riesgo cibernético institucional y marítimo nacional.
- Crear los cargos de oficial de seguridad de la información para salvaguardar la infraestructura crítica institucional.
- Impulsar la formación y capacitación en materia de seguridad de la información, ciberseguridad y ciberdefensa en los diferentes planteles educativos navales.
- Adiestrar y entrenar personal en los niveles estratégico operacional y táctico.
- Obtener implementar nuevos equipos y sistemas para fortalecer capacidades.

---

[27] Secretaría de Marina. (2022). Revista Secretaría de Marina- Armada de México. Núm. 273, septiembre- octubre 2022. https://www.gob.mx/cms/uploads/attachment/file/804371/Rev_273_SEPTIEMBRE-OCTUBRE.pdf

[28] El término ciberespacio se refiere al entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones (TIC), en que interactúan y se comunican las entidades públicas, privadas y la sociedad en general, coadyuvando al desarrollo nacional y garantizando el ejercicio de los derechos y libertades como en el mundo físico. Se considera el quinto entorno operacional para proporcionar Seguridad y Defensa de las Fuerzas Armadas; los cuatro entornos operacionales previos son el marítimo, el aéreo, el terrestre y el espacial. Para más información se puede consultar: Glosario de términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio. https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf

[29] Secretaría de Marina (2021). Estrategia Institucional de Ciberespacio, México. https://www.gob.mx/semar/documentos/unidad-de-ciberseguridad-278750?state=published.

- Impulsar la investigación y desarrollo tecnológico para fortalecer las capacidades.
- Proteger las infraestructuras críticas de información propias y correspondientes a las instalaciones estratégicas del país.

En los avances que se han realizado sobre el tema, en su "Avance y resultados de 2020 con respecto al Plan Sectorial" la Secretaría de Marina detalla que para esta acción se gestionó con la Universidad Naval (UNINAV) para incluir temas de Ciberseguridad dentro programa de estudios del Centro de Capacitación y Formación del personal de la Armada de México y la implementación del Curso Básico de Ciberseguridad; además de que se elaboraron 52 dossiers de concientización, 23 boletines y cinco alertas de ciberseguridad.[30]

En el caso de la segunda acción puntual sobre contribuir con el esfuerzo nacional para reducir la vulnerabilidad cibernética se reconocen las siguientes líneas de acción:

- Mantener y generar mecanismos de cooperación con Fuerzas Armadas agencias nacionales e internacionales.
- Realizar acciones conjuntas con la Secretaría de Defensa Nacional para desarrollar capacidades a través de una estrategia de ciberdefensa.
- Generar mecanismos de coordinación, colaboración y cooperación con el sector público como privado y Academia.
- Promover acuerdos de cooperación en reuniones de Estado mayores, foros y comités sobre el tema a nivel nacional e internacional.
- Participar en eventos y ejercicios de ciberdefensa y ciberseguridad.
- Apoyar con productos de concientización a la comunidad marítima y portuaria para mitigar vulnerabilidades.
- Coordinar, colaborar y cooperar en materia de seguridad en el ciberespacio con diferentes unidades y establecimientos navales.

Sobre los avances sobre la segunda acción puntual, se destaca la participación en el III Foro Iberoamericano de Ciberdefensa, así mismo se propuso que la Secretaría de Marina, recibiera la Secretaria Pro Tempore del Foro Iberoamericano de Ciberdefensa en el 2021; y en la planeación y capacitación del ejercicio TRADEWINDS 2021 y 2022.

Con la tercera acción puntual sobre consolidar operaciones en el ciberespacio se enlistas las líneas de acción referentes:

- Mantener el monitoreo permanente de la estructura tecnológica institucional para detectar ciberamenazas y vulnerabilidades.
- Incluir las operaciones en el ciberespacio dentro del esquema general de operaciones navales de la Armada de México.

[30]Secretaria de Marina (2020). Programa Sectorial de Marina 2020-2024. Avance y Resultados 2020. https://transparencia.semar.gob.mx/rendicion%20de%20cuentas/Avance_y_Resultados_del_PSM_2020.pdf

- Formalizar el Centro de Operaciones del Ciberespacio de la Armada de México (CSIRT-Marina).
- Mantener la interacción del CSIRT-Marina con el Centro de Mando y Control de la Armada de México para mantener actualizado el panorama operacional.
- Evaluar la ciberseguridad de los sistemas institucionales que soportan las operaciones navales y los procesos críticos.
- Obtener tecnología especializada para aplicación de cadena de custodia el tratamiento de la evidencia digital.

Para la tercera acción se destacan entre los avances la participación en ciber ejercicios, así como que se realizaron 10 cursos de Ciberseguridad gestionados por la UNINAV, un curso con la Junta Iberoamericana de Ciberdefensa y cinco cursos gestionados por NORTHCOM.

Para el caso de la última acción puntual sobre desarrollar marco jurídico, normatividad y doctrina, la estrategia menciona las siguientes líneas de acción:

- Promover las reformas legales que den sustento a la actuación de la Secretaría de Marina en el ciberespacio.
- General la doctrina de la Armada de México en materia de seguridad en el ciberespacio.
- Desarrollar documentos normativos internos para prevenir eventos o incidentes.
- Implementar los planes y protocolos de intercambio de información, contingencia y recuperación at eventos.
- Desarrollar procedimientos para la ejecución de operaciones en el ciberespacio.

En esta última acción se ha gestionado la Normatividad interna y el inicio de la Doctrina de Seguridad en el Ciberespacio para ello se han elaborado productos de Ciberseguridad en materia de Normatividad y Doctrina como Manual de Gestión de Seguridad de la Información de la Secretaría de Marina; Directiva para Respuesta a Incidentes; Directiva para Dispositivos USB; Directiva de Confidencialidad; Directiva de Expedientes Físicos; y la Metodología ARSISM-2020.

Asimismo, para mantener mecanismos de cooperación regional e internacional, del 29 al 31 de octubre de 2019; y del 27 al 28 de octubre de 2020, se han llevado a cabo reuniones de la Junta de Interoperabilidad de Mando y Control, entre la Armada de México, la Secretaría de la Defensa Nacional y el Comando Norte de EUA, en la Ciudad de México, logrando acuerdos sobre el Intercambio de Información, Ciberseguridad, Seguridad en las Comunicaciones y enlace de datos tácticos.

En el caso de los asuntos de seguridad y ciberdefensa de acuerdo con el Reglamento Interior de la Secretaría de Marina y el Manual de Organización General de la Secretaría de Marina, el Estado Mayor General de la Armada planea,

conduce y ejecuta actividades de seguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría, así como auxilia en el ámbito de su competencia con las demás instituciones del Estado. Al respecto, se apoya de la entonces Unidad de Ciberseguridad y ahora EMCOGCIBER, que aparte de publicar la Estrategia Institucional para el Ciberespacio, ha conducido actividades de capacidades humanas en Materia de seguridad en el ciberespacio y fortalecido de la cooperación nacional e internacional en materia de seguridad en el ciberespacio. [31]

Para el caso de la Secretaría de Defensa Nacional (SEDENA), el 25 de junio de 2020 se presentó su programa sectorial. En él se enlistan 6 objetivos prioritarios, 33 estrategias prioritarias y 209 acciones puntuales. De acuerdo con el tema de Ciberseguridad se destaca el objetivo prioritario 5 "Hacer más eficiente la operatividad de las Fuerzas Armadas de tierra y aire", ya que en la explicación de su relevancia se alude a la prioridad del ciberespacio por el avance de las tecnologías mostrando que es necesario su atención, puesto que la información y datos que utiliza la SEDENA están depositados en su mayoría en el empleo de las tecnologías de la Información y de las Comunicaciones, por ende son vulnerables.

Al respecto al Estrategia prioritaria 5.6 alude a fortalecer las capacidades del Centro de Operaciones del Ciberespacio en contra de incidentes de ciberseguridad hacia la infraestructura crítica de la Secretaría de la Defensa Nacional, para ello se enlistan 6 acciones puntuales para el mismo:

- Fortalecer las capacidades del Centro de Operaciones del Ciberespacio, mediante desarrollos tecnológicos para responder a incidentes de Ciberseguridad hacia la infraestructura crítica de la SEDENA.
- Capacitar al personal del Centro de Operaciones del Ciberespacio para la protección de las infraestructuras críticas de información de esta Secretaría de Estado.
- Implementar campañas de sensibilización en el Ejército y F.A.M. para impulsar la cultura de la ciberseguridad.
- Revisar la "Estrategia Conjunta SEDENA-SEMAR en materia de Ciberdefensa y Ciberseguridad" para mantener la interoperabilidad entre ambas Fuerzas Armadas.
- Participar en eventos internacionales de Ciberdefensa y Ciberseguridad para mantener la coordinación y cooperación con Fuerzas Armadas de otros países.
- Participar en eventos nacionales de Ciberdefensa y Ciberseguridad para mantener la coordinación.[32]

La Estrategia Conjunta SEDENA-SEMAR en materia de Ciberdefensa y Ciberseguridad, es un ejemplo de actividades de coordinación y cooperación

[31]Secretaría de Marina (2021) 3er Informe de Labores 2020-2021. https://transparencia.semar.gob.mx/informes_labores/3ER_INF_LAB_SEMAR_2020-2021.pdf

[32] PROGRAMA Sectorial de Defensa Nacional 2020-2024, 15 de junio de 2020, México. https://dof.gob.mx/nota_detalle.php?codigo=5595529&fecha=25/06/2020

entre dependencias, se han celebrado reuniones el 15 y 27 de marzo, 10 de octubre y el 25 de noviembre de 2019, y 6 de febrero de 2020 en la Ciudad de México, en las que se ha revisado, actualizado la estrategia al igual que los trabajos realizados[33]. En el tercer informe de labores de la Secretaría de Marina (2020-2021) se menciona que se continúa materializando la Estrategia generándose un protocolo de actuación.

También en esta actividad coordinada se destaca en el tercer informe de labores de la SEDENA del 2020-2021 la firma del "Glosario de Términos SEDENA-MARINA en Materia de Seguridad en el Ciberespacio", por parte de los directores de la Unidad de Ciberseguridad de Marina y el Centro de Operaciones del Ciberespacio de SEDENA, realizada de manera virtual el 25 de junio de 2021, en la Ciudad de México.

IX. Panorama de la Ciberseguridad en los Estados

En el marco de las entidades federativas la situación es variada, se menciona la ciberseguridad en los Planes Estatales de Desarrollo como Baja California, Coahuila y Chihuahua, en otros hacen referencia a la seguridad de la información o seguridad informática. Sólo en tres entidades se ha presentado una propuesta legislativa sobre ciberseguridad como es el caso de San Luis Potosí, Ciudad de México y Sinaloa; sin embargo, no hay mayores avances al respecto. También, en algunos casos se ha buscado implementar medidas para fortalecer la seguridad de información dentro de la administración estatal con lineamientos o un área dedicada a la aplicación de buenas prácticas en la misma.

En el rubro de la Unidad de Policía Cibernética se halla adscrita a la Secretaría, la Procuraduría o la Fiscalía y dentro del código penal. Sólo Morelos y Sinaloa tienen tipificado el delito informático, en otros casos se alude a violencia digital, acceso no autorizado a sistemas informáticos, suplantación de identidad con medios electrónicos, fraude con medios electrónicos, violación contra la privacidad y ciberacoso.

A manera de resumen el Cuadro 1 presenta los hallazgos sobre la situación en materia de ciberseguridad para los estados.

Cuadro 1. Ciberseguridad en los estados de la República Mexicana

Estado	Legislación				Policía Cibernética			Políticas, programas o Iniciativas Pública
	Iniciativa de Ley	Mención en ley	Lineamientos	Código Penal	Secretaría	Fiscalía	Procuraduría	
Aguascalientes		X		X	X			X
Baja California				X	X			
Baja California Sur				X	X		X	
Campeche				X	X			
Coahuila		X		X			X	X
Colima		X		X	X			X
Chiapas				X	X			X

[33]Secretaría de la Defensa Nacional. 2 Informe de Labores 2019-2020. http://transparencia.sedena.gob.mx/pdf/Informe_de_Labores_2019-2024/2do_Informe_de_Labores_2019-2024.pdf

Estado	Legislación				Policía Cibernética			Políticas, programas o Iniciativas Pública
	Iniciativa de Ley	Mención en ley	Lineamientos	Código Penal	Secretaría	Fiscalía	Procuraduría	
Chihuahua		X		X		X		X
Ciudad de México	X	X		X	X			X
Durango		X		X	X			X
Guanajuato		X	X	X	X			X
Guerrero				X	X			
Hidalgo				X	X			X
Jalisco				X		X		X
México		X	X	X	X			X
Michoacán		X		X	X		X	
Morelos		X		X	X			X
Nayarit				X		X		
Nuevo León		X		X	X			X
Oaxaca		X	X	X	X			
Puebla		X		X	X			X
Querétaro		X		*	X			X
Quintana Roo				X	X			X
San Luis Potosí	X	X		X	X			X
Sinaloa	X			X	**	***		
Sonora		X	X	X	X			
Tabasco		X	X	X		X		X
Tamaulipas		X		X	X	X		
Tlaxcala		X		X	X			X
Veracruz		X	X	X	X			
Yucatán				X	X	X		X
Zacatecas				X	X			X

Fuente: Elaboración propia con información del Anexo 7. *Ciberseguridad en los estados de la República Mexicana.*
***** El Código Penal de Querétaro no menciona delitos informáticos, así como fraude o suplantación de identidad por medios electrónicos
****** No se halló una Unidad de Policía Cibernética en la Secretaría de Seguridad Pública, pero cuenta con una Dirección de Programas Preventivos que ha llevado campañas de concientización sobre el tema.
******* No se halló una Unidad de Policía Cibernética en la Fiscalía General, pero cuenta con una Unidad Especializada para la investigación de delitos informáticos tipificados en su código penal.

X. Discusiones sobre Ciberseguridad en el Congreso

Durante la LXIV Legislatura tanto en el Senado de la República como en la Cámara de Diputados se presentaron 11 iniciativas sobre el tema de ciberseguridad, seis de estas iniciativas fueron presentadas en el Senado y las cinco restantes en la Cámara de Diputados. A continuación, se describe a nivel general el contenido de las iniciativas:

- Cuatro de las iniciativas implican promulgar una nueva ley.
- Tres son propuestas de reforma a la Ley de Seguridad Nacional.
- Dos están enfocadas en la creación de una efeméride.
- Una es propuesta de cambio en la constitución, donde la iniciativa tiene por objeto facultar al Congreso de la Unión para legislar en materia de ciberseguridad.
- Una implica modificaciones a la Ley de Austeridad Republicana, donde se busca establecer austeridad en la adquisición y arrendamiento de equipo y servicios de cómputo que se usan para garantizar la operación de programas sociales y labores de ciberseguridad.

- Una más es una modificación a la Ley General del Sistema Nacional de Seguridad Pública.

De las 11 iniciativas, 10 se encuentran en pendiente; sólo la iniciativa de declarar el mes de octubre de cada año como "El Mes Nacional de la Ciberseguridad" fue aprobada.

Además, durante la LXV Legislatura del Congreso se inscribieron cuatro propuestas: la primera como reforma en diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública; la segunda propone incluir en la legislación la figura de incidentes cibernéticos con el objeto de crear un Registro Nacional de Incidentes Cibernéticos; y la tercera para reformar los artículos 11 y 13 de la Ley de la Fiscalía General de la República. Dos de estas iniciativas presentadas plantean la creación de una dependencia federal especializada para combatir este tipo de delitos.[34] Las tres propuestas anteriores se encuentran pendientes. La cuarta está pendiente de turnarse a Comisión en la sesión ordinaria de la Cámara de Diputados y se encuentra agregada en orden del día desde el pasado 6 de octubre de 2022. Esta iniciativa tiene el objetivo determinar la distribución de competencias en materia de ciberseguridad entre el Consejo Nacional de Seguridad Pública y la Secretaría de Seguridad y Protección Ciudadana; así como crear una Fiscalía Especializada en Delitos Cibernéticos, una Red de Colaboradores Comunitarios en Ciberseguridad y Juzgados Federales Especializados.

Entre los avances al respecto, se destaca que la Junta de Coordinación Política instaló, en febrero de 2022, una Mesa Permanente de trabajos en materia de Ciberseguridad. La Junta es el órgano colegiado en el que se impulsan entendimientos y convergencias políticas con las instancias y órganos que resulten necesarios a fin de alcanzar acuerdos para que el Pleno esté en condiciones de adoptar las decisiones que constitucional y legalmente le corresponden[35]; en este sentido, se espera que la acción permita promover un marco normativo en materia de ciberseguridad.[36]

Entre sus discusiones se ha considerado los alcances del marco internacional en la materia, se exploraron las prioridades a atender en el caso mexicano, así como la valoración de algunas de las iniciativas que se han presentado para el fortalecimiento de la ciberseguridad. Asimismo, se ha contado con la presencia de autoridades y sector privado.[37]

---

[34] Aguirre J. (2022). "Ciberseguridad, desafío para México y trabajo legislativo" Cuaderno de investigación No. 87, Instituto Belisario Domínguez, Senado de la República, Ciudad México. Disponible en: http://bibliodigitalibd.senado.gob.mx/handle/123456789/5551.

[35]Ley orgánica del Congreso General de los Estados Unidos Mexicanos. https://www.diputados.gob.mx/LeyesBiblio/pdf/LOCGEUM.pdf

[36]Cámara de Diputados, "Se instala mesa permanente de trabajos en materia de ciberseguridad", 25 de febrero de 2022, Nota 1853. https://comunicacionsocial.diputados.gob.mx/index.php/jucopo/se-instala-mesa-permanente-de-trabajos-en-materia-de-ciberseguridad#gsc.tab=0

[37] Diputado Javier Lopez Casarin. (@LopezCasarinJ) "Dentro de la Mesa Permanente de Trabajo en Materia de Ciberseguridad. El día de hoy llevamos a cabo la mesa con el Sector Privado. Construimos consensos, trabajo coordinado y se fortalece la ruta para un marco jurídico sólido para nuestro país." 9 mayo de 2022, https://twitter.com/LopezCasarinJ/status/1523874797251448832?s=20&t=hFQgkKTQQur_slbMFXOMsQ

XI. Posible Comisión y Agencia Nacional de Ciberseguridad

El 6 abril de 2021, durante la LXIV legislatura del Congreso, la Senadora Jesús Lucia Trasviña Waldenrath presentó un proyecto de decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del Código Penal Federal. En dicha iniciativa propone expedir la Ley General de Ciberseguridad la cual tendrá por objeto regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad (CNC) y de la Agencia Nacional de Ciberseguridad (ANC), así como establecer la distribución de competencias y las bases de coordinación entre la Federación, las Entidades Federativas y los Municipios, en esta materia.

Entre las competencias de la Federación se resalta el integrar la CNC; proponer, ejecutar y evaluar la Estrategia Nacional de Ciberseguridad, el Programa Nacional de Ciberseguridad y demás instrumentos programáticos en la materia previstos en la Ley de Planeación y distribuir a los integrantes del Sistema Nacional de Seguridad Pública, la CNC y la ACN.

Sobre la Comisión alude a que será la instancia superior de coordinación y seguimiento a las políticas públicas en materia de ciberseguridad, como parte del Sistema Nacional de Seguridad Pública. La Comisión estará Presidida por el Titular de la SSCP y en su suplencia por el Titular de la Agencia Nacional de Ciberseguridad. Asimismo, se integrará por la Conferencia de Ciberseguridad; la Conferencia de Ciberdefensa; la Agencia Nacional de Ciberseguridad y las Oficinas Estatales de Ciberseguridad. También la CNC podrá funcionar en Pleno o en grupos de trabajo. En el caso de Pleno se reunirá cada seis meses a convocatoria de la o el titular de la SSPC.

Sobre la Conferencia de Ciberseguridad estará compuesta por los representantes de la Agencia Nacional de Ciberseguridad por parte del Gobierno Federal y por las personas designadas por parte de los gobiernos de las Entidades Federativas, los cuales deberán tener conocimientos de Ciberseguridad. En el caso de la Conferencia de Ciberseguridad estará integrada por las personas designadas por parte de la Secretaría de la Defensa Nacional y la Secretaría de Marina, los cuales deberán tener conocimientos de Ciberseguridad.

La CNC como instancia deliberativa tendrá las siguientes atribuciones: establecer los instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendientes a cumplir los objetivos y fines de la Ciberseguridad; emitir acuerdos y resoluciones generales, para el funcionamiento de la Comisión; establecer los lineamientos para la formulación de políticas generales en materia de Ciberseguridad; promover la efectiva coordinación de las instancias que integran la Comisión, y dar seguimiento de las estrategias y acciones que para tal efecto se establezcan; formular propuestas para los programas nacionales de Ciberseguridad en los términos de la Ley de la materia; evaluar el cumplimiento de los objetivos y metas de los programas de Ciberseguridad y otros relacionados;

llevar a cabo la evaluación periódica de los programas de Ciberseguridad y otros relacionados; expedir políticas en materia de suministro, intercambio, sistematización y actualización de la información que sobre Ciberseguridad generen las Instituciones de los tres órdenes de gobierno y de los poderes judiciales; establecer medidas para vincular a la Comisión con otros organismos internacionales, nacionales, regionales o locales; promover políticas de coordinación y colaboración tanto con el Poder Judicial de la Federación como con los Poderes Judiciales de las Entidades Federativas; promover políticas de coordinación y colaboración con la Fiscalía General de la República y de los Estados; crear grupos de trabajo especializados en Ciberseguridad, para el apoyo de sus funciones, y las demás que se establezcan en otras disposiciones normativas y las que sean necesarias para el funcionamiento de la Comisión.

Asimismo, la propuesta establece que la Comisión en su carácter de parte integrante del Consejo de Seguridad Nacional como del Consejo Nacional de Seguridad Pública estará integrada por el titular del SSPC, quien la presidirá; los o las titulares o a quien se designe de la Secretaría de Defensa Nacional; de Marina; de Gobernación; de Relaciones Exteriores; de Comunicaciones y Transportes; de Energía; de Hacienda y Crédito Público; de Economía; de Educación Pública; de la Fiscalía General de la República y los gobernadores de los Estados. También define que la Comisión se integrará por una Conferencia con la persona encargada en materia de Ciberseguridad de cada Secretaría integrante, a persona encargada en materia de Ciberdefensa de cada Secretaría integrante, por la Agencia Nacional de Ciberseguridad y las Oficinas estatales de Ciberseguridad.

En el caso de la Agencia se menciona que será la encargada de la gobernanza de la generación de la política pública y acuerdos que se generen en la CNC y vinculación con actores del sector público y privado.[38] La ANC estará integrada por un titular que desempeñara las funciones de Subsecretario de Seguridad Pública; un Secretario General que desempeñaría las funciones de la Dirección General de Gestión de Servicio, Ciberseguridad y Desarrollo Tecnológico; un Coordinador de Seguridad que desempeñará las funciones de Coordinador de Ciberseguridad, Administración y Análisis de Información de Seguridad Pública y los funcionarios del Gobierno Federal que puedan ser invitados por el Titular de la Agencia a colaborar de forma permanente o temporal.

La ANC contará con las siguientes atribuciones:

- Coordinar el desarrollo, implementación, evaluación, actualización y mejora continua de la Estrategia Nacional de Ciberseguridad.

[38]Iniciativa de la Senadora Jesús Lucía Trasviña Waldenrath, con proyecto de decreto por el que se expide la ley general de ciberseguridad y se derogan diversas disposiciones del código penal federal, 6 de abril de 2021, Senado de México, México. https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-04-06-1/assets/documentos/Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf.

- Impulsar ante las instancias Federales, Entidades Federativas y Organismos Constitucionalmente Autónomos, el cumplimiento de la Estrategia Nacional de Ciberseguridad.
- Evaluar, en coordinación con las autoridades competentes, el cumplimiento de la Estrategia Nacional Ciberseguridad, así como coordinar la formulación de propuestas de actualización y modificación de la Estrategia para su presentación al Titular del Ejecutivo Federal.
- Establecer mecanismos de coordinación y colaboración de los equipos de respuesta a incidentes públicos y privados a través del establecimiento de un Equipo Nacional de Respuesta a Incidentes Tecnológicos.
- Realizar las actividades de coordinación de los tres órdenes de gobierno y la iniciativa privada para realizar las funciones de Ciberseguridad en el país.
- Desarrollar, implementar, evaluar y actualizar las políticas públicas, disposiciones de seguridad de la información, estándares, y guías en materia de ciberseguridad para instancias públicas y privadas.
- Proponer criterios técnicos de vanguardia para la detección, monitoreo, pronóstico y medición de riesgos en las tecnologías de la información y comunicaciones del sector público y privado.
- Promover el establecimiento de mecanismos de coordinación y colaboración entre los equipos de respuesta a incidentes cibernéticos públicos y privados.
- Proponer la armonización legal en la materia de Ciberseguridad, para contar con instrumentos nacionales e internacionales para el cumplimiento de los objetivos de la Ley de Ciberseguridad.
- Realizar mediciones de la ciberseguridad de las instituciones públicas y privadas a fin de que se establezcan mecanismos de mejora continua para mantener los mecanismos de ciberseguridad vigentes y adecuados, para responder a las amenazas derivadas de las nuevas tecnologías.
- Coordinar programas de cultura y capacitación de los funcionarios de gobierno y público en general, con instituciones educativas, centros de investigación, entidades públicas y privadas tanto nacionales como internacionales.
- Emitir la política de seguridad para las Infraestructuras Críticas de Información y coordinar las acciones derivadas de ésta, atendiendo los estándares y mejores prácticas internacionales en la materia.
- Evaluar en coordinación con el personal especializado designado por las instituciones públicas o privadas que tengan a su cargo infraestructuras que puedan ser consideradas críticas de información, las características específicas de las infraestructuras conforme al procedimiento establecido para tales efectos, a fin de determinar su criticidad y el impacto de las afectaciones a su operación.
- Requerir tanto a las Entidades Federativas como a los Órganos Constitucionalmente Autónomos y los particulares, información para la integración del Registro Nacional de las Infraestructuras Críticas de

Información, conforme a las disposiciones reglamentarias que al efecto se emitan.

- Integrar, actualizar y administrar el Registro Nacional de las Infraestructuras Críticas de Información, conforme a las disposiciones de la presente Ley, su reglamento y demás disposiciones aplicables.
- Supervisar los análisis de riesgos de las Infraestructuras Críticas de Información.
- Desarrollar un Mapa de Riesgos de las Infraestructuras Críticas de Información que describa la afectación de cada una de ellas sobre las demás.
- Establecer mecanismos para el monitoreo y generación de alertas de Infraestructuras Críticas de Información.
- Establecer mecanismos permanentes de comunicación con los operadores de las Infraestructuras Críticas de Información para, en su caso, la emisión de alertas tempranas.
- Definir estándares de Protección de Infraestructuras Críticas de Información.
- Participar y coordinar ejercicios y simulacros para la protección de las Infraestructuras Críticas de Información.
- Coordinar la atención de incidentes en las Infraestructuras Críticas de Información a través de un equipo especializado de respuesta en incidentes en Infraestructuras Críticas de Información.
- Desarrollar mecanismos para la evaluación de la ciberseguridad en Infraestructuras Críticas de Información.
- Impulsar marcos jurídicos relacionados con protección de Infraestructuras Críticas de Información.
- Establecer esquemas de cooperación con organismos internacionales y autoridades extranjeras para la protección de las Infraestructuras Críticas de Información.
- Reportar ante las autoridades competentes la posible comisión de hechos que afecten la seguridad, a fin de determinar la responsabilidad penal a que haya lugar.
- Implementar mecanismos de coordinación pública y privada con procedimientos y recursos específicos que permitan el cumplimiento de la presente ley en materia de prevención, investigación, procuración e impartición de justicia conforme a la atribución de cada instancia de colaboración.
- Las demás que se establezcan en otras disposiciones jurídicas o le asigne, en el ámbito de su competencia el presidente de la República.[39]

Prosiguiendo con el tema, el 14 de octubre de 2021, durante el LXV legislatura del Congreso, la Senadora presentó la iniciativa con proyecto de Decreto por el que

[39]Iniciativa de la Senadora Jesús Lucía Trasviña Waldenrath, con proyecto de decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del código penal federal, 6 de abril de 2021, Senado de México, México. https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-04-06-1/assets/documentos/Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf.

se reforman diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública, en materia de creación de la Comisión Nacional de Ciberseguridad.

La iniciativa considera importante implementar un programa rector de ciberseguridad en materia de Seguridad Nacional a razón de los avances tecnológicos, su injerencia en múltiples aspectos de la actividad humana y el incremento de riesgos y peligros en el tema. Asimismo, tiene la finalizad de realizar una adecuación legislativa a la Ley General del Sistema Nacional de Seguridad Pública para brindar reconocimiento legal a la Ley General de Ciberseguridad para regular la integración, organización y funcionamiento de la CNC y de la ANC.

En el caso específico de las reformas a la Ley General del Sistema Nacional de Seguridad Pública, se espera incluir entre las definiciones para los efectos de la Ley del artículo 5 como "a los órganos contemplados dentro de la Ley General de Ciberseguridad, Comisión Nacional de Ciberseguridad, así como las instituciones de la Federación, Entidades Federativas y Municipios que realicen funciones de Ciberseguridad".

En el asunto del Título Segundo de las instancias de coordinación y la distribución de competencias del SNSP, se propone una modificación del artículo 10 agregando a la CNC como parte de éste. Asimismo, se propone un nuevo capítulo con el numeral IX, posterior al artículo 38, para detallar las atribuciones de la Comisión.

Entre las facultades de la Comisión que integran en la iniciativa se encuentra que formulará políticas integrales y sistemáticas, así como programas y estrategias en materia de ciberseguridad, planteará la Estrategia Nacional de Ciberseguridad y el Programa Nacional de Ciberseguridad procurando su ejecución y evaluación anual. Además, la iniciativa alude a la Agencia Nacional de Ciberseguridad como la encargada de la gobernanza de la generación de la política pública y acuerdos que se generen en la Comisión Nacional de Ciberseguridad.[40]

XII. Acciones por parte de otras dependencias

Algunas dependencias han tomado acciones en materia de ciberseguridad con el objetivo de prevenir ataques que afecten sus funcionen o causen pérdidas millonarias.

Ejemplo de lo anterior en el caso de sector financiero mexicano, es que en mayo de 2018 la entonces Procuraduría General de la República, las Autoridades como la Secretaría de Hacienda y Crédito Público, el Banco de México, la Comisión Nacional Bancaria y de Valores, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), la Comisión Nacional del

[40]Iniciativa de la Senadora Jesús Lucía Trasviña Waldenrath, con proyecto de decreto por el que se reforman diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública, en materia de en materia de Creación de la Comisión Nacional de Ciberseguridad, 14 de octubre de 2021, Senado de México, México. https://infosen.senado.gob.mx/sgsp/gaceta/65/1/2021-10-14-1/assets/documentos/Ini_Morena_Sen_Trasvina_Creacion_Com_Ciberseguridad.pdf

Sistema de Ahorro para el Retiro y la Comisión Nacional de Seguros y Fianzas y algunas Asociaciones Financieras, formalizaron las Bases de Coordinación en Materia de Seguridad de la Información cuya finalidad fue definir un mecanismo de coordinación para dar respuesta efectiva a incidentes de seguridad de la información en el sector financiero. En este sentido las instituciones se comprometieron a conformar, cada una, un equipo responsable de detectar incidentes de seguridad de la información y a reportarlos de forma inmediata a las autoridades.

Asimismo, las Bases de Coordinación permitieron la creación del Grupo de Respuesta a Incidentes, con el que se busca acelerar la reacción ante ataques al sistema financiero del país.[41]

Por parte del Banco de México, desde 2018 con la creación de su Dirección de Ciberseguridad, a cargo del Gobernador, han incrementado acciones en la materia de forma preventiva, ejemplo de ello es su Estrategia de Ciberseguridad, en la cual se realizó ajustes en rubros como:

1) Gobernanza, Cumplimiento y organización.
2) Protección de Datos.
3) Gestión de Riesgos de Seguridad
4) Gestión de Identidad y Autenticación.
5) Respuesta a Incidentes.
6) Administración de Terceros y Proveedores.
7) Protección de Equipos y Punto Final.
8) Protección de Aplicaciones y Bases de Datos.
9) Protección de Redes y Centros de Datos.
10) Capacitación y concientización en Seguridad[42].

En este sentido, el Banco de México ha logrado mejorar su postura en ciberseguridad al integrar la ciberseguridad y seguridad de la información como un tópico relevante en la organización, trascendiendo los componentes tecnológicos; su capacidad de identificación, categorización, evaluación de riesgos a la información para protegerla, con base en su valor para la institución; sus metodologías de mitigación y gestión de riesgos a la ciberseguridad; sus capacidades de detección, análisis, contención, respuesta y recuperación ante incidentes avanzados de seguridad de la información, y su colaboración y comunicación con otras autoridades ante incidentes de ciberseguridad que se presenten en el sistema financiero.

Por otra parte, la Secretaría de Infraestructura Comunicaciones y Transportes ha llevado a cabo acciones para promover la cultura de la ciberseguridad por medio de guías como la Guía para el uso de redes y dispositivos de telecomunicaciones

[41] BANXICO (2018) Bases de Coordinación en Materia de la Información. https://www.banxico.org.mx/sistema-financiero/d/%7BD0502AA8-7721-5C2C-5C8F-05858CBB4AE7%7D.pdf
[42] BANXICO (2021) Estrategia de Ciberseguridad del Banco de México. https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf

en apoyo a la educación[43], así como la Guía de Ciberseguridad para el uso de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo[44]. El documento busca apoyar las actividades que se realizan por teletrabajo, como política pública para afrontar los efectos de la pandemia del Covid-19; así como identificar las amenazas que puede afectar la ciberseguridad en los hogares. Por lo que se muestra que, ante la emergencia sanitaria, se establecieron diferentes políticas públicas a fin de concientizar a la población de los riesgos existentes en materia de seguridad informática.

En el caso del Instituto Federal de Telecomunicaciones (IFT) ha llevado a cabo diversas acciones en el ámbito de la ciberseguridad, donde se puede destacar su participación en talleres, mesas de trabajo y foros cuyo objetivo fue la construcción de la Estrategia Nacional de Ciberseguridad.[45] En este contexto el IFT lideró, en coordinación con el Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes, el grupo de trabajo sobre Protección de la Sociedad y Derechos. Como parte de las labores, en el grupo de trabajo, realizadas para la implementación de la Estrategia, se coordinaron mesas de trabajo con la participación de organizaciones públicas, privadas y de la sociedad civil. Lo anterior con los objetivos de 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; establecer una estrategia de gestión de riesgos en materia de ciberseguridad que permita identificar las principales amenazas a las que se encuentra expuesta la población, así como concientizar e incentivar un uso responsable de las TIC; y para 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.[46]

El Instituto emitió su Hoja de Ruta 2021-2025, que estableció un plan estratégico para desarrollar el ecosistema digital, que va desde la infraestructura y las redes hasta los servicios digitales. Esta Hoja de Ruta aborda el ecosistema digital desde una visión integral, prestando mayor énfasis en los desarrollos tecnológicos de 5G, internet de las cosas, inteligencia artificial, blockchain, ciberseguridad, entre otros.

En este sentido dentro de la Hoja de Ruta se integraron dos Líneas de Acción Regulatorias: desarrollar y difundir recomendaciones, lineamientos, disposiciones técnicas y/o buenas prácticas en materia de ciberseguridad y colaborar con las entidades involucradas en materia de ciberseguridad en el ámbito de las facultades del Instituto. Ambas bajo el objetivo estratégico de "Promover el

[43] https://www.gob.mx/cms/uploads/attachment/file/570011/10082020_Gui_a_de_ciberseguridad_en_apoyo_a_la_educacio_n_-_VF_para_publicar.pdf
[44] https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf.
[45] IFT (2018) Plan de Acciones en Materia de Ciberseguridad. https://ciberseguridad.ift.org.mx/files/guias_y_estudios/5_upr_planaccionesciberseguridad.pdf
[46] Gobierno de México (2018). Memoria y Recomendaciones ENCS. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf

desarrollo del ecosistema digital y la adopción de nuevas tecnologías y casos de uso digitales".[47]

Como actividad continua por parte del IFT, se difunden a través de las redes sociales institucionales diversos materiales informativos que promueven las mejores prácticas relativas a la seguridad y la protección de información en la red, en temáticas como virus informáticos, robo y pérdida de información, aplicaciones no seguras, Wi-Fi público, consejos para descargar aplicaciones, phishing y fraude.

Sumado a lo anterior, el IFT ha compartido enfoques basados en riesgo para enfrentar las amenazas a la ciberseguridad; así como las medidas que ha desarrollado e implementado en esta materia en el Foro Bilateral de Ciberseguridad México-EE.UU: Mejores prácticas desde una perspectiva pública y privada en Ciberseguridad del Diálogo Económico de Alto Nivel México-Estados Unidos.[48]

Asimismo, en el marco del ciclo de conferencias "Hacia una Política Nacional de Ciberseguridad", para crear un espacio de diálogo y compartir conocimientos y necesidades desde los diversos sectores, se presentó el Micrositio de Ciberseguridad para Usuarios de Servicios de Telecomunicaciones, como una acción del regulador para promover la confianza en el ecosistema digital.

En el Micrositio se conjunta la información disponible en materia de seguridad digital generada por el IFT y la Unión Internacional de Telecomunicaciones, el Instituto Nacional de Ciberseguridad de España, la Guardia Nacional, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, la Secretaría de Infraestructura, Comunicaciones y Transportes, el Sistema Nacional de Protección de Niñas, Niños y Adolescentes y la Secretaría de Seguridad Ciudadana de la Ciudad de México, entre otros.

Otra acción más a reconocer es que el IFT y la CONDUSEF firmaron un convenio de colaboración a fin de establecer bases generales de coordinación, colaboración y ejecución de acciones, dentro del marco de sus respectivas atribuciones y ámbitos de competencia, para promover el uso responsable de los servicios digitales y, en particular, para fomentar el acceso seguro a Internet y la confianza en la realización de operaciones financieras en línea.

También, por parte del IFT se han publicado Códigos de Mejores Prácticas en materia de ciberseguridad para equipos móviles y en dispositivos del internet de las cosas (IoT, por sus siglas en inglés). En el caso del primero de ellos tiene por objeto recopilar recomendaciones y promover el uso y cuidado responsable de la información personal contenida en equipos móviles.[49] El segundo busca incentivar la innovación tecnológica en el sector de los Dispositivos IoT, retomando para ello

[47] IFT (2021). Hoja de Ruta 2021-2025. http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025
[48]Secretaría de Economía (2022). Reporte T-MEC. Foro Bilateral de Ciberseguridad entre México y Estados Unidos. https://www.gob.mx/cms/uploads/attachment/file/765847/Reporte-TMEC_n135-esp_20221004_.pdf
[49] IFT. (2022a). Código de Mejores Prácticas para la Ciberseguridad en Equipos Terminales Móviles. https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_etm.pdf

mejores prácticas internacionales, con un enfoque basado en gestión de riesgos, enfatizando la seguridad por diseño.[50] Otra publicación es el estudio "El papel de la Ciberseguridad en el proceso de la transformación digital en México" que identifica y analiza las amenazas y vulnerabilidades en materia de ciberseguridad dentro de las redes de telecomunicaciones del servicio móvil que pudieran inhibir la transformación digital en México.[51]

XIII. Aspectos internacionales

En el espacio internacional, dentro del Tratado entre México, Estados Unidos y Canadá, el tema de ciberseguridad está considerado como un elemento que daña la confianza en el comercio digital. Además de que se espera que las partes desarrollen capacidades para la respuesta a incidentes; así como fortalecer los mecanismos de colaboración para cooperar en la identificación y mitigación de intrusiones maliciosas. De igual modo, se detalla que los enfoques basados en riesgos pueden ser más efectivos que la regulación prescriptiva para tratar las amenazas, por lo que las partes procurarán emplear y alentar a las empresas a utilizar el enfoque con el fin de identificar y protegerse contra los riesgos, así como detectar, responder y recuperarse de eventos de ciberseguridad.[52]

En el caso del Tratado Integral y Progresista de Asociación Transpacífico, en el capítulo de Comercio Electrónico, en su artículo 14.16 alude a la Cooperación en Asuntos de Ciberseguridad, donde se reconoce la importancia de desarrollar las capacidades de las entidades nacionales responsables de la respuesta a incidentes de seguridad informática y utilizar los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas.[53]

De acuerdo con el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT) de 2020, México se encuentra en el puesto 52 a nivel global, avanzando 11 lugares en comparación a 2018. A nivel América se haya en el cuarto puesto detrás de Brasil, Canadá y Estados Unidos.

El ICG fue lanzado por primera vez en 2015 con el fin de ayudar a los miembros de la UIT a identificar áreas de mejora y animar a los países a tomar medidas, a través de la sensibilización sobre el estado de la ciberseguridad en todo el mundo. El Índice recoge 82 preguntas sobre los compromisos de ciberseguridad de los

[50] IFT. (2022b). Código de Mejores prácticas para la Ciberseguridad de los Dispositivos del Internet de las Cosas. https://ciberseguridad.ift.org.mx/files/guias_y_estudios/codigos_ciberseguridad_iot.pdf
[51] Cuevas J. (2021). El papel de la Ciberseguridad en el proceso de la transformación digital en México. https://centrodeestudios.ift.org.mx/admin/files/estudios/1639064122.pdf
[52] Gobierno de México. Capítulo 19. Comercio Digital en Textos finales del Tratado entre México, Estados Unidos y Canadá (TMEC). Disponible en línea: https://www.gob.mx/cms/uploads/attachment/file/465801/19ESPComercioDigital.pdf
[53] Gobierno de México. Capítulo 14. Comercio Electroníco en Textos finales del Tratado Integral y Progresista de Asociación Transpacífico (CPTPP). Disponible en línea: https://www.gob.mx/cms/uploads/attachment/file/86482/14._Comercio_Electr_nico.pdf

Estados miembros en cinco pilares medidas legales, medidas técnicas medidas organizativas medidas de desarrollo de capacidades, medidas de cooperación.[54]

Por parte de instrumentos jurídicos internacionales, los Estados miembros del Consejo de Europa impulsaron en 2001 la firma del Convenio sobre la Ciberdelincuencia o Convenio de Budapest. Este Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otros medios digitales, que se centra en el fraude informático, la pornografía infantil y las violaciones de la seguridad en la red. También propone una serie de poderes y procedimientos como la búsqueda en redes de computadoras y la intercepción y conservación de información.

Su principal objetivo es promover una política criminal común enfocada en proteger a la sociedad contra el cibercrimen. De esta manera, se ofrece un marco internacional integral, considerado referente global, para la armonización de los esfuerzos de los Estados y para fomentar la cooperación internacional. El Convenio ha sido adoptado por 65 países. Entre los países no miembros del Consejo de Europa, pertenecientes a nuestro continente se encuentran: Argentina, Canadá, Chile, Colombia, Costa Rica, República Dominicana, Panamá, Paraguay, Perú y los Estados Unidos.[55]

Otro beneficio del Convenio, además de proporcionar un marco legal para la cooperación internacional en materia de ciberdelito y evidencia digital, es que los Estados podrán ser miembros del Comité del Convenio sobre la Ciberdelincuencia, organismo intergubernamental que se ocupa del ciberdelito, en los Estados Parte comparten información y experiencias, evalúan la implementación del Convenio o lo interpretan a través de Notas de Orientación.[56]

México se encuentra entre los países invitados a adherirse al Convenio, sin embargo, es importante detallar que un requisito para el procedimiento de Adhesión es que esté disponible un proyecto de ley que indique que un Estado ya ha implementado o es posible que pueda implementar las disposiciones del Convenio de Budapest en su legislación nacional. En el caso de México la adhesión a este Convenio podría ir acompañada de cambios en la legislación mexicana, particularmente en el Código Penal Federal, con el objetivo de proteger los derechos humanos y la seguridad jurídica.[57]

---

[54] UIT (2020) Global Cybersecurity Index, Suiza. Disponible en línea: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[55] Consejo de Europa. *The Budapest Convention and its Protocols*. Disponible en línea: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[56] Consejo de Europa (2021) Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios. Disponible en línea: https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

[57] Centeno D. (2018). México y el Convenio de Budapest: posibles incompatibilidades. Red en Defensa de los Derechos Digitales, México. https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf

1. Estados Unidos

De acuerdo con los resultados del Indicé de Ciberseguridad Global de la UIT, Estados Unidos ocupa el primer puesto, a pesar de que no se ha respondido el cuestionario, pero por los datos que cuenta la UIT es que se entrega dicha categoría. Estados Unidos es el único país con una puntuación perfecta en las áreas de medidas legales, técnicas, cooperativas, organizativas y en desarrollo de capacidad. [58]

Por parte de la presidencia de Biden, en mayo de 2021, se emitió una orden ejecutiva para trazar el nuevo curso en materia de ciberseguridad de la nación y para proteger las redes del gobierno federal. La orden se integra en 6 secciones con diferentes acciones y tiempos para su cumplimiento:

- La sección 1 se refiere a una política de prevención, detección, evaluación y remediación de incidentes cibernéticos como prioridad máxima y esencial para la seguridad nacional y económica.
- Como parte de la sección 2, se plantea eliminar las barreras para compartir información sobre amenazas, entre sus acciones plantea que los proveedores de servicios de tecnologías de la información y tecnología operativa aumenten el intercambio de información frente a amenazas, incidentes y riesgos.
- En el caso de la sección 3 se dirige a la modernización de la ciberseguridad del gobierno federal, para ello plantea la adopción y el uso de la tecnología en la nube, la implementación de la Arquitectura de Confianza Cero y la adopción de autenticación multifactorial y cifrado de datos en reposo y en tránsito, además de establecer un marco para colaborar en las actividades de ciberseguridad y respuesta a incidentes relacionadas con la tecnología en la nube.
- Por la sección 4 se busca la mejora de la seguridad de la cadena de suministro de software. En ella se detallan los pasos, capacidades y mecanismos más para garantizar que los productos funcionen de manera segura y según lo previsto, de forma que se puedan resistir ataques y tener controles adecuados para evitar la manipulación por parte de actores maliciosos.
- La sección 5 se encamina a establecer una Junta de Revisión de Seguridad Cibernética. Dicha junta tendría la función de revisar y evaluar, con respecto a incidentes cibernéticos significativos que afecten a los sistemas de información de la administración Federal o sistemas no federales, actividad de amenazas, vulnerabilidades, actividades de mitigación y respuestas de agencias.

[58] UIT. (2020). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

- La sección 6 plantea la estandarización del manual del gobierno federal para responder a vulnerabilidades e incidentes de ciberseguridad.[59]

De acuerdo con la Ley de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés) de 2018, se modificó la Ley de Seguridad Nacional de 2002 para rediseñar la Dirección Nacional de Protección y Programas del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) como Agencia de Ciberseguridad y Seguridad de las Infraestructuras de tal forma que se transfirió los recursos y las responsabilidades de la dirección a la Agencia.[60]

En este sentido, parte de la responsabilidad en materia de ciberseguridad recae en el DHS ya que investiga la actividad cibernética maliciosa. Sus responsabilidades de ciberseguridad y seguridad de infraestructura crítica se centran en cuatro objetivos: i) redes civiles seguras; ii) fortalecer la seguridad y la resiliencia de la infraestructura crítica; iii) evaluar y contrarrestar los riesgos de ciberseguridad en evolución, y iv) combatir el cibercrimen.[61]

Por su parte, CISA lidera el trabajo estratégico y unificado en Estados Unidos para fortalecer la seguridad, la resiliencia y la fuerza laboral del ecosistema cibernético. Además, conecta a las partes interesadas de la industria y el gobierno entre sí y proporciona recursos, análisis y herramientas para ayudarlos a construir su propia resiliencia y seguridad cibernética, de comunicaciones y física, lo que a su vez ayuda a garantizar una infraestructura segura y resistente para los estadounidenses.[62]

También, por parte de la Oficina del Secretario del DHS se cuenta con una Oficina de Política Cibernética, Infraestructura, Riesgo y Resiliencia, (CIRR, por sus siglas en inglés), el objetivo de la CIRR es liderar el desarrollo de políticas y estrategias de ciberseguridad, tecnología e infraestructura para el DHS.[63]

En el caso del Departamento de Estado cuenta con la Oficina de Ciberespacio y Política Digital a cargo del Secretaría Adjunto de Estado. Dicha oficina lidera y coordina el trabajo del Departamento sobre el ciberespacio y la diplomacia digital para fomentar el comportamiento responsable del Estado en el ciberespacio y promover políticas que protejan la integridad y seguridad de la infraestructura de internet, sirvan a los intereses de los Estados Unidos, promuevan la competitividad y defiendan los valores democráticos.[64]

---

[59] White House (2021. Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[60] Congress.Gov (2018). H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018. https://www.congress.gov/bill/115th-congress/house-bill/3359?q=%7B%22search%22%3A%5B%22Cybersecurity%22%2C%22Cybersecurity%22%5D%7D&r=31&s=10

[61] Departamento de Seguridad Nacional (s.f.) Secure Cyberspace and Critical Infrastructure. https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

[62] Departamento de Seguridad Nacional (s.f.). Cybersecurity. https://www.dhs.gov/topics/cybersecurity

[63] Departamento de Seguridad Nacional (s.f.). Cyber, Infrastructure, Risk & Resilience Policy. https://www.dhs.gov/cyber-infrastructure-resilience-policy

[64] Departamento de Estado (s.f.). Bureau of Cyberspace and Digital Policy. https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/

La Ley de Mejora de la Seguridad Cibernética de 2014 actualizó la función del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) para incluir identificación y desarrollo de marcos de riesgos de seguridad cibernética para uso voluntario por parte de propietarios y operadores de infraestructuras críticas. Esto formalizó el trabajo previo del NIST de desarrollo de la Versión 1.0 del Marco de Ciberseguridad bajo la Orden Ejecutiva (EO) 13636, "Mejora de la seguridad cibernética en infraestructuras críticas" (febrero de 2013), y proporcionó una guía para la futura evolución del Marco. El Marco es un marco proactivo impulsado por las empresas para la gestión voluntaria de los ciber riesgos, diseñado para empresas de todos los tamaños que operan en diversos sectores de la economía.[65]

El NIST ha trabajado en colaboración con las partes interesadas, incluidos los representantes de la industria, el mundo académico y el gobierno, a través de un proceso consultivo formal para desarrollar el Marco para la Mejora de la Ciberseguridad de las Infraestructuras Críticas, un marco voluntario para reducir los riesgos cibernéticos de las infraestructuras críticas. Al respecto, CISA ayuda a las organizaciones a utilizar el marco de seguridad cibernética.[66]

En 2023, se lanzó la Estrategia Nacional de Ciberseguridad de la Presidencia de Biden. La Estrategia planea reequilibrar la responsabilidad de defender el ciberespacio y realinear los incentivos para favorecer las inversiones a largo plazo para ello reconoce que los actores más grandes, más capaces y mejor posicionados del ecosistema digital, ya sea en el sector público o privado, pueden y deben asumir una mayor parte de la carga para mitigar el riesgo cibernético.[67] La estrategia busca construir y potenciar la colaboración en 5 pilares:

- Defender la Infraestructura Crítica. Se plantea establecer regulaciones de ciberseguridad para asegurar la infraestructura crítica, armonizar y racionalizar la nueva y existente regulación, habilitar a entidades regulatorias para proporcionar seguridad, colaboración a escala público-privada, integrar los centros de ciberseguridad federales, actualizar los planes y procesos federales de respuesta a incidentes y modernizar las defensas federales
- Interrumpir y desmantelar posibles amenazas. En este pilar se espera integrar medidas federares de interrupción para posible ciberactividad criminal, mejorar la colaboración entre el sector público y el privado para desarticular las amenazas, aumentar la velocidad y alcance en el intercambio de información y notificación de víctimas, evitar el uso abusivo de las infraestructuras estadounidenses y luchar contra la ciberdelincuencia para derrotar el ransomware.

[65] Instituto Nacional de Estándares y Tecnología (2018). Marco de Ciberseguridad. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018es.pdf
[66] Cybersecurity Infrastructure Security Agency. CISA's Role in Cybersecurity. https://www.cisa.gov/cybersecurity
[67] Departamento de Estado. (2023). Announcing the Release of the Administration's National Cybersecurity Strategy. https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/

- Dar forma a las fuerzas de mercado para impulsar la seguridad y la resiliencia. Como parte de este pilar se espera responsabilizar a los administradores de nuestros datos, impulsar el desarrollo de dispositivos IoT seguros, desplazar la responsabilidad por productos y servicios de software inseguros, utilizar subvenciones federales y otros incentivos para incorporar la seguridad, aprovechar la contratación pública federal para mejorar la rendición de cuentas y explorar un seguro cibernético federal de respaldo.
- Invertir en un futuro resiliente. Bajo este pilar se espera asegurar la base técnica de internet, revitalizar la investigación y el desarrollo federales para la ciberseguridad, preparar el futuro post-cuántico, asegurar el futuro de energía limpia, apoyar el desarrollo de un ecosistema de identidad digital y desarrollar una estrategia nacional para reforzar nuestra mano de obra cibernética.
- Forjar alianzas internacionales para perseguir metas compartidas. Como parte de este pilar se espera crear una coalición para contrarrestar las amenazas al ecosistema digital, fortalecer la capacidad de los socios internacionales, expandir la capacidad de EE.UU. para ayudar a los aliados y socios, construir coaliciones para reforzar las normas mundiales de comportamiento estatal responsable y asegurar las cadenas mundiales de suministro de información, comunicaciones, productos y servicios de tecnología operativa,[68]

2. Reino Unido

Un caso emblemático a nivel internacional es el de Reino Unido. En el Índice Global de Ciberseguridad publicado por la Unión Internacional de Telecomunicaciones, en su edición de 2017, se encontraba en el puesto 12 a nivel global[69], sin embargo, en 2018[70] paso al primer lugar con la puntuación más alta en el rubro legal y organizativo, ya que contaba con una serie de instrumentos jurídicos para hacer frente a la ciberdelincuencia como es el caso de la Ley sobre el uso indebido de computadoras.

En la última edición de 2020, bajo a segundo lugar por una diferencia de 0.5 puntos frente a Estados Unidos en la categoría de "Medidas técnicas", la cual evalúa la existencia de instituciones y marcos técnicos que se ocupan de la ciberseguridad; sin embargo, el reporte no detalla si esto es considerado una debilidad o una falla.[71]

En el caso de la organización en materia de Ciberseguridad, la oficina del Gabinete, quien apoya al Primer Ministro y garantiza el funcionamiento eficaz del

[68] White House. (2023). National Cybersecuriry Strategy. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[69] UIT (2017) Global Cybersecurity Index, Suiza. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
[70] UIT (2018) Global Cybersecurity Index, Suiza. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[71] UIT (2020) Global Cybersecurity Index, Suiza. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

gobierno, es la encargada de la Estrategia Cibernética Nacional, que comprende la Estrategia Nacional del Reglamento de Redes y Sistemas de Información. También tiene la responsabilidad general de mejorar la seguridad y la resistencia de las infraestructuras nacionales críticas.

La Estrategia Cibernética Nacional tiene por objeto apoyar y ampliar una serie de otras prioridades para el Gobierno en materia de seguridad, defensa, política exterior y la agenda económica. En este sentido la Estrategia será una de las subestrategias que cumplirán con las ambiciones de la Revisión Integrada, dicha revisión incluye los esfuerzos nacionales para mejorar la resiliencia, abordar las amenazas estatales, la delincuencia organizada grave y el terrorismo, mantener nuestra ventaja estratégica a través de la ciencia y la tecnología y dar forma al orden internacional.

El Consejo de Seguridad Nacional ejercerá la supervisión ministerial de estas estrategias, supervisando la implementación y considerando el equilibrio general y la dirección de la estrategia del Reino Unido. El progreso en relación con los objetivos de la estrategia también se evaluará a través del Marco de Planificación y Desempeño del Gobierno y los Planes de Entrega de Resultados.

A partir de la Estrategia Nacional de Ciberseguridad 2016-2021[72] del Reino Unido permitió liderar un esfuerzo nacional sostenido para fortalecer la seguridad cibernética, aumentar la conciencia pública sobre los riesgos cibernéticos, hacer crecer el sector de la seguridad cibernética y desarrollar una amplia gama de capacidades a través del ciberespacio para responder a las amenazas de actores hostiles. Ejemplo de ello es que en 2017 se lanzó formalmente el Centro Nacional de Ciberseguridad (NCSC, por sus siglas en inglés) como como parte del *Government Communications Headquarters* (GHCQ) para ser la autoridad nacional del Reino Unido en el entorno de seguridad cibernética: compartiendo conocimientos, abordando vulnerabilidades sistémicas y proporcionando liderazgo en temas clave de seguridad cibernética nacional.

En el caso del GHCQ es la agencia de inteligencia, cibernética y de seguridad. Sus prioridades están definidas por el Consejo de Seguridad Nacional y la Estrategia de Seguridad Nacional, misma que es definida por la oficina del Gabinete.

En este sentido, las principales responsabilidades del NCSC en virtud de la nueva estrategia de 2022[73] son:

- Tomar medidas directas para reducir los daños cibernéticos en el Reino Unido proporcionando protección a escala a través de servicios digitales.

[72] Gobierno de Reino Unido (2022). National Cyber Strategy. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#annex-a-cyber-as-part-of-the-governments-wider-agenda

[73] Gobierno de Reino Unido (2016). National Cyber Security Strategy 2016 to 2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

- Apoyar a todas las partes de la sociedad del Reino Unido para que se protejan a sí mismos proporcionando experiencia personalizada y conocimiento.
- Proporcionar información técnica a la política y regulación del Ministerio del Interior (Home Office) sobre los temas de mayor importancia para la seguridad cibernética.
- Proporcionar capacidades soberanas del Reino Unido a través del Centro Nacional de Claves criptográficas del NCSC, que protege la información y los servicios críticos.
- Apoyar el crecimiento de las habilidades cibernéticas y la inversión al proporcionar la base técnica para cada nivel de educación cibernética e involucrar y apoyar a la industria, catalizando la inversión en el sector cibernético.

Asimismo, el NCSC es el punto de contacto nacional con los socios internacionales (de la Unión Europea) en materia de redes y sistemas de información, la coordinación de las solicitudes de acción o información y la presentación de las estadísticas anuales de incidentes, recaen en sus responsabilidades.[74]

También el NCSC es el Equipo de Respuesta a Incidentes de Seguridad Informática, se encarga de supervisar los incidentes de ciberseguridad a nivel nacional; proporciona análisis de amenazas en tiempo real, defensa contra ciberataques nacionales, asesoramiento técnico y respuesta a incidentes cibernéticos importantes para ayudar a minimizar los daños.[75]

En el caso de seguridad en 2020 se creó la Fuerza Cibernética Nacional (NCF, por sus siglas en inglés), la cual es responsable de operar en y a través del ciberespacio para contrarrestar, interrumpir, degradar y desafiar a aquellos que harían daño al Reino Unido o sus aliados, para mantener al país seguro y para proteger y promover los intereses del Reino Unido en el país y en el extranjero. La NCF es una asociación entre defensa e inteligencia, la responsabilidad de las actividades del NCF está a cargo conjuntamente del Secretario de Estado de Asuntos Exteriores, del Commonwealth y de Desarrollo y del Secretario de Estado de Defensa. Además del GCHQ y el Ministerio de Defensa, el Servicio Secreto de Inteligencia y el Laboratorio de Ciencia y Tecnología de Defensa son socios centrales que aportan técnicas de espionaje e investigación de vanguardia.[76]

También se cuenta con la Unidad Nacional de Delitos Cibernéticos (NCCU, por sus siglas en inglés) de la Agencia Nacional del Crimen (NCA, por sus siglas en

[74] Gobierno de Reino Unido (2022). National Cyber Strategy. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#annex-a-cyber-as-part-of-the-governments-wider-agenda
[75] NCSC. About the NCSC. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
[76] Gobierno de Reino Unido (2020). National Cyber Force Explainer. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041113/Force_Explainer_20211213_FINAL__1_.pdf

inglés), la cual proporciona liderazgo nacional y coordinación de la respuesta, con el apoyo de una red de Unidades Regionales de Delitos Cibernéticos (RCU, por sus siglas en inglés) dedicadas en cada una de las nueve regiones policiales de Inglaterra y Gales, en asociación con sus contrapartes en la Policía de Escocia y el Servicio de Policía de Irlanda del Norte, así como la Unidad de Delitos Cibernéticos del Servicio de Policía Metropolitana.

En el caso de la NCA parte integrante de las fuerzas de seguridad del Reino Unido, de la ley del Reino Unido, además tendrá fuertes vínculos bidireccionales con las fuerzas policiales locales y otros y otras agencias de inteligencia. Asimismo, es responsable ante el Ministerio del Interior.

En el caso del Departamento de Asuntos Digitales, Cultura, Medios de Comunicación y Deporte (DCMS, por sus siglas en inglés) es responsable de la aplicación general del Reglamento Redes y Sistemas de Información, incluida la coordinación de las autoridades competentes y el NCSC. El DCMS publica orientaciones para que las autoridades competentes apoyen la aplicación general de Reglamento Redes y Sistemas de Información en todo el Reino Unido.

El Reglamento de Seguridad de Redes y Sistemas de Información (NIS, por sus siglas en inglés) establecen múltiples autoridades competentes que son responsables de la supervisión y aplicación de los Reglamentos en cada sector o región cubierto. El Gobierno ha publicado una guía para las autoridades competentes a fin de ayudarlas a desempeñar sus funciones en virtud del Reglamento. En este sentido la autoridad clave para la implementación del NIS en materia de infraestructura digital es la Oficina de Comunicaciones (Ofcom).

En enero de 2022 se lanzó la Estrategia de Seguridad Cibernética del Gobierno 2022-2030 para garantizar que las funciones centrales del gobierno sean resistentes a los ataques cibernéticos, fortaleciendo al Reino Unido como nación soberana y consolidando su autoridad como una potencia cibernética democrática y responsable, su implementación será por medio del Centro de Seguridad del Gobierno para el Ciberespacio que se encuentra alojado por el departamento de Hacienda y Aduanas de su Majestad[77]. Asimismo, se apoyará de la Junta Asesora de Seguridad Cibernética del Gobierno un organismo compuesto por expertos externos independientes para construir mejores vínculos entre el gobierno, el sector privado y la academia.[78]

[77] Gobierno de Reino Unido (2022). Cyber Security Operations Coordination Support. https://www.civilservicejobs.service.gov.uk/csr/jobs.cgi?jcode=1789936#:~:text=The%20Government%20Security%20Centre%20for,Cyber%20Security%20Strategy%20(GCSS).

[78] Gobierno de Reino Unido (2022). Government Cyber Security Strategy: 2022 to 2030. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html#chapter-9-implementing-the-strategy

3. Arabia Saudita

De acuerdo con el Índice de Ciberseguridad de la UIT Arabía Saudita resultó empate en la puntuación con Reino Unido con una puntuación global de 99.54.[79] Desde 2017 cuenta con la Autoridad Nacional de Ciberseguridad (NCA, por sus siglas en inglés), establecida por el Decreto Real 2/11/1439, es la entidad gubernamental a cargo de la ciberseguridad en el país, y sirve como la autoridad nacional en sus asuntos. La NCA tiene funciones regulatorias y operativas relacionadas con la ciberseguridad y trabaja en estrecha colaboración con entidades públicas y privadas, a través de comités sectoriales, para mejorar la postura de ciberseguridad del país con el fin de salvaguardar sus intereses vitales, la seguridad nacional, las infraestructuras críticas, los sectores de alta prioridad y los servicios y actividades gubernamentales.[80]

En 2020, la NCA presentó una Estrategia Nacional de Ciberseguridad, la cual considera seis temas principales:

- Unificar. Refiere a la integración de los componentes de regulación de la seguridad cibernética a nivel reglamentario, presupuestos, indicadores de desempeño, marco de gobernanza entre las organizaciones y direcciones estratégicas nacionales.
- Administrar. Alude a identificar las infraestructuras críticas y la gestión de riesgos cibernéticos. Se espera reducir amenazas y vulnerabilidades con procedimientos de gestión de riesgo; también se incluye proporcionar un modelo de referencia para estándares y controles cibernéticos nacionales.
- Asegurar. El tema se ocupa de asegurar la protección del ciberespacio en 4 elementos: sensibilización y difusión nacional; identidades digitales nacionales; cifrado nacional y recursos críticos de internet.
- Defender. En el tema se busca el desarrollo de mecanismos nacionales de defensa cibernética. Al respecto se consideran 5 elementos: preparación en inteligencia y análisis de amenazas; gestión de vulnerabilidades; monitoreo y coordinación en la detección de amenazas; respuesta e investigaciones de incidentes; y recuperación más continuidad de la infraestructura crítica.
- Construir. El tema se ocupa de garantizar la existencia de una base nacional que integré investigación en el campo de ciberseguridad, apoyé a la innovación y la inversión en el campo; gestión de capital humano especializado en ciberseguridad; así como trabajar en adoptar un enfoque para garantizar la seguridad de sistemas, dispositivos y servicios.[81]

La Estrategia fue pensada para desarrollarse durante 5 años, a través de iniciativas y proyectos implementados por 3 vías: i) proyectos de alto rendimiento, refiere al lanzamiento de proyectos específicos urgentes que tengan un impacto tangible en el aumento de la madurez de la ciberseguridad; ii) Programa Catalizador de

[79] UIT. (2020). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf
[80] National Cybersecurity Authority (s.f.) About NCA. https://nca.gov.sa/en/about
[81] National Cybersecurity Authority (s.f.) About National Cybersecurity Strategy https://nca.gov.sa/en/strategic

Ciberseguridad, alude a la prestación de servicios básicos de ciberseguridad a organizaciones nacionales para elevar el nivel general de ciberseguridad en Arabia Saudita, e iii) iniciativas y proyectos nacionales de cinco años de duración con impactos estratégicos a largo plazo. [82]

Con el mismo Decreto Real 2/11/1439, el Equipo de Respuesta a Emergencias Informáticas (CERT, por sus siglas en inglés) de la Comisión de Tecnologías de la Información y las Comunicaciones pasó a la NCA. La misión principal del CERT Saudí es crear conciencia sobre la ciberseguridad. En este sentido, aumenta el nivel de conocimiento y conciencia sobre los riesgos de ciberseguridad y los intentos de mitigar su impacto mediante la emisión de advertencias sobre las vulnerabilidades más recientes y peligrosas, también lanza programas y campañas de sensibilización y coopera y colabora con otros equipos de respuesta.[83]

Entre las funciones de la NCA, se tiene el mandato de desarrollar y actualizar políticas, mecanismos de gobernanza, marcos, estándares, controles y lineamientos relacionados con la ciberseguridad; compartirlos con las entidades pertinentes y dar seguimiento a su cumplimiento. Al respecto, se han emitido los siguientes, controles y estándares:

- Controles de ciberseguridad para cuentas de redes sociales de las organizaciones.
- Controles esenciales de ciberseguridad.
- Controles de ciberseguridad en la nube.
- Control de ciberseguridad del teletrabajo.
- Controles de ciberseguridad de sistemas críticos.
- Controles de ciberseguridad de tecnología operativa.
- Controles de ciberseguridad de datos.
- Marco de trabajo de seguridad cibernética.
- Estándares criptográficos nacionales.
- Marco de educación superior de ciberseguridad.
- Directrices de ciberseguridad para el comercio electrónico.[84]

Como parte de las facultades del CERT de Arabia Saudita, trabaja como coordinador para mitigar incidentes de seguridad; clasifica datos para conformar medidas de seguridad que permitan reducir el riesgo de divulgación de información protegida; realiza análisis y respuesta de vulnerabilidad, así como acciones para fomentar conciencia sobre la ciberseguridad.[85]

También, la Comisión de Comunicación, Espacio y Tecnología (CST, por sus siglas en inglés) tiene como objetivo regular la ciberseguridad para lograr salvaguardar

[82] National Cybersecurity Authority (2020) National Cybersecurity Strategy. https://nca.gov.sa/national_cybersecurity_strategy-en.pdf
[83] Saudi Computer Emergency Response Team (2022). About US. Disponible en linea: https://cert.gov.sa/en/about-us/
[84] National Cybersecurity Authority (s.f.) Controls and Guidelines. https://nca.gov.sa/en/legislation.
[85] Saudi Computer Emergency Response Team (s.f.). RFC 2350 Saudi CERT. https://cert.gov.sa/documents/15/RFC_2350_-_Saudi_CERT.pdf

el interés público y el interés del usuario; para mantener la confidencialidad de las comunicaciones y la seguridad de la información; así como aumentar el nivel general de madurez de la ciberseguridad del sector postal y de las TIC. Al respecto, por parte de la CST se cuenta con la siguiente normativa y requisitos de ciberseguridad para los proveedores de servicios del sector TIC y postal:

- Marco Regulatorio de Ciberseguridad para Proveedores de Servicios en TIC. En el marco se presentan un conjunto de requisitos de seguridad cibernética que deben implementar los Proveedores de servicios TIC.[86]
- Reglamento de Operaciones de Ciberseguridad en los Sectores TIC y Postal. En el documento se detallan las facultades del Centro de Operaciones de Ciberseguridad del CST además de los mecanismos para fomentar la cooperación conjunta entre los proveedores de servicios en el sector, y para impulsar los esfuerzos relacionados con la preparación y respuesta a la ciberseguridad.[87]

Desde 2007 hay una Ley contra el delito cibernético, la cual tiene como objetivo prevenir los delitos cibernéticos mediante la identificación de estos y la definición de sus castigos. El objetivo es garantizar la seguridad de la información, la protección del interés público, la moral, la protección de los derechos del uso legítimo de las computadoras y las redes de información, y la protección de la economía nacional.[88]

4. Unión Europea

En 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva Estrategia de Ciberseguridad de la (UE o Unión). El objetivo de esta estrategia es reforzar la resiliencia de Europa frente a las ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables.[89]

La nueva estrategia incluía propuestas estratégicas concretas para la implantación de instrumentos normativos, de actuación y de inversión. Entre ellas fue un Escudo Cibernético en toda la UE, dicho escudo estaría compuesto por Centros de Operaciones de Seguridad que utilicen Inteligencia Artificial y aprendizaje automático para detectar señales tempranas de ataques cibernéticos. La estrategia, también introdujo diálogos cibernéticos con países y organizaciones regionales e internacionales, incluida la Organización del Tratado del Atlántico

[86] Communication & Information Technology Commission (2020). Cybersecurity Regulatory Framework for Services Providers in the Information and Communication Technology Sector. https://www.cst.gov.sa/en/RulesandSystems/CyberSecurity/Documents/CRF-en.pdf
[87] Communication & Information Technology Commission (2022). Regulations for Cybersecurity Operations in ICT & Postal Sector. https://regulations.citc.gov.sa/PublishedDocuments/GovernorApprovalDecision_465/b1d3c2f6-5423-482b-aec7-bfa7287975d7_Regulations%20for%20Cybersecurity%20Operations%20in%20ICT%20%20Postal%20Sector.pdf
[88] Gobierno de Arabia Saudita (2021). Cybersecurity in the Kingdom. Disponible en línea: https://www.my.gov.sa/wps/portal/snp/content/cybersecurity#header2_5
[89] Comisión Europea (2020). The EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Norte (OTAN), un Programa de Acción en las Naciones Unidas para abordar la seguridad internacional en el ciberespacio y un *Toolkit* sobre ciberdiplomacia de la UE para prevenir, disuadir y responder frente ataques cibernéticos. Respecto al financiamiento se planeó que en el Marco Financiero Plurianual 2021-2027 incluyera la ciberseguridad en el marco del Programa Europa Digital. Mientras, la financiación de la investigación en ciberseguridad está prevista en el marco de Horizonte Europa, con un enfoque especial en el apoyo a las Pequeñas y Medianas Empresas. Y por parte del Fondo Europeo de Defensa (FED) se incluye que apoyará las soluciones europeas de ciberdefensa como parte de la base tecnológica e industrial de defensa europea.[90]

También se incluyó la creación de una Unidad Cibernética Conjunta, pensada como un espacio para facilitar una cooperación estructurada entre los Estados miembros y todas las instituciones, organismos y agencias de ciberseguridad relevantes de la UE. Entonces, la Unidad funcionaría como una plataforma de recopilación de recursos y conocimientos especializados de las distintas comunidades cibernéticas de la UE y sus Estados miembros con el fin de prevenir y desalentar los ciber incidentes masivos y de responder eficazmente ante ellos.[91]

Previo a la Estrategia, en 2019 se contaba con el Reglamento de Ciberseguridad con el que, por primera vez, se introdujeron normas a escala de la UE para la certificación de la ciberseguridad de los productos, procesos y servicios. Por otro lado, estableció un nuevo mandato permanente para la Agencia de Ciberseguridad de la UE (ENISA, por sus siglas en inglés)[92]. ENISA mejora la fiabilidad de los productos, servicios y procesos de las TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la Unión y ayuda a Europa a prepararse para los desafíos del mañana en materia de ciberseguridad. Mediante el intercambio de conocimientos, la creación de capacidades y la sensibilización, ENISA coopera con las principales partes interesadas para fortalecer la confianza en la economía conectada, impulsar la resiliencia de las infraestructuras de la Unión y, por último protege a la sociedad y a la ciudadanía europea de las amenazas digitales.[93] Asimismo, ENISA ha estado apoyando directamente a los Estados miembros de la UE durante más de una década en el desarrollo y la implementación de directrices para sus respectivas estrategias nacionales de ciberseguridad a fin de generar confianza, resiliencia y niveles suficientes de transparencia en un dominio puntuado por altos niveles de confidencialidad. Gracias en parte al apoyo de ENISA, todos

[90] Comisión Europea. (s.f.). Estrategia de Ciberseguridad de la UE para la Década Digital: preguntas y respuestas. https://digital-strategy.ec.europa.eu/es/node/10364

[91]Consejo Europeo (2021). Ciberseguridad: el Consejo adopta unas Conclusiones sobre la exploración del potencial de una Unidad Cibernética Conjunta https://www.consilium.europa.eu/es/press/press-releases/2021/10/19/cybersecurity-council-adopts-conclusions-on-exploring-the-potential-of-a-joint-cyber-unit/

[92] La nueva Agencia de la UE para la Ciberseguridad se basa en las estructuras de su predecesora, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, aunque con un papel reforzado y un mandato permanente. Ha mantenido el mismo acrónimo, ENISA. https://www.consilium.europa.eu/es/policies/cybersecurity/#challenges

[93] ENISA. (s.f.). Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad. https://www.enisa.europa.eu/about-enisa/about/es

los Estados miembros de la UE cuentan con una estrategia nacional de ciberseguridad concreta desde 2017.[94]

En 2020, el Parlamento Europeo y el Consejo, llegaron a un acuerdo sobre una propuesta para crear el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad (ECC por sus siglas en inglés) respaldado por una Red de Centros Nacionales de Coordinación (Red). Para 2021, el Consejo adoptó el Reglamento por el que se crea el ECC y la Red, siendo sus principales objetivos mejorar la ciberresiliencia, contribuir a la implantación de la tecnología de última generación en materia de ciberseguridad, proporcionar apoyo a las empresas emergentes y las pymes del sector de la ciberseguridad, reforzar la investigación y la innovación en materia de ciberseguridad y contribuir a llenar el déficit de capacidades en materia de ciberseguridad. Bucarest es la sede del centro, la cual fue elegida por los Estados miembros de la UE.[95]

El ECC y la Red tomarán decisiones estratégicas de inversión y pondrán en común recursos de la UE, sus Estados miembros e, indirectamente, la industria para mejorar y reforzar las capacidades tecnológicas y de ciberseguridad industrial, mejorando la autonomía estratégica abierta de la UE. El ECC desempeñará un papel clave en la consecución de los ambiciosos objetivos de ciberseguridad del Programa Europa Digital[96] y del programa Horizonte Europa[97].

5. Organización de Estados Americanos

La Organización de los Estados Americanos (OEA) es el principal foro regional para el diálogo, análisis de políticas y toma de decisiones en asuntos del hemisferio. La OEA reúne a los líderes de todas las naciones de las Américas para tratar temas y oportunidades de la región, además lleva múltiples temas bajo los pilares de la democracia, los derechos humanos, la seguridad y el desarrollo. [98]

La Organización cuenta con el Comité Interamericano contra el Terrorismo (CICTE) que tiene como propósito prevenir y combatir el terrorismo en las Américas, pero

[94] ENIS. (s.f.). National Cybersecurity Strategies. https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[95] Consejo Europeo (s.f.). Selección de la sede del Centro Europeo de Competencia en Ciberseguridad. https://www.consilium.europa.eu/es/policies/cybersecurity/seat-selection-cybersecurity-centre/#why

[96] Europa digital es un programa de financiamiento centrado en llevar tecnología digital a las empresas, ciudadanos y Administraciones públicas. Con un presupuesto total previsto de 7 500 millones de euros, el programa facilitará la financiación estratégica para responder a estos retos, apoyando proyectos en cinco ámbitos clave: supercomputación, inteligencia artificial, ciberseguridad, competencias digitales avanzadas y garantía de un amplio uso de las tecnologías digitales en toda la economía y la sociedad, también a través de centros de innovación digital. https://digital-strategy.ec.europa.eu/es/activities/digital-programme

[97] Horizonte Europa es un programa de financiación de la investigación y la innovación hasta 2027, cuenta con un presupuesto de 95 500 millones de euros. El programa se conforma en 3 pilares: Ciencia Excelente, con el que se busca reformar y ampliar la excelencia de la base científica de la Unión; Desafíos mundiales y competitividad industrial europea, donde se pretende impulsar las tecnologías y soluciones clave para sustentar las políticas de la Unión y los objetivos de Desarrollo Sostenible en seis clústeres (Salud; cultura, creatividad y sociedad inclusiva; seguridad civil para la sociedad; mundo digital industria y espacio; clima energía y movilidad; y alimentación, bioeconomía, recursos naturales, agricultura y medio ambiente); por último pilar es Europa Innovadora que planea estimular las innovaciones de vanguardia y creadora de mercados y los ecosistemas que propician la innovación. https://research-and-innovation.ec.europa.eu/system/files/2022-06/rtd-2021-00013-02-00-es-tra-01.pdf

[98] OEA (s.f.). Quienes Somos. https://www.oas.org/es/acerca/quienes_somos.asp

sobre todo brinda asistencia política y técnica a sus Estados Miembros a través de diferentes programas acordados en su Plan de Trabajo Anual, tales como: Ciberseguridad, Controles Fronterizos, Financiamiento de Terrorismo, Prevención de la Proliferación de Armas de Destrucción Masiva y Extremismo Violento. A través de CICTE y el Programa de Seguridad Cibernética, se compromete a desarrollar y promover la agenda de seguridad cibernética en las Américas. En cooperación con una amplia gama de entidades nacionales y regionales de los sectores público y privado en temas políticos y técnicos, la OEA busca construir y fortalecer la capacidad de seguridad cibernética en los Estados Miembros a través de asistencia técnica y capacitación, mesas redondas de políticas, ejercicios de gestión de crisis y el intercambio de mejores prácticas relacionadas con las tecnologías de la información y la comunicación.[99]

El Programa de Seguridad Cibernética se centra en apoyar a los Estados Miembros en el desarrollo de capacidades de ciberseguridad a nivel técnico y de políticas públicas. En este sentido, ha apoyado en la formación de 17 estrategias nacionales de ciberseguridad en la región, cuenta con 2 informes regionales sobre el nivel de capacidad en ciberseguridad de los Estados Miembros de la OEA, se han capacitado más de 2000 mujeres en ejercicios cibernéticos, 600 jóvenes estudiantes se han beneficiado de la capacitación en seguridad digital para ingresar al campo de ciberseguridad y 15,000 ciudadanos capacitados en operaciones cibernéticas, ciberseguridad, liderazgo en ciberseguridad y regulaciones internacionales sobre el tema. Otros objetivos de este programa son mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional, así como aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de internet[100]

Adicionalmente, dentro de la OEA también existe el Comité Jurídico Interamericano (CJI), el cual sirve de cuerpo consultivo de la OEA en asuntos jurídicos; promueve el desarrollo progresivo y la codificación del derecho internacional, y estudia los problemas jurídicos referentes a la integración de los países.[101] En materia de ciberseguridad el CJI ha publicado un informe y resolución sobre Derecho Internacional y Operaciones Cibernéticas del Estado el cual brinda parámetros sobre la aplicación del derecho internacional al ciberespacio y presenta puntos de convergencia y divergencia en cuanto al entendimiento de dichas normas internacionales en los Estados miembros de la OEA, incluso sus reacciones frente a las amenazas cibernéticas.[102]

[99] OEA (s.f.) Cybe Security. https://www.oas.org/en/topics/cyber_security.asp
[100] OEA. (s.f.) Programa de Ciberseguridad. https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp
[101] OEA. (s.f.). Comité Jurídico Interamericano. https://www.oas.org/es/acerca/comite_juridico.asp
[102] OEA. (s.f.) Comité Jurídico Interamericano publica informe y resolución sobre Derecho Internacional y Operaciones Cibernéticas del Estado en los cuatro idiomas de la organización. https://www.oas.org/es/sla/ddi/boletines_informativos_CJI_%C2%A0Derecho_Internacional_y_Operaciones_Ciberneticas_del_Estado_Febrero-2021.html

6. Organización del Tratado del Atlántico Norte

La Organización del Tratado del Atlántico Norte (OTAN)[103] es una alianza de países de Europa y Norteamérica. Constituye un enlace único entre estos dos continentes, lo que les permite consultar y cooperar en el campo de la defensa y la seguridad y realizar juntos operaciones multinacionales de gestión de crisis. Desde julio de 2016, la ciberdefensa forma parte de la tarea central de la OTAN de defensa colectiva, el objetivo principal de la OTAN en materia de ciberdefensa es proteger sus propias redes, operar en el ciberespacio (incluso a través de las operaciones y misiones de la Alianza), ayudar a los aliados a mejorar su resiliencia nacional y proporcionar una plataforma para la consulta política y la acción colectiva. Además, como parte de la Cumbre de la OTAN de 2018 en Bruselas, se acordó establecer un Centro de Operaciones del Ciberespacio como parte de la Estructura de Mando reforzada de la OTAN.[104]

El Centro de Seguridad Cibernética proporciona servicios especializados relacionados con la ciberseguridad para prevenir, detectar, responder y recuperarse de incidentes, además actúa como un centro para el intercambio de información cibernética en tiempo real. El Centro también coordina la actividad operativa de la OTAN en el ciberespacio, garantizando la libertad de acción en este ámbito y haciendo que las operaciones sean más resistentes a las amenazas cibernéticas.[105]

También se cuenta con el Centro de Excelencia de Ciberdefensa Cooperativa en Tallin (Estonia), el cual es una instalación de investigación y formación acreditada que se ocupa de la educación, investigación y desarrollo en materia de ciberdefensa. El Centro proporciona una valiosa experiencia en ciberdefensa y organiza ejercicios cibernéticos en los que participan tanto aliados como socios de la OTAN. Asimismo, por parte de la Escuela de la OTAN de Oberammergau, en Alemania, imparte formación relacionada con la ciberdefensa para apoyar las operaciones, la estrategia, la política, la doctrina y los procedimientos de la Alianza. Por último, la Academia de Comunicaciones e Información de la OTAN, en Oeiras (Portugal), imparte formación a la fuerza de trabajo de ciberdefensa de la Alianza y la Escuela de Defensa de la OTAN en Roma (Italia) fomenta el pensamiento estratégico sobre cuestiones político-militares, incluidas las relacionadas con la ciberdefensa.[106]

[103] Actualmente la OTAN cuenta con 30 países miembro: Albania, Alemania, Bélgica, Bulgaria, Canadá, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, Francia, Grecia, Hungría, Islandia, Italia, Letonia, Lituania, Luxemburgo, Macedonia del Norte, Montenegro, Noruega, Países Bajos, Noruega, Polonia, Portugal, Reino Unido, República Checa, Rumania y Turquía.
[104] OTAN. (2022). Cyber defence. https://www.nato.int/cps/en/natohq/topics_78170.htm
[105] OTAN (s.f.). NATO's Cyber Security Centre. https://www.ncia.nato.int/what-we-do/cyber-security.html
[106] OTAN (2021). Factsheet NATO Cyber Defence. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

7. Unión Internacional de Telecomunicaciones

La Unión Internacional de Telecomunicaciones (UIT) considera a la ciberseguridad una prioridad temática, en este sentido cuenta con un programa de ciberseguridad que ofrece a sus miembros la oportunidad y las herramientas para reforzar las capacidades nacionales en materia de ciberseguridad, con el fin de mejorar la seguridad y la resiliencia, así como fomentar la confianza en la utilización de las TIC, para que el mundo digital sea más seguro para todos.[107] Como parte del Programa cuenta con la segunda edición de la "Guía para desarrollar una Estrategia Nacional de Ciberseguridad", la cual tiene el objetivo de instruir a los líderes nacionales y a los responsables políticos en el desarrollo de sus estrategias en la materia y en el pensamiento estratégico sobre ciberseguridad, preparación cibernética y resiliencia.[108]

También cuenta con el Programa de Mentorías Cibernético para mujeres con el cual se involucra modelos a seguir en el campo de la ciberseguridad y los conecta con mujeres talentosas en África, la región árabe y Asia-Pacífico. El programa se compone de tres partes, que presentan círculos mensuales de tutoría con actividades que incluyen seminarios web inspiradores y cursos de capacitación técnica y de habilidades blandas. El programa pretende aumentar la calidad y diversidad de las competencias de las mujeres en este ámbito y paliar al mismo tiempo la carencia de mano de obra cualificada en ciberseguridad .[109]

Desde 2015, la UIT ha emitido el índice Global de Ciberseguridad, el cual es una referencia que mide el compromiso de los países con la ciberseguridad a nivel global, para crear conciencia sobre la importancia y las diferentes dimensiones del problema. Para la medición, el nivel de desarrollo o compromiso de cada país se evalúa a lo largo de cinco pilares: i) medidas legales, ii) medidas técnicas, iii) medidas organizativas, iv) desarrollo de capacidades y v) Cooperación, y luego se agregan en una puntuación general.[110] Una opción de la UIT para la mejora en la preparación, protección y las capacidades de respuesta a incidentes de ciberseguridad de los Estados Miembros es mediante la realización de Ciber simulacros. Un Ciber simulacro es un evento anual durante el cual se simulan ataques cibernéticos, incidentes de seguridad de la información u otros tipos de interrupciones para probar las capacidades cibernéticas de una organización, desde poder detectar un incidente de seguridad hasta la capacidad de responder adecuadamente y minimizar cualquier impacto relacionado. Hasta la fecha, la UIT ha organizado alrededor de 40 eventos Ciber simulacros en todo el mundo para

[107] UIT. (s.f.). Mandate Cybersecurity. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/about-cybersecurity.aspx
[108] UIT. (2021). The NCS Guide 2021. https://ncsguide.org/the-guide/
[109] UIT. (2022). Women in Cyber Mentorship Programme 2022. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme-2022.aspx
[110] UIT. (s.f.). Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

mejorar la capacidad y las capacidades de ciberseguridad a través de la colaboración y la cooperación regionales.[111]

Las Comisiones de Estudio de la UIT ofrecen a los Miembros la oportunidad de compartir experiencias, presentar ideas, intercambiar opiniones y llegar a un consenso sobre las estrategias adecuadas para abordar las prioridades de las TIC o para la conformación de recomendaciones (normas) para los diversos campos de las telecomunicaciones internacionales. En el caso de ciberseguridad la UIT tiene la Comisión de Estudio 2 del Sector de Desarrollo, la cual tiene la cuestión protección de las redes de información y comunicación: mejores prácticas para desarrollar una cultura de ciberseguridad bajo estudio.[112] También se cuenta con la Comisión de Estudio 17 sobre seguridad del Sector de Normalización, la cual tiene a su cargo 12 cuestiones de estudio: 1) Coordinación de la seguridad de las telecomunicaciones/TIC; 2) Arquitectura y marco de seguridad; 3) Gestión de la seguridad de la información de telecomunicaciones; 4) Ciberseguridad; 5) Lucha contra el spam por medios técnicos; 6) Aspectos de seguridad de los servicios de telecomunicaciones ubicuos; 7) Servicios de aplicaciones seguras; 8) Seguridad de la computación en nube; 9) Tele biometría; 10) Arquitectura y mecanismos de gestión de identidades; 11) Tecnologías genéricas para admitir aplicaciones seguras; y 12) Lenguajes formales para software y pruebas de telecomunicaciones.[113]

Con la última Conferencia de Plenipotenciarios celebrada en 2022 en Bucarest se incluyó adoptar el Plan Estratégico de la Unión para 2024-2027. En este Plan se definió la meta 1 "Conectividad universal: permitir y fomentar el acceso universal a unas telecomunicaciones/TIC asequibles, seguras y de alta calidad", donde destaca entre sus finalidades una mayor preparación de los países en materia de ciberseguridad, mediante capacidades esenciales, a saber, existencia de una estrategia, de equipos nacionales de intervención en caso de emergencia o incidente informáticos y de legislación. También como parte del este plan se prevé que los trabajos de la UIT relacionados con la infraestructura y los servicios de telecomunicaciones/TIC inclusivos y seguros permitan lograr mayor capacidad de los Miembros de la UIT para desplegar infraestructuras de telecomunicaciones/TIC inclusivas, seguras y resilientes, a fin de hacer frente a incidentes de ciberseguridad, para fomentar la confianza y la seguridad en la utilización de las telecomunicaciones/TIC, y adoptar prácticas de gestión de riesgos; aprovechar mejor las asociaciones exclusivas de la UIT para fomentar la capacitación y la formación en materia de competencias digitales y sensibilización del público

[111] UIT. (2023). CyberDrill 2023. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CyberDrill-2023/CyberDrill-2023.aspx
[112] UIT. (s.f.). ITU-D Study Groups 1 and 2. https://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG02-RGQ03.2&stg=2
[113] UIT. (s.f.). List of questions. SG17:Security. https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/questions.aspx

respecto de la ciberseguridad; y prestar asistencia a los Miembros de la UIT en la formulación de sus estrategias de ciberseguridad a escala nacional.[114]

8. Organización para la Cooperación y Desarrollo Económicos

En el marco de la Organización para la Cooperación y Desarrollo Económicos (OCDE) se alude al concepto de Seguridad Digital, entendido como los aspectos económicos y sociales de la ciberseguridad, al contrario de los aspectos técnicos con la aplicación de la ley o la seguridad nacional e internacional. La OCDE ha estado facilitando la cooperación internacional y desarrollando análisis de políticas y recomendaciones en seguridad digital su trabajo en esta área tiene como objetivo desarrollar y promover políticas que fortalezcan la confianza sin inhibir el potencial de las TIC para apoyar la innovación, la competitividad y el crecimiento.[115]

La OCDE cuenta con su Marco de Políticas sobre Seguridad Digital. Este documento busca que los formuladores de políticas comprendan la dimensión económica y social de la ciberseguridad para ello presenta las recomendaciones generadas por la organización como son:

- Gestión de riesgos de seguridad digital.[116]
- Estrategias Nacionales de Seguridad Digital.[117]
- Seguridad digital de actividades críticas.[118]
- Seguridad digital de productos y servicios.[119]
- El Tratamiento de las vulnerabilidades de seguridad digital.[120]

Respecto a la Recomendación de Gestión de Riesgos de Seguridad Digital menciona nueve principios interrelacionados de alto nivel que forman la base del enfoque económico y social de la ciberseguridad.

1. Cultura de seguridad: concienciación, habilidades y empoderamiento. Todas las partes interesadas deben crear una cultura de seguridad digital basada en la comprensión del riesgo de seguridad digital y cómo gestionarlo.
2. Responsabilidades y obligaciones. Todas las partes interesadas deben asumir la responsabilidad de la gestión de la seguridad digital, riesgo en función de sus roles, el contexto y su capacidad de actuar.
3. Derechos humanos y valores fundamentales. Todas las partes interesadas deben gestionar el riesgo de seguridad digital de manera transparente y coherente con los derechos humanos y los valores fundamentales.

[114] UIT. (2022). Actas Finales de la Conferencia de Plenipotenciarios Bucares, 2022. https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2022-PDF-S.pdf
[115] OCDE. (s.f.). Digital security. https://www.oecd.org/digital/digital-security/
[116] Para más información consultar: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479
[117] Para mayor detalle: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480
[118] Para más información consultar: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456
[119] Para mayor detalle consultar: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481
[120] Para más información consultar: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482

4. Cooperación. Todas las partes interesadas deben cooperar, incluso a través de las fronteras.
5. Estrategia y gobernanza. Los líderes y tomadores de decisiones deben asegurarse de que el riesgo de seguridad digital esté integrado en su estrategia general de gestión de riesgos, y se gestiona como un riesgo estratégico que requiere medidas operativas.
6. Evaluación de riesgos y ciclo de tratamiento. Los líderes y tomadores de decisiones deben asegurarse de que el riesgo de seguridad digital sea tratado basándose en una evaluación continua del riesgo.
7. Medidas de seguridad. Los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo.
8. Innovación. Los líderes de innovación y los tomadores de decisiones deben asegurarse de que se considere la innovación.
9. Resiliencia, preparación y continuidad. Los líderes y tomadores de decisiones deben asegurarse de que un plan de preparación y continuidad basado en la evaluación de riesgos de seguridad digital sea adoptado, implementado y probado, para garantizar la resiliencia.[121]

En el caso de la Recomendación de Estrategias Nacionales de Seguridad Digital, la recomendación se distribuye en tres aspectos: i) institucional, se resalta la coordinación intergubernamental, que la estrategia cuente con el apoyo del más alto nivel de gobierno y asignación de responsabilidades claras; ii) contenido, al respecto recomienda que considere la concientización y formación de habilidades, respuesta a incidentes y coordinación de vulnerabilidades, normas de gestión, industria, investigación e innovación, seguridad de productos y servicios, y tratamiento de vulnerabilidades, transformación digital, asociaciones y cooperación internacional; y iii) aplicación, se recomienda asignar recursos suficientes y evaluar, revisar y mejorar la estrategia y las políticas de implementación regularmente.[122]

La Recomendación de seguridad digital de actividades críticas alude a aquellas actividades económicas y sociales cuya interrupción o perturbación tendría graves consecuencias para la salud, la seguridad y la protección de los ciudadanos; el funcionamiento eficaz de los servicios esenciales para la economía y la sociedad y del gobierno; o para la prosperidad económica y social en general. Asimismo, la recomendación da orientación para los responsables de la formulación de políticas sobre cómo definir lo que deben hacer los operadores, establecer el marco institucional adecuado, fomentar la confianza de las asociaciones y cooperar a nivel internacional.[123]

[121] OCDE. (2022). OECD Policy Framework on Digital Security. https://www.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en
[122] Ibidem.
[123] Ibidem.

En el caso de la Recomendación sobre seguridad digital de productos y servicios reconoce que la seguridad digital de los productos y servicios, y que los incentivos de mercado no son suficientes para asegurar que se arregle las brechas en la gestión de riesgos de seguridad digital. Al respecto esta recomendación incluye orientación sobre políticas para realinear los incentivos del mercado y empoderar a las partes interesadas para mejorar la seguridad digital de los productos y servicios, para ello describe áreas de acción (cooperación interna e internacional, responsabilidad de los proveedores, transparencia e intercambio de información, políticas flexibles y por último innovación y competencia) para los formuladores de políticas y brinda orientación sobre qué herramientas de políticas pueden ser efectivas.[124]

La Recomendación del tratamiento de las vulnerabilidades de seguridad digital reconoce que las debilidades (en código o sistema) en productos y sistemas de información pueden ser explotadas para dañar actividades económicas y sociales. En este sentido, esta recomendación considera establecer una clara separación de responsabilidades; animar a los investigadores o desarrolladores a crear un entorno seguro, fomentar una confianza que pueda ayudar a resolver problemas entre los participantes y facilitar procesos coordinados sobre la divulgación de vulnerabilidades, reconocimiento e integración de buenas prácticas, así como mejorar la cooperación internacional.[125]

9. Organizaciones de las Naciones Unidas

En 2015, la Organizaciones de las Naciones Unidas (ONU) contaba con un Grupo de Expertos Gubernamentales de Naciones Unidas (UN-GGE, por sus siglas en inglés) sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, el cual examinó las amenazas reales y potenciales derivadas de la utilización de las TIC por los Estados y analizó las acciones necesarias para hacerles frente, incluidas normas, reglas, principios y medidas de fomento de la confianza. En su informe final resalta que se ha avanzado en el reconocimiento de los riesgos que el uso malintencionado de las TIC representa para la paz y la seguridad internacionales, admitiendo que las TIC pueden ser una fuerza impulsora para acelerar los progresos hacia el desarrollo, y en consonancia con la necesidad de preservar la conectividad mundial y el flujo libre y seguro de la información, consideró útil señalar posibles medidas que podrían adoptarse para su labor futura, entre ellas, aunque no exclusivamente, las siguientes:

- La realización por los Estados, individual y colectivamente, de una labor de profundización de los conceptos relativos a la paz y la seguridad internacionales en el uso de las TIC en el plano jurídico, técnico y político.
- El aumento de la cooperación a nivel regional y multilateral a fin de fomentar un entendimiento común sobre los posibles riesgos que representa para la

[124] Ibidem.
[125] Ibidem.

paz y la seguridad internacionales el uso malintencionado de las TIC y sobre la seguridad de las infraestructuras fundamentales sustentadas en esas tecnologías.[126]

Asimismo, hasta 2021 se tenía el UN-GGE sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, el cual ha continuado estudiando en el período de 2019-2021, con miras a promover un entendimiento común y la aplicación eficaz, las posibles medidas de cooperación para encarar las amenazas reales y potenciales en el ámbito de la seguridad de la información. Como parte de su informe final recopilaron normas, reglas y principios de comportamiento responsable de los Estados; el derecho internacional; las medidas de fomento de la confianza; y la cooperación y asistencia internacionales en el ámbito de la seguridad de las tecnologías de la información y las comunicaciones y la creación de capacidad.[127]

El actual Secretario General de la ONU, Antônio Guterres, ha expresado su preocupación por el uso malicioso de las TIC, por lo que ha hecho de la promoción de un entorno pacífico de TIC una de sus prioridades clave. En mayo de 2018, el Secretario General lanzó su Programa de Desarme, dentro de la Agenda del Programa, señala que la interconectividad global significa que la frecuencia y el impacto de los ataques cibernéticos podrían ser cada vez más generalizados, afectando a un número exponencial de sistemas o redes al mismo tiempo.

Para abordar estos desafíos, el Secretario General ha incluido dos puntos de acción sobre el ciberespacio en el plan de implementación de la Agenda de Desarme:

- El Secretario General pondrá sus buenos oficios a disposición para contribuir a la prevención y solución pacífica de los conflictos derivados de actividades maliciosas en el ciberespacio (Acción 30).
- El Secretario General colaborará con los Estados Miembros para ayudar a fomentar una cultura de rendición de cuentas y adhesión a las nuevas normas, reglas y principios sobre comportamiento responsable en el ciberespacio (Acción 31).[128]

Por otra parte, la Oficina de las Naciones Unidas de Lucha Contra el Terrorismo gestiona varias iniciativas en el ámbito de las TIC, incluido un proyecto sobre el uso de las redes sociales para reunir información de fuentes abiertas y pruebas digitales a fin de combatir el terrorismo y el extremismo violento respetando los derechos humanos. Asimismo, realiza capacitaciones especializadas en foros internacionales acerca de los usos y seguridad de los sistemas aéreos no tripulados.[129] También cuenta con un programa de ciberseguridad, que tiene por objeto mejorar las capacidades de los Estados Miembros y las organizaciones privadas para prevenir los

[126] ONU. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. https://digitallibrary.un.org/record/799853
[127] ONU. (2021). Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/89/PDF/N2107589.pdf?OpenElement
[128] ONU. (s. f.). Developments in the field of information and telecommunications in the context of international security. https://www.un.org/disarmament/ict-security/
[129] ONU. (s. f.). Cybersecurity. https://www.un.org/counterterrorism/cybersecurity

ciberataques perpetrados por agentes terroristas contra infraestructuras críticas algunas acciones significativas fue que en 2019 implementó la Fase I del Programa de Ciberseguridad para el Sudeste Asiático, impartiendo un taller de sensibilización para los 11 Estados Miembros, también organizó un taller piloto de capacitación a fondo para Tailandia, Brunei, Filipinas, Bangladesh y la República Democrática Popular de Laos; y para 2020 implementó la Fase I de ciberseguridad para África Oriental.[130]

10. Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford

El Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford, es un centro internacional para la investigación sobre la creación de capacidad de ciberseguridad eficiente y efectiva. El GCSCC ha creado un modelo para revisar la madurez de la capacidad de ciberseguridad en cinco áreas o dimensiones que tiene como objetivo permitir a las naciones autoevaluarse, comparar, planificar mejor las inversiones y las estrategias nacionales de ciberseguridad, y establecer prioridades para el desarrollo de capacidades.[131]

El Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés) busca ofrecer una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, asignándole una etapa específica que corresponde a su grado de logro en materia de ciberseguridad. Las cinco etapas de madurez, que se fijan por medio de una evaluación, van desde la más básica (inicial) hasta la más avanzada (dinámica). El CMM sigue un enfoque integral que entiende la capacidad dentro de cinco dimensiones:

(i) Política y estrategia. Esta dimensión explora la capacidad de un país para desarrollar y entregar una estrategia nacional de ciberseguridad, así como para mejorar su seguridad cibernética resiliencia al mejorar su respuesta a incidentes, defensa cibernética e infraestructura crítica.

(ii) Cultura y sociedad. Revisa elementos como la comprensión de los riesgos cibernéticos, el nivel de confianza en los servicios de internet al igual que con el gobierno y comercio electrónico. También incluye la comprensión de los usuarios sobre la protección de la información personal en línea, los canales para denuncia de delitos cibernéticos y el rol de los medios de comunicaciones y las redes sociales en la configuración de los valores de ciberseguridad.

(iii) Educación, capacitación y habilidades. Esta dimensión considera la disponibilidad, calidad y adopción de programas para diversos grupos de partes interesadas, incluyendo el gobierno, el sector privado y la población en su conjunto, así como programas de sensibilización sobre

[130] ONU. (s. f.).Counter-Terrorism Centre. Cybersecurity. https://www.un.org/counterterrorism/cct
[131] Universidad de Oxford. (s.f.). Global Cyber Security Capacity Centre. About Us. https://gcscc.ox.ac.uk/about-us

ciberseguridad, educación formal sobre ciberseguridad y programas de formación profesional.

(iv) Marcos legales y regulatorios. La dimensión examina la capacidad para diseñar y promulgar legislación nacional que directa e indirectamente se relaciona con la ciberseguridad, con especial énfasis en los temas de requisitos reglamentarios de ciberseguridad, legislación relacionada con el delito cibernético. También, se considera la capacidad de hacer cumplir tales leyes, ejecución, enjuiciamiento, organismos reguladores y capacidades judiciales; y cuestiones como los marcos de cooperación formales e informales para combatir el cibercrimen.

(v) Estándares, organizaciones y tecnologías. Aborda de manera efectiva y generalizada el uso de tecnología de ciberseguridad para proteger a individuos, organizaciones e infraestructura. Esta Dimensión examina específicamente la implementación de estándares y buenas prácticas de ciberseguridad, el despliegue de procesos y controles, y el desarrollo de tecnologías y productos para reducir riesgos de ciberseguridad.[132]

Los marcos normativos de otros países se mencionan en el Anexo 10.

XIV. Dominios en materia de Ciberseguridad

Respecto al marco normativo en materia de ciberseguridad aplicado a las redes y, en particular, a las redes 5G, se considera que este debe cubrir al menos los siguientes dominios:

1. Gobernanza, cumplimiento y organización de seguridad de información sobre las redes;
2. Protección de datos en las redes;
3. Gestión de riesgos de seguridad en las redes;
4. Gestión de identidad y autenticación sobre las infraestructuras críticas de redes;
5. Respuesta a incidentes en las redes;
6. Administración de terceros y proveedores en infraestructuras críticas de redes;
7. Protección de Equipos y Punto Final que utilizan las redes;
8. Protección de Aplicaciones y Bases de Datos que soportan las redes;
9. Protección de Redes y Centros de Datos que albergan los servicios de las redes;
10. Capacitación y concientización en Seguridad en redes (públicos y privados).

[132] Centro Global de Capacidad en Seguridad Cibernética (2021). Cybersecurity Capacity Maturity Model for Nations (CMM). https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

A continuación, se describe brevemente lo que significa cada uno de estos dominios y si son considerados por el marco normativo mexicano en materia de ciberseguridad y por las iniciativas de leyes federales y estatales.

La **gobernanza, cumplimiento y organización de seguridad de información** sobre las redes se refiere al conjunto de políticas, reglas o marcos que definen las políticas de seguridad y las responsabilidades de las principales partes interesadas respecto a la seguridad de la información en las redes. Asimismo, incluye mecanismos de monitoreo y rendición de cuentas.

Respecto a un marco regulatorio en materia de ciberseguridad o una Estrategia Nacional de Ciberseguridad, la idea de la gobernanza implica definir una estructura, roles y responsabilidades de cada una de las partes interesadas o entidades y autoridades encargadas del avance de la economía digital y la reducción de riesgos, las cuales deben ser consistentes y estar alineadas para evitar duplicidades y optimizar esfuerzos. De igual forma, la gobernanza implica establecer mecanismos de monitoreo, evaluación, cumplimiento y coordinación al interior del gobierno y con las partes interesadas no gubernamentales.[133]

La **protección de los datos** en las redes se relaciona con la seguridad de los datos, la cual implica todas las medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, así como todas las medidas de protección para garantizar la integridad de los datos.

En el marco de la protección de datos, la existencia de un marco legal y regulatorio para proteger a la sociedad y promover un entorno digital seguro y protegido es clave, ya que permite la prevención y monitoreo, y facilita el manejo y respuesta frente a incidentes cibernéticos, asimismo, para aprovechar las nuevas tecnologías se necesita de sistemas sólidos de protección de datos. [134].

La **gestión de riesgos de seguridad** en las redes incluye una comprensión clara de los riesgos y amenazas, así como de los activos de alto valor y los sistemas de alto impacto del país que requieren mayores niveles de protección. La gestión de riesgos requiere una anticipación proactiva de las amenazas y una evaluación continua de las vulnerabilidades dentro de las dependencias digitales más críticas del país como son empresas, infraestructuras, servicios, y activos de energía, telecomunicaciones, transporte, servicios financieros, entre otros.

---

[133] Council of Europe (CoE),Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU*). 2021. Guide to Developing a National Cybersecurity Strategy* 2nd Edition – Strategic engagement in cybersecurity. Creative Commons Attribution-NonCommercial 3.0 IGO (CC BY-NC 3.0 IGO). https://ncsguide.org/the-guide/good-practice/, https://ncsguide.org/wp-content/uploads/2021/11/2021-Guide-1.pdf.

[134] UIT (2020) *Global Cybersecurity Index*, Suiza. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Respecto al enfoque de gestión de riesgos alude a que los riesgos no se pueden eliminar por completo, por eso la necesidad de gestionarlos de forma eficaz. En este sentido, se espera que las organizaciones públicas y privadas estén preparadas para las crisis, y sigan procesos de gestión del riesgo de seguridad digital (evaluación de riesgos, tratamiento de riesgos y planes de continuidad) para adaptarse a situaciones críticas.[135]

La **gestión de identidad y autenticación sobre las infraestructuras críticas**[136] de redes es el proceso organizativo para garantizar que los usuarios o dispositivos tengan el acceso adecuado a los recursos tecnológicos o infraestructuras críticas. Incluye la identificación, autenticación y autorización de un usuario(s) o dispositivo(s) para tener acceso a aplicaciones, sistemas o redes. El objetivo principal de la gestión de identidades es garantizar que solo los usuarios o dispositivos autenticados tengan acceso a las aplicaciones, sistemas, entornos informáticos o redes específicos para los que están autorizados.[137]

La **respuesta a incidentes** en las redes es la protección de la información de una organización mediante el desarrollo y la aplicación de un proceso de actuación ante posibles eventos (planes, funciones definidas, formación, comunicaciones, supervisión de la dirección) con el fin de descubrir rápidamente un ataque y, a continuación, contener eficazmente los daños, erradicar la presencia del atacante y restablecer la integridad de la red y los sistemas. Al respecto, un incidente de seguridad de la información se puede definir como un evento único o una serie de eventos que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información; y un incidente de seguridad cibernética se puede definir como una interrupción de las TIC que limita o elimina la disponibilidad esperada de servicios, la publicación, adquisición y modificación no autorizada de información.[138]

La respuesta a estos incidentes va de la mano con la gestión de riesgos y con el establecimiento de capacidades apropiadas de respuesta a incidentes para abordar los desafíos operativos por medio de Equipos de Respuesta a Emergencias Informáticas (CERT, por sus siglas en inglés), Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) o Equipos de Respuesta a Incidentes Informáticos (CIRT, por sus siglas en inglés) ya sea que actúen a nivel

---

[135] OCDE (2021). *Siete lecciones aprendidas sobre seguridad digital durante la crisis de COVID-19* . https://www.oecd.org/coronavirus/policy-responses/siete-lecciones-aprendidas-sobre-seguridad-digital-durante-la-crisis-de-covid-19-c8fa9059/

[136] Infraestructuras Críticas (IC, por sus siglas en inglés) se define como los sistemas, servicios y funciones clave, cuya interrupción, destrucción o explotación podría tener un impacto en servicios esenciales como la salud, la seguridad o el bienestar económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. El concepto de Infraestructuras de Información Críticas (CII, por sus siglas en inglés) alude a sistemas de Tecnologías de la Información y TIC que operan funciones clave de la infraestructura crítica de una nación Microsoft (2014). *Critical Infrastructure Protection: Concepts and Continuum.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVtZU

[137] https://www.computerweekly.com/es/definicion/Gestion-de-identidades-o-gestion-de-IDs

[138] ENISA (2016). *Strategies for Incident Response and Cyber Crisis Cooperation,* https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

nacional, gubernamental, sectorial, etc.[139] La respuesta a un incidente significa coordinación frente al mismo, gestión de vulnerabilidades, conocimiento de la situación, transferencia de conocimientos e intercambio de información sobre amenazas e inteligencia. De esta forma se puede tener capacidad y recuperación ágil, así como mejorar su resiliencia frente a las ciber amenazas, reduciendo el posible impacto.,

La **administración de terceros y proveedores en infraestructuras críticas**[140] de redes indica la explotación o ataque de la cadena de suministro de las TIC, compuesta por hardware, software, servicios administrados de proveedores y proveedores de servicios; así como verificar que los proveedores mantengan una cultura de seguridad adecuada y un programa gestión de riesgos de la cadena de suministro para abordar adecuadamente los riesgos que preocupan a su organización.[141]

La **protección de equipo y punto final** que utilizan las redes se refiere a las salvaguardas implementadas, estrategias y soluciones tecnológicas para protección de los dispositivos de punto final[142] de las amenazas y el acceso no autorizado.[143]

La **protección de aplicaciones y bases de datos** que soportan las redes se entiende como la gama de herramientas, controles y medidas diseñadas para establecer y preservar la confidencialidad, integridad y disponibilidad de la base de datos, protegiendo los datos en la base de datos, el sistema de gestión de bases de datos, cualquier aplicación asociada.[144]

Sobre **la protección de redes y centro de datos** que albergan los servicios de las redes se refiere a la protección de servidor de base de datos físico o el servidor de base de datos virtual y el hardware subyacente; y la infraestructura informática o de red utilizada para acceder a la base de datos.[145]

Al respecto, la **protección de equipo, aplicaciones, bases de datos**, redes y centro de datos se entendería como de importancia primordial para todas las etapas involucradas en la prestación de servicios críticos, considerando que hay aplicaciones críticas que soportan procesos de servicio críticos dependiente de las redes de comunicación. [146]

Dentro del rubro de **capacitación y concientización en seguridad**, alude a abordar los desafíos relacionados la creación de capacidad en seguridad cibernética a

[139]Council of Europe et al. Op Cit.
[140] Relaciones con entidades externas. Las entidades externas pueden incluir proveedores de servicios, vendedores, socios del lado de la oferta, socios del lado de la demanda, alianzas, consorcios e inversionistas, y pueden incluir tanto partes contractuales como no contractuales. NIST. *Third-party Relationships*. https://csrc.nist.gov/glossary/term/third_party_relationships
[141] CISA. Information and Communications Technology supply chain risk management. https://www.cisa.gov/supply-chain
[142] Los dispositivos de punto final son dispositivos que reciben cualquier señal, como portátiles, teléfonos inteligentes, dispositivos de internet de las cosas, sensores, etc.
[143] NIST. *Endpoint Protection Platform*. https://csrc.nist.gov/glossary/term/endpoint_protection_platform
[144] IBM. *Database Security*. https://www.ibm.com/cloud/learn/database-security#toc-database-s-3h4XsKVC
[145] Ibidem.
[146] ENISA (2014) Op. Cit.

nivel personal e institucional, considerando la concientización entre las partes interesadas, incluidas las entidades gubernamentales, los ciudadanos, las empresas y otras organizaciones. En este sentido, se reconoce una necesaria coordinación de actividades de desarrollo de capacidades identificando aquellos grupos de la sociedad que requieren una atención especial en lo que respecta a la capacidad y la creación de capacidades en materia de ciberseguridad y la sensibilización.[147]

El Cuadro 2 presenta aquellos dominios que son considerados por la normatividad mexicana en materia de ciberseguridad. Al respecto, el Programa Sectorial de Seguridad y Protección Ciudadana, la Estrategia Institucional para el Ciberespacio de la Secretaría de Marina y el Programa Sectorial de la Secretaría de Defensa conviene detallar que las acciones por implementarse en el marco de los dominios son internas y planeadas a desarrollarse.

Cuadro 2. Dominios en materia de Ciberseguridad en la normatividad mexicana

Dominio	Normativa.					
	ENC (2017)	EDN	Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos	Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024	Estrategia Institucional para el Ciberespacio 2021-2024 de la Secretaría de Marina	Programa Sectorial de la Secretaría de Defensa Nacional 2020-2024
Gobernanza, Cumplimiento y organización de Seguridad de información sobre las redes	X	X	X			
Protección de Datos en las redes	X		X			
Gestión de Riesgos de Seguridad en las redes	X	X	X	X	X	
Gestión de Identidad y Autenticación sobre la infraestructura critica de redes	X		X	X	X	X
Respuesta a Incidentes en las redes		X	X	X	X	X
Administración de Terceros y Proveedores en infraestructuras críticas de redes			X			
Protección de Equipos y Punto Final que utilizan las redes						
Protección de Aplicaciones y Bases de Datos que soportan las redes	X					
Protección de Redes y Centros de Datos que albergan los servicios de las redes				X	X	
Capacitación y concientización en Seguridad en redes (públicos y privados)	X	X		X	X	X

Fuente: Elaboración propia con información citada en la nota

Por su parte, el Cuadro 3 muestra los dominios que son considerados en las iniciativas de leyes federales y estatales. Cabe señalar que las Iniciativas de Ley General de Ciberseguridad del 2 de septiembre del Senador Miguel Mancera y la del 6 de abril de 2021 de la Senadora Jesús Lucia Trasviña se mencionan

[147] Council of Europe. Op. Cit.

mecanismos para la implementación de algunos de los dominios antes mencionados.

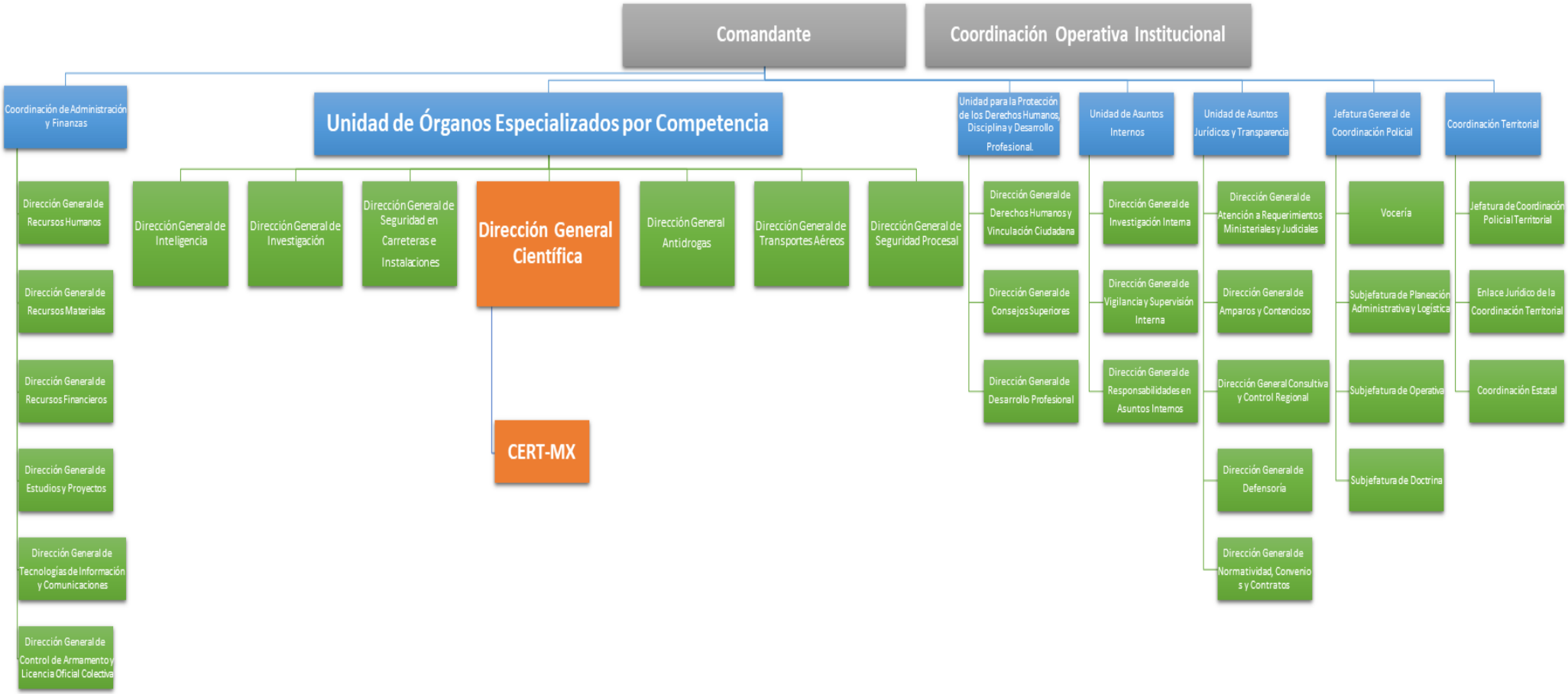
Cuadro 3. Dominios en materia de Ciberseguridad en las Iniciativas de Ley

	Iniciativas						
Dominio	Ley especializada en la materia de Ciberdelitos 27 de marzo de 2019	Ley General de Ciberseguridad 2 de septiembre de 2020	Ley General de Ciberseguridad 6 de abril de 2021	Ley General de Ciberseguridad 6 de octubre de 2022	Ley de Ciberseguridad para la Ciudad de México	Ley de Ciberseguridad del Estado de San Luis Potosí y sus Municipios	Ley de Ciberseguridad del Estado de Sinaloa
Gobernanza, Cumplimiento y organización de Seguridad de información sobre las redes		X	X	X		X	X
Protección de Datos en las redes	X	X	X				
Gestión de Riesgos de Seguridad en las redes		X	X		X	X	X
Gestión de Identidad y Autenticación sobre la infraestructura critica de redes	X	X	X				
Respuesta a Incidentes en las redes		X	X	X	X	X	X
Administración de Terceros y Proveedores en infraestructuras críticas de redes	X	X	X				
Protección de Equipos y Punto Final que utilizan las redes		X	X				
Protección de Aplicaciones y Bases de Datos que soportan las redes		X	X				
Protección de Redes y Centros de Datos que albergan los servicios de las redes	X	X	X				
Capacitación y concientización en Seguridad en redes (públicos y privados)		X	X	X	X	X	X

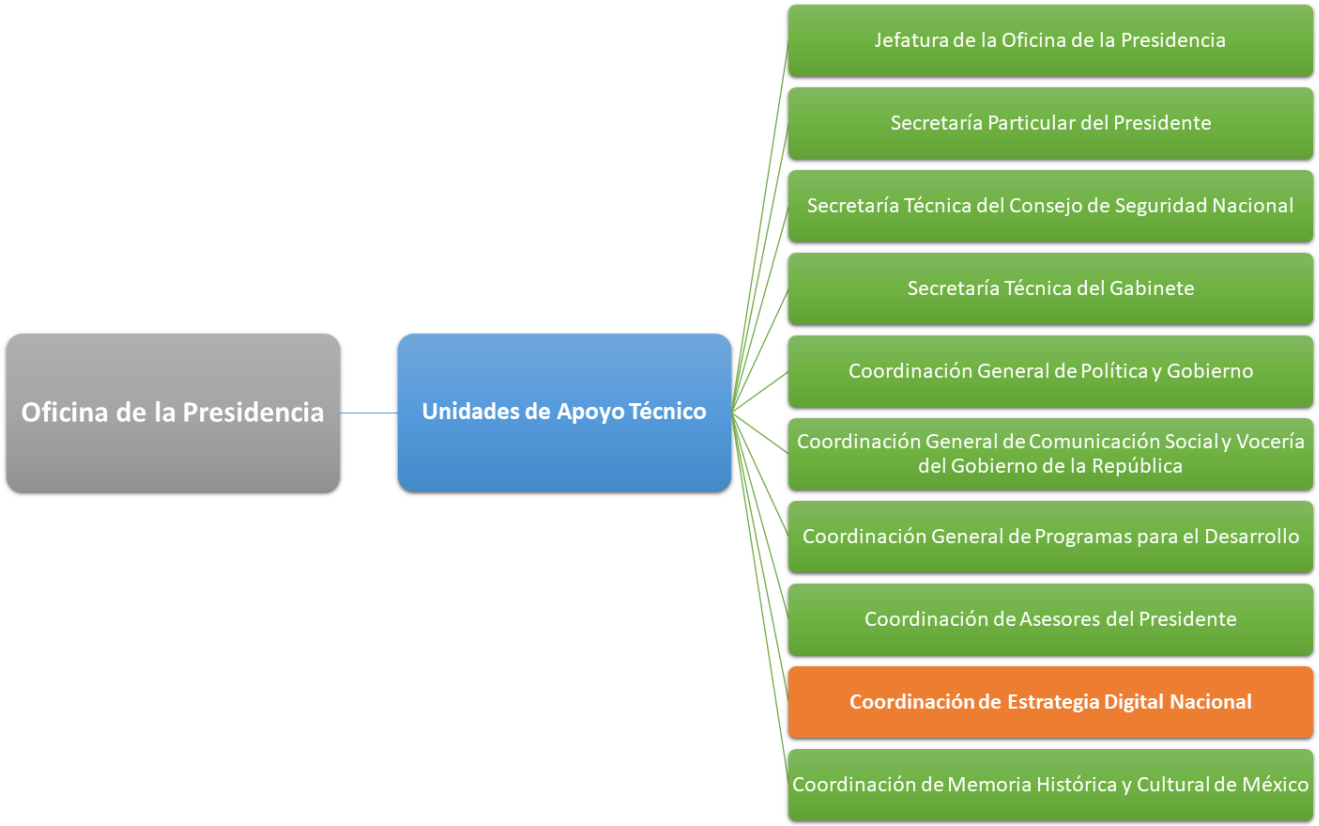
Fuente: Elaboración propia con información del Anexo 6. Iniciativas presentadas en el Congreso y del Anexo 7. *Ciberseguridad en los estados de la República Mexicana.*

XV. ANEXO

Anexo 1. Organigrama Guardia Nacional[148]



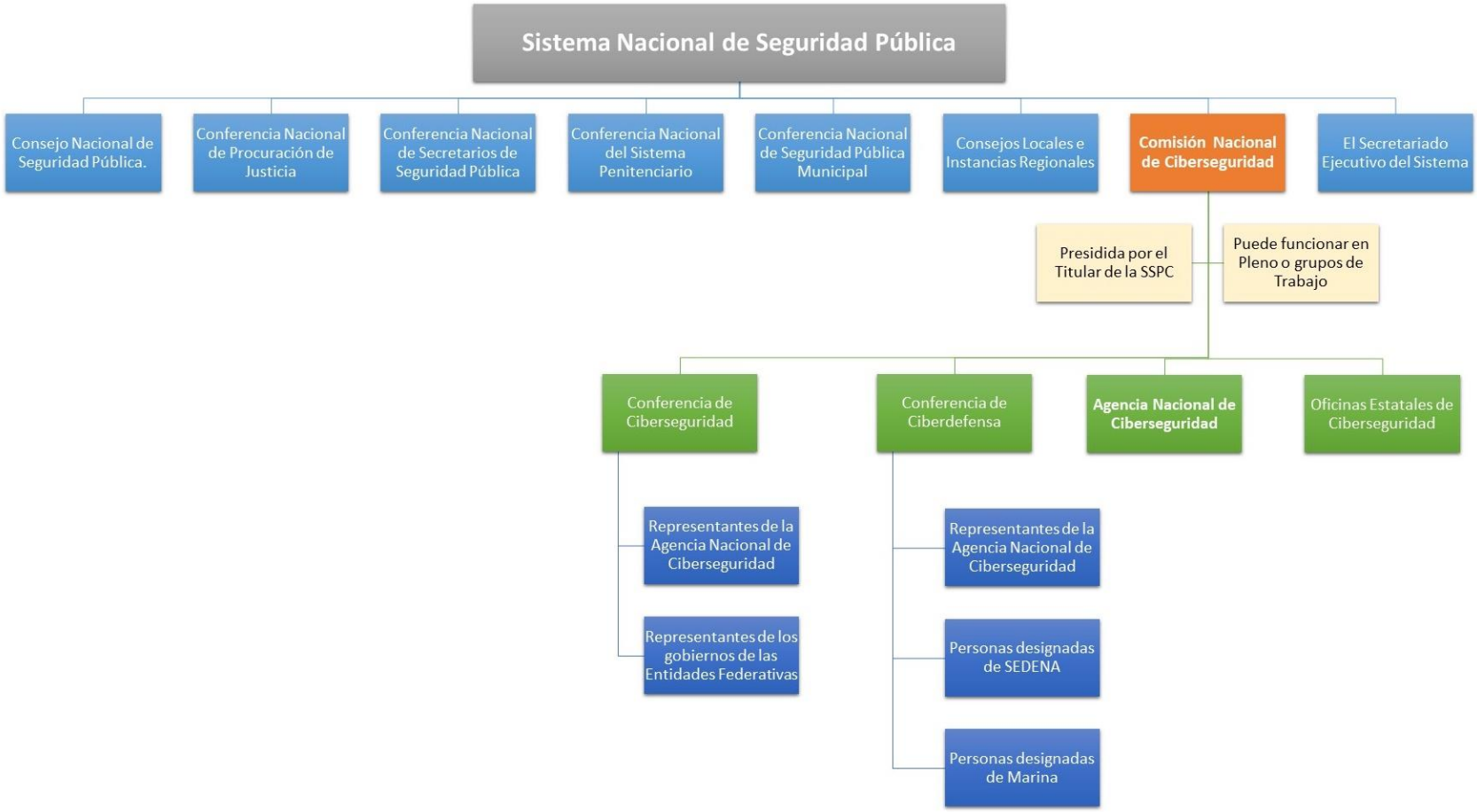
Anexo 2. Organigrama Oficina de la Presidencia[149]



[148] MANUAL de Organización General de la Guardia Nacional, 16 de noviembre de 2021. https://dof.gob.mx/nota_detalle.php?codigo=5635311&fecha=16/11/2021#:~:text=El%20Manual%20de%20Organizaci%C3%B3n%20General%20se%20encuentra%20integrado%20principalmente%20por,integran%20la%20Estructura%20Org%C3%A1nica%20B%C3%A1sica

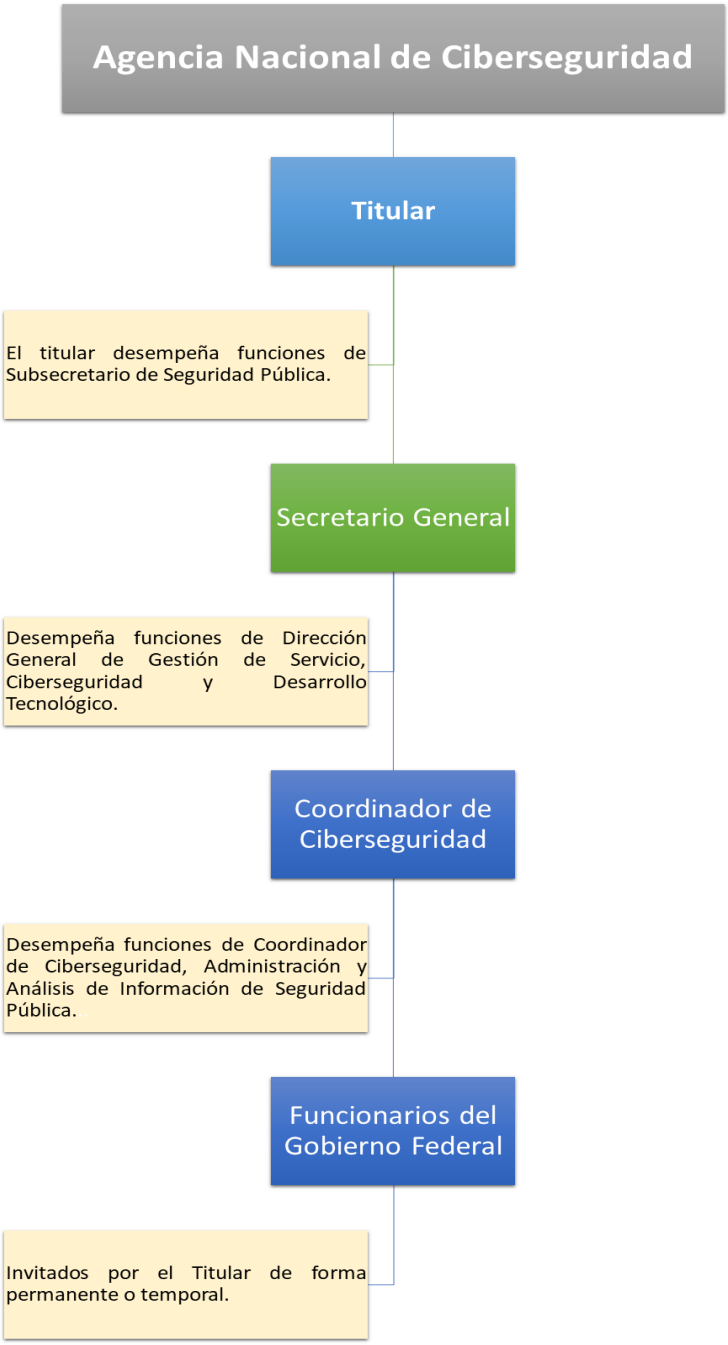
[149] REGLAMENTO de la Oficina de la Presidencia de la República, 9 de diciembre de 2019. https://www.dof.gob.mx/nota_detalle.php?codigo=5581283&fecha=09/12/2019

Anexo 3. Organigrama CNC y ANC[150]



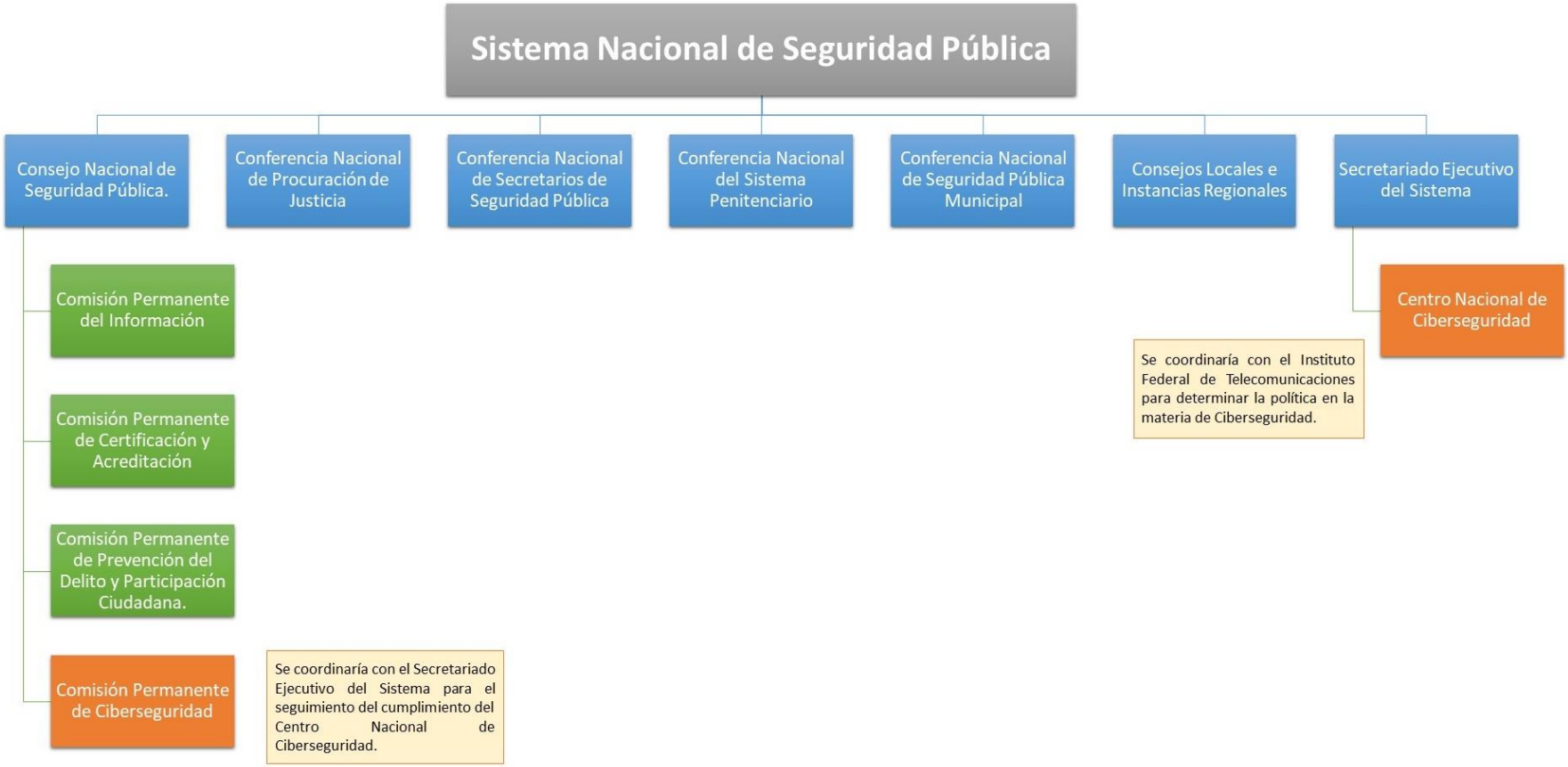
[150] Iniciativa de la Senadora Jesús Lucía Trasviña Waldenrath, con proyecto de decreto por el que se expide la ley general de ciberseguridad y se derogan diversas disposiciones del código penal federal, 6 de abril de 2021, Senado de México, México. https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-04-06-1/assets/documentos/Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf.

Anexo 4. Organigrama ANC[151]



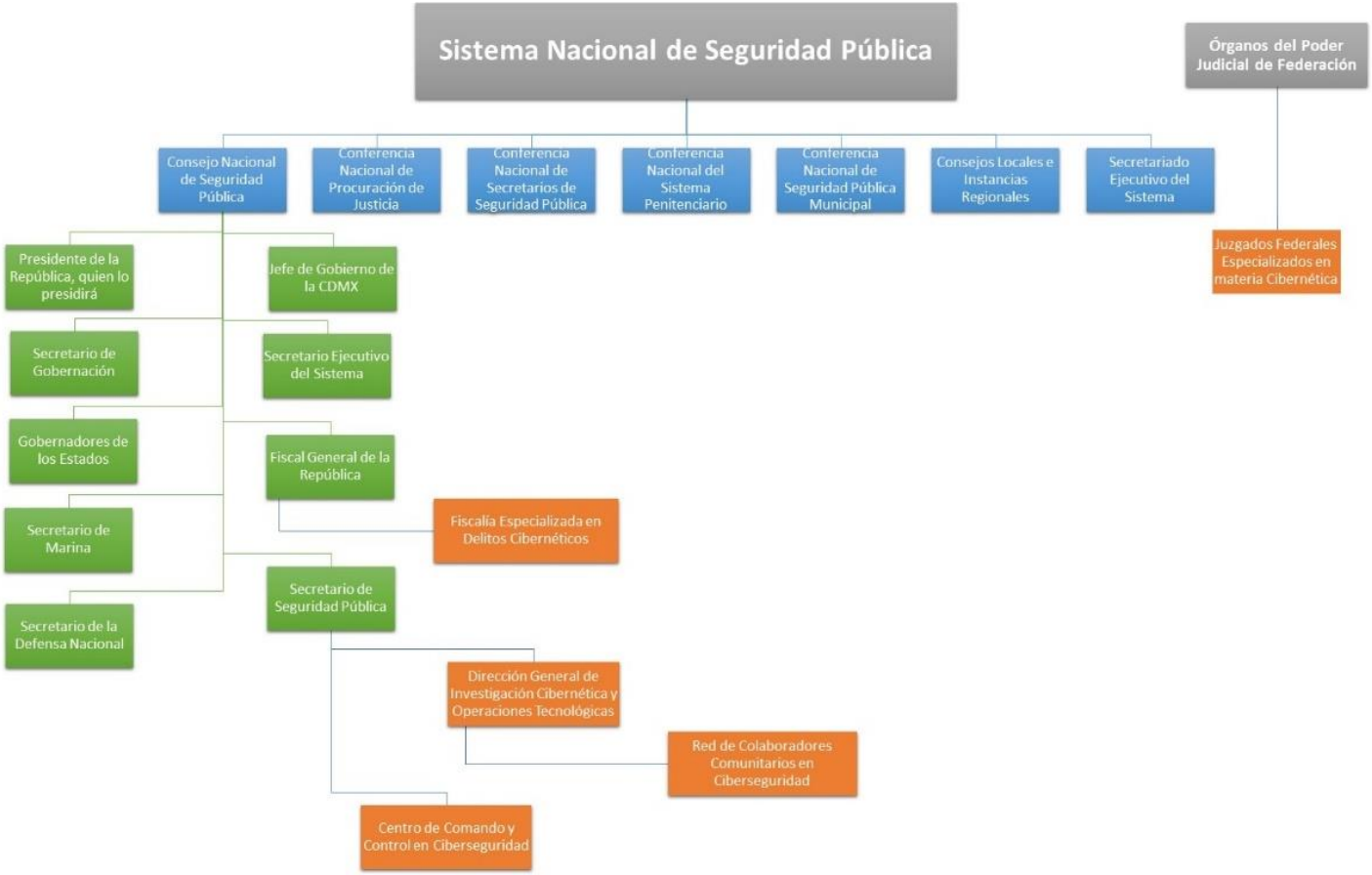
[151] Iniciativa de la Senadora Jesús Lucía Trasviña Waldenrath, con proyecto de decreto por el que se expide la ley general de ciberseguridad y se derogan diversas disposiciones del código penal federal, 6 de abril de 2021, Senado de México, México. https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-04-06-1/assets/documentos/Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf.

Anexo 5. Organigrama Comisión Permanente y Centro Nacional de Ciberseguridad[152]



[152] Iniciativa del Senador Ángel Mancera Espinosa por la que expide la Ley General de Ciberseguridad, 1 de septiembre de 2020. https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2020-09-02-1/assets/documentos/Inic_PRD_Sen_Mancera_ciberseguridad.pdf

Anexo 6. Organigrama Iniciativa Ley General de Ciberseguridad.[153]



[153] Iniciativa de la Diputada Juanita Guerra Mena por la que expide la Ley General de Ciberseguridad. http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/10/asun_4406432_20221006_1665067295.pdf

Anexo 7. Iniciativas presentadas en el Congreso

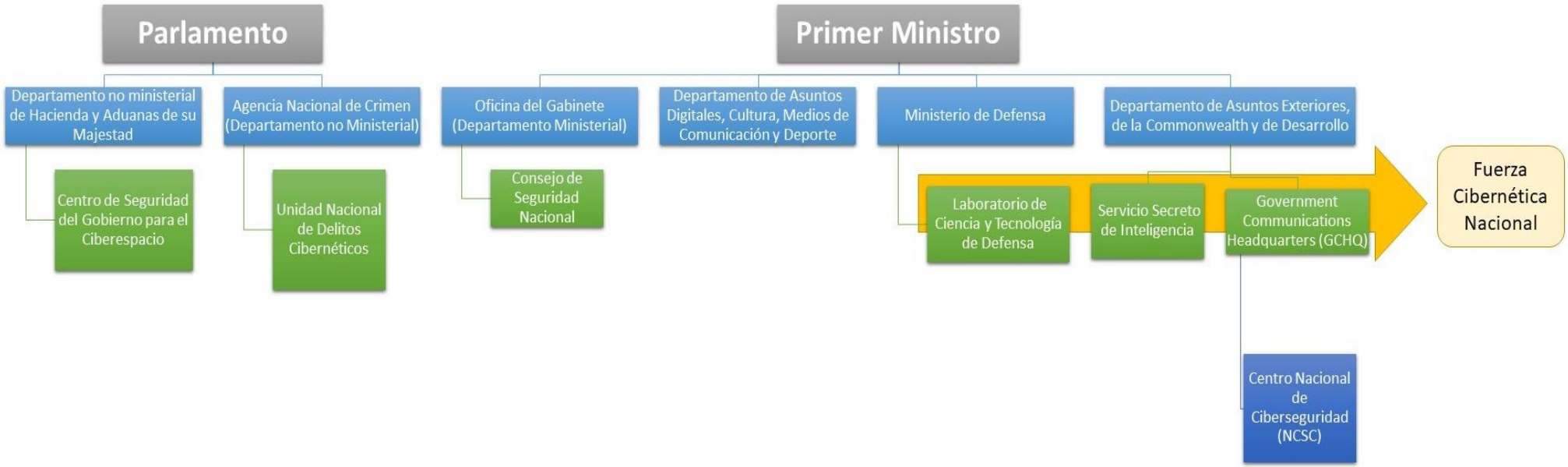
Propuesta de Legislador	Fecha	Asunto	Estatus	Fuente
Sen. Alejandra Lagunes Soto Ruíz	23 de octubre de 2018	**Objetivo:** Declarar el mes de octubre de cada año como -El Mes Nacional de la Ciberseguridad.	Aprobada	• Iniciativa • Estatus
Sen. Jesús Lucía Trasviña Waldenrath	27 de marzo de 2019	**Objetivo:** Reformar y derogar diversas disposiciones del Código Penal Federal relativos a ciberdelitos o delitos cometidos por medio de sistemas informáticos, dando paso a crear una Ley especializada en la materia de Ciberdelitos, a fin de erradicar el mal uso de las herramientas dentro del campo de la tecnología de la información, ya que estos influyen directamente sobre la sociedad moderna y que actualmente dentro del ciberespacio es utilizado con fines legítimos. La iniciativa tiene por objeto establecer las bases de integración y acción para preservar la seguridad informática nacional, por medio de un Proyecto de Decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática.	Pendiente. Se turnó a las Comisiones Unidas de Justicia; Seguridad Pública y de Estudio Legislativos, Primera.	• Iniciativa • Estatus
Dip. Javier Salinas Narváez	29 de octubre de 2019	**Objetivo:** Facultar al Congreso de la Unión para legislar en materia de ciberseguridad a través de una iniciativa que reforma el Artículo 73 de la Constitución Política De Los Estados Unidos Mexicanos.	Pendiente en Comisión de Cámara de Origen.	• Iniciativa • Estatus
Sen. José Ramón Enríquez Herrera	11 de abril de 2020	**Objetivo:** Establecer como amenaza a la seguridad nacional los actos que vulneren la ciberseguridad y que lesionen a los habitantes y a las instituciones, por medio de un Proyecto de Decreto por el que se adiciona la fracción XIV al Artículo 5 de la Ley de Seguridad Nacional. "Artículo 5.- Para los efectos de la presente Ley, son amenazas a la seguridad nacional: XIV. Actos que vulneren la ciberseguridad y que lesionen a los habitantes y a las instituciones"	Pendiente. Se turnó a las Comisiones Unidas de Seguridad Pública; De Ciencia y Tecnología; y de Estudio Legislativos, Primera.	• Iniciativa. • Estatus
Dip. María Eugenia Hernández Pérez	28 de junio de 2020	**Objetivo:** Establecer mecanismos legales en materia de ciberseguridad, como parte de la Estrategia Digital Nacional, por medio de un Decreto por el que se adicionan las fracciones XIV y XV al artículo 5; una fracción VI al artículo 6; todos de la Ley de Seguridad Nacional.	Pendiente en Comisión de Cámara de Origen.	• Iniciativa. • Estatus.

Propuesta de Legislador	Fecha	Asunto	Estatus	Fuente
		"Artículo 5. Para los efectos de la presente ley, son amenazas a la seguridad nacional: XIV. Actos ilícitos perpetuados en el ciberespacio que atenten contra la estabilidad, soberanía y la paz del Estado." "Artículo 6. Para los efectos de la presente ley, se entiende por: VI. Ciberespacio: Ámbito artificial creado por medios informáticos."		
Dip. María Eugenia Hernández Pérez	12 de agosto de 2020	**Objetivo**: Declarar el 23 de noviembre de cada año, como -Día Nacional de la Ciberseguridad-. (En conmemoración del día en que se elaboró el Convenio de Budapest).	Pendiente en Comisión de Cámara de Origen.	• Iniciativa • Estatus
Dip. Carlos Iván Ayala Bobadilla	12 de agosto de 2020	**Objetivo**: crear el marco regulatorio para la Universidad encargada de impartir educación superior a nivel licenciatura, especialidad, maestría, doctorado y opciones terminales, en materia de desarrollo tecnológico e innovación en el país, como organismo público con personalidad jurídica, patrimonio propio, autonomía técnica y de gestión, como institución de educación pública del Estado Mexicano. Lo anterior, a través de una iniciativa con Proyecto de Decreto por el que se expide la Ley que crea la Universidad de Tecnologías de la Información, Comunicaciones e Innovación.	Pendiente en Comisión de Cámara de Origen.	• Iniciativa • Estatus
Sen. Miguel Ángel Mancera Espinosa	2 de septiembre de 2020	**Objetivo:** Establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la ciberseguridad en las instituciones del Estado y la sociedad; por medio de una iniciativa con aval del grupo parlamentario que contiene Proyecto de Decreto que reforma y adiciona diversas disposiciones del Código Penal Federal, de la Ley General del Sistema Nacional de Seguridad Pública, de la Ley de Seguridad Nacional; y, expide la Ley General de Ciberseguridad.	Pendiente. Se turnó a las Comisiones Unidas de Justicia; y de Estudios Legislativos, Segunda.	• Iniciativa • Estatus
Dip. José Salvador	2 de marzo de 2021	**Objetivo**: Establecer austeridad en la adquisición y arrendamiento de equipo y servicios de cómputo que se usan para garantizar la operación de programas sociales y labores de ciberseguridad, por	Pendiente en Comisión de Cámara de Origen.	• Iniciativa • Estatus

Propuesta de Legislador	Fecha	Asunto	Estatus	Fuente
Rosas Quintanilla		medio de una iniciativa que reforma el artículo 16 de la Ley Federal de Austeridad Republicana.		
Sen. Gustavo Enrique Madero Muñoz	25 de marzo de 2021	**Objetivo:** Prevenir y sancionar los delitos cibernéticos a través de una iniciativa con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal, en materia de delitos cibernéticos.	Pendiente. Se turnó a las Comisiones Unidas de Estudio Legislativos, Segunda.	• Iniciativa • Estatus
Sen. Jesús Lucía Trasviña Waldenrath	6 de abril de 2021	**Objetivo:** Regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad, por medio de una Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del Código Penal Federal.	Pendiente. Se turnó a las Comisiones Unidas de Justicia y Estudios Legislativos, Segunda.	• Iniciativa • Estatus
Sen. Jesús Lucía Trasviña Waldenrath	12 de octubre de 2021	**Objetivo**: incluir en la legislación la figura de incidentes cibernéticos con el objeto de crear un Registro Nacional de Incidentes Cibernéticos el cual se enfocará en concentrar la información de los Incidentes en materia de ciberespacio que ocurran dentro de la utilización de las Tecnologías de la Información y la Comunicación. Además, propone que a fin de garantizar el derecho de acceso a la información en posesión de los sujetos obligados, la consulta será prioritariamente por parte de las instituciones de Seguridad Pública que estén facultadas en cada caso, a través de las y los servidores públicos que cada institución designe, y en casos excepcionales por parte de personas que demuestren un interés directo en la información; la reserva y consulta de información atenderá en todo momento a los principios de confidencialidad y reserva temporal, mediante justificación y certeza que demuestre claramente ser de interés público y de seguridad nacional, con el propósito de mantener una amplia protección de seguridad cibernética y no vulnere los derechos de otras personas o entes. Para tal fin modifica los artículos 5, 10 y 38 bis de la Ley General del Sistema Nacional de Seguridad Pública.	Pendiente. Se turnó a las Comisiones Unidas de Seguridad Pública y de Estudio Legislativos, Segunda.	• Iniciativa • Estatus
Sen. Jesús Lucía Trasviña Waldenrath	14 de octubre de 2021	**Objetivo:** Regular la integración, organización y funcionamiento la Comisión Nacional de Ciberseguridad. Entre lo propuesto destaca: 1) definir que los órganos de ciberseguridad son la Comisión Nacional de Ciberseguridad (CNC) y las instituciones de la federación, entidades	Pendiente. Se turnó a las Comisiones Unidas de Estudio Legislativos.	• Iniciativa • Estatus

Propuesta de Legislador	Fecha	Asunto	Estatus	Fuente
		federativas y municipios que realicen funciones de ciberseguridad; 2) establecer la Comisión Nacional de Ciberseguridad estará integrada por la o el titular de la SSPC, SEDENA, SEMAR, SEGOB, SRE, SCT, SENER, SHCP, SE, SEP, FGR y las y los gobernadores de los estados; 3) determinar que la CNC estará integrada por una Conferencia; 4) indicar que la CNC cumplirá sus objetivos y fines, formulará políticas integrales y sistemáticas, así como programas y estrategias en materia de ciberseguridad; y, 5) señalar que la CNC planteará la Estrategia Nacional de Ciberseguridad y el Programa Nacional de Ciberseguridad procurando su ejecución y evaluación anual. Para tal fin modifica los artículos 5, 10 y 38 bis de la Ley General del Sistema Nacional de Seguridad Pública.		
Dip. Lidia García Anaya	15 de diciembre de 2021	**Objetivo**: Crear la Fiscalía Especializada en materia de Ciberseguridad. Para ello propone: 1) señalar que la FGR contará con la Fiscalía Especializada en materia de Ciberseguridad para el ejercicio de sus facultades; y, 2) señalar que la Fiscalía Especializada en materia de Ciberseguridad podrá investigar y perseguir los delitos de competencia Federal en el que los medios electrónicos y tecnológicos constituyan o representen un medio de comisión relevante y trascendente, a excepción de delincuencia organizada. Para dicho fin se propone una reforma los artículos 11 y 13 de la Ley de la Fiscalía General de la República.	Pendiente en Comisión de Cámara de Origen.	• Iniciativa • Estatus
Dip Juanita Guerra Mena	6 de octubre de 2022	**Objetivo:** Determinar la distribución de competencias en materia de ciberseguridad para el Consejo Nacional de Seguridad Pública; la Secretaría de Seguridad y Protección Ciudadana acompañado de la creación de un Centro de Comando y Control en Ciberseguridad a su cargo; así como la creación de una Fiscalía Especializada en Delitos Cibernéticos, una Red de Colaboradores Comunitarios en Ciberseguridad y Juzgados Federales Especializados en materia Cibernética.	Pendiente de ser turnada a Comisión.	• Iniciativa

Anexo 8. Organigrama Reino Unido[154]



[154]Gobierno de Reino Unido. Departments, agencies and public bodies. https://www.gov.uk/government/organisations

Anexo 9. Ciberseguridad en los estados de la República Mexicana

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
Aguascalientes	De acuerdo con la Ley Orgánica de la Administración Pública del estado de Aguascalientes, la Secretaría de Administración (SA) tiene la facultad de desarrollar, regular, administrar y supervisar los servicios de tecnologías de la información y comunicaciones de la Administración Pública Estatal, promoviendo su innovación, modernización y mantenimiento. Como parte de la SA, la Dirección General de Mejores Prácticas Gubernamentales cuenta con la atribución de coordinar y supervisar en lo general los proyectos de sistemas de información, diversos de telecomunicaciones, infraestructura de procesamiento, impresión, almacenamiento y normas de operación de informática y de seguridad de la información administradas por las Dependencias y Entidades. Asimismo, la Dirección cuenta con una Jefatura de Departamento de Seguridad de la Información y una Unidad Especializada en Seguridad de la Información.	Como parte de las unidades operativas que dependen de la Subsecretaría de Seguridad Pública del estado, se cuenta con la Dirección General de la Policía Cibernética, la cual tiene en objetivo de identificar conductas de delitos cibernéticos, cometidas a través de la Internet, mediante la búsqueda de datos en fuentes públicas de información para líneas de investigación.	En el Plan Estatal de Desarrollo 2016-2022 en su tercer eje "Aguascalientes con gobierno íntegro, austero y abierto", se considera entre las líneas de acción del programa "Gobierno Cercano y Moderno" el "Actualizar la infraestructura y servicios tecnológicos Procesamiento, Impresión, Comunicación y Almacenamiento), bajo un esquema integral de seguridad de la información.	Se tiene tipificado el delito de acceso informático indebido como aquel en que se acceda a información contenida en un aparato para el procesamiento de datos sin autorización de propietarios; o bien al interferir el buen funcionamiento de un sistema operativo, programa de computadora, base de dato o cualquier archivo informático. Otro delito tipificado en el tema de ciberseguridad es el de violación a la intimidad personal.	• Reglamento interior de la Secretaría de Seguridad Pública del Estado de Aguascalientes. • Ley orgánica de la administración pública del estado de Aguascalientes • Reglamento interior de la Secretaría de Administración del estado de Aguascalientes • Manual de organización de la Secretaría de Administración de Aguascalientes • Plan Estatal de Desarrollo de Aguascalientes 2016-2022 • Código Penal del Estado de Aguascalientes
Baja California		De acuerdo con la Ley del Sistema Estatal de Seguridad Ciudadana de Baja California, el Centro Estatal de Inteligencia Preventiva a través de la Unidad de Policía Cibernética es quien garantiza la seguridad en materia de delitos informáticos mediante la prevención e investigación. Anteriormente la Unidad de Policía Cibernética era parte de la Fiscalía General.	En el pasado Plan Estatal de Desarrollo de 2020-2024, en la política pública operativa de "Gobierno Austero y Hacienda Ordenada", como parte de la Estrategia de "generar políticas, lineamientos e instrumentos técnicos en materia de innovación, tecnologías y telecomunicaciones en el Estado", se consideró como línea de acción el	Dentro del delito de hostigamiento, se considera el medio tecnológico o cibernético. También el delito contra la intimidad y la imagen considera la divulgación de contenido digital. En el marco de la extorsión, si se utiliza como medio cualquiera de comunicación electrónica o digital es una agravación de la pena. Se incluye el delito de acceso Ilícito a sistemas y equipos de informática, además de agravarse la pena si el acto se cometa en	• Ley Estatal de Seguridad Ciudadana de Baja California. • Página del Centro Estatal de Inteligencia Preventiva. • Plan Estatal de Desarrollo 2020-2024 • Plan Estatal de Desarrollo 2022-2027

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
			"generar estándares en materia de ciberseguridad para salvaguardar la confidencialidad, integridad y disponibilidad de la información". Con las elecciones de 2021 del estado, en el Plan Estatal de Desarrollo 2022-2027, como parte de la política transversal de "Gestión Pública Honesta y al servicio de la Gente" en el marco de gobierno digital se incluyó entre las líneas de política el soporte tecnológico para la gestión de los procesos institucionales, en donde se reconoce el riesgo de la vulneración cibernética. Se espera, entre los resultados, procesos tangibles de gestión de tecnologías de la información alineados a mejores prácticas reconocidas a nivel mundial.	contra de equipo del Estado o Municipios; así como quien suplante la identidad con fines ilícitos usando medios informáticos, telemáticos o electrónicos.	• Código Penal para el Estado de Baja California.
Baja California Sur		Como parte de la Procuraduría General del estado, su Unidad de Análisis de Información tiene una División Cibernética, la cual se encarga de prevenir el delito desde plataformas tecnológicas, mediante difusión de estrategias enfocadas a la seguridad digital de la sociedad.		En el marco de acoso sexual, se incluye el delito de Ciberacoso, en el que se considera el agravante de si se contacta a un menor de edad por medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos. En el caso de la usurpación de identidad se toma en cuenta el medio informático. En el rubro de los delitos contra la intimidad sexual se incluye el de	• Manual Especifico de Organización dela Unidad de Análisis de la Información de la Procuraduría General de Justicia del Estado de Baja California Sur. • Ley del Sistema Estatal de Seguridad Pública de Baja California Sur

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
		Asimismo, como parte del Sistema Estatal de Seguridad Pública se cuenta con la policía estatal preventiva, la cual está integrada por unidades especializadas de análisis táctico, investigación y operaciones, entre las que destaca la Policía Cibernética que es parte de la Unidad de Investigación y Análisis.		violación a la misma al divulgar contenido digital.	• Reglamento interno de la Policía Estatal Preventiva del Estado de Baja California Sur. • Código Penal para el Estado Libre y Soberano de Baja California Sur.
Campeche		Desde 2017 se cuenta con la Unidad de Policía Cibernética como parte de la Secretaría de Protección y Seguridad Ciudadana del Estado de Campeche.		Dentro del delito de fraude se incluye a quien alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, alteración de programas sistematizados, o del empleo no autorizado de datos, o engaño semejante. En el rubro de delitos informáticos se incluyen a quien por medio de un ordenador acceda a una o más bases de datos de sistemas informáticos con el propósito de conocer, copiar, alterar o destruir la información que contengan; a través de medios informáticos o electrónicos, intercepte, interfiera, reciba, use, altere o destruya un sistema, soporte o programa de cómputo o los datos contenidos en este; o sirviéndose de medios informáticos o electrónicos, altere o configure dispositivos de la misma naturaleza, para obtener, modificar o transmitir información. También se encuentra tipificada la violación a la intimidad personal considerando el caso de divulgación ´de imágenes, videos o	• Informe de avances en materia de seguridad pública del estado de Campeche 2020. • Código Penal del Estado de Campeche

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				audios de contenido íntimo sexual de una persona sin su consentimiento.	
Coahuila	Dentro del Programa Estatal de Seguridad Pública 2017-2023 bajo el Objetivo General de "salvaguardar y garantizar la integridad física y patrimonial de la sociedad coahuilense, la paz, el orden y el respeto a los derechos humanos en coordinación con los tres órdenes de gobierno" y en el marco del Objetivo Específico de fortalecer la actuación y coordinación interinstitucional, se ha incluido entre sus líneas de acción el reorientar estrategias de operación apoyadas en la aplicación de tecnología e inteligencia policial generando un modelo óptimo de ciberseguridad. Asimismo, bajo el objetivo específico sobre los servicios de Seguridad Pública de "fortalecer la cobertura y operación de la Red Estatal de Telecomunicaciones y modernizar la unidad del Sistema Estatal de Información con tecnología de última generación" se incluyó en las líneas de acción el generar la infraestructura necesaria que permita estructurar mediante el uso de la tecnología la construcción de la ciberseguridad en el Estado.	La Procuraduría General del Estado cuenta entre sus unidades con la Coordinación General de Análisis de Información y de Inteligencia Patrimonial y Económica, quien tiene a su cargo a la Unidad de Policía Cibernética.	En 2018 se creó el Centro de Innovación Industrial Coahuila 4.0. En su primera fase de operaciones, el Centro se enfocó en la especialización de capital humano en temas de: iniciación y sensibilización en industria 4.0; visión artificial inteligente; sistemas interactivos basados en realidad aumentada; digitalización, IoT, big data y data analytics; y ciberseguridad. En 2021, se creó el Comité de Gobierno Digital del Gobierno del Estado de Coahuila de Zaragoza, mediante un decreto publicado en el Periódico Oficial del Gobierno del estado Su finalidad es asesorar a las dependencias y entidades de la Administración Pública Estatal en materia del uso de tecnologías de información y comunicación. En dicho comité se incluyó un Subcomité de Seguridad Cibernética	En el marco del acoso sexual se considera la comisión del delito por medios informáticos, audiovisuales o virtuales. Para el caso de suplantación de identidad, se tiene cotejado el medio electrónico o telemático Bajo los delitos contra la información privada en medios informáticos se tiene contemplado el acceso y transmisión privada en medios de información contenida en un sistema informático; así como la afectación de datos o información de contenidos en un sistema informático. Al respecto, se contempla un incremento a la pena en caso de que se afecté un sistema informático de periodistas o trabajadores de medios de comunicación. En el rubro de los delitos contra la intimidad sexual se incluye el de violación a la misma al divulgar contenido digital.	• Reglamento de la Ley Orgánica de la Procuraduría General de Justicia de Coahuila. • Manual de organización de la Procuraduría General de Justicia de Coahuila • Programa Estatal de Seguridad Pública de Coahuila 2017-2023 • Primer Informe de Gobierno del Estado de Coahuila 2018 • Cuarto Informe del Gobierno del Estado de Coahuila 2021 • Decreto por el que se crea el Comité de Gobierno Digital del Gobierno del Estado de Coahuila de Zaragoza • Código Penal de Coahuila de Zaragoza
Colima	En 2019 el gobierno de Colima atendiendo la Ley para el Impulso de la Sociedad de la Información y el Conocimiento, presentó la Agenda Digital del Estado de Colima.	Como parte de la Secretaría de Seguridad Pública del Estado la Dirección de Información y Análisis coordina la implementación		Bajo los delitos de hostigamiento sexual, acoso laboral y acoso sexual se considera agravante el uso de medios de radiodifusión, telecomunicaciones, informáticos	• Reglamento Interior de la Secretaría de Seguridad Pública del Estado de Colima.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	En ella, como parte de las líneas de acción del Objetivo habilitador 1: Acceso universal a las TIC, dentro de la Meta se implementa un modelo de seguridad informática que planteó apoyar tecnologías que mejoren la confiabilidad de las comunicaciones y su integridad. También, como parte de las líneas de acción del Objetivo habilitador 2: Economía Digital, se consideró capacitar a las MiPymes en los beneficios del uso de TIC, incluyendo la seguridad y protección de datos. A raíz de la Ley para el Impulso de la Sociedad de la Información y el Conocimiento, se creó el Instituto Colimense para la Sociedad de la Información y el Conocimiento, el cual cuenta con una Dirección de Desarrollo Telemático que tiene entre sus funciones el emitir recomendaciones, con la participación de las dependencias y entidades competentes, respecto a las mejores prácticas susceptibles de desarrollarse e implementarse a través de proyectos e iniciativas estratégicas en materia de tecnologías, conectividad y seguridad de la información; así como proponer protocolos de seguridad de la información. Con el Plan Estatal de Desarrollo 2021-2027 se planificó una actualización de la Agenda Digital.	de la Unidad de policía Cibernética en el Estado.		o cualquier otro medio de transmisión de datos, requiera o comparta imágenes, audio o video. En el ámbito de fraude se incluye la manipulación indebida informática.	• Plan Estatal de Desarrollo de Colima 2021-2027 • Agenda Digital Colima • Ley para el impulso de la Sociedad de la Información y el Conocimiento. • Reglamento interior del Instituto Colimense para la Sociedad de la Información y el Conocimiento. • Manual de Organización del Instituto Colimense de la Sociedad de la Información y el Conocimiento • Código Penal para el Estado de Colima
Chiapas	Dentro de la Agenda Legislativa 2021-2024 del Congreso del Estado, se reconoció que la ciberseguridad es una responsabilidad compartida, por lo que se buscará proponer reforzar el marco normativo de las instituciones de seguridad pública haciendo especial énfasis en la capacitación y	Como parte de la Secretaría de Seguridad Ciudadana se cuenta con el Área de la Policía Cibernética quien realiza patrullaje cibernético, efectúa la vigilancia, identificación y		Bajo el delito de fraude, se considera bajo la misma sanción a quien por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice	• Manual de organización de la Secretaría de Seguridad y Protección Ciudadana.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	profesionalización de las distintas corporaciones policíacas con perspectiva de Derechos Humanos, de Género e Interculturalidad.	monitoreo de conductas constitutivas de delito en tecnologías de la información y la red pública de internet; así como prevenir, atender y desarrollar investigación de delitos electrónicos.		operaciones, transferencias o movimientos de dinero o valores. En el marco de suplantación de identidad se considera equiparable a quien, mediante el uso de un medio informático, telemático, electrónico, o el uso de una red electrónica o de internet, monte o cargue sitios de internet falsos o simulados, o intercepte datos de envío. Se tiene tipificado el acceso ilícito a sistemas de informática a quien sin autorización o con ella, pero en perjuicio modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos. Además de agravarse en caso de alguna dependencia pública.	• Agenda Legislativa 2021-2024 del Congreso del Estado de Chiapas • Código Penal para el Estado de Chiapas
Chihuahua	Como parte del Plan Estatal de Seguridad Ciudadana y Procuración de Justicia 2022-2027 en el eje estratégico de "Sistema de Inteligencia y Coordinación Interinstitucional" bajo la estrategia de "Generar productos de análisis de información estadística delictiva; además de información de resultados institucionales; y de aquellos generados por la Inteligencia y análisis criminal, que identifique estructuras delincuenciales y objetivos prioritarios generadores de violencia, además de productos de análisis criminal que tengan fundamentación metodológica y científica derivada del uso de las nuevas tecnologías de la información y comunicación, de la actividad cibernética en Internet, de los análisis de informática forense, y los análisis de contexto criminal, e informes sustentables que abonen al combate de la impunidad, manteniendo una cercanía comunitaria con la policía	En el estado se cuenta con la Dirección de Análisis de Evidencia Digital e Informática Forense, constituida por el Departamento de Informática Forense, el Departamento de Análisis Delictivo y el Departamento de Información Cibernética, perteneciente a la Fiscalía General del Estado. La Dirección de Análisis de Evidencia Digital e Informática Forense es la Unidad de Policía Cibernética del Estado.	A través de un Convenio entre la Universidad Autónoma de Chihuahua y la Fiscalía General del Estado se ha creado un portal de internet para el combate a delitos cibernéticos en instituciones públicas y privadas. Chihuahua Futura, iniciativa con el apoyo del sector privado, gobiernos municipal y estatal, la academia y diferentes organizaciones civiles, gestó el Centro e Ciberseguridad para el municipio de Chihuahua, con el objetivo promover y	Dentro del delito de fraude se considera al que alcance un lucro indebido para sí o para otro, valiéndose de alguna manipulación informática, alteración de programas sistematizados, del empleo no autorizado de datos o artificio semejante. Se encuentra tipificado como delito la destrucción, alteración o perdida contenida en sistema o equipo de informática de oficina o archivos públicos, protegidos por algún mecanismo de seguridad. Bajo los delitos de uso y acceso ilícito a los sistemas informáticos de comunicación se incluyen acceso autorizado o excedido para la copia, modificación, destrucción, deterioro, intercepción o use,	• Sobre la Dirección de análisis de Evidencia Digital e Informática Forense • Reglamento Interior de la Fiscalía General del Estado de Chihuahua. • Portal de Ciberseguridad Chihuahua. • Sobre el Centro de Ciberseguridad C3 • Sobre Chihuahua Futura • Nota. Certificaran a alumnos y docentes en materia de seguridad digital • Plan Estatal de Seguridad

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	preventiva" se incluyó la línea de acción de "Potenciar las áreas con un enfoque de modernidad y vanguardia al contar con mayores capacidades en materia de Ciberseguridad y en una mejor y mayor atención del área de Evidencia Digital e Informática Forense hacia las Fiscalías Regionales y Especializada". Dentro del Programa Sectorial de Gestión y eficiencia Gubernamental de la Secretaría de Coordinación del Gabinete, en el Objetivo 7 de "Disponer de los recursos tecnológicos a las actividades sustantivas de las secretarías para elevar su eficacia, eficiencia y calidad", se incluyó ampliar el equipo dedicado a la Ciberseguridad como una acción.		proveer diferentes soluciones de ciberseguridad a las organizaciones. La Secretaría de Educación y Deporte de Chihuahua puso en marcha el Programa de Chihuahua Digital: Vanguardia en Ciberseguridad, para capacitar a estudiantes y docentes de las Universidades Tecnológicas y Politécnica del Estado de Chihuahua en competencias de esa especialidad.	información contenida en equipos informáticos o de comunicación; o bien, utilice indebidamente, datos o información personal de otro para ostentarse como tal sin consentimiento. Así como el diseño, programación, fabricación de medios para acceso a cualquier dispositivo físico, que tengan por objeto violar uno o más mecanismos de seguridad.	Ciudadana y Procuración de Justicia 2022-2027 de Chihuahua. • Programa Sectorial de Gestión y Eficiencia Gubernamental de la Secretaría de Coordinación de Gabinete de Chihuahua. • Código Penal del Estado de Chihuahua
Ciudad de México	De acuerdo con la Ley de Operación e Innovación Digital para la Ciudad de México, la Agencia Digital de Innovación Pública de la Ciudad de México tiene entre sus atribuciones la de dirigir la entrega y soporte oportuno de servicios tecnológicos de información y comunicaciones interdependenciales, utilizando estándares internacionales de calidad en el servicio, disponibilidad, capacidad, continuidad y seguridad de la información; así como formular los lineamientos de seguridad informática. En materia de Ciberseguridad, en 2019 celebró un convenio con CISCO para realizar eventos en materia de fomento a las TICS, ciberseguridad, creación de habilidades técnicas, de alfabetización y desarrollo digital.	Como parte de la Secretaría de Seguridad Ciudadana se cuenta con la Unidad de Policía Cibernética de la Subsecretaría de Inteligencia e Investigación Policial. La Policía Cibernética tiene la finalidad de prevenir, por medio del monitoreo y patrullaje en la red pública, cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes de la Ciudad de México.	En el Congreso de la Ciudad de México el Diputado Christian Von Roehrich presentó, en enero de 2020, la Iniciativa con Proyecto de Decreto por la que se expide la Ley de Ciberseguridad para la Ciudad de México, en dónde se incluye la creación de una Fiscalía Especializada en Delincuencia Cibernética, una oficina de Ciberseguridad, un Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad, Unidades de Ciberseguridad y una Autoridad Investigadora. La iniciativa fue turnada para su análisis y dictaminación a las comisiones unidas de	Bajo el delito de Fraude se considera al que para obtener algún beneficio para sí o para un tercero, por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución.	• Sobre la Subsecretaría de Inteligencia e Investigación Policial • Iniciativa con Proyecto de Decreto por la que se expide la Ley de Ciberseguridad para la Ciudad de México • Nota "Buscan crear la Ley de Ciberseguridad para la Ciudad de México" • Ley de Operación e Innovación Digital para la Ciudad de México. • Nota. Anuncian colaboración entre Cisco y el Gobierno

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
			Seguridad Ciudadana, y de Ciencia, Tecnología e Innovación.		de la Ciudad de México para apoyar en el desarrollo digital de la Entidad. • Código Penal para el Distrito Federal
Durango	De acuerdo con la Ley de Gobierno Digital del Estado de Durango, la Comisión de Gobierno Digital del estado, tiene entre sus atribuciones el instruir el desarrollo de una plataforma tecnológica que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan los Trámites y Servicios Digitales gubernamentales.	Se cuenta con una Unidad de Política Cibernética perteneciente a la Policía Estatal de la Secretaría de Seguridad Pública del Estado.	El gobierno municipal de Durango por medio de su Dirección de Fomentó Económico, en este año presento 4 diplomados de Capacitación en ciberseguridad por parte de la "Centro de Ciberseguridad 05000".	Bajo el delito de usurpación de identidad se considera equiparable a quien, por el uso de medio electrónico o telemático, obtenga algún lucro indebido para sí o para otro o genere un daño a otro, valiéndose de alguna manipulación informática o intercepción de datos de envío. En el marco de los delitos contra la seguridad en los medios informáticos se tipifica, el acceso a un sistema informático, con o sin autorización, para copiar, imprimir, se use, revele, transmita o se apodere del uso de datos o información reservados. También se considera por separado si el acceso es a un sistema informático de una entidad pública.	• Nota. Policía Cibernética, prevención y asesoría para los duranguenses. • Nota. Diplomados en Ciberseguridad • Ley de Gobierno Digital del Estado de Durango. • Código Penal del Estado Libre y Soberano de Durango
Guanajuato	En el Programa Estatal de Gobierno 2018-2024, como parte de la Agenda Transversal para la Innovación, bajo el objetivo de detonar la innovación y el emprendimiento para el desarrollo sostenible se incluyó como líneas de acción el impulsar programas de capacitación al personal especializado en ciberseguridad. Por parte de la Secretaría de Finanzas, Inversión y Administración se cuenta con los Lineamientos de Tecnologías de la Información y Comunicaciones de la Administración Pública Estatal, en los cuales se incluye un capítulo de prácticas para	Como parte de la Secretaría de Seguridad Pública se cuenta con la Coordinación de la Policía Estatal Cibernética, la cual está adscrita a la Comisaría de Inteligencia de la Comisaría General de las Fuerzas de Seguridad Pública del Estado. La Coordinación tiene el propósito de realizar acciones preventivas y procedimientos basados en inteligencia, análisis de	En el portal del Gobierno del estado, se cuenta con la sección "Efecto-Prevención", un repositorio de artículos, infografías y videos con el objetivo de prevenir cualquier evento que pueda dañar, lesionar o afectar la vida de una persona, una familia o una comunidad y brindar el apoyo que se requiera en caso de que se presente alguna situación que ponga en peligro la vida de	Bajo la categoría de delitos informáticos, se considera el acceso sin consentimiento en una base de datos, sistema, equipos o medios de almacenamiento informáticos, con el propósito de obtener un beneficio indebido; agravando el caso si es en instituciones de seguridad pública. En el rubro de afectación a la intimidad se incluye el divulgar contenido a través de cualquier medio.	• Reglamento de la Secretaría de Seguridad Pública de Guanajuato. • Lineamientos de actuación de la Coordinación de la Policía Estatal Cibernética de Guanajuato. • Portal Efecto Prevención. • Nota. Programa de digitalización Guanajuato.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	salvaguardar la seguridad de la información. Asimismo, la Secretaría cuenta con la Dirección General de Tecnologías de Información, la cual cuenta con la facultad de establecer directrices correspondientes a la seguridad de la información y de los desarrollos de soluciones de sistemas de la administración pública estatal.	modos de operación de actores o grupos delictivos, así como hechos ilícitos donde se utilicen o empleen medios electrónicos y tecnológicos.	las personas. Entre las temáticas se tiene una dedicada a Ciberseguridad. Por parte de la Secretaría de Innovación, Ciencia y Educación Superior en colaboración con CISCO se presentó el Programa de Digitalización Guanajuato que incluye un curso en el marco de Ciberseguridad. Se incluyo la carrera técnica de Ciberseguridad Enel Bachillerato Bivalente Militarizado en León e Irapuato.		• Plan Estatal de Gobierno 2018-2024 de Guanajuato. • Lineamientos de Tecnologías de la Información y Comunicaciones de la Administración Pública Estatal de Guanajuato. • Reglamento interior de la Secretaría de Finanzas Inversión y Administración • Código Penal para el Estado de Guanajuato.
Guerrero		En la Secretaría de Seguridad Pública se cuenta con la Unidad de Policía Cibernética, adscrita a la Subsecretaría de Prevención y Operación Policial, la cual tiene objetivo dirigir las acciones y procedimientos tecnológicos basados en inteligencia, análisis de modos de operación de actores o grupos delictivos, así como hechos ilícitos en cuya comisión se utilicen medios electrónicos y tecnológicos.		En el delito de fraude específico se incluye aquel con la finalidad de obtener algún beneficio se acceda a los sistemas o programas informáticos del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores. Dentro del delito de Usurpación de identidad equiparada se impondrán las mismas penas si por algún uso o medio informático, telemático o electrónico obtenga algún lucro indebido; así como que asuma, suplante, se apropie o utilice a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona que no le pertenezca o utilice sus datos personales para producir un daño moral o patrimonial.	• Decreto por el que se crea la Unidad de la Policía Cibernética de la Secretaría de Seguridad Pública del estado de Guerrero. • Código Penal para el Estado Libre y Soberano de Guerrero.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				También se encuentra tipificado el delito de la divulgación no consentida de imágenes o videos íntimos o sexuales, dónde se incluye las por medio de aplicaciones tecnológicas de mensajería y/o plataformas digitales de sistema de mensajería instantánea por mensaje cortos, de mensajería multimedia, redes sociales digitales u otro sistema de mensajería, sea cual fuese su denominación	
Hidalgo	En el marco de actualización del Plan Estatal de Desarrollo de 2016-2022, se consideró entre las acciones del Gabinete sectorial de Educación y Cultura el Difundir la cultura de prevención de delitos cibernéticos en la población estudiantil hidalguense. Asimismo, en el Gabinete de Seguridad se incluyó como acción el actualizar el código penal en materia de delitos cibernéticos para que responda las necesidades actuales.	Por parte de la Secretaría de Seguridad Pública del estado, Se cuenta con la Policía Cibernética, de la Secretaría de Seguridad Pública. En su portal web, se detalla que se realizan pláticas de prevención de delitos cibernéticos.		Dentro del delito de acceso ilícito a sistemas y equipos de informática se considera aquel que sin consentimiento copie, modifique, destruya, conozca o provoque la pérdida de la información contenida en sistemas o equipos de informática, sumado a que las penas se incrementarán cuando los sistemas pertenezcan a una institución pública estatal o municipal. Bajo el delito de usurpación de identidad no se detalla el medio informático, pero se incluye cualquier medio y con fines ilícitos, se apodere, apropie, transfiera, utilice o disponga de datos personales de otra persona sin autorización de su titular u otorgue su consentimiento para llevar a cabo la usurpación de su identidad. En el rubro de los delitos de violación a la intimidad sexual se incluye el divulgar contenido a través de cualquier medio.	• Reglamento interior de la Secretaría de Seguridad del estado de Hidalgo • Portal de la Unidad de Ciberseguridad. • Plan Estatal de Desarrollo 2016-2022 del Estado de Hidalgo. • Código Penal para el Estado de Hidalgo.
Jalisco	En el marco del Plan Estatal de desarrollo 2018-2024, bajo el eje estratégico de "Seguridad ciudadana, justicia y Estado de	Como parte de la Fiscalía General del Estado de Jalisco, se cuenta con la		Se encuentra tipificado el delito de obtención ilícita de información electrónica, aludiendo a quien sin	• Portal de la Policía Cibernética de Jalisco.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	Derecho, se incluyó entre las estrategias el promover acciones preventivas de hostigamiento, acoso y delitos cibernéticos en centros educativos, culturales, deportivos y comunitarios donde se reúnen niños, niñas y adolescentes.	Unidad de la Policía Cibernética adscrita al Centro de Inteligencia y Comunicaciones para la Seguridad. La Policía Cibernética brinda orientación a la ciudadanía respecto de los pasos que deberá seguir para presentar una denuncia en caso de ser víctima de un delito cometido a través del uso de las tecnologías de la información, además de que la Policía Cibernética colabora con el Ministerio Público de así requerirlo en las investigaciones.		autorización y de manera dolosa, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática. Bajo el delito de suplantación de identidad se consideran equiparables al que por algún uso de medio electrónico, telemático o electrónico obtenga algún lucro indebido; así como al que asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. Bajo el delito de violación a la intimidad sexual se incluye el divulgar contenido a través de cualquier medio.	• Plan Estatal de Desarrollo 2018-2024 de Jalisco. • Código Penal para el Estado Libre y Soberano de Jalisco.
Estado de México	En el marco del Programa Sectorial Pilar Seguridad 2017-2023 del estado, bajo el objetivo de transformar las instituciones de seguridad pública se incluyó en la línea de acción de fortalecer el modelo de inteligencia policial dos actividades específicas: fortalecer, diseñar e implementar estrategias en materia de ciberseguridad con el propósito de proteger y salvaguardar la integridad, patrimonio y derechos de las personas; así como identificar amenazas cibernéticas en contra de instalaciones estratégicas del Estado. Como parte de la Secretaría de Finanzas del estado se tiene la Dirección General del Sistema Estatal de Informática quien es la encargada de promover el uso extensivo y aplicación creativa de las tecnologías de información con el propósito de automatizar	Por parte de la Secretaría de Seguridad del Estado, se cuenta con la Unidad de Policía Cibernética adscrita a la Unidad de Inteligencia e Investigación para la Prevención. La Policía Cibernética implementa procedimientos de vigilancia, identificación, monitoreo y rastreo de la red pública de internet para la prevención y combate de los delitos que se cometan usando medios electrónicos y tecnológicos.	Como una buena práctica es que la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, cuenta con la Dirección General de Servicios Tecnológicos y Plataforma Digital, quien entre sus atribuciones diseña, coordina y supervisa la aplicación, el desarrollo y la difusión de políticas y estándares en materia de seguridad informática, de telecomunicaciones y ciberseguridad para la Secretaría Ejecutiva, Plataforma Digital Estatal y las requeridas por el	Dentro del delito de acoso sexual se incluye quien, sin consentimiento divulgue contenido en forma directa, informática, audiovisual, virtual o por cualquier otro medio.	• Portal de la Policía Cibernética del estado de México. • Programa Sectorial Pilar Seguridad 2017-2023 del estado de México. • Reglamento interno de las Secretaría de Finanzas del estado de México. • Portal. Políticas y lineamientos de seguridad informática. • Portal. Políticas y lineamientos de seguridad de la información.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	los procesos que agilicen los servicios y trámites, y hacer más eficiente la gestión en las oficinas públicas estatales. Asimismo, ha publicado lineamientos y políticas en materia de seguridad informática y de la información.		Sistema Estatal Anticorrupción.		• Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción. • Código Penal del Estado de México.
Michoacán		En la Secretaría de Seguridad Pública del estado se cuenta con la Unidad de Policía Cibernética como una unidad de prevención, atención, vinculación, reacción, respuesta, investigación y gestión, la cual tiene por objeto dirigir las acciones y procedimientos tecnológicos basados en inteligencia, análisis de modos de operación de actores o grupos delictivos, así como hechos ilícitos en cuya comisión se utilicen medios electrónicos y tecnológicos. Dentro de la Procuraduría General de Justicia del estado cuenta con la Fiscalía Especializada en Delitos Cibernéticos, la cual tiene por objeto la investigación y persecución de las conductas criminales en las que se vean inmersos elementos cibernéticos, informáticos y computacionales; así como las conductas típicas antijurídicas culpables,	La Secretaría de Finanzas y Administración del estado cuenta la Subdirección de Gobierno Digital, encargada de promover criterios para el establecimiento de programas y acciones en materia de gobierno digital en las dependencias y entidades. Asimismo, la Subdirección tiene un Departamento de Ciberseguridad.	En el ámbito del delito de violencia digital a la intimidad sexual, se incluye a quien capture la intimidad sexual sin consentimiento, así como comparta a un tercero, publique o amenace con compartir o publicar, incluso se considera como agravante cuando las imágenes, audios, videos o datos se hayan obtenido a través de robo, acceso no autorizado o intervención de comunicaciones o de archivos privados. También se encuentra tipificado la violación de comunicación privada con quien revele, divulgue o utilice, información o imágenes obtenidas en una intervención de comunicación privada.	• Acuerdo por el que se crea la Unidad de Policía Cibernética en Michoacán. • Acuerdo por el que se modifica la denominación y estructura de la Unidad de servicios de Inteligencia de la Procuraduría General de Justicia del estado de Michoacán. • Estructura orgánica del Secretaría de Finanzas y Administración del estado de Michoacán • Manual de organización de la Secretaría de Finanzas y Administración. • Código Penal para el Estado de Michoacán de Ocampo •

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
		relacionadas con el uso de computadoras o medios electrónicos. En este sentido, la "conducta típica antijurídicas culpable" se refiere a los elementos para considerarla como delito. El primero de ellos alude a si se habla de una conducta típica, entendida como aquella que se acomoda a la descripción objetiva, es decir, que contenga voluntad y nexo o relación causal, de una conducta delictiva, por violar un precepto, una norma, penalmente protegida. Respecto a la antijuridicidad, se refiere a que si la conducta es típica o penalmente prohibida sería antijuridica si contraviene al orden jurídico o existe causa que la justifiqué, es decir que se consideré como un ilícito justificado. El último elemento de culpabilidad se sustenta en la reprensión que se hace a quien realizó o participó en el injusto, es decir, que se presente el nexo que une al sujeto con el acto delictivo.			
Morelos	En el Plan Estatal de Desarrollo 2019-2024, bajo el eje rector "Paz y seguridad" dentro del objetivo estratégico de mejorar las condiciones de seguridad pública en el estado para recuperar la paz y la	Por parte de la Comisión Estatal de Seguridad del Estado de Morelos, se cuenta con la Unidad de Policía Cibernética adscrita		Se encuentra tipificado el delito de Ciberacoso sexual, el cuál alude a quien, haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio	• Manual de Organización de la Comisión Estatal de Seguridad del estado de Morelos.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	tranquilidad de los morelenses, generando así las condiciones para su desarrollo humano integral, se incluyó la línea de acción de fortalecer las capacidades e infraestructura tecnológica de la Unidad de la Policía Cibernética. Dentro de la Secretaría de Administración del Estado se cuenta con la Dirección General de Tecnologías de la Información y Comunicaciones, cuyas atribuciones destaca la de fijar las Políticas para la adquisición, implementación y operación de Tecnologías de la Información y Comunicaciones, con el propósito de garantizar la seguridad de la información, su estandarización y optimizando los recursos técnicos y económicos de la Administración Pública Central, basándose en estándares internacionales y mejores prácticas	a la Dirección General de Unidades Especiales.		de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del acoso sexual. Se encuentra tipificado el delito informático, en los que se menciona a quien use o entre a una base de datos, sistema de computadores o red de computadoras para diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar; intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos; o bien, haga uso de la red de Internet para realizar actos en contra de las personas o cosas, que produzcan alarma, temor o terror en la población. Bajo el delito de suplantación de identidad se considera equiparable al que, por algún uso de los medios informáticos o electrónicos, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades.	• Plan Estatal de Desarrollo 2019-2024 del estado de Morelos. • Reglamento interior de la Secretaría de Administración del estado de Morelos. • Código Penal para el Estado de Morelos.
Nayarit		Dentro de la Fiscalía General, se cuenta con la Unidad en Materia de Delitos Cibernéticos, como una de las comandancias de investigación de la Fiscalía.		Dentro del marco de delitos informáticos se consideran a quien utilice o tenga acceso a una base de datos, sistemas o red de computadoras o a cualquier parte de esta para diseñar, ejecutar o alterar, con el fin de defraudar; así como a quien intercepte, interfiera,	• Reglamento interior de la Ley Orgánica de la Fiscalía General del Estado de Nayarit • Código Penal del Estado de Nayarit

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red con el fin de defraudar. También se encuentra tipificado la violación de comunicación privada aquella persona que revele difunda, exponga, divulgue, comparta, distribuya o publique contenido íntimo sexual, erótico o pornográfico, de una persona sin su consentimiento mediante correo electrónico, mensajes telefónicos, redes sociales o por cualquier otro medio electrónico, de almacenamiento o impreso, grabado o digital.	
Nuevo León	Como parte de la Secretaría de Administración se cuenta con la Dirección de Infraestructura Tecnológica, la cual entre sus atribuciones tiene que diseñar, evaluar y publicar políticas y normas en materia de ciberseguridad para el uso de la infraestructura, telecomunicaciones, portales de internet, sistemas y programas integrales tecnológicos.	En la Secretaría de Seguridad Pública del estado se cuenta con la policía cibernética, encargada de prevenir y combatir los delitos en los que se utilicen medios electrónicos y tecnológicos, mediante el ciber patrullaje en la web, el análisis de sistemas, ingeniería social, equipos informáticos y de telecomunicaciones.	En febrero de 2022, el gobierno de Nuevo León y Cisco Networks firmaron un convenio de colaboración para un Programa de Fomento de Habilidades Digitales que incluye entre los cursos uno sobre introducción a la Ciberseguridad. Se cuenta con un clúster de Tecnologías de la Información y Comunicaciones en Nuevo León. En él se encuentra la Secretaría de Economía, la Secretaría de Trabajo y el Instituto de Innovación y Transferencia de Tecnología más actores de la academia e industria. Asimismo, entre los	Dentro de los delitos cometidos en la administración y procuración de justicia se incluye a quien indebidamente conozca, obtenga, copie o utilice información contenida en cualquier sistema informático de alguna institución de seguridad pública o procuración de justicia, protegido por algún medio de seguridad, incluso si se cuenta con autorización de acceso. Asimismo, se encuentra tipificado el delito contra la intimidad personal, a quien (es) revelen, difundan, distribuyan, publiquen o exhiban mediante correo electrónico, mensajes telefónicos, redes sociales o por cualquier otro medio, imágenes, audios o videos de contenido erótico, sexual o pornográfico, de una persona sin su consentimiento.	• Portal. Conoce qué tipo de delitos investiga la policía cibernética y denuncia. • Nota. Anuncian alianza gobierno de NL y CISCO. • Portal Clúster TIC de Nuevo León. • Portal. Sobre los Subcomités del Clúster TIC de Nuevo León. • Reglamento Interior de la Secretaría de Administración. • Código Penal para el Estado de Nuevo León

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
			subcomités del Clúster se encuentra uno sobre ciberseguridad, con el objetivo de crear una cultura de prevención de ataques de ciberseguridad, la elaboración de la estrategia en esta materia, además de buscar resolver la necesidad de contar con capacidades para responder a accidentes e incidentes.	Se tiene contemplado el delito de suplantación de identidad y de fraude, pero no se detalla el caso de medios informáticos, pero como regla común se aumentará la pena su se utilizó un instrumento electrónico. En el marco del delito de robo se contempla el apoderamiento material o mediante vía electrónica de los documentos que contengan datos en computadoras, o el aprovechamiento o utilización de dichos datos.	
Oaxaca	Por parte de la Secretaría de Administración del Estado se cuenta con la Dirección General de Tecnologías de Innovación Digital (DGTID), la cual tiene el objetivo de consolidar, dirigir y administrar el uso y aprovechamiento de la infraestructura tecnológica, informática, de telecomunicaciones, de internet, así como también de todos los centros de cómputo de las Entidades y Dependencias de la Administración Pública Estatal,, impulsando el desarrollo de la automatización, la ciberseguridad e innovación digital que fortalezca la provisión de servicios en línea a la ciudadanía oaxaqueña público en general. Por parte de la DGTID se cuenta con un Manual de Políticas de Seguridad de la Información para el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones en las Dependencias de la Administración Pública del Estado de Oaxaca.	Por parte de la Secretaría de Seguridad Pública del Estado se cuenta la Unidad de Policía Cibernética, la cual brinda orientación a la ciudadanía en relación con el proceso que deben seguir para presentar una denuncia en caso de ser víctima de un delito cometido a través del uso de las tecnologías de la información. Los policías cibernéticos monitorean sitios web y fuentes abiertas y realizan campañas informativas y preventivas en Instituciones Educativas en el Estado. También atienden denuncias ciudadanas y asesoran a los ciudadanos para el uso correcto y seguro de las tecnologías de la información.		Se encuentra tipificada la divulgación ilícita de información clasificada de la base de datos o sistemas informáticos de las instituciones de seguridad pública. También se considera el delito de suplantación de identidad digital como quien, mediante alguna manipulación de medios electrónico se apodere, transfiera, utilice o disponga de información personal, documentos, imágenes o correos electrónicos. En el marco de los delitos contra la seguridad informática y electrónica se consideran el delito de defraudación informática a quien, sin autorización, altere, modifique, borre, destruya o disponga de datos o información contenida en un sistema informático divulgue, por cualquier medio, datos o información contenida. Asimismo, se detalla el delito de intrusión informática, para aquél que intercepte, interfiera o acceda a la información contenida en un	• Facebook de la Unidad de Policía Cibernética de Oaxaca. • Nota. Atiende policía Cibernética en Oaxaca 486 Denuncias en 2018. • Decreto que crea la Dirección General de Tecnologías e Innovación Digital. • Manual de políticas de Seguridad de la Información para la Administración Pública de Oaxaca. • Portal que es la DGTID de Oaxaca. • Código Penal para el Estado Libre y Soberano de Oaxaca

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				sistema informático sin autorización. Y de igual forma se tiene tipificado a quien diseñe, programe, fabrique, introduzca, importe, exporte, comercialice o distribuya programas que tenga por objeto violar uno o más mecanismos de seguridad de equipos informáticos; y al que destruya datos contenidos en un sistema informático o electrónico, a través de la introducción de algún virus. Además, las penas se duplicarán si las acciones se ejecutan contra sistemas, equipos u otros dispositivos informáticos o electrónicos del Estado o Municipios; cuando los datos o información contenida en un sistema informático o electrónico, se refieran a datos personales o datos personales sensibles; o cuando las conductas delictivas sean realizadas por personas con acceso autorizado.	
Puebla	En enero de 2020 se modificó la Ley de Planeación para el Desarrollo del Estado de Puebla mediante el cual se creó el Comité de Planeación para el Desarrollo del Estado de Puebla (COPLADEP). El COPLADEP es el órgano público, colegiado e interinstitucional en materia de planeación, cuyos objetivos fundamentales son promover y coadyuvar en la formulación, actualización, instrumentación y evaluación del Plan Estatal de Desarrollo y de los programas sectoriales, especiales y regionales, mediante la participación del sector público, social y privado, en el marco del Sistema Estatal de Planeación Democrática. El COPLADEP se apoya de Subcomités que fungen como órganos auxiliares. En el	Dentro de la Secretaría de Seguridad Pública se cuenta con Dirección de Policía Estatal Cibernética adscrita la Dirección General de Servicios Técnicos. La Policía Cibernética realiza funciones de Atención ciudadana, prevención del delito, investigación de fenómenos delictivos, patrullaje web y coadyuva con líneas de investigación de Fiscalía General del Estado (FGE) y Fiscalía General de la República (FGR).		Bajo el delito de Ciber acoso se considera a quien hostigue o amenace por medio de las TICS, redes sociales, correo electrónico o cualquier espacio digital y cause un daño en la dignidad personal, o afecte la paz, la tranquilidad o la seguridad de las personas. Bajo el delito de fraude se reconoce al que dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, dañe o perjudique el patrimonio de otro, mediante el uso indebido de mecanismos cibernéticos. En el rubro de delitos informáticos se considera, al que sin autorización	• Reglamento Interior de Secretaría de Seguridad Pública del Estado de Puebla. • Ley de Planeación para el Desarrollo del Estado de Puebla • Lineamientos para el funcionamiento del COPLADEP • Subcomité de Gobierno Democrático, innovador y trasparente. Informe

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	Subcomité de Gobierno Democrático, Innovador y Transparente, en 2020 se instaló el Grupo de Trabajo Intersecretarial de Ciber Seguridad. También en 2021 se llevó a cabo la identificación, alineación y la propuesta de mejores prácticas en materia de TIC, las cuales fueron apegadas a las Normas: Gestión de Configuraciones y Activos, Gestión de Incidentes, Gestión de Seguridad de la Información y Gestión de Cambios. De acuerdo con el Reglamento Interior de la Secretaría de Administración, la Subsecretaría de Transparencia y Gobierno Digital, a través de la Dirección General de Gobierno Digital y demás direcciones, está facultada para que, de forma transversal, defina, implemente y monitoree la seguridad de la información en los sistemas y la infraestructura tecnológica de las dependencias y entidades a resguardo de la Secretaría de Administración.			modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad; al que con o sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado o de seguridad pública; así como a quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan. Se encuentra tipificado el delito de violación a la intimidad sexual para quien divulgue contenido erótico sexual sin consentimiento por cualquier medio.	Anual de Trabajo 2020. • Subcomité de Gobierno Democrático, innovador y trasparente. Informe Anual de Trabajo 2021. • Reglamento Interior de la Secretaría de Gobernación. • Código Penal del Estado libre y soberano de Puebla
Querétaro	Dentro de la Secretaría de Planeación y Finanzas se cuenta con la Dirección de Tecnologías de la Información la cual entre sus atribuciones tiene que implementar medidas de seguridad que garanticen la integridad y confidencialidad de la información, para brindar estabilidad y disponibilidad en los servicios de tecnologías de la información para las dependencias del Poder Ejecutivo y sus órganos desconcentrados. En este sentido en 2021 emitió la Normatividad de TIC del Poder Ejecutivo del Estado de Querétaro, el cual incluye una sección tercera de la seguridad.	Por parte de la Secretaría de Seguridad Ciudadana del Estado de Querétaro en la Unidad de Análisis e Información se cuenta con un Área de Policía Cibernética, la cual entre sus funciones implementa procedimientos de vigilancia, identificación, monitoreo y rastreo de la red pública de internet para la prevención y combate de los delitos que se cometen a través de los medios electrónicos y tecnológicos; así como recopilar, analizar y explotar información con la finalidad de identificar, disuadir, prevenir y combatir	En 2020, en el municipio de Marques, Ernest and Young inauguraron el Centro de Operaciones de Ciberseguridad, el cual ofrece servicios de monitoreo de seguridad, respuesta a incidentes, gestión de vulnerabilidades e inteligencia de amenazas para el sector privado.	Bajo el delito de falsificación y uso indebido de documentos se tiene contemplado a quien adquiera, utilice o detente equipos electromagnéticos, electrónicos o de comunicación remota para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas, tarjetas de crédito, tarjetas de débito u otros documentos. Se contempla el delito de fraude, pero no se detallan medios electrónicos o informáticos en los supuestos.	• Reglamento de la Ley de la Secretaría de Seguridad Ciudadana del Estado de Querétaro. • Reglamento orgánico de la Secretaría de Seguridad Pública del Municipio de Querétaro. • EY. Sobre Centro de Operaciones de Ciberseguridad, CYBERSOC. • Reglamento Interior de la Secretaría de Planeación y Finanzas.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
		delitos que utilizan como medio, origen o destino las tecnologías de información y comunicación. Asimismo, a nivel municipal, el municipio de Querétaro cuenta con la policía cibernética preventiva municipal, la cual se encuentra bajo la supervisión de la persona titular de la Unidad de Análisis e Inteligencia Policial para la Prevención y Combate al Delito de la Secretaría de Seguridad Pública del Municipio de Querétaro.			• Normatividad de TIC del Poder Ejecutivo del Estado de Querétaro. • Código Penal del Estado de Querétaro
Quintana Roo		Se cuenta con la Unidad de Policía Cibernética adscrita a la Dirección de la Unidad de Inteligencia de la Secretaría de Seguridad Pública del Estado de Quintana Roo.	El Instituto Quintanarroense de Innovación Tecnología ha coordinado una Estrategia de Capacitación "Jus4Geelks", en la cual se incluye entre sus acciones el Desarrollo de API (Application Programming Interfaces) de trámites y servicios gubernamentales con el objetivo de garantizar mejor calidad de los servicios públicos, menores costos de transacción para la gente, más transparencia, y más ciberseguridad para los quintanarroenses.	Se encuentra tipificado el ciberacoso sexual, como quien, con fines lascivos y utilizando la coacción, intimidación, inducción, seducción o engaño, entable comunicación a través de cualquier TIC, con una persona menor de 18 años de edad o persona que no tiene capacidad para comprender el significado del hecho aún con su consentimiento. También, se tiene contemplado el delito de violencia digital considerando a quien difunda, revele, publique, comparta o altere contenido audiovisual, conversaciones telefónicas, grabaciones de voz, imágenes estáticas o en movimiento, de naturaleza sexual o erótica de otra persona, mayor de edad, sin su consentimiento a través de	• Reglamento interno de la Secretaría de Seguridad Pública del Estado de Quintana Roo. • Instituto Quintanarroense de Innovación Tecnológica Modelo de Transformación Digital de Quintana Roo. • Código Penal para el Estado Libre y Soberano de Quintana Roo

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				cualquier TIC, medio digital o impreso. Bajo el delito de usurpación de identidad se incluye aquel que por algún uso del medio informático, telemático o electrónico, o use la red de Internet montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecta la confiabilidad y variación de la navegación de la red para obtener lucro indebido. En el rubro de falsificación de documentos y uso de documentos falsos se considera a quien accede indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.	
San Luis Potosí	En enero de 2016 se creó la Unidad de Sistemas e Informática (USI) por medio de un Acuerdo Administrativo. La USI es la encargada de implementar la política pública de Gobierno Digital en la administración pública estatal, a través del uso y aprovechamiento estratégico de las Tecnologías de la Información. Como parte de la USI se cuenta con una Dirección de Seguridad Informática, la cual tiene entre sus atribuciones el desarrollo e implementación de políticas de seguridad y esquemas de	Se cuenta con una Unidad de Policía Cibernética, constituida por elementos de la Dirección General de Tecnologías de la Información e Inteligencia en Seguridad Pública, es parte de la estructura de la Secretaría de Seguridad Pública, en ella se llevan a cabo acciones de prevención a través de	En 2019 se expidió el Esquema en materia de conectividad y seguridad a fin de que las dependencias y entidades de la Administración Pública del Estado cuenten con un instrumento para la implementación de la seguridad de la información. El esquema está a cargo de la USI.	Dentro del delito contra la identidad de las personas se considera a quien se atribuya por medios electrónicos, informáticos, redes sociales o cualquier otro medio, la identidad de otra persona causando un daño patrimonial, moral, o algún lucro indebido. También se considera equiparable si por algún uso de medio electrónico, telemático o	• Ley del Sistema de Seguridad Pública del Estado de San Luis Potosí. • Diagnóstico del estado de fuerza y capacidades institucionales del estado de San Luis Potosí. 2019. • Acuerdo Administrativo,

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	conectividad, basados en mejores prácticas, entre otras. En el marco del Plan Estatal de Desarrollo 2021-2027, como parte del tema de Gobierno digital para la certidumbre patrimonial, el Objetivo sobre "Promover el desarrollo estatal con políticas de innovación gubernamental, tecnologías de información y comunicación para fortalecer la confianza ciudadana en sus instituciones" bajo el cual se integra la Estrategia 1.2 de "Propiciar un entorno de certeza y confianza favorable para la adopción y el uso de las TIC", en la cual resalta la línea de acción de "Concientizar en la privacidad y protección de datos personales, respecto a la seguridad de la información y los delitos informáticos a los que estamos expuestos, entre los funcionarios públicos de las dependencias y entidades de las Administración Pública Estatal involucrados en la transformación digital del Estado y la ciudadanía". Asimismo, bajo el tema de paz y seguridad, en el marco de la estrategia de "Desarrollar acciones integrales mediante la implementación de infraestructura tecnológica para realizar actividades operativas en materia de Prevención Social del delito" se consideró la línea de acción de realizar campañas de información para prevenir a la ciudadanía sobre delitos cibernéticos y el mecanismo de atención a víctimas.	capacitaciones a diferentes instituciones educativas y empresas públicas y privadas, así como a funcionarios de la Fiscalía General del Estado, con quien se establece una coordinación permanente. La Policía Cibernética es la encargada de prevenir, atender y combatir incidentes que se cometen a través de medios digitales, además de coadyuvar con las Fiscalías, así como autoridades jurisdiccionales.	Actualmente cuenta con una guía de implementación. En la LXII Legislatura del Congreso del Estado de San Luis Potosí, el 19 de octubre de 2020 se presentó una iniciativa ciudadana de nueva ley mediante la cual se buscaba expedir la Ley de Ciberseguridad para el Estado y sus Municipios, misma que fue declarada improcedente. En la LXIII legislatura el 13 de septiembre de 2021 se volvió a presentar con un resultado de improcedente. Sin embargo, en el marco de la sesión de trabajo de la Comisión de Justicia se reconoció la relevancia del tema y para fortalecer la iniciativa se determinó allegarse de más información que permita que la autoridad estatal cuente con los recursos para su aplicación, además de ampliar sus alcances para lograr la vinculación con las autoridades federales en la materia.	electrónico se obtenga algún lucro indebido para sí o para otro, valiéndose de alguna manipulación informática o intercepción de datos de envío. Así como a quien asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. En el delito de abuso sexual equiparado se considera a quien mediante el uso de medios electrónicos o de cualquier tecnología, contacte, obligue, induzca o facilite a una persona menor de dieciocho años, o de una persona que por su condición no tenga la capacidad de comprender el significado del hecho, o que no tiene capacidad para resistirlo, a realizar actos de exhibicionismo corporal o sexuales simulados o no. Se considera delito de difusión ilícita de imágenes a quien transmita, publique, o difunda imágenes, sonidos o grabaciones de contenido sexual, que pueden o no contener texto, obtenidas con o sin el consentimiento de la víctima, sin autorización para su difusión por cualquier medio.	mediante el cual se crea la Unidad de Sistemas e Informática del Poder Ejecutivo de San Luis Potosí. • Reglamento interior de la Unidad de Sistemas e Informática • Esquema estatal de conectividad y seguridad • Página del esquema estatal de conectividad y seguridad • Plan Estatal de Desarrollo 2021-2027 • Iniciativas de la LXII legislatura del Congreso del estado de San Luis Potosí. • Iniciativa ciudadana para nueva ley, mediante la cual se expira la "Ley de Ciberseguridad de SLP". 20 de octubre de 2020 • Iniciativas de la LXIII del Congreso del estado de SLP. • Iniciativa ciudadana para nueva Ley de Ciberseguridad de SLP. 13 de

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
					septiembre de 2021. • Congreso del Estado de SLP. Análisis de iniciativa de Ciberseguridad. • Código Penal del Estado de San Luis Potosí.
Sinaloa		La Fiscalía General cuenta con Fiscalías y Unidades Especializadas las cuáles apoyan con la investigación científica de los delitos, como es el caso de la Agencia del Ministerio Público Especializada en Delitos contra el Patrimonio, la cual tiene entre sus funciones la investigación científica de delitos de abuso de confianza, fraude, delitos informáticos, despojo, usura y encubrimiento por receptación, de acuerdo con el Código Penal para el Estado de Sinaloa. . Dentro de la Secretaría de Seguridad Pública de Sinaloa, no se cuenta con una Unidad de Policía Cibernética, sin embargo, la Dirección de Programas Preventivos es quien ha llevado a cabo programas para informar sobre los delitos informáticos como "Conecta Seguro", el cual busca sensibilizar a la población acerca de redes	En diciembre de 2020 se presentó una iniciativa para expedir la Ley de Ciberseguridad del Estado de Sinaloa por parte de la Diputada Jesús Angélica Díaz Quiñónez y del Diputado Víctor Antonio Corrales Burgueño. La iniciativa fue turnada a la Comisión de Ciencia y Tecnología u quedó como asunto pendiente de la pasada legislatura 2018-2021. La iniciativa tiene como objetivo garantizar la seguridad cibernética del Estado de Sinaloa y sus Municipios, la seguridad cibernética será una herramienta utilizada y aprovechada para garantizar la gobernabilidad del Estado de Sinaloa, y como una capacidad de alto nivel, para coadyuvar en el desarrollo tecnológico, político, económico y social.	Dentro del delito de suplantación de identidad se considera equiparable al que, por algún uso de medio informático, telemático o electrónico, obtenga algún lucro indebido para sí o para otro o, genere un daño patrimonial, mediante el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizadas para suplantar identidades. Además de que se incluye a quien asuma, se apropie o utilice indebidamente a través de internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca para ostentarse como tal. En el delito de acoso sexual se reconoce que se incurre en él si quien sin consentimiento y en perjuicio de la intimidad del sujeto, con propósitos de lujuria o erótico sexual, grabe, reproduzca, fije, ofrezca, almacene, importe o exporte de cualquier forma, imágenes, texto, sonidos o la voz, de una persona, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio.	• Secretaría de Seguridad y Protección Ciudadana. Programa de Fortalecimiento de Capacidades para la Prevención y Combate a Delitos de Alto Impacto. • Nota. Oferta Secretaría de Seguridad Pública programas preventivos dirigido a niñez y adolescencia • Iniciativa de proyecto de Decreto por el que se propone expedir la Ley de Ciberseguridad del Estado de Sinaloa. • Comisión de Ciencias y Tecnología del Congreso de Sinaloa. Informe de Actividades Correspondiente periodo del 1 de octubre de 2020 al

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
		sociales, protección de la intimidad, grooming, usurpación de identidad, fraudes y extorsiones.		Bajo el delito informático se contempla a quien use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; así como al que intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. En el marco del delito de violación a la intimidad sexual se incluye el de violación a la misma al divulgar contenido digital.	31 de enero de 2021. • Informe 2021 de la Fiscalía General del Estado de Sinaloa. • Código Penal para el Estado de Sinaloa
Sonora	Se cuenta con el Comité de Desarrollo Tecnológico, un organismo de participación colegiada de las dependencias y entidades del gobierno para planear, organizar, difundir, evaluar y vigilar lo referente al uso de las TIC. El Comité cuenta con un Manual de Políticas y estándares de seguridad informática a fin de unificar criterios entre las áreas y procesos destinados a sistematizar la gestión pública y en cumplimiento a la responsabilidad de impulsar la modernización y aprovechamiento óptimo de los recursos informáticos y tecnológicos del Gobierno Estatal.	Como parte de la Secretaría de Seguridad Pública de Sonora se cuenta con la Dirección General de la Unidad cibernéticas adscrita directamente al secretario.		En el delito de Violación a la Intimidad se reconoce a quien exponga, distribuya, exhiba, genere, videograbe, audiograbe, fotografíe, filme, elabore, reproduzca, transmita, comercialice, oferte, intercambie, reciba u obtenga, información privada por medio de amenazas, engaño, vulneración de datos o cualquier otro; revele o divulgue, información apócrifa, alterada o difunda sin consentimiento de la persona afectada o su derecho a la identidad personal o se realice cualquier forma de violencia digital, mensajes de texto, imágenes, textos o grabaciones de voz o conversaciones o audiovisuales y las publique en redes sociales, correo electrónico o las difunda por cualquier otro	• Reglamento Interior de la Secretaría de Seguridad Pública del Estado de Sonora. • Sobre el Comité De Desarrollo Tecnológico del Estado de Sonora. • Manual de políticas y Estándares de Seguridad Informática del Estado de Sonora. • Código penal del Estado de Sonora

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				medio digital, impreso o tecnológico, Dentro de los delitos contra el funcionamiento del sistema estatal de seguridad pública se reconocen se reconoce como delito a quien acceda sin autorización o sin tener derecho para hacerlo, a la información contenida en las bases de datos del Sistema Estatal de Seguridad Pública; así como a quien ingrese dolosamente o permita dolosamente el acceso de información errónea o indebida, o que dañe o pueda dañar en cualquier forma la información, las bases de datos o los equipos o sistemas que contengan la información del Sistema Estatal de Seguridad Pública. Se contempla el delito de usurpación de identidad o personalidad, sin embargo, no se detalla el medio electrónico o informático, pero se alude al que por cualquier medio usurpe la personalidad o identidad.	
Tabasco	Por parte de la Secretaría de Administración, la Dirección General de Tecnologías de Información y Comunicaciones es la responsable de dirigir y establecer las políticas, normas y programas en materia de tecnologías de la información y la comunicaciones, incluyendo, administración del conocimiento, bienes y servicios con integración parcial y total de sistemas de cómputo y comunicaciones de seguridad e integridad de los datos e información, ente otros de las Dependencias, Órganos y Entidades de la Administración Pública. En este sentido ha emitido las Políticas, normas y Estándares en TIC para el gobierno	Se cuenta con una Unidad de Policía Cibernética llamada Unidad de Investigación de Delitos Informáticos adscrita la Fiscalía General del Estado de Tabasco. Dicha Unidad tiene la finalidad de detectar hechos delictivos cometidos a través de medios informáticos o electrónicos, los cuales serán detectados mediante el ciberpatrullaje, denuncias anónimas, y con esto	Durante 2021 se implementó el Chatbot de ciberseguridad del CONALEP y U-Report México para prevenir el ciberacoso entre la población estudiantil, interactuando con ellos a través del Whatsapp donde recibirán información relacionada.	Dentro del delito de suplantación de identidad se considera equiparable a quien mediante el uso de un medio informático, telemático o electrónico obtenga un lucro indebido o genere un daño patrimonial a otro, valiéndose de alguna manipulación informática o intercepción de datos de envió, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a bases de datos automatizados para suplantar identidades	• Portal de la Unidad de investigación de Delitos Informáticos. • Evaluación Estratégica de la Política de Seguridad Pública y Protección Ciudadana del Ejercicio Fiscal 2021: Tabasco. • Reglamento interno de la Secretaría de Administración de Tabasco.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	de Tabasco con un capítulo dedicado a la Seguridad de la Información para promover una cultura de seguridad de la información en el ámbito de la Administración Pública Estatal. Asimismo, ha publicado un Manual de Seguridad Informática como material de consulta. Como parte del Programa Estatal de Protección de los derechos de Niñas, Niños y Adolescentes 2021-2024, se incluyó entre las acciones el definir una estrategia de ciberseguridad dirigida a madres, padres, personas cuidadoras, niñas, niños y adolescentes para contribuir a la prevención de las violencias, reducir la brecha digital e impulsar la navegación segura a fin de realizarse de forma conjunta entre la Fiscalía General del Estado y la Unidad del Secretariado Ejecutivo del Sistema Estatal de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes del Estado de Tabasco.	conocer los sitios, modus operandi y responsables de las diferentes conductas delictivas a fin de proteger a las personas en general y especialmente a niñas, niños, adolescentes y grupos en condición de vulnerabilidad.		En el rubro de los delitos contra la seguridad en los medios informáticos y magnéticos se enlista el de acceso sin autorización para al que intercepte, interfiera, reciba, use o ingrese por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal, o a un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos; el de daño informático, a quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, sistemas o redes de cómputo; y el de falsificación informática, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos, soporte lógico, siempre que para ello se requiera autorización y no la obtenga. Se encuentra tipificado el delito de sexting en el que se contempla a quien reciba u obtenga de una persona, imágenes, textos o grabaciones de voz o audiovisuales de contenido erótico, sexual o pornográfico de aquélla y las revele, publique, difunda o exhiba sin su consentimiento, a través de mensajes telefónicos, publicaciones en redes sociales,	• Políticas, normas y Estándares en las TIC para el gobierno de Tabasco. • Manual de Seguridad Informática Básica. • Programa Estatal de Protección de los Derechos de Niñas, Niños y Adolescentes 2020-2024. • 3er Informe de Gobierno de Tabasco 2021. • Código Penal para el Estado de Tabasco.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				correo electrónico o por cualquier otro medio.	
Tamaulipas	Por parte de la Secretaría de Administración se cuenta con la Subsecretaría de Innovación y Tecnologías de la Información, la cual entre sus atribuciones tiene que asegurar el diseño y establecimiento del esquema de seguridad informática para los centros de cómputo y las aplicaciones e infraestructura del Gobierno del Estado bajo normas internacionales; verificando su instalación y mantenimiento.	Por parte de la Secretaría de Seguridad Pública se cuenta con la Unidad de Policía Cibernética adscrita a la Dirección de Análisis e Inteligencia. Asimismo, la Fiscalía General de Justicia del Estado dentro de su policía de investigación cuenta con una subinspección de la policía cibernética.		Se tiene tipificado el delito de ciberacoso como a quien hostigue o amenace por medio de las TIC, tales como redes sociales, mensajería instantánea, correo electrónico o cualquier otro medio digital y cause un daño en la dignidad personal, o afecte la paz, la tranquilidad o la seguridad de las personas. Se consideran como delitos de acceso ilícito a sistemas de equipo de informática el de al que sin autorización o sin ella modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso incluyendo el caso específico de que la propiedad sea de alguna dependencia pública; o que en su caso use, utilice, copie o modifique información contenida en sistemas o equipos de informática. Dentro del delito de robo de identidad se considera a quien por cualquier medio usurpe o suplante la identidad de una persona con fines ilícitos a través de medios electrónicos, informáticos, redes sociales o cualquier otro medio de comunicación, con el propósito de causar un daño patrimonial, moral, psicológico, ya sea para beneficio propio o de otra persona. En este sentido se considera equiparable el caso de que diseñe herramientas, tecnología digital o programas	• Reglamento interior de la Secretaría de Seguridad Pública del Estado de Tamaulipas. • Reglamento de la Policía de Investigación de la Fiscalía General de Justicia del Estado de Tamaulipas • Reglamento interno de la Secretaría de Administración de Tamaulipas. • Código Penal para el Estado de Tamaulipas

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				informáticos, que tenga como propósito atacar bases de datos públicos o privados, donde se resguarde información sobre identidad de personas; así como acceda ilegalmente a un sistema informático que contenga datos sobre la identidad de personas. También se tiene tipificado el delito de violación a la intimidad para quien difunda contenido íntimo por cualquier medio.	
Tlaxcala	Dentro de la Ley de Archivos del Estado de Tlaxcala se detalla que los Titulares de las entidades públicas garantizarán que se elaboren los instrumentos de descripción archivística correspondientes al ámbito de su competencia de acuerdo con los estándares nacionales e internacionales bajo el principio de la seguridad de la información, mediante el establecimiento de niveles de acceso de acuerdo con las funciones, atribuciones y derechos de los interesados y de los usuarios.	Por parte de la Secretaría de Seguridad Ciudadana del estado se cuenta con una Unidad de Policía Cibernética perteneciente a la Dirección de Inteligencia para la Prevención. Dicha Unidad tiene el objetivo de vigilar, identificar y monitorear el ciberespacio, con el propósito de prevenir e identificar conductas delictivas, así como atender y desarrollar la investigación de delitos electrónicos, informáticos y/o cibernéticos.	Como una buena práctica es que la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Tlaxcala considera una Oficina de Sistemas y Plataformas Digitales, la cual de sus atribuciones destaca que propone, ejecuta y evalúa las políticas de informática, sistemas, seguridad de la información y ciberseguridad de la Secretaría. En 2020 se creó la ingeniería de Redes Inteligentes y Ciberseguridad dentro de la Universidad Tecnológica de Tlaxcala.	En el rubro de delitos conta la seguridad en los medios informáticos se contemplan a quien sin autorización o con autorización acceda a sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita o se apodere de datos o información reservados. En este sentido la conducta se agravará en el caso de dicho sistema pertenezca a una entidad pública y podrían incrementar las penas si el sistema es concerniente al régimen financiero de las entidades públicas o es cometido por funcionarios o empleados que estén a su servicio; así como se haya afectado un sistema o dato referente a la salud, administración de justicia, procuración de justicia, seguridad pública o a la prestación de cualquier otro servicio público. En el delito de fraude se considera equiparable al que alcance un lucro indebido para sí o para otro, valiéndose de alguna manipulación informática, alteración de programas	• Manual de Organización de la Secretaría de Seguridad Ciudadana de Tlaxcala. • Reglamento interior de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de Tlaxcala. • IV Informe de Gobierno. 2020. Estado de Tlaxcala. • Ley de Archivos del Estado de Tlaxcala • Código Penal para el Estado Libre y Soberano de Tlaxcala.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				sistematizados, del empleo no autorizado de datos. También se tiene tipificas el delito de violación a la intimidad sexual a quien divulgue contenido íntimo, sexual o erótico sin consentimiento de la víctima ya sea impreso, grabado o digital.	
Veracruz	De acuerdo con la Ley Orgánica del Poder Ejecutivo del Estado de Veracruz le corresponde a la Secretaría de Finanzas y Planeación del Gobierno del Estado de Veracruz, entre otras, integrar y mantener actualizada la informática del Estado, en este sentido ha expedido las Políticas para la seguridad de la Información, Seguridad Informática y desarrollo de Software en la Administración Pública del Estado de Veracruz. También la Secretaría de Finanzas y Planeación orienta y establece las disposiciones para optimizar el uso de la infraestructura de los servicios digitales disponibles para las Dependencias y Entidades del Ejecutivo, primordialmente para establecer la Ciberseguridad en su Centro de Datos de la Secretaría, en la emisión de Comprobantes Fiscales Digitales por Internet y la Oficina Virtual de Hacienda del Estado; el desarrollo e innovación de sistemas digitales que provoquen un ejercicio de la función pública eficiente, expedito y transparente. Asimismo, se han generado recomendaciones por parte de la Administración Estatal sobre la navegación con seguridad.	Por parte de la Secretaría de Seguridad Pública se cuenta con la Unidad de Policía Científica Preventiva perteneciente al Centro Estatal de Control, Comando, Comunicaciones y Computo. Dicha Unidad se encarga de la prevención de delitos cibernéticos.		En el ámbito de delitos informáticos de reconocen a quien ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; al igual que intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red. También al que sin autorización o con autorización modifique, destruya o provoque pérdida, conozca, copie o utilice información del estado o de una instancia seguridad pública. Además de que, si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación. Bajo el delito de fraude se incluye a quien, por cualquier medio, ingrese a sistemas o programas de informática de naturaleza financiera e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, con el propósito de obtener algún beneficio para sí o de un tercero. En el caso del delito de suplantación de identidad se	• Manual Especifico de la Organización de la Dirección General del Centro Estatal de Control, Comando, Comunicaciones y Cómputo. • Políticas para la seguridad de la Información, Seguridad Informática y desarrollo de Software en la Administración Pública del Estado de Veracruz. • Proyecto de Presupuesto Estatal de Veracruz. Ejercicio Fiscal 2021. • Portal. Navega con seguridad del Gobierno de Veracruz. • Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				toman en cuenta la conducta al que, por algún uso de los medios informáticos o electrónicos, suplante identidades, con el propósito de generar un daño patrimonial o moral u obtener un lucro indebido para sí o para otro. Igualmente, se considera el delito de violación a la intimidad sexual a quien divulgue contenido intimo ya sea impreso, grabado o digital, sin el consentimiento de la víctima.	
Yucatán	Como parte de la agenda 2040 de Yucatán bajo el eje rector de "Yucatán con Seguridad Paz Justicia y buen gobierno", se incluyó la estrategia de Fortalecer las capacidades en el estado en materia de Ciberseguridad a través de 6 líneas de acción: establecer diagnósticos sobre el entorno de la ciberseguridad en el estado; promover normativas y procesos en materia de ciberseguridad; establecer alianzas estratégicas entre gobierno, sociedad y organizaciones privadas para la promoción de la ciberseguridad; impulsar el establecimiento de indicadores de seguimiento en materia de ciberseguridad; poner en marcha proyectos de difusión de temas de ciberseguridad; y reforzar la profesionalización en materia de ciberseguridad. En el marco del Plan Estatal de Desarrollo 2018-2024, en el objetivo 7.1 de Preservar altos niveles de paz en el Estado, se incluyó la línea de acción de capacitar a la población para la prevención, detección y denuncia de los delitos cibernéticos.	De acuerdo con el Primer Informe de Gobierno.2019 del gobierno de Yucatán, la Secretaría de Seguridad Pública ha integrado un grupo especializado para atender delitos cibernéticos, el cual interactúa con la Unidad Especializada de Delitos Cibernéticos de la Fiscalía General del Estado. Pública (SESNSP). Asimismo, la Fiscalía General del Estado cuenta con funciones de prevención del delito en materia cibernética dentro de la Unidad Especializada en Atención a los Delitos cometidos por Medios Electrónicos y Cibernéticos.	En 2021 el Sistema de Investigación, Innovación y Desarrollo Tecnológico del Estado de Yucatán (SIIDETEY), mediante la atención a delegaciones visitantes se vinculó a diversos miembros del SIIDETEY con sus contrapartes en países como Finlandia e Israel para establecer mecanismos de cooperación en temas como inteligencia artificial y ciberseguridad.	Se encuentran tipificados como delitos informáticos y cibernéticos al que sin autorización, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos informáticos protegidos por algún mecanismo de seguridad; incluyendo a quien sustraiga, elimine o cambie información contenida en él; con la intención de provocar un desperfecto en su funcionamiento que lo deje total o parcialmente inoperable; intercepte comunicaciones privadas con la intensión de recabar información personal o financiera. Además, se contempla al que estando autorizado para acceder a sistemas y equipos de informática del Estado, sustraiga información para beneficio personal o ajeno, o quien facilite esto a un tercero que no cuente con autorización, así como modifique o provoque perdida de información También se incluye a quien utilizando información que aparente provenir de instituciones financieras o empresas de servicios	• Informe de Resultados 2019. Respuestas a las preguntas del Congreso de Yucatán. • Facebook de la Unidad Cibernética de Yucatán. • Agenda 2040. Yucatán con Seguridad, Paz, Justicia y buen Gobierno. • Plan Estatal de Desarrollo 2018-2024 de Yucatán. • Código Penal del Estado de Yucatán

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
				informáticos o electrónicos o dependencias del Poder Ejecutivo u otro poder u organismo del estado: provoque la instalación de programas informáticos en ordenadores o teléfonos inteligentes a fin de acceder a la información contenida en ellos o la que se genere o que provoque la sustracción o revelación de audio, video, fotografías digitales o información personal o financiera. El delito de ciberacoso se encuentra tipificado como quien intimide y asedie a cualquier persona, a pesar de su oposición, por medio de las TIC. Bajo el delito contra la intimidad personal se incluye a quien intervenga o intercepte las comunicaciones privadas directas o por medios electrónicos a fin de causar perjuicio o daño, y sin consentimiento de ésta o sin autorización de autoridad competente. Aunque se tiene contemplado el delito de fraude no se detalla ninguna conducta referente al uso de medios informáticos o electrónicos en las conductas.	
Zacatecas	Dentro del Programa Estatal de Protección de Niñas, Niños y Adolescentes de Zacatecas 2022-2027 se incluyó la acción puntual de "definir e implementar una estrategia de Ciberseguridad dirigida a madres, padres, personas cuidadoras, niñas, niños y adolescentes, para contribuir a la prevención de las violencias, reducir la brecha digital e impulsar la navegación segura. Esto a fin de contribuir a la estrategia prioritaria 4.4 de Asegurar a las niñas, niño y adolescentes el	Por parte de la Secretaría de Seguridad Pública del estado, se cuenta con una Unidad de Policía Cibernética, adscrita a su División Científica. La Policía Cibernética de Zacatecas se encarga de detectar y atender los posibles delitos como fraude, amenazas, pornografía infantil, acoso	Como una buena práctica la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Zacatecas para la plataforma Digital Estatal del Sistema Estatal Anticorrupción consideró implementar y operar criterios generales de seguridad de la	Se consideran delitos contra la seguridad en los medios informáticos y magnéticos al que ingrese o use por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal o dispositivo electrónico, a un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos, así	• Reglamento interno de la Secretaría de Seguridad Pública de Zacatecas. • Programa Estatal de Protección de Niñas, niños y Adolescentes Zacatecas 2022-2027.

Entidad	Legislación	Unidad de Policía Cibernética	Iniciativas	Código Penal	Fuente
	acceso a las Tecnologías de la Información y Comunicación, mediante la reducción de la brecha digital, así como fomentar la navegación segura en internet.	sexual, extorsión, tráfico y trata de personas y sobre derechos de autor, que se pueden cometer a través de celulares, computadoras y tabletas.	información, así como una mejora continua de los controles.	como a quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, dispositivos electrónicos, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético. También se incluye como conducta contra la seguridad en los medios informáticos al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal, dispositivo electrónico, en un sistema de redes de computadoras, base de datos o soporte lógico, siempre que para ello se requiera autorización y no la obtenga. Asimismo, los anteriores delitos se consideran agravantes si se cometan por servidores públicos o ex servidores públicos dentro del año siguiente al término de su función. También se tiene tipificado el delito contra la intimidad sexual a quien divulgue contenido intimo impreso, grabado o digital.	• Lineamientos para el funcionamiento de la Plataforma Digital Estatal del Sistema Anticorrupción de Zacatecas. • Código Penal para el Estado de Zacatecas

Anexo 10. Autoridades y legislación en materia de ciberseguridad

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
Reino Unido	La Estrategia Nacional de Ciberseguridad del Reino Unido 2016-2021 establece una visión para que el Reino Unido sea seguro y resistente a las ciber amenazas, próspero y confiado en el mundo digital, cuya última actualización se realizó en 2022. El Reglamento de Seguridad de Redes y Sistemas de Información establecen múltiples autoridades competentes que son responsables de la supervisión y aplicación de los Reglamentos en cada sector o región cubierto por los Reglamentos. El Gobierno ha publicado una guía para las autoridades competentes a fin de ayudarlas a desempeñar sus funciones en virtud del Reglamento.	El Centro Nacional de Seguridad Cibernética (NCSC) se lanzó formalmente en 2017 para ser la autoridad nacional del Reino Unido en el entorno de seguridad cibernética: compartiendo conocimientos, abordando vulnerabilidades sistémicas y proporcionando liderazgo en temas clave de seguridad cibernética nacional. el NCSC colabora con otras entidades gubernamentales pertinentes y dirige las iniciativas para reducir cuantitativamente los efectos de los ataques de programas de extorsión. Establecida en 2020, la Fuerza Cibernética Nacional (NCF) es responsable de operar en y a través del ciberespacio para contrarrestar, interrumpir, degradar y desafiar a aquellos que harían daño al Reino Unido o sus aliados, para mantener al país seguro y para proteger y promover los intereses del Reino Unido en el país y en el extranjero. Establecida en el transcurso de la Estrategia Nacional de Seguridad Cibernética 2016-2021, la red nacional de delitos cibernéticos de las fuerzas del orden ha desarrollado una respuesta totalmente integrada al delito cibernético, lista para ofrecer una respuesta basada en inteligencia a todas las formas de ataques cibernéticos contra individuos, organizaciones o sectores enteros. El Consejo de Seguridad Cibernética del Reino Unido se lanzó en marzo de 2021 y es una primicia mundial para la profesión de seguridad cibernética. Su misión es ser la voz de la profesión, aportando claridad y estructura a la creciente fuerza laboral cibernética y la gama de calificaciones, certificaciones y títulos que existen en todo el campo.	Gobierno de Reino Unido (2022). National Cyber Strategy. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#annex-a-cyber-as-part-of-the-governments-wider-agenda Departamento de Asuntos Digitales, Cultura, Medios de Comunicación y Deporte del Reino Unido (2018) Security of Network and Information Systems Guidance for Competent Authorities. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701050/NIS_-_Guidance_for_Competent_Authorities.pdf
Arabia Saudita	Desde 2007 hay una Ley contra el delito Cibernético, la cual tiene como objetivo prevenir los delitos cibernéticos mediante la identificación de estos y la definición de sus castigos. El objetivo es garantizar la seguridad de la información, la protección del interés público, la moral, la protección de los derechos del uso legítimo de las computadoras y las redes de información, y la protección de la economía nacional. En 2020 se presentó la Estrategia Nacional de Ciberseguridad, preparada por la Autoridad Nacional de Ciberseguridad, para desarrollarse durante 5 años a través de 14 iniciativas y 70 proyectos, implementados	La Autoridad Nacional de Ciberseguridad (NCA), establecida en 2017 por un Decreto Real, es la entidad gubernamental a cargo de la ciberseguridad en el país, y sirve como la autoridad nacional en sus asuntos. La NCA tiene funciones regulatorias y operativas relacionadas con la ciberseguridad y trabaja en estrecha colaboración con entidades públicas y privadas, a través de comités sectoriales, para mejorar la postura de ciberseguridad del país con el fin de salvaguardar sus intereses vitales, la seguridad nacional, las infraestructuras críticas, los sectores de alta prioridad y los servicios y actividades gubernamentales en alineación con visión 2030. El Decreto Real también generó el traspaso del Equipo de Respuesta a Emergencias Informáticas (CERT) de la Comisión de Comunicaciones y Tecnologías de la Información al NCA. La misión principal del CERT Saudí es crear conciencia sobre la ciberseguridad, en este sentido aumenta el nivel de conocimiento y conciencia sobre los riesgos de ciberseguridad y los intentos de mitigar su impacto mediante la emisión de advertencias sobre las	Gobierno de Arabia Saudita (2021). Cybersecurity in the Kingdom. Disponible en línea: https://www.my.gov.sa/wps/portal/snp/content/cybersecurity#header2_5 National Cybersecurity Authority (2020) National Cybersecurity Strategy. Disponible en línea: https://nca.gov.sa/files/national_cybersecurity_strategy-en.pdf Saudi Computer Emergency Response Team (2022). About US. Disponible en linea: https://cert.gov.sa/en/about-us/

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
	por tres vías: proyectos de alto rendimiento; programa catalizador de ciberseguridad y proyectos nacionales de cinco años de duración con impactos estratégicos a largo plazo.	vulnerabilidades más recientes y peligrosas, también lanza programas y campañas de sensibilización y coopera y colabora con otros equipos de respuesta.	
República de Corea	En 2019, la Oficina de Seguridad Nacional presidencial presentó una nueva Estrategia Nacional de Ciberseguridad, con ella buscaba garantizar operaciones estables del Estado, responder a los ataques cibernéticos y construir una base sólida de ciberseguridad en Corea. Asimismo, se establecieron el Plan Básico de Ciberseguridad Nacional y el Plan Nacional de Implementación de la Ciberseguridad para dar forma e implementar la Estrategia. En julio de 2020 el gobierno anunció el New Deal coreano para superar la recesión económica después de la pandemia y cambiar el paradigma en toda la economía y la sociedad de Corea. La ciberseguridad está incluida en el proyecto Digital New Deal en el segundo subproyecto, dónde se centra en "avanzar en la ciberseguridad" el objetivo del proyecto es hacer que el entorno digital sea más seguro, permitir servicios y fomentar la industria de la seguridad.	Cada Ministerio y organismo debía perseguir los objetivos establecidos en la Estrategia Nacional de Ciberseguridad, cumplir con los principios básicos, y llevar a cabo las tareas estratégicas en promover las leyes, instituciones y políticas relacionadas con la ciberseguridad. La Oficina de Seguridad Nacional era quien supervisaba periódicamente la aplicación de esta Estrategia y la mejora de la ciberseguridad de las personas empresas y entidades gubernamentales. Para la implementación del New Deal se realiza por medio de reuniones estratégicas presididas por el presidente con la participación de todo el gobierno, los gobiernos locales y las empresas privadas. El Servicio Nacional de Inteligencia tiene a su cargo, en compañía con su Centro Nacional de Seguridad Cibernética, la supervisión de la política nacional de seguridad cibernética, previene las crisis cibernéticas y detecta ataques, realiza investigación de intrusiones cibernéticas y análisis de información sobre amenazas y proporciona un servicio de información pública sobre ciberseguridad.	National Security Office (2019) National Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf Ministry of Economy and Finance (2020) The Korean New Deal,. https://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4948#:~:text=The%20Korean%20New%20Deal%2C%20announced,employment%20and%20social%20safety%20net. National Intelligence Service (2021) Duties and services. Disponible en: https://eng.nis.go.kr/EID/1_2.do
España	En España existe la Estrategia Nacional de Ciberseguridad de 2019, la cual desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017, considera el antecedente y estructura en el rubro de ciberseguridad de Estrategia de Ciberseguridad Nacional de 2013 y la posterior aprobación de la Ley de Seguridad Nacional de 2015. La Estrategia busca una seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales; un uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso; protección del ecosistema empresarial y social de los ciudadanos;	La Estrategia Nacional de Ciberseguridad de 2019 define la estructura orgánica de la ciberseguridad en España, la cual se compone de tres órganos: El Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad que apoya al Consejo de Seguridad Nacional y asiste al presidente en la dirección y coordinación de la política de ciberseguridad, así como fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y el sector privado, y el Comité de Situación que gestiona las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales. Además, esta estructura se complementa con la Comisión Permanente de Ciberseguridad que facilita la coordinación interministerial a nivel de operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad.	Gobierno de España (2019). Estrategia Nacional de Ciberseguridad. https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019 Gobierno de España (2020) España Digital 2025. https://portal.mineco.gob.es/RecursosArticulo/mineco/prensa/ficheros/noticias/2018/Agenda_Digital_2025.pdf

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
	cultura y compromiso don la ciberseguridad y potenciación de las capacidades humanas y tecnológica; así como seguridad del ciberespacio en el ámbito internacional. En la Agenda de España Digital 2025 se considera reforzar la capacidad española en ciberseguridad al disponer de 20.000 especialistas en ciberseguridad, Inteligencia Artificial y datos en 2025, para esto cuenta con dos organismos el Centro Criptológico Nacional, que lidera la acción desde el punto de vista de la seguridad nacional y la protección de las Administraciones Públicas; y el Instituto Nacional de Ciberseguridad (INCIBE), que se centra en el desarrollo de estas líneas de actuación en torno a ciudadanía y empresas.	El INCIBE es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española y las empresas, especialmente para sectores estratégicos, es decir, es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. El Centro de Respuesta a Incidentes de Seguridad de referencia para los ciudadanos y entidades de derecho privado en España (INCIBE-CERT) es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por INCIBE.	
Estados Unidos	De acuerdo con la Ley de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de 2018, se modificó la Ley de Seguridad Nacional de 2002 para rediseñar la Dirección Nacional de Protección y Programas del Departamento de Seguridad Nacional (DHS) como Agencia de Ciberseguridad y Seguridad de las Infraestructuras de tal forma que se transfirió los recursos y las responsabilidades de la dirección a la agencia. La Ley de Mejora de la Seguridad Cibernética de 2014 actualizó la función del Instituto Nacional de Estándares y Tecnología (NIST) para incluir identificación y desarrollo de marcos de riesgos de seguridad cibernética para uso voluntario por parte de propietarios y operadores de infraestructuras críticas. Esto formalizó el trabajo previo del NIST de desarrollo de la Versión 1.0 del Marco de Ciberseguridad bajo la Orden Ejecutiva (EO) 13636, "Mejora de la seguridad cibernética en infraestructuras críticas" (febrero de 2013), y	CISA lidera el trabajo estratégico y unificado en Estados Unidos para fortalecer la seguridad, la resiliencia y la fuerza laboral del ecosistema cibernético. En este sentido Conecta a las partes interesadas en la industria y el gobierno entre sí y con recursos, análisis y herramientas para ayudarlos a construir su propia resiliencia y seguridad cibernética, de comunicaciones y física, lo que a su vez ayuda a garantizar una infraestructura segura y resistente para el pueblo estadounidense. El NIST trabajó en colaboración con las partes interesadas, incluidos los representantes de la industria, el mundo académico y el gobierno, a través de un proceso consultivo formal para desarrollar el Marco para la Mejora de la Ciberseguridad de las Infraestructuras Críticas, un marco voluntario para reducir los riesgos cibernéticos de las infraestructuras críticas. Al respecto, CISA ayuda a las organizaciones a utilizar el marco de seguridad cibernética.	Congress.Gov (2018). H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018. https://www.congress.gov/bill/115th-congress/house-bill/3359?q=%7B%22search%22%3A%5B%22Cybersecurity%22%2C%22Cybersecurity%22%5D%7D&r=31&s=10 Instituto Nacional de Estándares y Tecnología (2018). Marco de Ciberseguridad. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018es.pdf Cybersecurity Infrastructure Security Agency. CISA's Role in Cybersecurity. https://www.cisa.gov/cybersecurity

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
	proporcionó una guía para la futura evolución del Marco de Ciberseguridad, el cual es un marco proactivo impulsado por las empresas para la gestión voluntaria de los ciber riesgos, diseñado para empresas de todos los tamaños que operan en diversos sectores de la economía.		
Canadá	Desde 2018, Canadá cuenta con su Estrategia Nacional de Seguridad Cibernética que establece un marco para guiar al Gobierno de Canadá a ayudar a proteger a los ciudadanos y las empresas de las amenazas cibernéticas y aprovechar las oportunidades económicas que brinda la tecnología digital. En 2019 para dar forma a la estrategia se presentó el Plan de Acción Nacional de Seguridad Cibernética 2019-2024 para la nueva Estrategia de Seguridad Cibernética de Canadá. El plan es un modelo para la implementación de la Estrategia, establece las iniciativas y los hitos que respaldan cada uno de los objetivos y presenta una hoja de ruta. Asimismo, se cuenta con un Programa de Cooperación en Seguridad Cibernética apoya proyectos a través de subvenciones y contribuciones para mejorar la seguridad de los sistemas cibernéticos vitales de Canadá.	El Centro Canadiense para la Seguridad Cibernética (CERT-CA) es la autoridad de Canadá en materia de seguridad cibernética. Lidera la respuesta del gobierno a los eventos de seguridad cibernética. El CERT-CA es el equipo de Respuesta a Incidentes de Seguridad Informática del Gobierno de Canadá, trabajando en estrecha colaboración con departamentos gubernamentales, infraestructura crítica, empresas canadienses y socios internacionales para responder y mitigar los eventos cibernéticos. El Servicio de Inteligencia de Seguridad Canadiense (CSIS), realiza la recopilación de inteligencia cibernética y las evaluaciones de amenazas cibernéticas.	Government of Canada (2018) National Cyber Security Strategy. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf Government of Canada (2019) National Cyber Security Action Plan 2019-2024. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf Government of Canada. Cyber Security Cooperation Program. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-en.aspx Government of Canada. About the Canadian Centre of Cyber Security. https://www.cyber.gc.ca/en/about-cyber-centre
Brasil	El 5 de febrero de 2020, Brasil publicó el Decreto Federal N° 10.222102 aprobando la Estrategia Nacional de Ciberseguridad (E-Ciber), la cual representa la visión del Gobierno Federal en Ciberseguridad para 2020-2023. La estrategia busca guiar a Brasil en la seguridad cibernética e incluye acciones para aumentar su resistencia frente a amenazas cibernéticas y fortalecer su desempeño a nivel internacional.	La E-Ciber considera un modelo de gobernanza centralizada a nivel nacional por medio de la creación de un Sistema Nacional de Ciberseguridad, el cual promovería la coordinación de los diversos actores relacionados con la ciberseguridad; el análisis conjunto de los retos a los que se enfrenta la lucha contra la ciberdelincuencia; ayudar en la formulación de políticas públicas; crear un consejo nacional de ciberseguridad; establecer grupos de discusión en ciberseguridad en diferentes sectores, coordinados por la Oficina de Seguridad Institucional de la Presidencia de la República, para fomentar las discusiones sobre el tema, a través de mecanismos informales de participación.	Gobierno de Brasil. DECRETO N° 10.222, Aprova a Estratégia Nacional de Segurança Cibernética. 5 de febrero de 2020. https://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
	Dentro de la Estrategia se incluye elaborar, bajo la coordinación de la Oficina de Seguridad Institucional de la Presidencia de la República, un proyecto de ley sobre ciberseguridad a fin de que contribuya a elevar la seguridad de las organizaciones y los ciudadanos.		
Mauricio	En 2017 presentó su Estrategia para el Ciber Crimen, previamente en 2003 se promulgó la Ley sobre el uso indebido de ordenadores y la ciberdelincuencia. Además, Mauricio se convirtió, el 15 de noviembre de 2013, en el primer país africano en adherirse al Convenio de Budapest sobre la Ciberdelincuencia. El Ministerio de Tecnologías de la Información en 2018 presentó el Plan Estratégico Mauricio Digital 2030, en él se adoptó una metodología basada en cinco olas estratégicas: gobierno digital, infraestructura de TIC, innovación, gestión del talento y ciberseguridad. Sobre esta última, se generaron una serie de recomendaciones y acciones a corto, mediano y largo plazo para situar a Mauricio a la vanguardia de la tecnología.	El propietario del proyecto para la implementación de la Estrategia de Ciber Crimen es el Ministerio de Tecnologías de la Información, las Comunicaciones y la Innovación, quien es el responsable de establecer el marco jurídico necesario para la aplicación de la estrategia. También se considera un Comité Nacional de Ciberdelincuencia y Seguridad el cuál actuará como órgano de toma de decisiones y contará con representantes del sector público, privado y academia. Existe la Junta Nacional de Computación, la cual cuenta con el CERT-MU, que es el organismo asesor en temas de seguridad de la información en el país. La responsabilidad del CERT nacional es brindar asistencia técnica a las fuerzas del orden con respecto al delito cibernético.	Mauritius Government (2017). Cybercrime Strategy 2017-2019. https://mitci.govmu.org/Documents/Strategies/National%20Cybercrime%20Strategy-%20August%202017.pdf Ministerio de Tecnologías de la Información de Mauricio (2018). Digital Mauritius 2030. https://mitci.govmu.org/SitePages/ViewAllReports.aspx?RType=Policies%20and%20Strategies
Tanzania	Tanzania cuenta con una ley sobre ciberdelitos de 2015, y sobre transacciones electrónicas del mismo año.	La Autoridad Reguladora de las Comunicaciones de Tanzania (TCRA) se le ha confiado el mandato de supervisar los problemas de ciberseguridad y seguridad en línea a través del Equipo de Respuesta a Emergencias Informáticas de Tanzania (TZ-CERT), el cual tiene la responsabilidad de coordinar la respuesta a incidentes de seguridad cibernética a nivel nacional y cooperar con entidades regionales e internacionales involucradas con la gestión de incidentes de seguridad cibernética. Asimismo, en su Ley de Comunicación electrónicas y postales detalla que la Autoridad en materia de Comunicaciones, en este caso la TCRA, podrá dictar reglamentos con respecto a la composición y los deberes del CERT.	República Unida de Tanzania (2015). The Cybercrimes Act. https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf TCRA, Quarterly Magazine of the Tanzania Communications Regulatory Authority, Julio-Septimbre 2019. https://www.tcra.go.tz/uploads/documents/sw-1619108547-July - September 2019 Edition.pdf TCRA. Cybersecurity and Safety key for Development, 20 de Agosto de 2021. https://www.tcra.go.tz/news/cybersecurity-and-safety-key-for-development

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
Ghana	En 2020 el Parlamento de Ghana aprobó la Ley de Ciberseguridad.	De acuerdo con la Ley de Ciberseguridad la Autoridad de Seguridad Cibernética de Ghana es quien regula las actividades de ciberseguridad en el país, promueve el desarrollo de esta y dispone sobre asuntos relacionados. En el caso de su composición el órgano de gobierno de la Autoridad es una Junta compuesta por los ministros responsables de Comunicaciones; el Interior; Seguridad Nacional; y Defensa. La Ley de Ciberseguridad también estableció un Comité Conjunto de Ciberseguridad con las funciones de colaborar con la autoridad, sectores e instituciones para la aplicación de las medidas de ciberseguridad, además el Comité es responsable ante la Junta en el desempeño de sus funciones.	Cibersecurity Act, 2020 (Act1038, Ghana. https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf
Singapur	Desde 2018, Singapur cuenta con una Ley de Ciberseguridad. La Ley establece un marco jurídico para la supervisión y el mantenimiento de la ciberseguridad nacional en Singapur.	Singapur cuenta con la Agencia de Seguridad Cibernética de Singapur (CSA), la cual busca mantener el ciberespacio de Singapur seguro y protegido para apuntalar su seguridad nacional e impulsar una economía digital. Mantiene una supervisión de las funciones nacionales de ciberseguridad y trabaja con líderes del sector para proteger la infraestructura de información crítica de Singapur. La CSA se encuentra en revisión de una posible actualización de la Ley de Ciberseguridad a fin de mantenerla al día con la economía digital, así como la actualización del código de prácticas de Ciberseguridad.	Cybersecurity Act 2018, Singapur, Disponible en línea: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312 CSA, Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs, 4 de marzo de 2022. https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis#:~:text=3%20The%20Cybersecurity%20Act%2C%20which,and%20services%20has%20increased%20significantly
Malasia	Desde 1997, Malasia cuenta con una Ley de Delitos Informáticos, para hacer frente a delitos como el acceso no autorizado a material informático y la modificación no autorizada de los contenidos informáticos. En 2020 presentó su Estrategia de Seguridad Cibernética 2020-2024.	Desde 2017, en Malasia existe la Agencia Nacional de Seguridad Cibernética (NACSA por sus siglas en inglés), la cual supervisa las funciones nacionales de seguridad cibernética detalladas por el Consejo Nacional de Seguridad de Malasia. NACSA puede formular, monitorear, coordinar y sincronizar la implementación de la política, el marco y la estrategia de seguridad cibernética para salvaguardar al gobierno, la Infraestructura Nacional de Información Crítica (CNII), las empresas y el público, en general, el desarrollo de talento, así como coordinación de temas de legislación y aplicación en colaboración con todas las entidades relevantes. También cuenta con un centro operativo de ciberseguridad conocido como Cybersecurity Malaysia, el cual busca liderar el desarrollo de un ecosistema cibernético más seguro y resistente para mejorar la seguridad nacional, la prosperidad económica y la armonía social a través de prestación de servicios de	NACSA (2022). About us. https://www.nacsa.gov.my/about-us.php Ministerio de Comunicaciones y Medios de Malasia. Ciber Security Maysia About us. https://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html Gobierno de Malasia (2020). Malaysia Cyber Security Strategy 2020-2024. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/Mala

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
		calidad; conocimiento cibernético y supremacía técnica y fomento continuo del talento y la experiencia https://www.cyberwiser.eu/sites/default/files/EE_NCSS_2019_en.pdf	ysiaCyberSecurityStrategy2020-2024Compressed.pdf
Estonia	En 2019 se presentó la Estrategia Nacional de Ciberseguridad 2019-2022, en ella se define que para la implementación de los objetivos estratégico se usará una propuesta horizontal, que implica a todas las partes interesadas que contribuyen en Estonia: el sector público (tanto civil como de defensa) los proveedores de servicios esenciales, los empresarios del sector y el mundo académico.	La implementación de la Estrategia de Ciberseguridad es organizada por el Ministerio de Asuntos Económicos y Comunicaciones. A nivel estratégico, la coordinación se lleva a cabo a través del Consejo de Seguridad, quien garantiza la aplicación de los objetivos.	Gobierno de la República de Estonia 2019. Cyber Security Strategy. https://www.cyberwiser.eu/sites/default/files/EE_NCSS_2019_en.pdf
Rusia	Rusia cuenta con la Doctrina de Seguridad de la Información de la Federación de Rusia, adoptada en 2016, la cual define el sistema de seguridad de la información. Actualmente en el Consejo se encuentra en discusión el Concepto de le Estrategia Nacional de Seguridad Cibernética a fin de que con su aprobación se pueda crear un grupo de trabajo para desarrollar la Estrategia con la participación de representantes del Consejo de Seguridad, del órgano ejecutivo federal autorizado para garantizar la seguridad, otros órganos ejecutivos federales, de órganos de supervisión, empresas comerciales, empresas con participación estatal y organizaciones estatales.	En Rusia la Unidad Responsable del desarrollo de las políticas en Seguridad de la Información es el Consejo de Seguridad. El sistema de seguridad de la información forma parte del sistema de seguridad nacional, el cual funciona sobre la base de la distribución de competencias entre los órganos legislativos, ejecutivos y judiciales.	K. Y. Nikolskaia y A. V. Minbaleev, "The Main Directions of Ensuring Cybersecurity in Russia and the World", 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2021, pp. 98-101, doi: 10.1109/ITQMIS53292.2021.9642786 Chislova, O., Sokolova, M. Cybersecurity in Russia. Int. Cybersecur. Law Rev. 2, 245–251 (2021). https://doi.org/10.1365/s43439-021-00032-9 Gobierno de Rusia (2016). Doctrine of Information Security. http://www.scrf.gov.ru/security/information/DIB_engl/#:~:text=The%20Doctrine%20is%20a%20strategic,of%20the%20Russian%20Federation%20 .
Australia	En 2016 se lanzó una Estrategia de Ciberseguridad y en 2020 se actualizó con un plan para invertir $1,670 millones de dólares australianos durante 10 años.	Previamente a la última elección del Primer Ministro, el Ministerio de Asuntos Internos lideraba el desarrollo de la política de seguridad cibernética para el gobierno australiano, incluida la implementación de la estrategia y el plan de acción de seguridad cibernética del gobierno. También lideraba el desarrollo de la política nacional de seguridad cibernética, así como la coordinación de la implementación de la Estrategia de Seguridad Cibernética de Australia.	Gobierno de Australia (2020) Australia´s Cyber Security Strategy 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf Ministerio de Asuntos Internos Overview.

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
		El Ministerio de Asuntos Internos era responsable de la coordinación de la política cibernética de Australia y de establecer la dirección estratégica del esfuerzo cibernético del Gobierno. Con la elección Anthony Albanese como Primer Ministro de Australia, él decidió que Claire O´Neil asumiera el cargo como Ministra de Asuntos Internos, al igual que Ministra de Ciberseguridad el pasado 1 de junio de 2022. Con dicho nombramiento se espera un reforzamiento en los temas de Ciberseguridad, ya que es la primera ocasión que el tema tiene su propia cartera de proyectos; sin embargo, aún no hay actualización al respecto en la página del Gobierno de Australia.	https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/overview Julia Talevski, 2 de junio de 2022, ARN, "Labor creates standalone cyber minister in new Cabinet line-up". https://www.arnnet.com.au/article/698646/labor-creates-standalone-cyber-minister-new-cabinet-line-up/
Emiratos Árabes Unidos	En 2017 se lanzó la Estrategia de Seguridad Cibernética de Dubái cuyo objetivo es fortalecer la posición de Dubái como líder mundial en innovación y seguridad. En 2019, se lanzó la Estrategia Nacional de Ciberseguridad de los Emiratos Árabes Unidos, a fin de crear una infraestructura cibernética segura y fuerte que permitiera a los ciudadanos cumplir sus aspiraciones y prosperar a las empresas. La Estrategia Nacional de Ciberseguridad estará vigente durante tres años a partir de la fecha de su lanzamiento en junio de 2019.	En 2020 se creó el consejo de Ciberseguridad con el objetivo de desarrollar una Estrategia Integral de Ciberseguridad y crear una infraestructura cibernética segura y sólida en los Emiratos Árabes Unidos (EAU). El consejo está presidido por el Jefe de Seguridad Cibernética del Gobierno de los EAU y contribuye a crear un marco legal y regulatorio que cubra todos los tipos de delitos cibernéticos, que asegure las tecnologías existentes y emergentes y establezca un 'Plan Nacional de Respuesta a Incidentes Cibernéticos' sólido para permitir respuesta ágil y coordinada a incidentes cibernéticos en el país. La autoridad Digital de Dubai se estableció en 2021 y paso a ser el organismo oficial de Dubái responsable de todos los asuntos relacionados con la tecnología de la información, los datos, la transformación inteligente y digital y la seguridad de la información. El Departamento de Smart Dubai, el Gobierno de Smart Dubai, el Establecimiento de Datos de Dubai, el Centro de Seguridad Electrónica de Dubai y el Centro de Estadísticas de Dubai funcionarán bajo la nueva autoridad.	Gobierno de los Emiratos Árabes Unidos. National Cybersecurity strategy 2019, https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/national-cybersecurity-strategy-2019 Gobierno de los Emiratos Árabes Unidos (2017). Dubai cyber security strategy. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/dubai-cyber-security-strategy Gobierno de los Emiratos Árabes Unidos (2021). Overseeing digital transformation in the UAE. https://u.ae/en/about-the-uae/digital-uae/overseeing-digital-transformation-in-the-uae#dubai-digital-authority Tariq Alfaham, 29 de noviembre de 2020. "Mohammed bin Rashid approves UAE Environment Policy, UAE Cybersecurity Council and UAE National Media Team" en Emirates News Agency-Wam. https://wam.ae/en/details/1395302891155

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
Omán	Omán cuenta con una Ley específica contra la delincuencia cibernética, que aborda cuestiones como la protección de datos y propiedad intelectual, la privacidad, el cumplimiento de contratos electrónicos, asuntos jurisdiccionales y sistemas de pago electrónico. También tiene la Ley de Transacciones Electrónicas, que se ocupa de las cuestiones que plantea el comercio electrónico y, en particular, de garantizar la validez de las compras en línea. El marco de gobierno electrónico de Omán también incluye sus propios requisitos de cumplimiento de seguridad.	El Equipo de Preparación para Emergencias Informáticas de Omán (OCERT) se lanzó oficialmente en abril de 2010 para analizar los riesgos y amenazas a la seguridad que pueden estar presentes en el ciberespacio. Se cuenta con el Centro Regional de Seguridad Cibernética de la UIT, el único en el mundo. OCERT ha sido designado para albergar el Centro, de conformidad con un acuerdo firmado en diciembre de 2012, entre la extinta Autoridad de Tecnologías de la Información y la UIT para ser el primer Centro Regional de Seguridad Cibernética de la UIT.	Ministerio de Transporte, Comunicaciones Y Tecnologías de la Información de Omán. The Cyber Crime Law https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=54 Ministerio de Transporte, Comunicaciones Y Tecnologías de la Información de Omán. Electronic Transactions Law. https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=56 Gobierno de Oman. 6 de marzo de 2013. With the participation of ITU & IMPACT ITA launches the first Regional Cyber Security Center. https://www.oman.om/wps/portal/!ut/p/a1/hZBND4IwDIZ_DUdp3RDFG4ZARI0xE4VdDJg5TZARRNF_L5p4wC96a_M8ad8ChxB4FI8OMi4PKovTR8_NDUUPcW6NZ8Zo4SDxyaTHbEqQGTUQ1QD-KBub_mQ5s5HQletbU5M6zsv_AzT3s1W33u86vQHrE8_Ad_8TaLmfiQzWwJ_YvxRtOXzgMIXJ82WRnSV0IIEXYicKUejnoh7vyzI_DTXUsKoqXSolU6Fv1VHDb8penUolmyTkxyAIr-MOT27VHZgWDEc!/dl5/d5/L0lKQSEvUUt3SS80RUkhL2Fy/ Gobierno de Omán. Oman National CERT. https://www.oman.om/wps/portal/index/gov/centralinitiative/cert/!ut/p/a1/hc_LboMwEAXQr2FZZmxTMNm5QqEhJSgi4uFNBZXrIBEcAS2_HxJI0yqP2d3RudIMSChAdtVvo6uxMV3VnrN0P5MtccI7gmvONwQFoW9OzDLqpGQG5QzwzgH81s9BPiShdwUMQ8TEX8VOmhGk0TJ45alHw8T9D9a7WCBI2TLyP1wWBM4VPDg

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
			yVR1ElHVr6svTpehqxjXIXn2rXvX2Tz-v9-N4HBYWWjhNk62N0a2yv8zBwluVvRIGKP5KOB4KbFYvYc4HcQL_dKCz/dl5/d5/L0lKQSEvUUt3RS80RUkhL2Fy/
Finlandia	Como parte de la actualización de la Estrategia de Ciberseguridad de Finlandia, el gobierno adopto en junio de 2021 un Programa de Desarrollo de la Ciberseguridad para 2021-2030. El Programa considera 4 temas: competencia de alto nivel, estrecha colaboración, una sólida industria nacional de seguridad cibernética y capacidades nacionales efectivas de seguridad cibernética. La implementación del Programa está respaldada por la Resolución del Gobierno de 2019 sobre la Estrategia Finlandesa de Ciberseguridad, que a su vez forma parte de la implementación de la Estrategia de Seguridad para la Sociedad y la Estrategia de Ciberseguridad de la Unión Europea. Actualmente sólo se cuenta con la versión en Finés y Sueco.	Finlandia cuenta con el Centro Nacional de Ciberseguridad Finlandés (NCSC-FI) el cual es el CSIRT nacional y Gubernamental del país. El NCSC-FI es parte de la Agencia Finlandesa de Transporte y Comunicaciones (TRAFICOM), creada en 2019 en la unión de la Autoridad Reguladora de Comunicaciones de Finlandia y la Agencia de Transportes. Al respecto, los proveedores de telecomunicaciones tienen la obligación legal de informar a NCSC-FI sobre incidentes importantes de seguridad de la información, amenazas a la seguridad de la información y fallas y perturbaciones. En el caso del Ministerio de Asuntos Exteriores, tiene la responsabilidad general de las obligaciones internacionales en materia de seguridad de la información. El Ministerio de Finanzas o Hacienda, es la autoridad competente en cuestiones de la seguridad de la información en las instituciones gubernamentales. Asimismo, se cuenta con la Resolución del Gobierno sobre la Seguridad Digital en la Administración Pública, de 8 de abril de 2020, la cual establece que el marco de seguridad digital incluye cuestiones relacionadas con la gestión de riesgos, la ciberseguridad, la seguridad de la información y la protección de datos. Po su parte, la Agencia Nacional de Suministros de Emergencia del Ministerio de Asuntos Económicos y Empleo, supervisa la protección de los proveedores de infraestructuras críticas en Finlandia. Al respecto, se cuenta con el Programa Seguridad Digital 2030, el cual busca desarrollar una tolerancia de la sociedad a las interrupciones cibernéticas.	Gobierno de Finlandia (2021). Cyber Security Development Programme: Higher level of cyber security brings growth and jobs. https://valtioneuvosto.fi/en/-/cyber-security-development-programme-higher-level-of-cyber-security-brings-growth-and-jobs Ministerio de Comunicaciones y Transportes de Finlandia. Development programme to improve the overall state of cyber security. https://www.lvm.fi/en/-/development-programme-to-improve-the-overall-state-of-cyber-security-1251144 Repositorio Institucional del Gobierno de Finlandia (2021). Kyberturvallisuuden kehittämisohjelma (Programa de Desarrollo de la Ciberseguridad). https://julkaisut.valtioneuvosto.fi/handle/10024/163219 TRAFICOM. About the NCSC-FI. https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert/rfc-2350 Ministerio de Asuntos Exteriores de Finlandia. Cyber security and the cyber domain. Disponible en línea: https://um.fi/cyber-security-and-the-cyber-domain Ministerio de Finanzas de Finlandia. Digital Security in the Public Sector. https://julkaisut.valtioneuvosto.fi/handle/10024/162265

País	Legislación en materia de Ciberseguridad	Autoridades de Ciberseguridad	Fuente
			Agencia Nacional de Suministros de Emergencia de Finlandia. Digital Security 2030. https://www.huoltovarmuuskeskus.fi/en/organisation/the-national-emergency-supply-agency/programmes/digital-security-2030 Ministerio de Finanzas de Finlandia. Digital security: Guidance of services and security. https://vm.fi/en/information-security-and-cybersecurity