DPL Ciberseguridad

dpl intelligence

Políticas de ciberseguridad en México. Un compendio para la toma de decisiones, la colaboración y la confianza digital

Presentación

Este documento de **DPL Inteligence** es un compendio de las políticas, acciones y programas en materia de ciberseguridad en México, en el marco de un debate y discusión sobre esta relevante materia.

El texto reúne las más recientes acciones en materia de ciberseguridad en México. Aborda desde la Estrategia Digital Nacional, la colaboración con Estados Unidos y las iniciativas legislativas en la materia, que abordan un sinfín de elementos, porque claramente la ciberseguridad es un aspecto transversal a un sinfín de actividades, industrias y negocios.

A través de este compendio identificamos que los aspectos clave de la política de ciberseguridad en México coinciden con una descoordinación institucional, la ausencia de una estrategia en la materia, un conjunto de iniciativas aisladas y desarticuladas e intentos por legislar sobre el tema con un enfoque de seguridad nacional.

El hecho de que las autoridades mexicanas y los legisladores empiecen a abordar el tema de la ciberseguridad es una señal de que se necesita reorientar y reordenar el tema tanto en el seno de las instituciones, en las políticas públicas y la legislación.

El desafío más apremiante es la intervención de Estados Unidos como vecino, socio comercial y potencia preocupada por la ciberseguridad, aprovechando una serie de mecanismos y plataformas de diálogo y colaboración con México. La Unión Americana ha mostrado interés en que México avance en materia de ciberseguridad, enfocado en su propia visión de la problemática y la tecnología.

Es en ese aspecto donde conviene incorporar una visión de Estado y no estrictamente geopolítica de la ciberseguridad en el país, a fin de que se cumplan objetivos superiores como lo son la protección de los derechos fundamentales, el interés superior de la niñez, la seguridad nacional, la privacidad y protección de los datos personales, así como el patrimonio y los bienes de las personas, los usuarios de los servicios financieros y los consumidores en el comercio electrónico.

El objetivo de este detallado compendio de las acciones, políticas e iniciativas en materia de ciberseguridad es construir sobre lo construido, articular esfuerzos y, sobre todo, construir confianza en el ecosistema digital.

Contenido

DPL Group

dpl news

DPL News es la agencia informativa especializada en el ecosistema digital número 1 de Iberoamérica y la cuarta a nivel global.

Potencializa tu negocio con nuestra comunicación 360

1. Key Opinion Leaders especialistas en el ecosistema digital.
2. Análisis y artículos de opinión especializada.
3. Entrevistas multimedia exclusivas con los principales exponentes de la industria, las políticas públicas y la regulación de las TIC.
4. Cobertura multimedia de reuniones, congresos y eventos internacionales.
5. Infografías, inteligencia de mercado y estadísticas del sector digital.
6. Cobertura y difusión en Facebook, Twitter, YouTube, LinkedIn e Instagram.
7. Boletines diarios enviados a nuestra base estratégica regional de contactos.

Contacto:
www.dplnews.com
erwin.negrete@digitalpolicylaw.com

Analistas de DPL Intelligence

Alejandro González

Nicolás Larocca

Dinorah Navarro

Paula Bertolini

Efrén Páez

Raúl Parra

Margarita Cruz

Valeria Romero

Mirella Cordeiro

Violeta Contreras

Actual marco normativo/institucional de ciberseguridad

Leyes y disposiciones que contienen temas de ciberseguridad

México no tiene una ley específica sobre ciberseguridad, pero sí existen disposiciones y recomendaciones en distintas normas:

- Constitución Política de los Estados Unidos Mexicanos (artículo 21).
- Ley General del Sistema Nacional de Seguridad Pública.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley de Seguridad Nacional.
- Ley Federal de Seguridad Privada.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Ley Federal de Telecomunicaciones y Radiodifusión.
- Código Penal Federal.
- Norma Federal de Transparencia y Acceso a la Información Pública.
- Normas Generales como la Norma Oficial Mexicana con respecto a los requisitos que deben observarse al guardar mensajes de datos.

Estrategia Nacional de Ciberseguridad (ENC)

En 2017, el gobierno de Enrique Peña Nieto lanzó la Estrategia Nacional de Ciberseguridad (ENC). La estrategia, que tiene como objetivo mejorar las capacidades de seguridad en el ciberespacio del país, contó con la colaboración del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), a través de su Programa de Seguridad Cibernética.

Plantea cinco objetivos estratégicos: Sociedad y Derechos; Economía e Innovación; Instituciones Públicas; Seguridad Pública y Seguridad Nacional. El objetivo de esta estrategia era implementarla a través de grupos de trabajo, pero en la administración de Andrés Manuel López Obrador no se le dio continuidad.

Documentos relacionados:

https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad.

Estrategia Digital Nacional

En septiembre de 2021 entró en vigor la Estrategia Digital Nacional que, entre otras cosas, promueve la implementación del Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre Instituciones, que busca fortalecer la coordinación entre autoridades para mejorar la prevención de incidencias cibernéticas.

Concretamente, el objetivo 5 de la estrategia incluye "promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales", aunque no detalla las acciones.

En el marco de la Estrategia Digital Nacional, en julio de 2021 se publicaron las Bases Técnicas de Seguridad Informática para las Dependencias y Entidades de la Administración Pública Federal.

Se tratan de recomendaciones mínimas de seguridad informática, cuya formulación considera un enfoque de seguridad en profundidad, características de seguridad de la información, así como acciones de prevención, detección y respuesta ante incidentes.

Documentos relacionados:

https://www.gob.mx/cedn

https://www.gob.mx/cms/uploads/attachment/file/651941/Seguridad_Informa_tica.pdf

Congreso de la Unión

Ley Federal de Ciberseguridad

El Congreso de la Unión se encuentra trabajando en la elaboración de una propuesta de Ley Federal de Ciberseguridad. Las comisiones de Ciencia, Tecnología e Innovación de la Cámara de Diputados y del Senado se comprometieron a presentar un borrador en septiembre de 2022.

Para ello, las y los legisladores están estudiando 15 proyectos de ley ingresados incluso años atrás por diferentes partidos políticos e instituciones de seguridad pública que convergen en la idea de crear un marco jurídico en la materia, ya sea a través de nuevas leyes o con modificaciones a la normativa existente, como el Código Penal y la Ley de Seguridad Nacional.

Actualmente, el Congreso de la Unión está trabajando bajo el formato de conferencia bicameral con el objetivo de alcanzar consensos sobre las distintas iniciativas y están escuchando las observaciones de asociaciones, organizaciones, dependencias gubernamentales, sector privado y la academia sobre los elementos que debe contener una Ley Federal de Ciberseguridad.

Si bien aún no hay un documento que unifique los diversos planteamientos, las iniciativas que analiza el Congreso contemplan ideas como la tipificación de ciberdelito, ciberamenaza y otros conceptos relacionados; la definición de las responsabilidades del Estado, la infraestructura de ciberseguridad con la que se debe contar y la creación de una agencia especializada en la materia.

Entre las iniciativas que analiza el Congreso se encuentran una para sancionar delitos informáticos presentada por el exsenador Omar Fayad (PRI); una que busca crear una Ley General de Ciberseguridad, ingresada por Lucía Trasviña (senadora de Morena); otra de Miguel Ángel Mancera (senador del PRD), que plantea reformar diversas leyes de seguridad, el Código Penal y expedir una ley general en la materia; así como una sobre el ciberdelito y la ciberamenaza, de Javier Salinas Narváez (diputado de Morena).

Desde la Cámara de Diputados en San Lázaro el análisis parlamentario lo lidera Javier López Casarín, presidente de la Comisión de Ciencia, Tecnología e Innovación, del Partido Verde Ecologista de México (PVEM); mientras que en el Senado lo hace Jorge Carlos Ramírez Marín, del Partido Revolucionario Institucional (PRI).

El objetivo del trabajo bicameral es que el proyecto para crear una Ley Federal de Ciberseguridad esté listo en septiembre o hacia finales de 2022, para poder ser sometido a discusión en 2023 y no demorar más tiempo la atención a este tema, pues ha estado en la mesa del Congreso de la Unión durante varios años.

Dado el ánimo legislativo por lograr consensos respecto de un nuevo marco jurídico, se recomienda mantenerse alertas durante los últimos tres meses del año para conocer el borrador de la iniciativa; de ser posible, participar en futuros procesos de consulta que se lleven a cabo en el Congreso y establecer contacto con los legisladores que lideran las comisiones encargadas.

El reciente hackeo a la Secretaría de la Defensa Nacional (Sedena) podría acelerar el proceso de deliberación en ambas cámaras del Congreso para expedir una ley en la materia.

Cámara de Diputados

Mesa permanente de ciberseguridad

El 25 de febrero de 2022, la Junta de Coordinación Política de la Cámara de Diputados, presidida por Rubén Moreira Valdez (PRI), instaló una mesa de trabajo permanente en materia de ciberseguridad, a petición del presidente de la Comisión de Ciencia, Tecnología e Innovación, Javier López Casarín (PVEM).

La mesa de trabajo tiene el objetivo de analizar y buscar consensos sobre un marco jurídico en ciberseguridad, por lo que en sus sesiones participa la Comisión especializada y se invitan a representantes de otras instituciones, como la Secretaría de Seguridad y Protección Ciudadana y la Secretaría de la Defensa Nacional.

Además, la mesa estudia los marcos internacionales en la materia, los elementos que se pueden aplicar en una ley nacional y otras iniciativas que se pueden agregar a una normativa federal en ciberseguridad.

La Comisión se ha reunido con diferentes organizaciones e instituciones desde su creación. En agosto, tuvo una reunión con la Oficina de las Naciones Unidas contra la Droga y el Delito en México, en la cual se abordaron algunos de los ciberdelitos que deben ser combatidos y contemplados en un marco legal.

En esa misma ocasión, el Consejo Ciudadano, la Secretaría de Economía y la Subsecretaría de Comercio Exterior asistieron a la mesa de trabajo. También ha recibido a empresas y asociaciones que presentan sus propuestas en relación con la intención de elaborar una Ley Federal de Ciberseguridad.

Documentos relacionados:

http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Boletines/2022/Febrero/25/1159-Se-instala-la-mesa-permanente-de-los-trabajos-en-materia-de-ciberseguridad

https://comunicacionsocial.diputados.gob.mx/index.php/jucopo/se-instala-mesa-permanente-de-trabajos-en-materia-de-ciberseguridad#gsc.tab=0

https://twitter.com/UNODCmexico/status/1559660292790960128

https://twitter.com/elconsejomx/status/1559677066458451968

Convenio Latinoamericano de Ciberseguridad

A través de una proposición con punto de acuerdo, la Cámara de Diputados exhortó a la Secretaría de Relaciones Exteriores (SRE) a promover la celebración de un Convenio Latinoamericano de Ciberseguridad.

Tres diputados de la bancada de Morena, María Eugenia Hernández Pérez, Mauricio Cantú González y Jesús Roberto Briano Borunda, pidieron a la Comisión Permanente que se exhortará a la SRE a impulsar los acuerdos diplomáticos necesarios para lograr dicho convenio entre la Comunidad de Estados Latinoamericanos y Caribeños (Celac).

Los legisladores argumentan que la mayoría de los países de la región no cuentan con un marco legal para enfrentar los ciberataques y sólo cinco se han adherido al Convenio de Budapest sobre ciberdelincuencia, un instrumento que facilita la cooperación internacional en el combate a los delitos informáticos.

Si se considera que los ciberdelitos no suelen afectar únicamente a un país, la bancada de Morena en la Cámara de Diputados señala que es necesario fomentar la colaboración entre las naciones de América Latina y el Caribe para reforzar la ciberseguridad.

En 2020, México asumió la Presidencia *pro tempore* de la Celac, un mecanismo intergubernamental, por lo que cuenta con el liderazgo para promover acciones coordinadas a favor de la ciberseguridad.

Crear un convenio de este tipo permitiría, de acuerdo con los diputados, una oportunidad estratégica para enfrentar las vulnerabilidades cibernéticas. En ese sentido, se pidió a la SRE que actúe con prontitud para materializar ese proyecto.

La proposición con punto de acuerdo se turnó en agosto de 2022 a la Segunda Comisión de Trabajo: Relaciones Exteriores, Defensa Nacional y Educación Pública para dictamen, y está pendiente en Comisiones de Cámara de Origen.

La presencia de Huawei en América Latina es amplia, debido a que participa en múltiples negocios en diversos países y provee tecnología para los gobiernos y las empresas. Por ello, sería relevante recomendar en reuniones con legisladores y la Secretaría de Relaciones Exteriores parámetros y estándares que un posible futuro Convenio Latianoamericano de Ciberseguridad debería tomar en cuenta.

Documentos relacionados:

http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/07/asun_4374501_20220706_1656527046.pdf

Ciberdelitos, pero sin modificar la Ley de Seguridad Nacional

La Comisión de Seguridad Ciudadana de la Cámara de Diputados rechazó, en abril de 2022, un proyecto de decreto presentado por la diputada María Eugenia Hernández Pérez (Morena) para reformar la Ley de Seguridad Nacional (artículos 5 y 6).

En su argumentación, el organismo señala que las propuestas de la diputada resultan improcedentes e innecesarias, debido a que dicha ley no pretende ser un catálogo para la tipificación de amenazas; que el ciberespacio no es un concepto de origen de la seguridad nacional; que ya existen instrumentos de política pública que reconocen la importancia de combatir los delitos, y que no se plantean otras reformas necesarias como la creación de una agencia nacional en la materia.

Uno de los sustentos de la diputada de Morena era que realizar modificaciones a la Ley de Seguridad Nacional no generaría un impacto presupuestario. Luego del rechazo a su propuesta, María Eugenia Hernández dijo que impulsará nuevas acciones legislativas en materia de ciberseguridad y ciberdelitos.

Aunque todavía no presenta otro proyecto en forma, la diputada pretende volver a plantear que se armonicen algunas leyes en materia de ciberdelitos sin la necesidad de crear una nueva ley, como lo busca el Congreso de la Unión, ya que esto tendría un impacto en el presupuesto y, a su juicio, limitaría la capacidad de maniobra del gobierno federal.

Documentos relacionados:

http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/04/asun_4361886_20220428_1651175077.pdf

https://comunicacionsocial.diputados.gob.mx/index.php/notilegis/informa-maria-eugenia-hernandez-que-impulsara-una-agenda-legislativa-para-combatir-delitos-cibernetico-s-y-tala-clandestina#gsc.tab=0

Cámara de Senadores

Foro 5G y ciberseguridad en México

La Comisión de Relaciones Exteriores Asia-Pacífico-África del Senado convocó al foro "La red 5G en México: conectividad total, oportunidades y desafíos" el 19 y 20 de abril de 2022 de manera virtual, con la participación de senadores, especialistas, representantes empresariales (incluido Huawei), el Instituto Federal de Telecomunicaciones (IFT) y la Asociación Nacional de Telecomunicaciones (Anatel).

Durante las jornadas, las y los ponentes expusieron cuáles consideran que son los desafíos para desarrollar 5G en el país; la importancia de tener una política digital que favorezca la conectividad, y los retos para garantizar la ciberseguridad ante los crecientes riesgos cibernéticos.

Cora Cecilia Pineda Alonso, presidenta de dicha Comisión, dijo que el Senado debe construir alternativas para combatir la brecha digital, pues el desarrollo económico no será posible sin que la población pueda acceder a Internet, y que durante la pandemia por la Covid-19 las telecomunicaciones y la conectividad impidieron que la economía y el PIB mexicano tuviera una caída drástica.

Los temas que se abordaron en el foro también incluyeron el precio y asignación del espectro radioeléctrico; las implicaciones de que las bandas sean muy caras y las empresas están optando por devolver las frecuencias; las posibles aplicaciones tecnológicas que habilitará 5G; el Comité Técnico 5G del IFT y las barreras locales a la instalación de infraestructura.

Por parte del gobierno, María Catalina Ovando Chino, titular de la Unidad de Tecnologías de la Información y Comunicaciones de la Secretaría de Infraestructura, Comunicaciones y Transportes, expuso que su visión de 5G es que se trata de una tecnología esencial para la transformación digital y la competitividad de diversos sectores.

El objetivo es aprovechar la innovación de un nuevo ecosistema y desplegar más infraestructura, especialmente en las zonas rurales. También se reconoció la necesidad de crear nuevos modelos de negocio, la capacitación de fuerza laboral en materia digital y la emisión de un marco jurídico de ciberseguridad a nivel nacional.

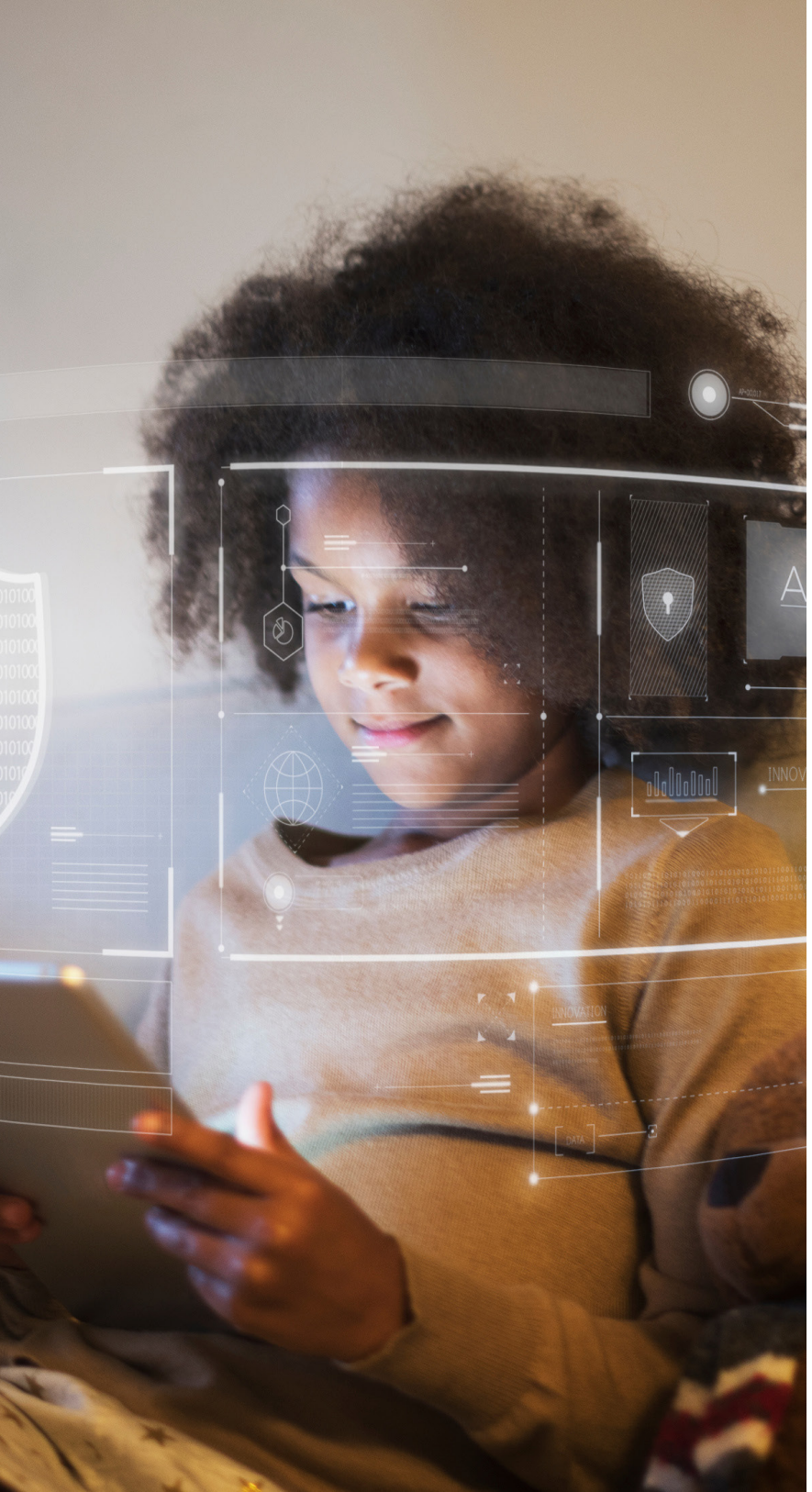
Documentos relacionados:

https://www.youtube.com/watch?v=qIXDxvUQV0Y

https://comunicacionsocial.senado.gob.mx/informacion/comunicados/3248-analizan-en-el-senado-importancia-de-garantizar-la-ciberseguridad

https://morena.senado.gob.mx/2022/04/21/urge-rafael-espino-a-legislar-en-materia-de-ciberseguridad/

https://comunicacionsocial.senado.gob.mx/informacion/comunicados/2475-buscan-en-el-senado-crear-marco-juridico-para-garantizar-uso-seguro-de-redes-digitales



Seguridad cibernética de niñas y niños

La Comisión de Derechos de la Niñez y la Adolescencia aprobó un dictamen para exhortar a la Secretaría de Gobernación, el Sistema Nacional de Protección de Niñas Niños y Adolescentes y la Secretaría de Seguridad Pública y Protección Ciudadana a implementar campañas de información sobre los riesgos de seguridad que puede haber para las infancias en Internet.

El 24 de abril de 2022, la Comisión dio luz verde al dictamen que fue ingresado por la senadora Geovanna del Carmen Bañuelos de la Torre, del Partido del Trabajo (PT), el 21 de octubre de 2021.

La proposición plantea que el acceso y uso de las Tecnologías de la Información y Comunicación por parte de niñas y niños implica riesgos a su seguridad, integridad, protección de datos y privacidad. Se considera que en el ciberespacio se pueden causar afectaciones a las infancias, ya sea a través del uso de Internet, las plataformas digitales o los videojuegos.

En ese sentido, la iniciativa argumenta que es deber del Estado ejecutar medidas y campañas orientadas a proteger a las niñas y niños de cualquier riesgo en Internet, protegiendo así el interés superior de la niñez.

Documentos relacionados:

http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/04/asun_4358117_20220426_1650988936.pdf

Congreso de la CDMX

Acciones contra delitos cibernéticos

La diputada de Morena, Leticia Estrada Hernández, puso a consideración del Pleno del Congreso de la Ciudad de México una proposición con punto de acuerdo para exhortar a la Secretaría de Seguridad Ciudadana a reforzar las acciones destinadas a prevenir la comisión de delitos cibernéticos contra personas adultas mayores.

Estrada Hernández plantea que los ciberdelitos contra este grupo poblacional incrementaron debido a la pandemia de la Covid-19, ya que en los primeros 9 meses de 2020 México fue el país que sufrió más ciberataques en América Latina.

Si bien todas las personas están expuestas a ser blancos de algún delito cibernético, la legisladora considera que las de mayor edad se encuentran especialmente vulnerables a ser víctimas, dada la falta de familiaridad con la tecnología y su mayor propensión a caer en engaños.

La proposición también toma en cuenta que la Secretaría ha reportado que cada día tres personas adultas mayores reportan haber sido víctimas de algún delito cibernético, principalmente fraude, acoso, extorsión y suplantación de identidad.

Además, se advierte que la Ciudad de México tiene el índice de envejecimiento más alto de México, con 90 personas adultas mayores por cada 100 niñas y niños menores a 15 años, por lo que se reconoce la necesidad de contar con acciones de protección específicas para este grupo poblacional.

Las medidas a las que hace exhorto la diputada contemplan los rangos administrativo, presupuestal y judicial, con la finalidad de garantizar una vida libre de violencia y el uso seguro de las tecnologías para las personas adultas mayores.

Documentos relacionados:

https://www.congresocdmx.gob.mx/media/documentos/8c026a48dbc45a5429d97403fc7fb07b03e7de70.pdf

Ley de Ciberseguridad para la CDMX

El 1 de febrero de 2022, la Comisión de Seguridad Ciudadana del Congreso capitalino solicitó una prórroga para elaborar un dictamen relativo a un proyecto de decreto que busca crear una Ley de Ciberseguridad para la Ciudad de México.

Si bien dicho proyecto fue presentado en noviembre de 2021 por el diputado Ricardo Rubio Torres, perteneciente al Partido Acción Nacional (PAN), su análisis todavía sigue vivo. La iniciativa plantea establecer que la seguridad cibernética es una herramienta que sirve para garantizar la gobernabilidad en la Ciudad de México y sus demarcaciones.

El artículo segundo del proyecto describe las finalidades de la seguridad cibernética. Entre ellas, garantizar el uso y aprovechamiento de las Tecnologías de la Información y Comunicación (TIC); la disponibilidad y confiabilidad de los procedimientos, trámites y servicios públicos; la seguridad de servidores públicos, empresas y ciudadanía; así como generar y fortalecer la confianza digital.

Además, el artículo 3 señala que todas las autoridades, dependencias, entidades, órganos, organismos autónomos, tribunales administrativos, fideicomisos y fondos públicos deben cumplir con disposiciones de ciberseguridad.

Otros de los elementos destacados del proyecto es que el artículo 4 plantea la creación de una autoridad encargada de liderar los trabajos de ciberseguridad, un equipo de inteligencia y respuesta a incidentes cibernéticos, unidades de ciberseguridad y una Fiscalía Especializada en Delincuencia Cibernética que sería parte de la Fiscalía General de la Ciudad de México. También contempla la necesidad de tipificar las conductas en materia de ciberseguridad.

Ricardo Rubio propone, asimismo, definir la obligación de que las autoridades cuenten con protocolos de control de crisis, se capaciten en materia de ciberseguridad, realicen dictámenes de seguridad cibernética para cualquier proyecto, actividad, procedimiento o trámite, al igual que otras acciones encaminadas al objetivo de fortalecer la ciberseguridad.

El proyecto de ley plantea que las autoridades deben planear y destinar recursos suficientes en materia de ciberseguridad y el presupuesto anual no podrá reducirse.

En ese sentido, se recomienda dar seguimiento a la propuesta, pues podría sentar una base para que las instituciones de la Ciudad de México inviertan en contratar tecnología moderna que les ayude a cumplir altos estándares de seguridad cibernética.

Documentos relacionados:

https://www.congresocdmx.gob.mx/media/documentos/da06539f3fae9b89a3b5a341d3083605b05dd4a1.pdf

https://www.congresocdmx.gob.mx/media/documentos/f72831cf8fe6360cb1212f942855b1ddfaa66991.pdf

Delitos cibernéticos

Con tres votos a favor, uno en contra y cero abstenciones, la Comisión de Ciencia, Tecnología e Innovación del Congreso de la Ciudad de México aprobó el 10 de enero de 2022 un dictamen de opinión relativo a un proyecto de decreto por el cual se adicionan diversas disposiciones al Código Penal local en materia de delitos cibernéticos.

La iniciativa la presentó el diputado Miguel Ángel Macedo Escartín, de Morena, en noviembre de 2021 y, luego de la opinión favorable en la Comisión de Ciencia, fue turnada a la Comisión de Administración y Procuración de Justicia.

El proyecto propone adicionar el artículo 230 bis al Código Penal en el cual se determinen penas para el delito de fraude por medio de la utilización de redes y señales de Internet, usando el engaño o aprovechando los errores de las personas mediante programas informáticos.

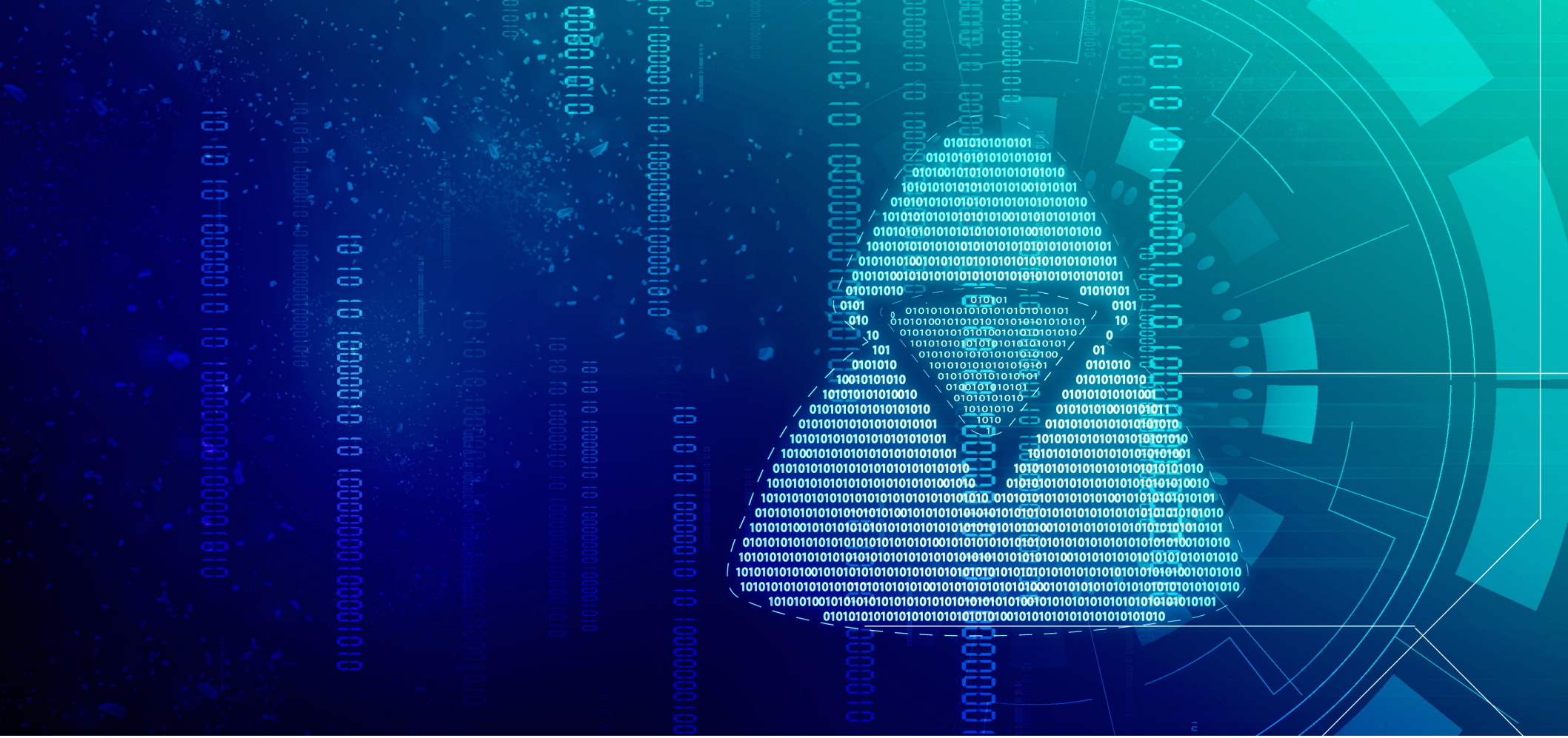
También contempla la adición del artículo 192 bis para aplicar penas a quienes utilicen las redes o Internet para atentar contra la seguridad, integridad y dignidad de niñas y niños, mediante el engaño, y la creación y propagación de programas informáticos. En ese caso, se consideran también delitos de índole sexual.

La Comisión de Ciencia, Tecnología e Innovación aprobó un dictamen de opinión favorable con tres votos a favor, uno en contra y cero abstenciones durante la sesión extraordinaria del 10 de enero de 2022.

Documentos relacionados:

https://www.congresocdmx.gob.mx/media/documentos/4e81795e1a3c51f824838e2af16845b9e247a36b.pdf

https://consulta.congresocdmx.gob.mx/consulta/webroot/img/files/iniciativa/59_19_30_21.pdf



Congreso de Puebla

Clasificación de delitos informáticos

Fernando Morales Martínez, presidente de la Comisión de Comunicaciones e Infraestructura del Congreso de Puebla, presentó una iniciativa para clasificar los delitos informáticos de usurpación de identidad y fraude cibernético, reformando los artículos 404 y 475 y adicionando los artículos 479 y 479 bis del Código Penal estatal.

De esta manera, el diputado de Movimiento Ciudadano plantea que el artículo 404 referente al delito de fraude también abarque el uso de mecanismos cibernéticos, sistema digital y las TIC para cometer este tipo de hechos; en el artículo 475 sobre delitos informáticos, se incluirían sanciones para cuando haya una revelación punible por parte de quienes sean encargados de la protección de datos personales y la seguridad pública.

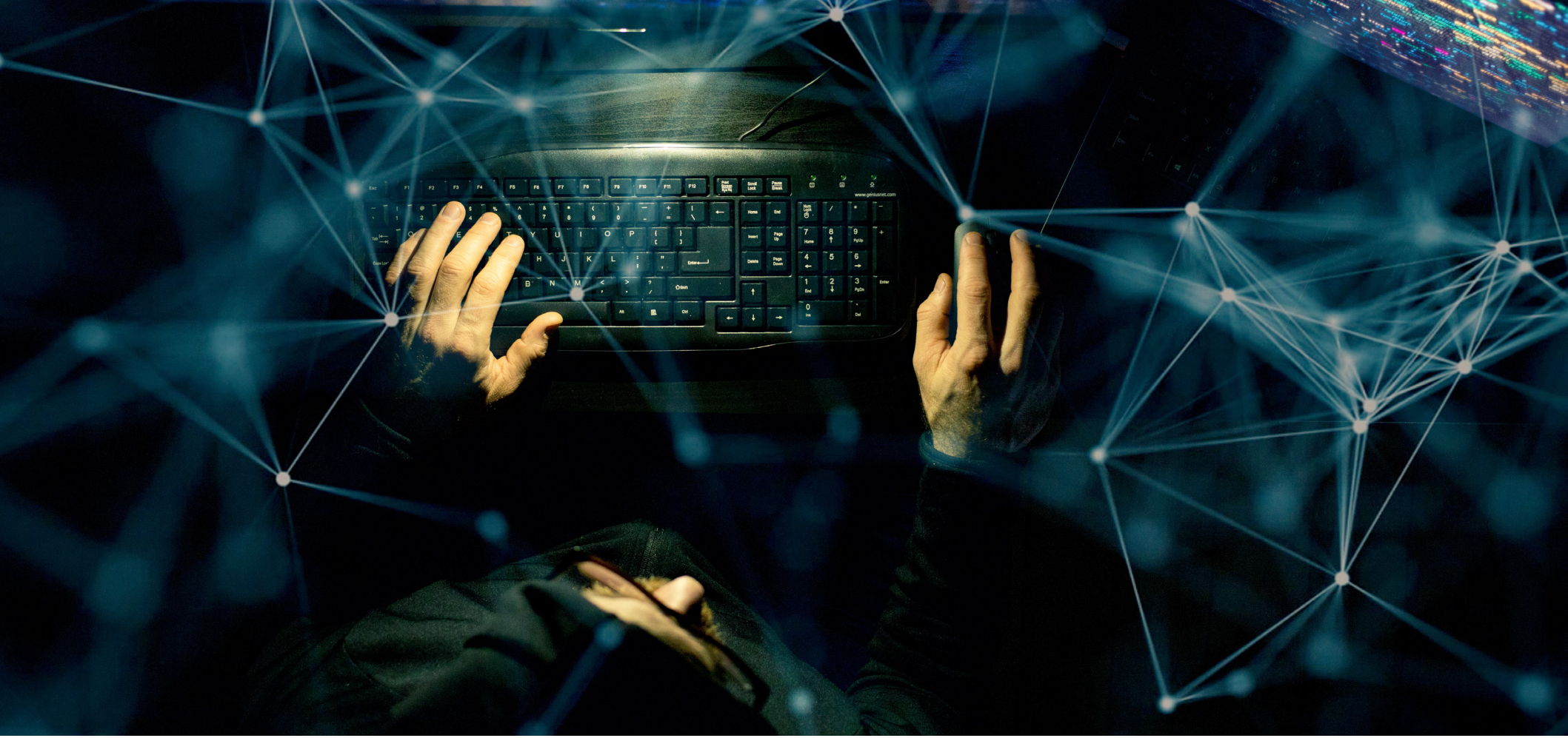
Uno de los artículos (artículo 479) que se añadirían al Código Penal contempla imponer prisión de dos a 10 años, multas económicas y suspensión de profesión en su caso cuando se realicen autorizaciones que vulneren la seguridad cibernética, ya sea a través de la usurpación de identidad o robo de identidad en Internet o el fraude cibernético.

Por último, plantea adicionar una clasificación de delitos informáticos que incluye el acceso ilícito a sistemas y equipos de informática, el acceso no autorizado a servicios informáticos, ataques cibernéticos, ciberterrorismo, amenazas cibernéticas, sabotaje informático y el espionaje informático.

Asimismo, se tipificaría el robo de *software*, revelación de secretos, delitos contra la indemnidad de privacidad de la información sexual, en materia de derecho de autor, engaño telefónico, extorsión telefónica, falsificación de títulos o documentos crediticios, alteración o manipulación de medios de identificación electrónica y difusión de imágenes falsificadas de personas.

El diputado de Movimiento Ciudadano sustenta su propuesta, ingresada en el Congreso en marzo de 2022, en que el uso de las TIC representa un avance para la sociedad, pero también conlleva potenciales riesgos, debido a que el entorno digital puede ser espacio para la comisión de diferentes delitos.

Por ello, reconoce la necesidad de modificar el marco jurídico con el fin de actuar contra la ciberdelincuencia. Además, la iniciativa se plantea como complementaria a la intención del Congreso de la Unión de crear una Ley Federal de Ciberseguridad.



Fuerzas de seguridad

Secretaría de la Defensa Nacional

La Secretaría de la Defensa Nacional (Sedena) opera el Centro de Operaciones del Ciberespacio (Cocem), donde el Ejército realiza operaciones militares para proteger los sistemas de Defensa Nacional.

El Cocem se comenzó a construir durante el sexenio de Enrique Peña Nieto, en 2016, y entró en operaciones en 2020, con la administración de Andrés Manuel López Obrador, cuando se detectaron y neutralizaron más de 5 mil posibles ciberataques.

Según la Cartera de Inversión 16071110002, inscrita en los proyectos estratégicos del actual sexenio, en 2022 se aprobaron 213.1 millones de pesos para equipar el Centro de Operaciones del Ciberespacio (Cocem), operado por el Ejército y cuya base se encuentra en el Campo Militar número 1 de la Ciudad de México.

Con lo invertido en años anteriores, 553.6 millones de pesos son los acumulados para la "adquisición de plataformas tecnológicas, mediante las cuales se habiliten y desarrollen las capacidades de defensa y seguridad en la cuarta dimensión de operaciones, denominada ciberespacio".

En 2021, la Auditoría Superior de la Federación (ASF) determinó que existen deficiencias en la administración y operación de los controles de ciberseguridad de la Sedena, las cuales podrían afectar sus operaciones y misiones.

En la revisión a la Cuenta Pública 2020, la ASF analizó cinco contratos de la Sedena relacionados con los servicios de mantenimiento para centro de datos, arrendamiento de comunicación satelital móvil y soporte técnico y mantenimiento para los equipos de seguridad lógica.

La auditoría también comprendió un análisis presupuestal de la Sedena con relación a los gastos en materia de Tecnologías de Información y Comunicaciones, así como una revisión a los procesos de ciberseguridad en la infraestructura y continuidad de las operaciones.

La ASF identificó deficiencias en la administración de los contratos por falta de soporte de los servicios proporcionados por los proveedores y pagados por la secretaría u omisión en la determinación de los criterios para efectuar los pagos por los servicios prestados por los proveedores, así como en la supervisión y seguimiento por parte del administrador del contrato.

Documentos relacionados:

https://www.24-horas.mx/2022/04/20/gasta-ejercito-mil-455-mdp-en-armarse-vs-ciberguerra/

https://www.eleconomista.com.mx/politica/Sistemas-del-Ejercito-vulnerables-a-los-ciberataques-ASF-20220225-0015.html

Marina

A principios de 2021, la Secretaría de Marina-Armada de México recibió de Brasil la Secretaría Pro-Tempore 2021-2022 del Foro Iberoamericano de Ciberdefensa, desde donde se promueven estrategias de cooperación regional en materia de ciberdefensa. El foro lo componen las Fuerzas Armadas de Argentina, Brasil, Chile, Colombia, España, México, Paraguay, Perú, Portugal y Uruguay.

Además, en 2021, la Marina publicó su "Estrategia Institucional para el ciberespacio 2021-2024". El objetivo de esta estrategia es orientar los esfuerzos institucionales para fortalecer las capacidades de ciberdefensa, ciberseguridad y seguridad de la información. Con esta estrategia se busca mantener la integridad y permanencia del Estado mexicano; reducir la vulnerabilidad cibernética mediante la coordinación y cooperación; desarrollar operaciones en el ciberespacio, y actuar conforme a derecho en materia de ciberseguridad.

Algunas de las acciones concretas que propone esta estrategia son:

- Crear los cargos de Oficial de Seguridad de la Información para salvaguardar la infraestructura crítica institucional.
- Impulsar la investigación y el desarrollo tecnológico.
- Generar mecanismos de coordinación, colaboración y cooperación con el sector público, sector privado y sector académico.
- Incluir las Operaciones en el Ciberespacio dentro del Esquema General de Operaciones Navales de la Armada de México.
- Formalizar el Centro de Operaciones del Ciberespacio de la Armada de México (CSIRT-Marina y sus Equipos de Misión).
- Promover las reformas legales que den sustento a la actuación de la Secretaría de Marina en elcCiberespacio.
- Generar la doctrina de la Armada de México en materia de Seguridad en el Ciberespacio.

Documentos relacionados:

https://www.gob.mx/cms/uploads/attachment/file/661788/Estrategia_Institucional_Ciberespacio_SM.pdf

Guardia Nacional y CERT-MX

El Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX) brinda 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, incluida 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.

Esta área tiene acuerdos de colaboración internacional con otras entidades de seguridad para llevar a cabo acciones preventivas y la presentación de delincuentes ante las autoridades correspondientes.

El equipo que opera en la Guardia Nacional cuenta con más de 4 mil colaboraciones establecidas a nivel internacional, de las cuales 80 por ciento son con Estados Unidos, que permiten emitir alertas y boletines técnicos en materia de ciberseguridad, así como avisos a la ciudadanía en general.

Ingenieros en sistemas y telecomunicaciones, especialistas en bases de datos, psicólogos y sociólogos son parte de los perfiles profesionales que analizan los distintos eventos en Internet para resguardar la ciberseguridad.

Al año, esta división recibe un promedio de 2,500 mandamientos ministeriales, que se relacionan con conductas donde interviene un dispositivo electrónico conectado a Internet.

Durante el último año, el CERT-MX realizó distintos foros y encuentros para fomentar la seguridad en línea y prevenir delitos. En septiembre, realizó junto al IFT la Segunda Edición del ciclo de "Conferencias de Ciberseguridad 2022"; charlas de protección de datos personales como medida de seguridad de niñas, niños y adolescentes; y en el marco de la Campaña Nacional Antifraude Cibernético realizó, junto con otras dependencias (Profeco, Asociación de Bancos de México y Condusef) un ciclo de charlas sobre ciberseguridad y protección.

Por otro lado, también la División Científica de la Guardia Nacional de México investiga los delitos cibernéticos. Tiene entre sus funciones vigilar, identificar, monitorear y rastrear la red pública de Internet, para prevenir conductas delictivas.

Documentos relacionados:

https://www.gob.mx/gncertmx?tab=%C2%BFQu%C3%A9%20es%20CERT-MX

https://www.gob.mx/gncertmx/articulos/actividades-recientes

Secretaría de Seguridad y Protección Ciudadana

La Secretaría de Seguridad y Protección Ciudadana (SSPC) publicó en octubre de 2021 un protocolo homologado de incidentes cibernéticos, que tiene como objetivo generar un sólo instrumento para hacer denuncias que involucren nuevas amenazas y delitos cibernéticos, con el fin de facilitar la actuación de las policías, el Ministerio Público y el Poder Judicial.

Según el documento, el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos permite 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 el bienestar de los ciudadanos.

Este protocolo está basado en el accionar con múltiples involucrados e incluye la creación de la Comisión Intersecretarial en el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, que aún no está conformada, junto con la coordinación de la dirección general científica a través del CERT-MX.

Además, durante la Conferencia Nacional de Secretarios de Seguridad Pública, que se desarrolló en Acapulco en agosto de 2022, se estableció una Coordinación Operativa de Ciberseguridad para implementar acciones conjuntas de prevención a nivel nacional.

Documentos relacionados:

https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf

https://abachainforma.com.mx/participa-la-sspe-en-la-conferencia-nacional-de-secretarios-de-seguridad-publica/

Otros organismos públicos

IFT

El Instituto Federal de Telecomunicaciones (IFT) y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) suscribieron en marzo de 2022 un Convenio Específico de Colaboración para realizar actividades, dentro del ámbito de sus respectivas facultades, con el fin de promover una cultura de protección de datos personales y fomentar la confianza y el uso responsable de las Tecnologías de la Información y Comunicación (TIC) y los servicios digitales.

En abril de 2022 el IFT aprobó el Cuarto Informe Trimestral de Actividades de 2021, donde informó de la habilitación del micrositio sobre ciberseguridad para usuarios desde niñas y niños, padres de familia, adultos mayores y pymes (*https://ciberseguridad.ift.org.mx/*).

El 31 de mayo de 2022 el IFT y la Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI) firmaron un convenio general de colaboración para trabajar de manera conjunta en acciones y programas que promuevan la educación y la cultura del uso responsable de las Tecnologías de la Información y la Comunicación (TIC). Uno de sus objetivos es promover una cultura de ciberseguridad.

El 15 de agosto de 2022 el IFT publicó una convocatoria sobre la primera edición del Concurso Nacional de Video "Navega Seguro, Seguro lo Logras", dirigido a la población estudiantil de nivel básico y medio superior de todo el país.

El regulador explicó que busca promover el conocimiento sobre los riesgos y posibles consecuencias de interactuar en el ecosistema digital sin atender las recomendaciones relacionadas a la ciberseguridad. Las inscripciones estuvieron abiertas hasta el 16 de septiembre. Los participantes tuvieron hasta el 11 de noviembre para enviar su video y se dará a conocer a los ganadores el 28 de noviembre del 2022 (*https://ciberseguridad.ift.org.mx/concurso_nacional_de_video*).

El 29 de agosto de 2022 el IFT inició con una serie de conferencias y talleres sobre ciberseguridad. La primera fue sobre ciberseguridad para empresas y un taller sobre seguridad en la Nube; le siguieron una mesa sobre ciberseguridad en el entorno digital; privacidad en el entorno digital; ciberseguridad en el comercio electrónico; y finalmente un taller sobre género, diversidad y ciberseguridad, en el cual se abordaron consejos de herramientas para niñas y mujeres.

El 30 de agosto de 2022 el órgano regulador mexicano presentó el Tercer Informe de Privacidad de la Información de los Usuarios en el Uso de Servicios Digitales. El documento puso a disposición de los usuarios las políticas de privacidad de sistemas operativos, equipos terminales, redes sociales y servicios digitales como comercio en línea, transporte y entretenimiento. Explican cuáles son los datos personales que los servicios recopilan (*https://www.ift.org.mx/usuarios-y-audiencias/tercer-informe-de-privacidad-de-la-informacion-de-los-usuarios-en-el-uso-de-servicios-digitales*).

INAI

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es un órgano constitucional autónomo de México encargado del cumplimiento de dos derechos fundamentales: el acceso a la información pública y la protección de datos personales.

El INAI suele monitorear los ataques cibernéticos a la Plataforma Nacional de Transparencia (PNT), una de las más hackeadas del país; instruye al gobierno para dar a conocer información, y realiza recomendaciones sobre seguridad en línea.

En mayo de 2022, el organismo instruyó a la Oficina de la Presidencia de la República dar a conocer las herramientas que se utilizaron para detectar cuentas robots y ciberacarreo en redes sociales

Además, el INAI suele publicar recomendaciones con el propósito de concientizar a la ciudadanía de un uso responsable y seguro de Internet. Las últimas publicadas en febrero de 2022 incluyen:

Revisar la configuración de las aplicaciones a través de las cuales se accede a Internet y sus servicios. Es ideal contar con cifrado de extremo a extremo.

Usar el modo incógnito reduce los datos que se comparten con el navegador. No guarda información sobre páginas *web*, ni historial, caché *web*, contraseñas, información de formularios, *cookies* u otros datos de sitios *web*, además borra archivos temporales cuando se finaliza la sesión.

Generar contraseñas seguras. Esto se logra conformándolas con palabras aleatorias, números y signos. Es recomendable cambiarlas frecuentemente.

Usar la autenticación de dos factores. Con esto, al tratar de ingresar a una cuenta se envía un código de verificación mediante una aplicación móvil o SMS, como un mecanismo para confirmar la identidad de la persona usuaria, lo que dificulta enormemente los ciberataques.

Actualizar sistemas operativos y aplicaciones. Considerando que las versiones antiguas tienen mayor riesgo de ser atacadas por ciberdelincuentes que encuentran vulnerabilidades en el programa, mientras que las recientes suelen incluir parches de seguridad.

Ser cauteloso con las redes inalámbricas gratuitas. Son utilizadas por los ciberdelincuentes para obtener datos, por lo que pueden usarse para navegación intrascendente y ocasional, nunca para servicios financieros como banca *online* o aquellos que requieran autenticación real de usuario.

Utilizar VPN para mejorar la privacidad. Estos sistemas ocultan la dirección IP del usuario y redirigen el tráfico a través de un túnel cifrado.

Realizar copias de seguridad para proteger la información personal y corporativa de un equipo informático.

Evitar la instalación de aplicaciones de sitios no seguros. La apertura de correos electrónicos o archivos adjuntos no solicitados que llegan de redes sociales o aplicaciones de mensajería.

Instalar antivirus confiables y prestar atención a los avisos sobre sitios inseguros.

Documentos relacionados:

https://home.inai.org.mx/wp-content/uploads/Recomendaciones_Manejo_IS_DP.pdf

Relación bilateral México-EE.UU.

Ciberseguridad, objetivo prioritario del Plan de Acción Bicentenario en México y EE.UU.

En el marco del Plan de Acción 2022-2014 del Entendimiento Bicentenario, México y EE.UU. colaborarán en diversos ámbitos de los sectores de la tecnología y las telecomunicaciones, como los semiconductores, 5G, la ciberseguridad y el comercio electrónico.

La ciberseguridad es uno de los temas prioritarios en los que México y Estados Unidos colaborarán en el marco del Plan de Acción 2022-2024 del Entendimiento Bicentenario —que conmemora los 200 años de las relaciones diplomáticas—, que tiene como objetivo "enfrentar organizaciones criminales de manera conjunta".

"Los gobiernos de ambos países están comprometidos en transformar la visión de protección a la salud y seguridad de nuestros ciudadanos a través de acciones concretas centradas en proteger a nuestra gente, prevenir la comisión de delitos transfronterizos y perseguir las redes criminales", señalaron en un comunicado conjunto.

Las otras áreas tecnológicas y de telecomunicaciones en las que ambos países cooperarán son 5G, semiconductores y comercio electrónico.

El *Plan de Acción 2022-2024 del Entendimiento Bicentenario* fue firmado el 31 de enero de 2022 por México y Estados Unidos. El plan fue diseñado para abordar los desafíos de seguridad

a través de tres metas, 11 áreas de coordinación, 26 objetivos conjuntos y 102 acciones coordinadas.

En la presentación, que se llevó a cabo en la Cancillería mexicana, funcionarios de alto nivel de los gobiernos de ambos países dieron a conocer la Hoja de Ruta con la *que operará el programa durante los próximos tres años*.

Por parte de México asistieron el secretario de Relaciones Exteriores, Marcelo Ebrard; la secretaria de Seguridad y Protección Ciudadana, Rosa Icela Rodríguez; mientras que por EE.UU. asistió el embajador Ken Salazar y, —vía remota desde Washington D.C.—, la subsecretaria para Asuntos de Seguridad Civil, Democracia y Derechos Humanos del Departamento de Estado, Uzra Zeya.

El acuerdo incluye un apartado dedicado específicamente a la seguridad cibernética. Se trata del Área de Cooperación 3.3, que tiene como objetivo conjunto 3.3.1 incrementar las cooperación para abordar las amenazas compartidas en el ciberespacio.

México y EE.UU. priorizan la ciberseguridad en grupo de trabajo de asuntos cibernéticos

En seguimiento al establecimiento del Entendimiento Bicentenario México-Estados Unidos para la Seguridad, la Salud Pública y las Comunidades Seguras, el 10 de agosto de 2022 *los representantes de ambos países llevaron a cabo el primer diálogo bilateral del Grupo de Trabajo de Asuntos Cibernéticos*.

El objetivo de la reunión fue avanzar la cooperación bilateral en temas cibernéticos en línea con el compromiso conjunto de los dos países de una Internet abierta e interoperable.

En ese sentido, ambos países reafirmaron la aplicabilidad del derecho internacional en el ciberespacio y seguirán fomentando la adhesión e instrumentación del marco para el comportamiento estatal responsable adoptado por la Asamblea General de las Naciones Unidas, para promover la estabilidad y responsabilidad en el ciberespacio.

Los gobiernos señalaron que tener un ciberespacio seguro es fundamental para el desarrollo óptimo de los sectores público y privado y para la gente del resto del mundo que se beneficia de un libre flujo de información en línea.

México y Estados Unidos colaboran en la materia en el Diálogo de Alto Nivel en Seguridad (DANS) y la administración del riesgo en el *Diálogo Económico de Alto Nivel (DEAN)*.

En la primera reunión del grupo de trabajo, las delegaciones abordaron la estrategia de cada país para combatir las amenazas en el ciberespacio. Además, presentaron las capacidades institucionales para prevenir la ciberdelincuencia, fomentar una mayor cultura de prevención y una mayor conciencia sobre la importancia de la ciberseguridad.

También presentaron iniciativas de cooperación en materia de ciberdefensa, ciberseguridad y protección de infraestructura crítica. Y finalmente se comprometieron a

construir una región más resiliente y ampliar la cooperación para atender las amenazas compartidas en el ciberespacio, para que las sociedades y las poblaciones de ambos países puedan beneficiarse de las oportunidades que ofrecen las tecnologías digitales y de la información.

Detalle de la iniciativa

En concreto, en la reunión bilateral del grupo de trabajo sobre Asuntos Cibernéticos, las delegaciones se comprometieron a:

- Coordinar, en el marco del Entendimiento Bicentenario y el DEAN, las iniciativas de cooperación bilateral centradas en cuestiones de economía digital, incluido el desarrollo de un ecosistema tecnológico seguro, resiliente y fiable.
- Reforzar los mecanismos de coordinación técnica para la atención y respuesta a los incidentes cibernéticos que afecten las infraestructuras críticas de información compartidas y nacionales.
- Intercambiar información de inteligencia sobre ciberamenazas que conduzca a la investigación de ciberdelitos en ambos países.
- Capacitar y promover una cultura de ciberseguridad dentro de las instituciones federales y estatales, con especial énfasis en aquellas que se dedican a la seguridad y justicia.
- Fomentar la conciencia de ciberseguridad y una cultura de denuncias de incidentes entre el público y el sector privado de cada país.
- Ampliar la cooperación entre el Departamento de Seguridad Nacional (DHS) de EE.UU., incluida la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) y la agencia de investigaciones de Seguridad Nacional (HSI), y sus contrapartes mexicanas en áreas como el intercambio de información, gestión de respuesta a incidentes, *ransomware*, aplicación de la ley e investigaciones, asociaciones público privadas y protección de la infraestructura crítica.
- Compartir información sobre recursos de ciberseguridad y apoyar la participación activa y el compromiso en iniciativas como el Marco de Ciberseguridad 2.0 del Instituto Nacional de Estándares y Tecnología (NIST) y la comunidad de la iniciativa Nacional para Educación en Ciberseguridad (NICE), lo que contempla la Iniciativa Regional para la Educación y Formación en Ciberseguridad (RICET).
- Dialogar y colaborar en procesos multilaterales sobre ciberseguridad, incluido el Grupo de Trabajo Sobre Medidas de Cooperación y Fomento de la Confianza en el Ciberespacio del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos (OEA).

• Participar en foros de múltiples partes interesadas, como el Foro Global de Experiencia Cibernética (GFCE), el Foro para la Gobernanza de Internet (IGF) y la Colación de la Libertad en línea.

• Coordinar junto con Canadá la convocatoria de una reunión Trilateral de Expertos en Ciberespacio en 2022, según los compromisos adquiridos en la Cumbre de Líderes de América del Norte de 2021.

DEAN 2022: México y EE.UU. priorizan ciberseguridad, electromovilidad y semiconductores

En la segunda reunión anual del Diálogo Económico de Alto Nivel (DEAN), que se realizó el 12 de septiembre de 2022 en la Ciudad de México, México y Estados Unidos profundizaron su cooperación en áreas como la ciberseguridad, la electromovilidad y los semiconductores.

Como parte de su gira por México, el secretario de Estado, Antony Blinken, y la secretaria de Comercio de Estados Unidos, señalaron que la Ley CHIPS fortalecerá la cadena de suministro de los semiconductores en América del Norte, para lo cual los gobiernos de ambos países crearon un grupo de trabajo para garantizar su resiliencia. Los funcionarios también destacaron la transición hacia la electromovilidad, que EE.UU. busca promover en el marco de su Ley de Reducción de la Inflación.

Mientras que la ex secretaria de Economía de México, Tatiana Clouthier, expuso los avances que ha tenido el DEAN en el primer año de su reactivación. Clouthier destacó el grupo de trabajo que ambos países crearon para garantizar la resiliencia de las cadenas de suministro de los semiconductores y las Tecnologías de la Información y la Comunicación (TIC).

La secretaria de Economía también resaltó la celebración de un foro virtual bilateral sobre ciberseguridad: "estamos convencidos de que es a través de la cooperación bilateral, especialmente en ciberseguridad, que ambos gobiernos podremos desarrollar mejores capacidades y una mejor coordinación en seguridad cibernética mediante el empleo de prácticas internacionales", declaró Clouthier.

Por su parte, Estados Unidos informó que el foro se denominó "Mejores prácticas desde una perspectiva pública y privada en ciberseguridad" y fue organizado por la Secretaría de Economía mexicana y el Departamento de Comercio estadounidense.

Agregó que se enfocó en el uso de una perspectiva basada en riesgos para abordar las amenazas e incidentes de ciberseguridad, así como en los recursos desarrollados por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés).

Finalmente, Clouthier detalló que el foro se realizó el 8 de septiembre y "contó con la participación de expertos del sector público y privado, quienes reafirmaron la necesidad de contar con estrategias que permitan detectar, prevenir, reaccionar y recuperarse de eventos cibernéticos y promover el uso de enfoques basados en riesgos con estándares internacionales".

Antecedentes y contexto: T-MEC y DEAN

Por la proximidad geográfica, la colaboración entre México y Estados Unidos es de larga data. El T- MEC, el nuevo Tratado entre México, Estados Unidos y Canadá firmado en 2020 —como una actualización al TLCAN de 1992 que entró en vigor en 1994—, posee dos capítulos dedicados al ámbito tecnológico y digital. El capítulo 18 se refiere a las telecomunicaciones y el 19 al comercio digital.

El artículo 19.15 del capítulo de comercio digital está dedicado a la ciberseguridad y establece que ambas partes procurarán "desarrollar las capacidades de sus respectivas entidades nacionales responsables de la respuesta a incidentes de ciberseguridad" y "fortalecer los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten las redes electrónicas y utilizar esos mecanismos para tratar rápidamente los incidentes de ciberseguridad".

Mientras que de los cuatro pilares que conforman el Diálogo Económico de Alto Nivel (DEAN) —establecido en 2013 y reactivado en septiembre de 2021 por los presidentes Joe Biden y Andrés Manuel López Obrador—, dos están escritos en clave tecnológica y uno de ellos trata específicamente sobre ciberseguridad.

El primer pilar, "Reconstruir juntos", tiene como objetivo fortalecer las cadenas de suministro, especialmente

de semiconductores; mientras que el tercero, "Asegurar las herramientas para la prosperidad futura", se refiere a la cooperación en materia de ciberseguridad, asienta que los dos países "fomentarán la compatibilidad regulatoria y la mitigación de riesgos en temas relacionados con Tecnologías de la Información y Comunicación, redes, ciberseguridad, telecomunicaciones e infraestructura".

Específicamente, propone "desarrollar oportunidades para fortalecer protecciones de seguridad cibernética en las cadenas globales de suministro y facilitar la colaboración y cooperación para enfrentar desafíos de seguridad cibernética a través de prácticas y estándares internacionales de la industria", como parte de su estrategia conjunta para mitigar amenazas cibernéticas.

Mientras que el Diálogo de Alto Nivel sobre Seguridad entre EE.UU. y México (DANS), establecido en octubre de 2021 tras la reactivación del DEAN, también incluye un objetivo, el 3, que aborda la ciberseguridad: propone "desbaratar las redes financieras de las ODT y reducir su posibilidad de lucrar con actividades ilícitas, tanto a nivel transnacional como en el ciberespacio".

Adicionalmente, México impulsará la cooperación regional sobre ciberseguridad en América, durante su presidencia del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA), para la que el país fue elegido el 28 de julio de 2022.

Además, la propia OEA, junto con el gobierno de Panamá y la Fundación Citi, inició en agosto de 2022 un programa para capacitar estudiantes que posteriormente se extenderá a otros países de la región, como Costa Rica, México, Guatemala y República Dominicana.

Tras realizar su Sondeo de Seguridad Empresarial 2022, el Comité de Seguridad de la American Chamber México —que agremia a mil 200 empresas— incluyó una recomendación sobre ciberseguridad, la número 6, que propone el "Diseño, creación e implementación de una Estrategia Nacional de Ciberseguridad —incluido un marco regulatorio que pueda ser flexible con los avance constante de la tecnología— que contemple la participación del sector público, sector privado y población en general" en el país.

Documentos relacionados:

19ESPComercioDigital.pdf (oas.org)

https://www.gob.mx/cms/uploads/attachment/file/668394/Hoja_Informativa_DEAN_-Traducci_nEEUU.pdf

https://www.state.gov/translations/spanish/ficha-informativa-dialogo-de-alto-nivel-sobre-seguridad-entre-ee-uu-y-mexico/

https://www.gob.mx/semar/prensa/plan-de-accion-2022-2024-del-entendimiento-bicentenario-mexico-y-estados-unidos-enfrentan-organizaciones-criminales-de-manera-conjunta-293668

https://mx.usembassy.gov/es/resumen-del-plan-de-accion-para-el-marco-bicentenario-ee-uu-mexico-para-la-seguridad-la-salud-publica-y-comunidades-seguras/

https://www.gob.mx/sre/prensa/comunicado-conjunto-grupo-de-trabajo-de-asuntos-ciberneticos-mexico-estados-unidos?idiom=es

2a Reunión Anual del Diálogo Económico de Alto Nivel México-Estados Unidos (DEAN) | Secretaría de Relaciones Exteriores | Gobierno | gob.mx (www.gob.mx)

Diálogo Económico de Alto Nivel México – Estados Unidos Logros Emblemáticos - Embajada de los Estados Unidos en Chile (usembassy.gov)

Ciberataques a los sistemas del gobierno

El sector gobierno es el que más ataques de ciberseguridad registró en los últimos años en México. El más reciente fue el hackeo masivo por parte del grupo internacional de activistas denominado Guacamaya, quienes vulneraron el sistema de cómputo de la Secretaría de la Defensa Nacional (Sedena) para acceder a información que data de 2016 hasta septiembre de 2022

Se trata del mayor ciberataque en la historia del país, pues dejó al descubierto miles de documentos confidenciales (sin testar) del gobierno del presidente Andrés Manuel López Obrador.

Detalles sobre el estado de salud de AMLO, las disputas entre los titulares de la Sedena y de la Secretaría de la Marina (Semar), la versión completa del "Culiacanazo", así como la débil seguridad de las aduanas, son algunos de los hallazgos expuestos en los seis terabytes de material.

Además de la sofisticada forma de hackeo, en esta ocasión fallaron los protocolos del organismo, ya que el 30 de agosto, unos días antes de que se conociera del ciberataque masivo, el Centro de Operaciones del Ciberespacio de la Sedena alertó de un virus utilizado para sustraer información de correos electrónicos.

De acuerdo con un mensaje enviado por la Sección de Respuestas a Incidentes del Centro de Operaciones del Ciberespacio a su unidad de monitoreo, un nuevo *malware* buscaba descargar secretamente correos electrónicos.

En los últimos años, el gobierno registró importantes vulnerabilidades a sus sistemas. A inicios de noviembre de 2019, se dio a conocer que Petróleos Mexicanos (Pemex) fue blanco de un ataque cibernético del que no se dieron mayores detalles, pero que el entonces secretario de Seguridad federal, Alfonso Durazo, minimizó y aseveró que fueron sólo en algunos equipos y que ya había sido controlado.

En tanto que el 23 de febrero de 2020 la Secretaría de Economía detectó un ataque cibernético en algunos de sus servidores. En aquella ocasión también minimizaron el ciberataque y aseguraron de inmediato que no hubo consecuencias mayores, aunque tampoco dieron más detalles.

Sin embargo, dicha dependencia tuvo la necesidad de suspender todos los plazos de los trámites que estaban en curso, tanto para los particulares como para la autoridad. Asimismo, suspendió el plazo para cualquier trámite nuevo que se ingresara de forma física.

DPL Group

dpl live

Promoting digital transformation

La mejor plataforma para dialogar, convocar y reunir a actores estratégicos del ecosistema digital.

Generamos influencia, conversación público-privada y potenciamos mensajes clave mediante el diseño de eventos, reuniones y seminarios virtuales, híbridos y/o presenciales en Iberoamérica.

¿Tienes una visión digital?

DPL Live la hace realidad. ¡Vive la experiencia!

Contacto:
erwin.negrete@digitalpolicylaw.com

Directora de DPL News
Paula Bertolini

Editora en Jefe de DPL News
Margarita Cruz

Diseño gráfico
Jéssica Galdámez

Comunicación digital
María Fernanda Aguirre

Directora de Mercadotecnia de DPL Group
Carolina González

Directora de DPL Live
Elizabeth Salazar

Director de Desarrollo de Negocios de DPL Group
Erwin Negrete

Director General de DPL Group
Jorge Bravo

Presidente de DPL Group
Jorge Fernando Negrete P.

www.dplnews.com
www.digitalpolicylaw.com

@dpl_news
Digital Policy & Law Consulting
DPL News
dpl_news
DPL News

dpl intelligence