INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE DECLARA EL MES DE OCTUBRE DE CADA AÑO COMO EL "MES NACIONAL DE LA CIBERSEGURIDAD".

El suscrito, senador Luis Donaldo Colosio del Grupo Parlamentario de Movimiento Ciudadano ante la LXVI Legislatura del Honorable Congreso de la Unión, conforme a lo dispuesto en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, así como por el artículo 8, numeral 1, fracción I, del Reglamento del Senado de la República, someto a consideración de esta honorable asamblea la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE DECLARA EL MES DE OCTUBRE DE CADA AÑO COMO EL "MES NACIONAL DE LA CIBERSEGURIDAD",** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

El avance de las tecnologías de la información y la comunicación (TIC) ha modificado indubitablemente nuestra forma de comprender el entorno y de relacionarnos con otras personas, con efectos profundos en todos los aspectos de nuestras vidas, incluyendo por supuesto la parte política y económica al contar con procesos más ágiles, sencillos, transparentes y eficientes. Hoy estas tecnologías son pieza esencial para el desarrollo de la economía mundial, pudiendo impulsar sociedades más justas, equitativas y democráticas.

No obstante, su uso también conlleva nuevos retos y riesgos, así como amenazas para los derechos humanos de la población, principalmente la protección de datos personales y el patrimonio de personas, organizaciones, empresas e instituciones, así como la seguridad pública e incluso la seguridad nacional. Ello demanda la coordinación de todos los sectores sociales, gobierno, industria, sociedad civil y academia para sentar las bases que permitan un aprovechamiento y disfrute seguro, responsable y confiable de dichas tecnologías y fortalecer las capacidades nacionales en la materia.

Como se mencionó, a la par del progreso tecnológico, también se han sofisticado las modalidades y técnicas delictivas en el ciberespacio, por ello, el impacto de la

ciberdelincuencia se ha incrementado de manera notable a nivel global y en México en los últimos años. Esta situación representa un desafío constante para la dignidad y la integridad de las personas, así como para la reputación y patrimonio de individuos, organizaciones, empresas e instituciones.

El avance tecnológico es tan significativo que la interconectividad de distintos aparatos electrónicos y ahora también digitales se ha disparado de manera exponencial y cada vez más acelerada bajo el esquema del Internet de las Cosas, por lo que las interacciones entre dichas máquinas versarán en miles de millones de dispositivos constantemente conectados, aumentando también de forma exponencial el volumen de información circulante, lo cual significa un desafío todavía mayor en materia de ciberseguridad.

En este contexto tan desafiante, resulta imprescindible la colaboración y corresponsabilidad de todos los sectores sociales para diseñar e implementar acciones que respondan de manera efectiva, adecuada y eficiente a los retos que plantea la evolución constante de las TIC mediante un ejercicio permanente y altamente adaptable.

Esta iniciativa constituye un llamado a todos los actores de la sociedad mexicana a sumarnos a una campaña de sensibilización y reconocimiento del impacto de la ciberseguridad en el desarrollo social, político, humano y económico de nuestro país, así como de la responsabilidad compartida en la construcción de un ciberespacio libre, diverso y sobre todo seguro.

El compromiso del Congreso de la Unión, empezando por el Senado de la República con la seguridad y con un ecosistema digital libre y plural para las personas, así como para las organizaciones, empresas e instituciones, es de vital importancia, por ello, se propone que, durante el mes de octubre de cada año, se realicen jornadas, talleres, foros, mesas de discusión, seminarios, elaboración de guías, debates, conferencias y campañas de difusión por el sector público, el social y el privado desde una perspectiva multiactor y multifactorial para fortalecer todos los aspectos clave de la ciberseguridad en México.

Esta propuesta también pretende incorporar a nuestro país a la reflexión y el diálogo internacionales sobre la responsabilidad compartida para generar soluciones

innovadoras, proteger los datos personales de todos los usuarios, fortalecer la confianza en el comercio electrónico y aumentar la resiliencia de la infraestructura digital.

Diversos países ya cuentan con una iniciativa de esta naturaleza, a destacar:

1. Estados Unidos de América.
   Origen de la iniciativa con el "Cybersecurity Awareness Month", lanzado en octubre de 2004 por el Departamento de Seguridad Interior junto con la Alianza Nacional de Ciberseguridad.

2. Unión Europea.
   Adoptó esta iniciativa en 2012 con el Mes Europeo de Ciberseguridad, impulsado por la Agencia de Ciberseguridad Europea, que también incluye múltiples actividades. En 2024 el tema eje fue el "social engineering"[1] (enfocado a diversas problemáticas como el phishing, smishing, deepfakes).

3. Canadá.
   También ha adoptado la iniciativa con el "Cyber Security Awarness Month", el cual también se realiza en octubre de cada año con el Communications Security Establishment como responsable.

4. Australia.
   El Centro Australiano de Ciberseguridad también es la autoridad responsable del manejo de esta iniciativa en el país.

5. India.
   El Equipo de Respuesta de Emergencia Informática, el cual es responsable de responder en materia de ciberseguridad también lanza en octubre de cada año la misma iniciativa en beneficio de la población.

[1] European Union Agency for Cybersecurity (ENISA). (2024, 30 de septiembre). *Promoting security in the digital world during the European Cybersecurity Month.* Disponible en: https://www.enisa.europa.eu/news/promoting-security-in-the-digital-world-during-the-european-cybersecurity-month?utm_source=chatgpt.com#contentList

6. Reino Unido.
   Múltiples instituciones y organismos públicos celebran en octubre la misma iniciativa con campañas regionales y diversos eventos.

Las principales campañas se han enfocado en lo siguiente a públicos específicos como padres de familia, tercera edad, niñez y adolescencia:

a) impulsar las contraseñas robustas/seguras y el uso de gestores de contraseñas;
b) higiene digital mediante la actualización de software, evitar descargas de software desconocido y realizar copias de seguridad;
c) alfabetización antifraude mediante el reconocimiento de los delitos más populares como phishing/smishing, deepfakes y la realización de reportes de incidentes; y
d) configuraciones seguras con bloqueos de pantalla, autenticación multifactorial.

Con dichas acciones se disminuye considerablemente el riesgo debido a comportamientos que facilitan la actividad criminal y el apoyo en la elaboración de las campañas entre los sectores público y privado aumentan fuertemente la efectividad, sobre todo cuando en efecto la repetición es anual y se pueden reutilizar los mismos materiales para generar cambios en la conducta, cambios que pueden ser medidos con encuestas y otros estudios poblacionales.

Parte de impulsar una iniciativa de esta naturaleza es visibilizar problemáticas que afectan cada vez más la vida de millones de personas y sus efectos sobre la sociedad, política, economía y desarrollo de la nación.

Atraer más atención a esta realidad también permitirá que las instituciones del Estado Mexicano cuenten con mayores y mejores mediciones del fenómeno. Instituciones como Banco de México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y el Instituto Nacional de Estadística y Geografía (INEGI) podrían recabar mucha más información sobre el impacto y afectaciones de estos ciberdelitos sobre la población, pues esta sigue siendo limitada y con ello permitir también a las

autoridades de todos los niveles y órdenes, tener un mejor diagnóstico para, a partir de él, implementar acciones contundentes y coordinadas en respuesta.

Como parte del Primer Informe de Gobierno, la titular del Ejecutivo Federal, Dra. Claudia Sheinbaum Pardo[2], informó que de enero a junio de 2025, la Agencia de Transformación Digital y Telecomunicaciones implementó medidas organizativas, técnicas y de gobernanza para elevar la ciberseguridad de la Administración Pública Federal, incluyendo monitoreo continuo de actividad maliciosa en el *dominio gob.mx* con alertas de acción de contención.

Se dio la baja de 21 páginas apócrifas que suplantaban instituciones públicas, además puso en marcha el "primer servicio de alertas tempranas", dio acompañamiento especializado que redujeron la reincidencia y modernizó el Centro de Operaciones de Ciberseguridad de Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), incrementando 40% su capacidad de detección y respuesta. Paralelamente, avanzó en la "Nube Mx" para proteger información gubernamental con la modernización del Centro de Datos Público en Aguascalientes e impulsó programas de capacitación con la Escuela Pública de Código para servidores públicos y público en general.

En materia de combate a los ciberdelitos[3], la Secretaría de Seguridad y Protección Ciudadana (SSPC) creó la Subsecretaría de Inteligencia e Investigación Policial, propuso la Ley del Sistema Nacional de Investigación e Inteligencia y fortaleció la Plataforma México.

En el mismo periodo, atendió 40 requerimientos ministeriales de evidencia digital, coadyuvando en 30 investigaciones sobre incidentes cibernéticos, gestionando también la desactivación de 36 sitios web apócrifos y 408 perfiles falsos, con 32 alertas públicas de riesgo. Asimismo, se robusteció el Registro Nacional de Incidentes Cibernéticos (RNIC) y se impulso la capacitación de elementos de las unidades de la policía cibernética de las entidades federativas.

[2] Gobierno de México. (2025). Primer Informe de Gobierno 2024-2025. Disponible en: https://www.informegobierno.gob.mx/
[3] Ídem

Todo ello fortalece la necesidad de avanzar en el apoyo decidido de este Senado y del Congreso de la Unión en las acciones realizadas por el gobierno federal e ir avanzando en los consensos para emitir una regulación que fortalezca todo el andamiaje de protección a las personas usuarias del ecosistema digital desde el Estado mexicano y esta iniciativa va en el sentido de visibilizar su importancia.

Cabe destacar que el 23 de octubre de 2018, se presentó una iniciativa con el mismo espíritu por la entonces senadora del Grupo Parlamentario del Partido Verde Ecologista de México, Alejandra Lagunes Soto Ruiz[4], iniciativa que fue votada por el Pleno de este Senado de la República el 24 de octubre de 2019 y enviada a Cámara de Diputados[5], sin embargo, infelizmente el trámite se detuvo y ha fenecido ante los cambios de legislatura. Por ello, consideramos vital retomar este esfuerzo legislativo para reforzar el compromiso en esta materia por parte de este cuerpo colegiado con la sociedad mexicana.

Como muestra de que el fenómeno de la ciberdelincuencia es cada vez mayor, no solo en México, sino en el mundo. De acuerdo con estimaciones para el 2021 realizadas por el Centro de Estudios Estratégicos e Internacionales con sede en Washington D.C. en colaboración con la empresa McAfee, el 1% del Producto Interno Bruto Mundial, es decir, alrededor de unos 945 mil millones de dólares se pierden por ciberdelitos[6]. Sin embargo, de acuerdo con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) los problemas de compatibilidad y escasez de datos dificultan la estimación, pero consideran igualmente que las pérdidas oscilan entre cientos de miles de millones de dólares a billones incluso, resaltando que los ingresos de los criminales

[4] Lagunes Soto Ruiz, Alejandra. (2018, 23 de octubre). *Iniciativa con Proyecto de Decreto que declara el mes de octubre, como "El Mes Nacional de la Ciberseguridad* [Iniciativa]. Cámara de Senadores del Congreso de la Unión, LXIV Legislatura. Disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2018-10-23-1/assets/documentos/Inic_PVEM_Mes_Ciberseguridad_231018.pdf

[5] Comisiones Unidas de Seguridad Pública; y Estudios Legislativos, Primera del Senado de la República. (2019, 24 de octubre). *Dictamen de las Comisiones Unidas de Seguridad Pública y Estudios Legislativos, Primera, por el que se aprueba iniciativa con Proyecto de Decreto por el que se declara el mes de octubre como "El Mes Nacional de la Ciberseguridad"* [Dictamen]. Cámara de Senadores del Congreso de la Unión, LXIV Legislatura. Disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-10-24-1/assets/documentos/Dict_Seguridad_Ciberseguridad.pdf

[6] Lewis, J. A., Malekos Smith, Z., & Lostri, E. (202). *The Hidden Costs of Cybercrime*. CSIS/McAffe. Disponible en: https://www.csis.org/analysis/hidden-costs-cybercrime?utm_source=chatgpt.com

son sustancialmente menores, pero las pérdidas son por las afectaciones en inversiones, tiempo, el costo de reparación y costo social total.[7]

De acuerdo con la CONDUSEF el monto reclamado en 2023 por fraudes cibernéticos fue de 20 mil millones de pesos con un 70% de los casos resueltos en favor del usuario. Igualmente se han disparado los fraudes bancarios mediante el uso de Inteligencia Artificial con reclamaciones por 22 mil millones de pesos en el primer semestre de 2025, y de dichos casos el 70% utiliza este tipo de tecnología de acuerdo con cifras de la Comisión Nacional Bancaria y de Valores (CNBV)[8]. La Encuesta Nacional de Victimización de Empresas (ENVE) del 2024[9] del INEGI da cuenta de que las pérdidas ocasionadas fueron aproximadamente por 124 mil millones de pesos por todos los delitos, sin embargo, a pesar de no existir un subapartado que, de cuenta de las pérdidas derivadas de ciberdelitos, sí existe un aumento año con año de pérdidas por dichos delitos. Lo anterior sin contar las pérdidas de la población en general, así como de organizaciones e instituciones.

En el 2018 hubo un ataque al Sistema de Pagos Electrónicos Interbancarios (SPEI) lo que se tradujo de acuerdo con el Banco de México en afectaciones por 300 millones de pesos.[10] Otro caso emblemático fue el secuestro (ransomware) que afectó a Pemex en 2019, cuando criminales exigieron 5 millones de dólares para liberar información de la petrolera, lo que generó paros administrativos.[11] A lo anterior sumamos que hubo pérdidas económicas por más de 20 mil millones de pesos en 2024 con más de 13

---

[7] Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2024). *New perspectives on measuring cybersecurity* (OECD Digital Economy Papers, No. 366). Disponible en: https://www.oecd.org/en/publications/new-perspectives-on-measuring-cybersecurity_b1e31997-en.html

[8] Hernández, Antonio. (2025, 05 de septiembre). *Alertan por repunte de fraudes bancarios con IA*. EL Universal. Disponible en: https://www.eluniversal.com.mx/cartera/alertan-por-repunte-de-fraudes-bancarios-con-ia/

[9] Instituto Nacional de Estadística y Geografía (INEGI). (2024, 10 de diciembre). *Encuesta Nacional de Victimización de Empresas* (ENVE). Disponible en: https://www.inegi.org.mx/programas/enve/2024/

[10] Redacción. (2018, 16 de mayo). *Banxico confirma que ciberataque a SPEI fue por 300 millones de pesos.* El Economista. Disponible en: https://www.eleconomista.com.mx/sectorfinanciero/Banxico-confirma-que-ciberataque-a-SPEI-fue-por-300-millones-de-pesos-20180516-0087.html

[11] Barrera, Adriana. (2019, 11 de noviembre). *Ransomware attack at Mexico´s Pemex halts work, threatens to cripple computers*. Reuters. Disponible en: https://www.reuters.com/article/technology/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUSKBN1XM041/

millones de víctimas por delitos cibernéticos en nuestro país en los últimos siete años, sobre todo debido al phishing, delito en el que los delincuentes fingen ser una entidad reconocida con la finalidad de obtener información privada del usuario, lo que se traduce en 500 dólares en promedio por usuario de pérdida debido a este ciberdelito.[12] Empresas como Coppel han sido afectadas por estos ciberdelitos, muestra de eso es el hackeo a 1800 tiendas, lo que limitó sus operaciones durante tres meses.[13]

Organismos empresariales se han pronunciado sobre los ciberdelitos. La Confederación Patronal de la República Mexicana (COPARMEX), el Consejo Coordinador Empresarial (CCE), la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (CANIETI), y la Asociación de Bancos de México (ABM) han solicitado a las autoridades el fortalecimiento del marco legal y presupuestal, una mayor coordinación entre autoridades, así como un reforzamiento de la gobernanza digital y mayores acciones para la prevención y educación al usuario.

Igualmente organizaciones de la sociedad civil como la Red en Defensa de los Derechos Digitales (R3D), SocialTIC, Artículo 19, Internet Society, el Consejo Ciudadano para la Seguridad y Justicia, la Asociación de Internet MX (AIMX) y la Alianza México CiberSeguro (AMCS), así como comunidades técnicas y de la academia como la Academia Mexicana de Ciberseguridad y Derecho Digital (AMCID), la Universidad Nacional Autónoma de México (UNAM) y el Instituto Politécnico Nacional (IPN) han solicitado la elaboración y adecuación de los marcos normativos de manera clara y sin carácter punitivo, reforzar las acciones para aumentar la higiene digital, impulsar los ecosistemas digitales seguros con infraestructura digital de manera garantista para los derechos digitales de la población y la profundización de la colaboración nacional e internacional en la materia.

[12] Patiño, Joaquín. (2025, 22 de julio). *Más de 13 millones de víctimas por fraudes cibernéticos en México*. El País. Disponible en: https://elpais.com/mexico/2025-07-23/mas-de-13-millones-de-victimas-por-fraudes-ciberneticos-en-mexico.html?utm_source=chatgpt.com
[13] Calderón, Christopher. (2024, 05 de septiembre). *¿Tuviste problemas con Coppel? Admite que hackeo en 1,800 tiendas limitó sus operaciones por 3 meses.* El Financiero. Disponible en: https://www.elfinanciero.com.mx/empresas/2024/09/05/tuviste-problemas-con-coppel-admite-que-hackeo-en-1800-tiendas-limito-sus-operaciones-por-3-meses/

El Gobierno de México, a través de la Secretaría de Seguridad y Protección Ciudadana, junto a la Guardia Nacional, ha organizado desde hace años la Semana Nacional de la Ciberseguridad[14], por lo que existe un precedente de esta naturaleza e incluso dicha semana normalmente recae en el mes de octubre, con diversas actividades, aunque por la importancia del tema consideramos más adecuado que los esfuerzos se realicen durante todo el mes y no solamente durante una semana, por todas las autoridades y no únicamente por el gobierno federal. Lo anterior debido al aumento de ciberdelitos, así como las afectaciones provocadas a la sociedad.

Por todo lo anterior, someto a consideración de esta honorable asamblea, la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE DECLARA EL MES DE OCTUBRE DE CADA AÑO COMO EL "MES NACIONAL DE LA CIBERSEGURIDAD"**.

ARTÍCULO ÚNICO. Se declara el mes de octubre de cada año, como el "MES NACIONAL DE LA CIBERSEGURIDAD".

TRANSITORIO

ÚNICO.- El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Dado en el Salón de Sesiones del Senado de la República del H. Congreso de la Unión, a los diez días del mes de septiembre de veinte veinticinco.

Luis Donaldo Colosio Riojas
Senador de la República

[14] Secretaría de Seguridad y Protección Ciudadana (SSPC). (s.f.) *Semana Nacional de la Ciberseguridad* [Artículo]. Disponible en: https://www.gob.mx/sspc/articulos/semana-nacional-de-la-ciberseguridad?utm_source=chatgpt.com