(19)

0011597

= Con dos anexos y una USB =

En San Luis Potosí, S.L.P., a 13 de septiembre de 2021

Asunto: **Iniciativa Ciudadana**

Legisladoras y legisladores de la LXIII Legislatura
del Congreso del Estado de San Luis Potosí
C.C. Secretarias y secretarios de las Comisiones
Presente

Jonathan López Torres, ciudadano mexicano y potosino, mayor de edad, en ejercicio de mi derecho de iniciar leyes que me concede el artículo 61 de la Constitución Política del Estado Libre y Soberano de San Luis Potosí, y de conformidad con lo dispuesto en los artículos 130, 131 y 133 de la Ley Orgánica del Poder Legislativo del Estado de San Luis Potosí y 61, 62, 64, 65 y 67 del Reglamento para el Gobierno Interior del Congreso del Estado de San Luis Potosí, **someto a consideración de ese Congreso una iniciativa de nueva ley, mediante la cual se expida la "Ley de Ciberseguridad del Estado de San Luis Potosí y sus Municipios"**, la cual encuentra su sustento y necesidad en la siguiente:[1]

Exposición de Motivos

Introducción

El ciberespacio es real, las amenazas cibernéticas en y a través del mismo con un impacto en el mundo físico también, y en el centro de todo están las sociedades, las empresas, los gobiernos, sus derechos, sus interacciones y sus logros. Las amenazas cibernéticas cada vez más frecuentes, complejas y destructivas atentan contra bienes jurídicamente tutelados y derechos como la vida, la integridad, la salud, el patrimonio, los activos de información, la privacidad, la reputación e incluso inciden en la opinión pública a través de información falsa, lo que crea desinformación, perjudicando a niñas, niños, adultos, empresas, instituciones gubernamentales y relaciones internacionales.

La dependencia tecnológica y los beneficios de su adopción para los gobiernos, empresas y sociedad son hechos notorios ampliamente comprobados local como internacionalmente, por lo que no es necesario su sustento, máxime que ello exacerba los riesgos que representan las amenazas cibernéticas, las cuales constituyen un mercado global emergente, en consolidación y ampliamente lucrativo.

[1] El presente escrito se estructura en los términos siguientes:
Presentación
Exposición de motivos
-Introducción, p. 1.
-Referentes, p. 2.
-Estructura de la iniciativa, p. 6.
-Descripción de la iniciativa, p. 8.
-Proyecto de iniciativa de nueva ley, p. 13.
-Conclusiones, p. 34.

Hoy en día resulta complejo medir y cuantificar las consecuencias directas e indirectas que puede tener un ataque cibernético a todas las actividades y servicios gubernamentales, sean infraestructuras críticas y/o servicios esenciales o no, constituyendo las instituciones gubernamentales del Estado de San Luis Potosí y sus municipios (orden estatal y municipal) una prioridad en su protección, en virtud de los servicios de gobierno que se prestan a la ciudadanía a través de los poderes ejecutivo, legislativo, judicial y órganos autónomos.

Garantizar la seguridad cibernética de las instituciones gubernamentales en el Estado y sus municipios es un asunto de seguridad pública que no puede postergarse más, y es en el Estado de San Luis Potosí en donde debe hacerse un esfuerzo histórico y sin precedentes por parte del Congreso del Estado para contar con la primera legislación en materia de ciberseguridad. Las amenazas cibernéticas no se detienen cada periodo electoral.

La presente iniciativa constituye una propuesta de marco jurídico básico, dinámico y prospectivo de un tema que debió discutirse, analizarse y legislarse desde años atrás y que pone a prueba el liderazgo del poder legislativo por el presente y por el futuro de la gobernabilidad, de la seguridad y de la prosperidad económica, política y social en el Estado de San Luis Potosí, en un camino que no puede elegir ni detener, pero sí proteger, me refiero al camino de la digitalización.

Referentes

Por mencionar sólo algunos, sirvan de contexto y apoyo a la presente exposición de motivos los siguientes referentes:

A. Año 2002. Creación de una cultura mundial de seguridad cibernética

Constituye el título de la resolución aprobada el 20 de diciembre de 2002 por la Asamblea General de las Naciones Unidas, cuyo anexo señala que:

> "Los rápidos progresos de las tecnologías de la información han cambiado el modo en que los gobiernos, las empresas, otras organizaciones y los usuarios individuales que desarrollan, poseen, proporcionan, gestionan, mantienen y utilizan esos sistemas y redes de información ("participantes") deben abordar la cuestión de la seguridad cibernética. Una cultura mundial de seguridad cibernética requerirá que todos los participantes tomen en consideración los nueve elementos complementarios siguientes:
>
> a) **Conciencia**. Los participantes deben tener conciencia de la necesidad de la seguridad de los sistemas y redes de información y de lo que pueden hacer por mejorar esa seguridad.
>
> b) **Responsabilidad**. Los participantes son responsables de la seguridad de los sistemas y redes de información en cuanto corresponde a sus funciones individuales. Deben examinar periódicamente sus propias políticas, prácticas, medidas y procedimientos y evaluar si son las que convienen en su contexto.
>
> c) **Respuesta**. Los participantes deben actuar de manera oportuna y cooperativa para prevenir y detectar los incidentes de seguridad y reaccionar ante ellos. Deben compartir la información sobre las amenazas y las vulnerabilidades, según convenga, y aplicar procedimientos para establecer una cooperación rápida y eficaz a fin de prevenir y detectar los incidentes de seguridad y reaccionar ante ellos. Para ello puede ser necesario compartir información y cooperar a través de las fronteras.

d) **Ética**. Dada la omnipresencia de los sistemas y redes de información en las sociedades modernas, los participantes deben respetar los legítimos intereses de los demás y reconocer que lo que hagan o dejen de hacer puede perjudicar a otros.

e) **Democracia**. Las medidas de seguridad deben aplicarse de manera compatible con los valores reconocidos de las sociedades democráticas, incluidos la libertad de intercambiar pensamientos e ideas, el libre flujo de la información, la confidencialidad de la información y las comunicaciones, la debida protección de la información personal, la franqueza y la transparencia.

f) **Evaluación de riesgos**. Todos los participantes deben realizar evaluaciones periódicas de los riesgos a fin de determinar las amenazas y vulnerabilidades; esas evaluaciones deben tener una base suficientemente amplia para abarcar los principales factores internos y externos, tales como la tecnología, los factores físicos y humanos, las políticas y los servicios de terceros que tengan consecuencias para la seguridad; permitir la determinación del nivel de riesgo aceptable; y ayudar a la selección de controles apropiados para gestionar el riesgo de posibles daños a los sistemas y redes de información, teniendo en cuenta la naturaleza y la importancia de la información que se debe proteger.

g) **Diseño y puesta en práctica de la seguridad**. Los participantes deben incorporar la seguridad como elemento esencial de la planificación y el diseño, el funcionamiento y el uso de los sistemas y redes de información.

h) **Gestión de la seguridad**. Los participantes deben adoptar un enfoque amplio de la gestión de la seguridad basado en una evaluación de los riesgos que sea dinámica e incluya todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones.

i) **Reevaluación**. Los participantes deben examinar y reevaluar la seguridad de los sistemas y redes de información e introducir las modificaciones apropiadas en las políticas, prácticas, medidas y procedimientos de seguridad que permitan hacer frente a las amenazas y vulnerabilidades a medida que se presentan o se transforman."[2]

B. Año 2009. Creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales

Constituye el título de la resolución aprobada el 21 de diciembre de 2009 por la Asamblea General de las Naciones Unidas, en la cual se señala que:

"Reconociendo además que, cada uno en su papel, los gobiernos, las empresas, las organizaciones y los propietarios y usuarios individuales de las tecnologías de la información deben asumir sus responsabilidades y adoptar medidas para mejorar la seguridad de esas tecnologías de la información,

[...]

Afirmando que la seguridad de las infraestructuras de información esenciales es una responsabilidad que los gobiernos deben asumir de manera sistemática y una esfera en la que deben desempeñar un papel rector a nivel nacional, en coordinación con los interesados competentes, quienes a su vez deben ser conscientes de los riesgos correspondientes, las medidas de prevención y las respuestas efectivas de manera acorde con sus respectivas funciones,

[Resolución en la que se propone:]

Marcos jurídicos

2 Resolución A/RES/57/239, aprobada por la Asamblea General de las Naciones Unidas el 20 de diciembre de 2002. Disponible en: https://undocs.org/es/A/RES/57/239

> 13. Examinar y actualizar las autoridades jurídicas (incluidas las relacionadas con los delitos cibernéticos [...] y el cifrado) que puedan estar anticuadas u obsoletas como resultado de la rápida incorporación de las nuevas tecnologías de la información y las comunicaciones y de la dependencia de esas tecnologías [...]
>
> Determinar si el país ha elaborado la legislación necesaria para la investigación y el enjuiciamiento de la delincuencia cibernética, indicando los marcos existentes [...]
>
> 14. Determinar la situación actual de las autoridades y procedimientos nacionales que se ocupan de la delincuencia cibernética, incluidas las competencias legales y las dependencias nacionales encargadas de las cuestiones relativas a la delincuencia cibernética, y el nivel de comprensión de esas cuestiones entre los fiscales, jueces y legisladores.
>
> 15. Evaluar la idoneidad de los códigos jurídicos y las autoridades actuales para hacer frente a los desafíos presentes y futuros de la delincuencia cibernética y del ciberespacio de forma más general."[3]

C. Año 2010. Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Constituye el primer informe del segundo Grupo de Expertos Gubernamentales creado por resolución aprobada por la Asamblea General de las Naciones Unidas,[4] en el cual se señala que:

> "1. Las amenazas reales y potenciales en la esfera de la seguridad de la información se cuentan entre los problemas más graves del siglo XXI. Estas amenazas pueden ocasionar daños considerables en las economías y en la seguridad nacional e internacional. Las amenazas proceden de una amplia gama de fuentes y se manifiestan en actividades desestabilizadoras dirigidas contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de una comunidad internacional interconectada.
>
> [...]
>
> 4. La red mundial de tecnologías de la información y las comunicaciones se ha convertido en teatro de actividades desestabilizadoras. Los motivos para crear inestabilidad varían profundamente y van desde el deseo de demostrar simplemente habilidad técnica, al robo de dinero o de información, pasando por su empleo en conflictos estatales. Las fuentes de esas amenazas incluyen agentes no estatales, como delincuentes y, quizás, hasta terroristas, así como los propios Estados. Estas tecnologías pueden ser utilizadas para dañar los recursos e infraestructuras de información.
>
> [...]
>
> 17. La creación de capacidad es de vital importancia para lograr el éxito en la tarea de garantizar la seguridad mundial de las tecnologías de la información y las comunicaciones, asistir a los países en desarrollo en sus esfuerzos por acrecentar la seguridad de su infraestructura nacional de información, de importancia crítica, y remediar la disparidad actual en la seguridad de las tecnologías de la información y las comunicaciones. [...]"[5]

---

[3] Resolución A/RES/64/211, aprobada por la Asamblea General de las Naciones Unidas el 21 de diciembre de 2009. Disponible en: https://undocs.org/es/A/RES/64/211

[4] Creado en cumplimiento de lo dispuesto en el párrafo 4 de la resolución A/RES/60/45 de la Asamblea General de las Naciones Unidas. Disponible en: https://undocs.org/es/A/RES/60/45

[5] Informe 2010 del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/60/PDF/N1046960.pdf?OpenElement

D. Año 2016. Departamento de Justicia de los Estados Unidos

En un discurso pronunciado en abril de 2016 por la entonces Procuradora General Adjunta de la División Criminal del Departamento de Justicia de los Estados Unidos (2014-2017) y considerada que bajo su dirección la división incrementó su experiencia en delincuencia cibernética,[6] Leslie R. Caldwell puntualizó lo siguiente:

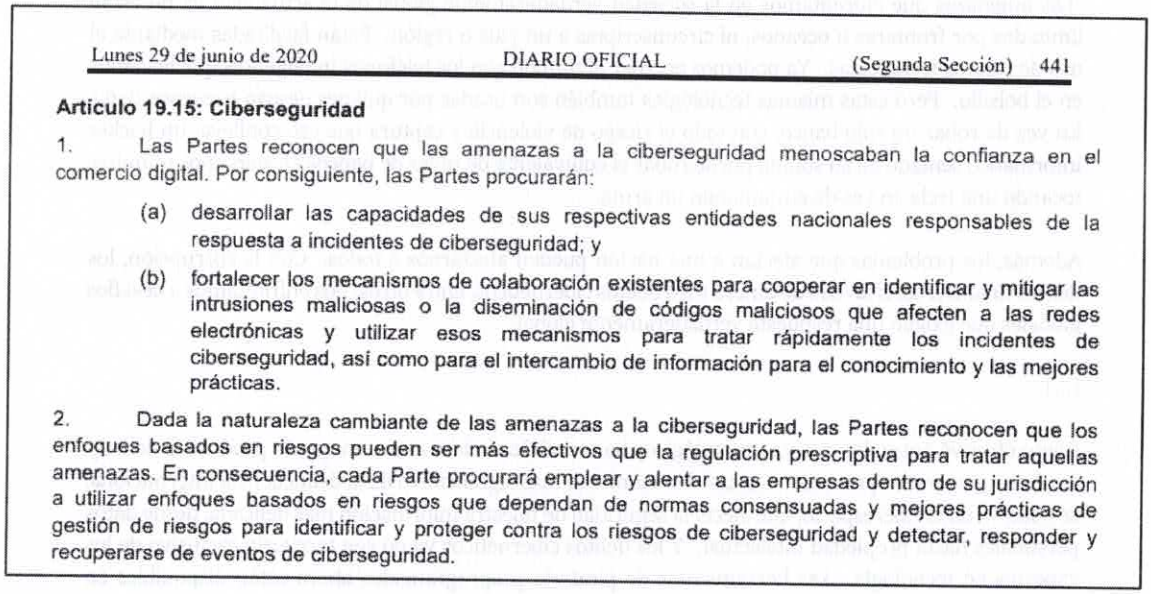
> "Las amenazas que enfrentamos en la sociedad verdaderamente global de la actualidad ya no están limitadas por fronteras u océanos, ni circunscriptas a un país o región. Están facilitadas mediante el uso de nuevas tecnologías. Ya podemos acceder al mundo con los teléfonos inteligentes que llevamos en el bolsillo. Pero estas mismas tecnologías también son usadas por quienes desean hacernos daño. En vez de robar un solo banco, con todo el riesgo de violencia y captura que eso conlleva, un hacker informático sentado en su sótano puede robar el equivalente de miles de bancos en solo unos minutos, tocando una tecla en vez de empuñando un arma.
>
> Además, los problemas que afectan a una nación pueden afectarnos a todos. Con la corrupción, los delitos financieros, el lavado de dinero y los delitos cibernéticos, entre otros, nos enfrentamos a desafíos globales que exigen una respuesta verdaderamente global.
>
> [...]
>
> Como observé antes, los avances tecnológicos han modificado la manera en que se produce el delito y los daños que puede provocar. Quizás el crecimiento más significativo de la delincuencia internacional se observa en el ciberespacio, que afecta la seguridad de nuestra información más delicada, desde datos personales hasta propiedad intelectual. Y los delitos cibernéticos ya no son territorio exclusivo de los expertos en tecnología. Las herramientas de piratería preprogramadas ahora están disponibles en foros delictivos en línea donde cualquier comprador puede adquirirlas, entre ellos miembros de mafias de delincuencia organizada.
>
> Los delitos cibernéticos pocas veces permanecen dentro de las fronteras de un país. Los hackers roban información personal ubicada en un país, luego quitan los datos de servidores en otro país y cuentan sus ganancias en un tercer país. Y los delincuentes cibernéticos sofisticados se aprovechan a sabiendas de fronteras internacionales y diferencias en sistemas legales, con la esperanza – a menudo muy justificada – de que los investigadores en los países donde están sus víctimas no podrán identificarlos u obtener evidencia desde el extranjero o de que sus países de residencia nunca los extraditarán para que se enfrenten a la justicia. Dado que los delincuentes cibernéticos actúan cruzando fronteras, nosotros también debemos coordinarnos y cruzar nuestras fronteras. Debemos ser innovadores, movernos con rapidez y trabajar juntos.
>
> [...]"[7]

[6] Leslie R. Caldwell. Perfil. Departamento de Justicia de los Estados Unidos. Disponible en: https://www.justice.gov/criminal/history/assistant-attorneys-general/leslie-r-caldwell

[7] La Procuradora General Adjunta Leslie R. Caldwell Ofrece Discurso en la Universidad Católica de Colombia Sobre Cooperación Internacional Estratégica en la Lucha Contra el Delito Internacional. Bogotá, Colombia, martes, 12 de abril de 2016. Noticias. Departamento de Justicia de los Estados Unidos. Disponible en: https://www.justice.gov/espanol/speech/la-vice-fiscal-general-adjunta-leslie-r-caldwell-habla-en-la-universidad-cat-lica-de

E. Año 2020. Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC)

El T-MEC fue establecido como un tratado "[...] que aborde los retos y las oportunidades futuras del comercio y la inversión, y contribuir con el fomento de sus respectivas prioridades en el tiempo".[8] En este sentido, el "Capítulo 19 Comercio Digital", en su artículo 19.15, establece un apartado titulado "Ciberseguridad", en el cual se aprecia lo siguiente:



Lunes 29 de junio de 2020 DIARIO OFICIAL (Segunda Sección) 441

Artículo 19.15: Ciberseguridad

1. Las Partes reconocen que las amenazas a la ciberseguridad menoscaban la confianza en el comercio digital. Por consiguiente, las Partes procurarán:

(a) desarrollar las capacidades de sus respectivas entidades nacionales responsables de la respuesta a incidentes de ciberseguridad; y

(b) fortalecer 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 y utilizar esos mecanismos para tratar rápidamente los incidentes de ciberseguridad, así como para el intercambio de información para el conocimiento y las mejores prácticas.

2. Dada la naturaleza cambiante de las amenazas a la ciberseguridad, las Partes reconocen que los enfoques basados en riesgos pueden ser más efectivos que la regulación prescriptiva para tratar aquellas amenazas. En consecuencia, cada Parte procurará emplear y alentar a las empresas dentro de su jurisdicción a utilizar enfoques basados en riesgos que dependan de normas consensuadas y mejores prácticas de gestión de riesgos para identificar y proteger contra los riesgos de ciberseguridad y detectar, responder y recuperarse de eventos de ciberseguridad.

De lo establecido en el T-MEC se puede observar que el Estado mexicano reconoció que las amenazas a la ciberseguridad menoscaban la confianza, en este caso, en el comercio digital, no obstante, el sector gubernamental federal y local no son ajenos a las amenazas a la ciberseguridad. En este sentido, el Estado de San Luis Potosí debe coadyubar en el ámbito de su competencia a efecto de desarrollar capacidades y mecanismos de colaboración gubernamentales para tratar rápidamente los incidentes de ciberseguridad, en concordancia con lo establecido por el T-MEC y dada su intervención con el sector comercial establecido en el Estado.

Estructura de la iniciativa

La presente iniciativa de nueva ley, mediante la cual se expida la Ley de Ciberseguridad del Estado de San Luis Potosí y sus Municipios, se compone de 11 (once) títulos, 71 (setenta y uno) artículos y 9 (nueve) artículos transitorios, con la estructura siguiente:

[8] DECRETO Promulgatorio del Protocolo por el que se Sustituye el Tratado de Libre Comercio de América del Norte por el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá, hecho en Buenos Aires, el treinta de noviembre de dos mil dieciocho [...] Publicado en el Diario Oficial de la Federación el 29 de junio de 2020. Disponible en: http://dof.gob.mx/2020/SRE/T_MEC_290620.pdf

Descripción de la iniciativa

TÍTULO PRIMERO. DISPOSICIONES GENERALES

Capítulo Único

En los artículos 1 a 7 se establecen el objeto, finalidades, ámbito de aplicación, contenido, definiciones, interpretación y supletoriedad del proyecto de ley.

TÍTULO SEGUNDO. DE LAS OBLIGACIONES ESTRUCTURALES EN MATERIA DE CIBERSEGURIDAD

Capítulo Único

En los artículos 8 a 28 se establecen una serie de obligaciones de carácter estructural en materia de ciberseguridad, es decir, obligaciones que integran un marco jurídico básico, integral, dinámico y prospectivo en la materia, cuya observancia y cumplimiento permitirá conducir de manera adecuada las políticas públicas estatales.

Las obligaciones versan sobre observancia y responsabilidad del cumplimiento del proyecto de ley; respeto a derechos humanos; liderazgo por parte de los titulares de las autoridades de todos los poderes y órganos autónomos estatales; obligación de cumplimiento de todos los servidores públicos y prestadores de servicios de las autoridades; neutralidad tecnológica; gestión de riesgos, crisis y resiliencia; cultura de ciberseguridad; ciberseguridad primero en toda actividad gubernamental; identificación de proveedores y dependencias tecnológicas; puntos de contacto; máxima diligencia; ciberseguridad progresiva; evidencia digital; análisis económico; cooperación; denuncias por faltas administrativas y procuración de justicia.

TÍTULO TERCERO. DE LAS AUTORIDADES EN MATERIA DE CIBERSEGURIDAD

Capítulo I. De la Oficina de Ciberseguridad

Capítulo II. Del Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad

Capítulo III. De las Unidades de Ciberseguridad

Capítulo IV. De la Fiscalía Especializada en Delincuencia Cibernética

En los artículos 29 a 42 se establecen las autoridades en materia de ciberseguridad, como las principales áreas encargadas de hacer cumplir el proyecto de ley. En dichos numerales se establece su objeto, los requisitos que tendrán que reunir las personas al frente de las autoridades y sus atribuciones.

Oficina de Ciberseguridad: será la autoridad encargada de coordinar los esfuerzos en materia de ciberseguridad y dependerá del titular del Poder Ejecutivo del Estado. Entre sus principales atribuciones tiene a su cargo la elaboración de la política general de ciberseguridad del Estado, la

cual será obligatoria para todas las autoridades estatales, así como la elaboración del índice de ciberseguridad.

EIRIC: es el Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad, el cual tiene por objeto la ejecución de acciones de inteligencia, preventivas y reactivas en materia de ciberseguridad, así como el análisis forense en la materia.

Unidades de Ciberseguridad: son las áreas encargadas de dar cumplimiento al proyecto de ley en cada autoridad estatal y aplicar la política general de ciberseguridad. Adicionalmente, podrán emitir políticas sectoriales de acuerdo con el sector al que pertenezcan.

Autoridad Investigadora: es la autoridad encargada de vigilar el cumplimiento del proyecto de ley desde el punto de vista del derecho administrativo sancionador.

Fiscalía Especializada en Delincuencia Cibernética: será la fiscalía con capacidades especializadas para la investigación de hechos que presumiblemente pueden constituir delitos en contra de la ciberseguridad del Estado.

Como se puede observar, la ciberseguridad es responsabilidad de todas las autoridades y en distintos frentes, que no puede atribuirse totalmente a una sola autoridad, ya que sería complicado de operar, por lo que se plantea la creación de una autoridad coordinadora, unidades ejecutoras, un equipo de inteligencia y de respuesta, una autoridad investigadora que indague y sancione incumplimientos en el ámbito administrativo, y una fiscalía especializada en el caso de la comisión de delitos en materia de ciberseguridad.

Todas estas autoridades necesitan los mejores perfiles profesionales a efecto de generar experiencia en la materia y perfeccionarse con el tiempo.

TÍTULO CUARTO. DE LAS POLÍTICAS EN MATERIA DE CIBERSEGURIDAD

Capítulo I. De la Política General de Ciberseguridad

Capítulo II. De las Políticas Sectoriales de Ciberseguridad

En los artículos 43 y 44 se establecen las políticas en materia de ciberseguridad. Una política general que establecerá los controles mínimos en la materia, que serán aplicados a todas las autoridades estatales, la cual se elaborará con la participación de todos los poderes estatales y organismos autónomos. Dada la división de poderes, si uno de ellos no está de acuerdo con la misma, deberá emitir su propia política que obligará a todas las autoridades que formen parte de dicho poder.

Es importante resaltar que, cada Unidad de Ciberseguridad podrá implementar controles adicionales a los previstos en la Política General que considere necesarios y, adicionalmente, podrá emitir una política sectorial de acuerdo con un sector o servicio público en específico. Lo cual busca brindar flexibilidad y apertura en su actuar.

TÍTULO QUINTO. DEL ÍNDICE, INFORMES Y EJERCICIOS EN MATERIA DE CIBERSEGURIDAD PARA LA MEJORA CONTINUA

Capítulo I. Del Índice de Ciberseguridad

Capítulo II. De los Informes Anuales en materia de Ciberseguridad

Capítulo III. De los Ejercicios en materia de Ciberseguridad

En los artículos 45 a 48 se establece la elaboración de un índice, informes y ejercicios en materia de ciberseguridad. El índice tiene como finalidad medir y evaluar las capacidades en todas las autoridades estatales en materia de ciberseguridad. Los informes, por su parte, tienen como finalidad reportar el grado de cumplimiento, los riesgos identificados, los ataques sufridos, de ser el caso, las áreas de oportunidad, entre otros. Los ejercicios tienen como finalidad ejecutar actividades controladas en donde se lleven a cabo auto ataques simulados, a efecto de analizar y evaluar las capacidades, entre ellas la de respuesta de las autoridades.

Todo lo anterior tiene como finalidad la mejora continua de la ciberseguridad en las autoridades estatales.

TÍTULO SEXTO. DE LOS PROVEEDORES TECNOLÓGICOS EXTERNOS

Capítulo I. De los Proveedores en materia de Ciberseguridad

Capítulo II. De los Proveedores de TIC

Capítulo III. De las Garantías para el Estado

En los artículos 49 a 55 se aborda lo relativo a los proveedores tecnológicos externos, entendiéndose por ellos las personas físicas y morales que presten servicios de TIC y de ciberseguridad a las autoridades, en donde se establecen obligaciones básicas y de relevancia para las autoridades estatales, dada la importancia de las inversiones a realizar en materia de ciberseguridad.

La primera, que los proveedores de servicios de ciberseguridad acrediten experiencia y que cuenten al menos con una certificación por una entidad reconocida; segunda, que sus productos y servicios cumplan con controles o especificaciones en materia de ciberseguridad; tercera, el establecimiento de sanciones y procedimientos claros en caso de incumplimiento, con sanciones proporcionales a los daños que puedan causar derivado de dichos incumplimientos; cuarta, de entrega de información y documentos; y, quinta, de respaldo y borrado seguro de información, de ser el caso.

En este sentido, y a efecto de cuidar los recursos que se invierten en la materia, el artículo 27 del proyecto de ley establece la obligación de realizar los análisis correspondientes a efecto de identificar, entre otros, los impactos económicos directos e indirectos de un ataque, con la finalidad

de tener un análisis de costo-beneficio; es decir, de la importancia de invertir o del costo de no hacerlo.

TÍTULO SÉPTIMO. DE LA OBLIGACIÓN DE COOPERACIÓN

Capítulo Único

En el artículo 56 se establece la obligación de todas las autoridades estatales de cooperar con la Oficina de Ciberseguridad con la información y documentos necesarios que estén relacionados con el cumplimiento del proyecto de ley y, en caso de incumplimiento, el requerimiento al titular de la autoridad estatal correspondiente y, si éste persiste, la vista a la Autoridad Investigadora para el inicio de los trámites de ley.

TÍTULO OCTAVO. DE LA INFORMACIÓN EN MATERIA DE CIBERSEGURIDAD

Capítulo Único

En los artículos 57 y 58 se establece que la información en materia de ciberseguridad que ponga en riesgo las finalidades previstas en el artículo 2 del proyecto de ley tendrá el carácter de reservada, dada la importancia de dicha información.

Asimismo, se establece que en la política general de ciberseguridad se establecerán los tipos de registros de cualquier acceso o acontecimiento en una tecnología de la información y comunicación que serán conservados y su plazo de conservación. Este aspecto de conservación de registros es importante en virtud de la probabilidad real de amenazas y ataques que aún no han sido descubiertos en las TIC de las autoridades, por lo que es necesario contar con registros-evidencias a efecto de su investigación y, en su caso, deslinde de responsabilidades. Este tema se relaciona con el contenido del artículo 24 del proyecto de ley.

TÍTULO NOVENO. DE LA ASISTENCIA Y COOPERACIÓN NACIONAL E INTERNACIONAL

Capítulo Único

En el artículo 59 del proyecto de ley se establece la posibilidad de que la Oficina de Ciberseguridad solicite asistencia a entidades nacionales e internacionales a efecto de desarrollar recursos humanos especializados en materia de ciberseguridad. Como ejemplo, el Instituto Federal de Telecomunicaciones, la Unión Internacional de Telecomunicaciones, la Organización de los Estados Americanos, la Organización para la Cooperación y el Desarrollo Económicos, el Banco Interamericano de Desarrollo, el *Forum of Incident Response and Security Teams* (FIRST), *The SANS Institute, Information Systems Audit and Control Association* (ISACA), *Computing Technology Industry Association* (CompTIA), Normalización y Certificación NYCE, S.C, entre otros.

Por su parte, el artículo 60 del proyecto de ley establece que las autoridades de ciberseguridad por sí, o a través de las autoridades competentes, y dentro del marco legal aplicable, podrán cooperar

y compartir información con otras autoridades estatales, federales e internacionales en asuntos de ciberseguridad.

TÍTULO DÉCIMO. DE LAS RESPONSABILIDADES EN MATERIA DE CIBERSEGURIDAD

Capítulo Único

En el artículo 61 del proyecto de ley se establece que todo acto u omisión de servidores públicos y prestadores de servicios de las autoridades estatales que incumpla el proyecto de ley o tenga por objeto o efecto contravenir o poner en riesgo las finalidades previstas en el artículo segundo del proyecto constituirá una falta administrativa grave en términos del artículo 50 de la Ley de Responsabilidades Administrativas para el Estado y Municipios de San Luis Potosí, por lo que serán investigadas y, en su caso, sancionadas en virtud de dicho ordenamiento.

Investigar y sancionar el incumplimiento en sede administrativa del proyecto de ley son actividades esenciales. De no hacerlo, la ley queda débil y propiciaría incumplimientos generalizados y recurrentes, por lo que este tema debe ser observado con máxima seriedad. De ahí que, se propone la calificación de falta administrativa grave, ya que no hay pequeños incumplimientos y, por más mínimos que sean, pueden poner en riesgo el objeto y finalidades del proyecto de ley.

TÍTULO DÉCIMO PRIMERO. DE LAS DELITOS EN CONTRA DE LA CIBERSEGURIDAD DEL ESTADO

Capítulo Único

En los artículos 62 a 71 se establecen los delitos en contra de la ciberseguridad del Estado, basados en los efectos que pueden generar las amenazas cibernéticas. Su investigación y sanción son esenciales a efecto de cumplir con el objeto y finalidades del proyecto de ley. Para ello, se propone la creación de la Fiscalía Especializada en Delincuencia Cibernética.

ARTÍCULOS TRANSITORIOS

Se proponen 7 artículos transitorios que establecen la entrada en vigor del proyecto de ley y de los plazos para llevar a cabo adecuaciones estructurales y el cumplimiento de diversas obligaciones.

Es menester resaltar que, el proyecto de ley busca generar experiencia en las autoridades estatales en la materia y abre la oportunidad de analizar la viabilidad de contar, en su momento, con una agencia estatal de ciberseguridad, autoridad que contará, al menos, con las atribuciones de la Oficina de Ciberseguridad.

Proyecto de iniciativa de nueva ley

Iniciativa de nueva ley, con proyecto de Decreto mediante la cual se expide la:

Ley de Ciberseguridad del Estado de San Luis Potosí y sus Municipios

TÍTULO PRIMERO

DISPOSICIONES GENERALES

Capítulo Único

Objeto

Artículo 1. La presente Ley es de orden público y tiene por objeto garantizar la seguridad cibernética del Estado de San Luis Potosí y sus municipios.

La seguridad cibernética será una herramienta utilizada y aprovechada para garantizar la gobernabilidad del Estado y como una capacidad de alto nivel para coadyubar en el desarrollo tecnológico, político, económico y social en el Estado de San Luis Potosí y sus municipios.

Finalidades

Artículo 2. La seguridad cibernética del Estado de San Luis Potosí y sus municipios tiene como finalidades garantizar:

I. El cumplimiento de las facultades, atribuciones y obligaciones de ley de las Autoridades, que en todo o en parte hagan uso de las tecnologías de la información y comunicación;

II. La disponibilidad, continuidad y confiabilidad de los procedimientos, trámites y servicios públicos de las Autoridades, que en todo o en parte hagan uso de las tecnologías de la información y comunicación;

III. La integridad, confidencialidad, disponibilidad, autenticidad y no repudio de la información en posesión de las Autoridades;

IV. La protección, funcionamiento, confiabilidad, rendimiento y disponibilidad de las tecnologías de la información y comunicación de las Autoridades o en su posesión;

V. La seguridad de servidores públicos, empresas y ciudadanos, cuya información esté en posesión de las Autoridades, y

VI. Generar y fortalecer la confianza digital de los servidores públicos, empresas y ciudadanos en los procedimientos, trámites y servicios públicos electrónicos a cargo de las Autoridades.

Las finalidades anteriores son críticas y esenciales para el adecuado funcionamiento de las Autoridades del Estado de San Luis Potosí.

Ámbito de aplicación

Artículo 3. Todas las autoridades, dependencias, entidades, órganos y organismos de los Poderes Ejecutivo, Legislativo y Judicial, los municipios, órganos, organismos autónomos, tribunales administrativos, fideicomisos y fondos públicos del orden estatal y municipal del Estado de San Luis Potosí están obligados a cumplir con esta Ley.

El cumplimiento de la presente Ley es independiente del cumplimiento de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de San Luis Potosí.

Contenido

Artículo 4. Para cumplir con el objeto de la presente Ley:

I. Se establecen obligaciones para las Autoridades a efecto de garantizar su seguridad cibernética, de los servidores públicos, de los prestadores de servicios y de los ciudadanos;

II. Se crea la autoridad encargada de liderar y coordinar los esfuerzos en materia de ciberseguridad en el Estado de San Luis Potosí;

III. Se crea un equipo de inteligencia y respuesta a incidentes de seguridad cibernética;

IV. Se crean las unidades de ciberseguridad como áreas encargadas de garantizar la seguridad cibernética de las autoridades;

V. Se crea la Fiscalía Especializada en Delincuencia Cibernética como parte de la Fiscalía General del Estado de San Luis Potosí;

VI. Se establece el tipo de falta administrativa para conductas que contravengan la presente Ley, y

VII. Se establecen los delitos en contra de la ciberseguridad del Estado de San Luis Potosí.

Definiciones

Artículo 5. Para los efectos de esta Ley se entenderá por:

I. **Amenaza cibernética**: cualquier circunstancia, situación, hecho, acción, omisión, incidente, evento de TIC y cualquier otra violación a políticas en materia de ciberseguridad con el potencial de dañar, perturbar, vulnerar, comprometer o poner en riesgo el cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley,

II. **Ataque**: la materialización de una amenaza cibernética;

III. **Autoridades**: todas las autoridades, dependencias, entidades, órganos y organismos de los Poderes Ejecutivo, Legislativo y Judicial, los municipios, órganos, organismos autónomos, tribunales administrativos, fideicomisos y fondos públicos del orden estatal y municipal del Estado de San Luis Potosí;

IV. **Autoridades en materia de ciberseguridad**: la Oficina de Ciberseguridad, el EIRIC, las Unidades de Ciberseguridad y la Fiscalía Especializada en Delincuencia Cibernética;

V. **Autoridad Investigadora:** la referida en el artículo 3°, fracción II, de la Ley de Responsabilidades Administrativas para el Estado y Municipios de San Luis Potosí;

VI. **Ciberseguridad o seguridad cibernética**:

A. Todas las actividades necesarias para preservar la operación, funcionamiento, disponibilidad, confiabilidad y continuidad de todas las actividades, procedimientos, trámites y servicios públicos de las Autoridades que dependan y/o hagan uso de las TIC en forma parcial o total o en cualquier parte de su proceso;

B. Todas las actividades necesarias para la protección de las TIC de las Autoridades o en su posesión, de sus usuarios y de terceros de amenazas cibernéticas y ataques;

C. La capacidad de preservar, al menos, la integridad, disponibilidad, confidencialidad, autenticidad y no repudio de la información en posesión de las Autoridades;

D. Cualquier actividad necesaria para prevenir, mitigar o suprimir amenazas cibernéticas, ataques o sus impactos, y

E. Cualquier otra actividad que sea necesaria para cumplir con las finalidades previstas en el artículo segundo de la presente Ley.

VII. **Dictamen de ciberseguridad:** la opinión técnica emitida por la Unidad de Ciberseguridad, en la que hace constar que todo proyecto, actividad, procedimiento, trámite y servicio de las Autoridades que en todo o en parte haga o pretenda hacer uso de las TIC cumple o no con los requisitos mínimos de ciberseguridad. Este dictamen aplica a cualquier contratación de servicios de TIC y de ciberseguridad.

VIII. **EIRIC:** el Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad del Estado de San Luis Potosí;

IX. **Estado:** el Estado Libre y Soberano de San Luis Potosí;

X. **Evento de TIC:** cualquier suceso o acontecimiento en una TIC;

XI. **Gestión de riesgos:** la identificación, valoración y ejecución de acciones para el control y mitigación del riesgo;

XII. **Ley:** la Ley de Ciberseguridad del Estado de San Luis Potosí y sus Municipios.

XIII. **Política general de ciberseguridad:** documento que establece los controles en materia de ciberseguridad necesarios para garantizar las finalidades previstas en el artículo segundo de la presente Ley;

XIV. **Política sectorial de ciberseguridad:** política complementaria a la política general de ciberseguridad, especializada en un sector gubernamental, procedimiento, trámite o servicio público específico;

XV. **Proveedores tecnológicos:** personas físicas o morales que presten servicios de TIC y de ciberseguridad;

XVI. **Resiliencia:** las capacidades de cualquier tipo para anticiparse, resistir, adaptarse, recuperarse y reducir la duración o impacto de una amenaza cibernética o ataque;

XVII. **Riesgo:** la posibilidad de materialización de una amenaza cibernética y sus consecuencias;

XVIII. **TIC:** las Tecnologías de la Información y Comunicación, que comprenden, al menos, todo tipo de tecnología en cualquier soporte para recolectar, almacenar, procesar, convertir, proteger, transferir, recuperar y/o cualquier otra interacción o actividad con cualquier tipo de información, datos, voz, imágenes y video. Incluye, infraestructura de cómputo, redes de telecomunicaciones, sistemas, bases de datos, hardware, software, plataformas, aplicaciones, interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital, sus componentes, medios que almacenen información, entre otros.

XIX. **Unidad de Ciberseguridad**: la unidad encargada de la ciberseguridad en las Autoridades, y

XX. **Vulnerabilidad**: la debilidad, error o defecto de cualquier tipo que pueda ser explotada por una amenaza cibernética.

Las definiciones anteriores se entenderán en singular o plural, según corresponda. A falta de definiciones expresas en la presente Ley, se aplicarán de manera supletoria las definiciones previstas en la Ley Federal de Telecomunicaciones y Radiodifusión, y las que se establezcan en las disposiciones que de esta Ley emanen.

Interpretación

Artículo 6. Corresponde a la Oficina de Ciberseguridad la interpretación de la presente Ley y de las disposiciones que de ésta emanen. Su interpretación estará sujeta al cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley.

Supletoriedad

Artículo 7. A falta de disposición expresa en la presente Ley, se aplicarán de manera supletoria las disposiciones del Código de Procedimientos Civiles del Estado de San Luis Potosí y la Ley de Procedimientos Administrativos del Estado y Municipios de San Luis Potosí.

TÍTULO SEGUNDO

DE LAS OBLIGACIONES ESTRUCTURALES EN MATERIA DE CIBERSEGURIDAD

Capítulo Único

Observancia general

Artículo 8. Las Autoridades deberán cumplir con las obligaciones en materia de ciberseguridad y su incumplimiento acarreará las responsabilidades y sanciones previstas en la presente Ley y demás ordenamientos legales.

Derechos humanos

Artículo 9. En la observancia y cumplimiento de la presente Ley, las Autoridades deberán respetar los derechos humanos previstos en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales en los que el Estado mexicano sea parte y en la Constitución Política del Estado.

Liderazgo

Artículo 10. Los titulares de las Autoridades u órganos de gobierno deberán liderar los esfuerzos necesarios para el cumplimiento de la presente Ley.

Por la obligación de liderazgo se entenderá todos los esfuerzos y gestiones para brindar facilidades y recursos económicos, técnicos y humanos especializados, necesarios y suficientes para cumplir con las finalidades previstas en el artículo segundo de la presente Ley.

Responsabilidad

Artículo 11. Los titulares de las Autoridades y de las Unidades de Ciberseguridad son responsables del cumplimiento de la presente Ley y de las disposiciones que de ésta emanen, en el ámbito de sus atribuciones.

Corresponsabilidad

Artículo 12. Los servidores públicos y prestadores de servicios de las Autoridades tienen la obligación de cumplir con las obligaciones previstas en la presente Ley y con las disposiciones que de ésta emanen.

Confianza digital

Artículo 13. Los titulares de las Autoridades y de las Unidades de Ciberseguridad deben realizar los esfuerzos que sean necesarios para generar, incrementar y fortalecer la confianza digital de los servidores públicos y ciudadanos en los procedimientos, trámites y servicios públicos electrónicos a su cargo.

Neutralidad tecnológica

Artículo 14. No se podrá excluir por disposición legal u orden administrativa una tecnología en particular que sea necesaria para el cumplimiento de la presente Ley, salvo que la misma contravenga su objeto.

Mejores prácticas

Artículo 15. Las Unidades de Ciberseguridad están obligadas a monitorear, identificar, analizar y, en su caso, implementar las mejores prácticas nacionales e internacionales en materia de ciberseguridad que coadyuven en el cumplimiento de la presente Ley.

Gestión de riesgos

Artículo 16. Las Unidades de Ciberseguridad deberán contar con procesos de gestión de riesgos.

Manejo de crisis y resiliencia

Artículo 17. Las Autoridades deberán de contar con protocolos de control de crisis y generar resiliencia en materia de ciberseguridad, incluidos planes de continuidad operativa.

Cultura de ciberseguridad

Artículo 18. Las Autoridades tienen la obligación de capacitar en materia de ciberseguridad, al menos dos veces por año, a todos sus servidores públicos y prestadores de servicios. De igual manera, tienen la obligación de abatir el desconocimiento en materia de ciberseguridad en empresas y ciudadanos, en particular, en niñas, niños y adolescentes.

Ciberseguridad primero

Artículo 19. Todo proyecto, actividad, procedimiento, trámite y servicio de las Autoridades que en todo o en parte haga o pretenda hacer uso de las TIC deberá contar de manera previa con un dictamen de ciberseguridad favorable.

Toda contratación que pretendan realizar las Autoridades de servicios de TIC y de servicios de ciberseguridad deberá contar de manera previa con el dictamen a que se refiere el párrafo anterior.

Proveedores y dependencias tecnológicas

Artículo 20. Las Autoridades deberán determinar sus dependencias tecnológicas y cadena de proveedores tecnológicos a efecto de la identificación de vulnerabilidades directas e indirectas que pongan o puedan poner en riesgo el cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley.

Punto de contacto

Artículo 21. Las Autoridades deberán contar con información de contacto, pública y disponible, las veinticuatro horas del día, los trescientos sesenta y cinco días del año, para la atención de asuntos en materia de ciberseguridad.

Máxima diligencia

Artículo 22. Todos los esfuerzos, acciones y obligaciones a efecto de cumplir con el objeto y finalidades de la presente Ley serán ejecutados por las Autoridades con la máxima diligencia.

Por máxima diligencia deberá entenderse el máximo cuidado, prudencia, agilidad y prontitud.

Ciberseguridad progresiva

Artículo 23. Las Autoridades deberán planear y destinar recursos suficientes y necesarios para el cumplimiento de la presente Ley. El presupuesto anual destinado y aprobado en materia de ciberseguridad por las Autoridades no podrá reducirse.

Evidencia digital

Artículo 24. Las Unidades de Ciberseguridad deberán documentar y configurar los controles en materia de TIC y de ciberseguridad, de tal manera que permitan generar evidencia de acciones u omisiones que, de manera directa o indirecta, dañen, perturben, vulneren, comprometan o pongan en riesgo las finalidades previstas en el artículo segundo de la presente Ley y que permitan constituir indicios o elementos de prueba para el inicio y sustanciación de procedimientos legales de responsabilidad administrativa y penal.

Impacto económico

Artículo 25. Las Autoridades deberán realizar los análisis necesarios a efecto de identificar los impactos económicos directos e indirectos en materia de Ciberseguridad. Los análisis contemplarán, al menos, inversiones, costos directos e indirectos de ataques y, en su caso, estimaciones.

Las Autoridades deberán tomar en consideración los análisis referidos en el párrafo anterior a efecto de cumplir con las finalidades previstas en el artículo segundo de la presente Ley y conducir de manera responsable y sustentada el cumplimiento de la presente Ley.

Cooperación institucional

Artículo 26. Las Unidades de Ciberseguridad deberán compartir información entre sí, con la Oficina de Ciberseguridad y con el EIRIC sobre vulnerabilidades, amenazas cibernéticas y ataques, a efecto de prevenirlos, mitigarlos o eliminar sus efectos.

Denuncias por faltas administrativas

Artículo 27. Todos los servidores públicos y prestadores de servicios de las Autoridades deberán denunciar ante la Autoridad Investigadora cualquier acto u omisión del que tengan conocimiento que contravenga lo previsto en la presente Ley.

Procuración de justicia

Artículo 28. Todos los servidores públicos y prestadores de servicios de las Autoridades, en caso de tener conocimiento de hechos que presumiblemente puedan constituir un delito en contra de la ciberseguridad del Estado, deberán presentar denuncia ante la Fiscalía Especializada en Delincuencia Cibernética del Estado.

TÍTULO TERCERO

DE LAS AUTORIDADES EN MATERIA DE CIBERSEGURIDAD

Capítulo I

De la Oficina de Ciberseguridad

Artículo 29. El Estado de San Luis Potosí contará con una Oficina de Ciberseguridad que dependerá de manera directa del titular del Ejecutivo del Estado, quien se encargará del estudio, diseño, análisis, instrumentación, coordinación y promoción de todas las acciones y esfuerzos necesarios en materia de ciberseguridad en el ámbito de las atribuciones que fijan esta Ley y demás disposiciones legales aplicables. En el ejercicio de sus atribuciones, la Oficina de Ciberseguridad estará dotada de autonomía técnica y de gestión para decidir sobre su funcionamiento y actuaciones.

La Oficina de Ciberseguridad contará con un equipo multidisciplinario con especialización técnica, legal y económica en la materia. El reglamento de la oficina establecerá la estructura y demás facultades con las que contará.

El titular de la Oficina de Ciberseguridad y el personal adscrito deberán guiarse por los principios de legalidad, objetividad, imparcialidad, certeza, eficiencia, eficacia, máxima diligencia, transparencia y rendición de cuentas.

Artículo 30. El titular de la Oficina de Ciberseguridad será nombrado y removido libremente por el titular del Ejecutivo del Estado.

Para ser titular de la Oficina de Ciberseguridad se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintinueve años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente;

V. Acreditar contar con conocimientos en materia de ciberseguridad y de TIC necesarios para el ejercicio del cargo, y

VI. Contar, al menos, con tres años de experiencia en el servicio público.

Artículo 31. La Oficina de Ciberseguridad tendrá las atribuciones siguientes:

I. Coordinar las acciones y esfuerzos en materia de ciberseguridad en el Estado y celebrar con las Autoridades los instrumentos adecuados para ello;

II. Elaborar la política general de ciberseguridad y modificarla cuando sea necesario;

III. Elaborar políticas sectoriales de ciberseguridad y modificarlas cuando sea necesario;

IV. Crear o modificar mediante acuerdo las áreas administrativas necesarias para su desempeño profesional, eficiente y eficaz, de acuerdo con su presupuesto autorizado;

V. Emitir opinión cuando lo considere pertinente o a solicitud de las Autoridades respecto de proyectos, actos o políticas de las Autoridades en la materia o relacionadas con las finalidades previstas en el artículo segundo de la presente Ley, sin que esas opiniones tengan efectos vinculantes. Las opiniones deberán publicarse;

VI. Promover una cultura de ciberseguridad en coordinación con las Autoridades;

VII. Asesorar a las Autoridades en la implementación de las políticas en materia de ciberseguridad;

VIII. Asesorar a las Autoridades en recursos humanos, técnicos y financieros en materia de ciberseguridad;

IX. Desarrollar capacidades en las Autoridades en materia de ciberseguridad;

X. Elaborar y publicar el índice de ciberseguridad del Estado;

XI. Elaborar programas de trabajo en materia de ciberseguridad;

XII. Elaborar informes cuatrimestrales de actividades que deberán ser presentados a los Poderes Ejecutivo y Legislativo del Estado;

XIII. Solicitar estudios que evalúen el desempeño de las facultades otorgadas a las Autoridades en materia de ciberseguridad, los cuales serán elaborados por expertos independientes;

XIV. Prestar asistencia y asesoramiento en el diseño y elaboración de leyes y reformas legales relacionadas con las TIC y la ciberseguridad en el Estado;

XV. Sensibilizar a los sectores educativos, empresariales y a la ciudadanía en materia de ciberseguridad;

XVI. Desarrollar, promover y solicitar estudios, trabajos de investigación e informes en materia de ciberseguridad;

XVII. Proponer modificaciones o mejoras a los planes de estudios a las instituciones educativas a efecto de mejorar el conocimiento, cultura y capacidades en materia de ciberseguridad;

XVIII. Compartir información de su competencia con las Autoridades correspondientes;

XIX. Emitir requerimientos de información y documentos relacionados con el ejercicio de sus atribuciones e integrar sus expedientes;

XX. Reiterar los requerimientos de información que formule en aquellos casos donde el desahogo de los mismos resulte insuficiente para tenerlos por desahogados;

XXI. Expedir copias certificadas, certificaciones o cotejos de los documentos existentes en las áreas a su cargo o que le sean presentados;

XXII. Expedir copias certificadas, certificaciones o realizar cotejos de documentos o información para integrarlos a sus expedientes;

XXIII. Emitir oficios de comisión a efecto de llevar a cabo las diligencias necesarias para el cumplimiento de sus atribuciones;

XXIV. Realizar a través de los servidores públicos adscritos las notificaciones de las determinaciones que emita, sin previo acuerdo de comisión;

XXV. Proporcionar la información que le sea requerida por cualquier autoridad administrativa o judicial;

XXVI. Emitir guías, lineamientos y cualquier documento que sea necesario para el cumplimiento de la presente Ley;

XXVII. Convocar a las Autoridades a reuniones y someter a su consideración asuntos de su competencia;

XXVIII. Participar en foros, reuniones, eventos y convenciones en materia de ciberseguridad;

XXIX. Presentar denuncias ante el ministerio público respecto de probables conductas delictivas en contra de la ciberseguridad del Estado de que tenga conocimiento y fungir como coadyuvante;

XXX. Presentar denuncias ante la Autoridad Investigadora por el incumplimiento de la presente Ley y de las disposiciones que de ésta emanen, y fungir como coadyuvante;

XXXI. Tramitar y resolver los asuntos de su competencia, y

XXXII. Las demás que le confieran esta Ley, su reglamento interno y otras disposiciones legales.

Capítulo II

Del Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad

Artículo 32. El Estado de San Luis Potosí contará con un EIRIC, que dependerá de manera directa del titular de la Oficina de Ciberseguridad, quien se encargará de la ejecución de las acciones de inteligencia, preventivas y reactivas en materia de ciberseguridad, así como del análisis forense en la materia.

El EIRIC contará con el personal necesario para el cumplimiento de su objeto. En su integración se adoptarán las mejores prácticas nacionales e internacionales.

Artículo 33. El titular del EIRIC será nombrado y removido libremente por el titular de la Oficina de Ciberseguridad.

Para ser titular del EIRIC se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintinueve años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente o, al menos, con una certificación vigente en la materia, emitida por entidad reconocida;

V. Acreditar contar con conocimientos técnicos en materia de ciberseguridad y de TIC necesarios para el ejercicio del cargo, y

VI. Acreditar contar, al menos, con cuatro años de experiencia en equipos de respuesta a incidentes de ciberseguridad, centros de operaciones de seguridad o equivalentes.

Artículo 34. El EIRIC cuenta con las atribuciones siguientes:

I. Coadyubar con la Oficina de Ciberseguridad en el cumplimiento de sus atribuciones previstas en la presente Ley y en las disposiciones de que de ésta emanen;

II. Realizar acciones de inteligencia y monitoreo de amenazas cibernéticas;

III. Analizar, diseñar, implementar y promover acciones preventivas en materia de Ciberseguridad;

IV. Realizar análisis forense que permita iniciar, sustanciar y aportar elementos de prueba en procedimientos de responsabilidad administrativa y penal;

V. Responder de manera inmediata con las herramientas a su alcance a efecto de contener, suprimir o mitigar los efectos de una amenaza cibernética, ataque o cualquier incidente que ponga en riesgo las finalidades previstas en el artículo segundo de la presente Ley;

VI. Dar aviso oportuno a las Autoridades correspondientes de cualquier amenaza cibernética;

VII. Emitir alertas en materia de ciberseguridad;

VIII. Desarrollar capacidades en las Unidades de Ciberseguridad que permitan replicar parte de sus actividades, y

IX. Las demás que le confieran esta Ley y otras disposiciones legales.

Capítulo III

De las Unidades de Ciberseguridad

Artículo 35. Todas las Autoridades contarán con una Unidad de Ciberseguridad, quienes serán las responsables de garantizar su seguridad cibernética y de cumplir con lo previsto en la presente Ley. Los municipios del Estado contarán, al menos, con una Unidad de Ciberseguridad.

Todas las áreas que conformen la estructura orgánica de las Autoridades están obligadas a cooperar con su Unidad de Ciberseguridad.

Artículo 36. El titular de la Unidad de Ciberseguridad de las Autoridades será nombrado y removido libremente por quien tenga facultades para ello.

Artículo 37. Para ser titular de la Unidad de Ciberseguridad se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintisiete años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente o con al menos una certificación vigente en la materia, emitida por entidad reconocida;

V. Acreditar contar con conocimientos técnicos en materia de Ciberseguridad y TIC necesarios para el ejercicio del cargo, y

VI. Acreditar contar, al menos, con cuatro años de experiencia en equipos de respuesta a incidentes de ciberseguridad, centros de operaciones de ciberseguridad o equivalentes.

Artículo 38. Las Unidades de Ciberseguridad cuentan con las atribuciones siguientes:

I. Aplicar la política general de ciberseguridad al interior de la Autoridad y, de ser el caso, diseñar e implementar los controles adicionales que considere necesarios;

II. Emitir políticas sectoriales en materia de ciberseguridad;

III. Desarrollar capacidades al interior de las Autoridades en materia de ciberseguridad;

IV. Preparar y recabar la información y documentos necesarios para la elaboración del índice a que se refiere el artículo 45 de la presente Ley;

V. Emitir los dictámenes a que se refiere el artículo 19 de la presente Ley y remitirlos a la Oficina de Ciberseguridad;

VI. Desahogar en tiempo y forma los requerimientos de información emitidos por la Oficina de Ciberseguridad y por el EIRIC;

VII. Emitir guías, lineamientos y cualquier documento que sea necesario para el cumplimiento de la presente Ley;

VIII. Emitir alertas en materia de ciberseguridad;

IX. Realizar con máxima diligencia cualquier acto que sea necesario para cumplir con las finalidades previstas en el artículo segundo de la presente Ley, y

X. Las demás que le confieran esta Ley y otras disposiciones legales.

Artículo 39. Una Unidad de Ciberseguridad podrá ser la responsable del cumplimiento de la presente Ley en dos o más Autoridades, cuando por el tamaño, estructura o presupuesto una Autoridad no pueda contar con su propia unidad.

La asunción de responsabilidad a que se refiere el párrafo anterior deberá formalizarse mediante acuerdo publicado en el Periódico Oficial del Estado, con la anuencia de los titulares de las

Autoridades y del titular de la Unidad de Ciberseguridad, quienes serán corresponsables del cumplimiento de la presente Ley.

Es responsabilidad de los titulares de las Autoridades analizar la viabilidad y procedencia del contenido del presente artículo, y asumir la responsabilidad del cumplimiento de la presente Ley en las Autoridades que así lo requieran en términos del párrafo primero del presente artículo.

Capítulo IV

De la Autoridad Investigadora

Artículo 40. La Autoridad Investigadora verificará, en el ámbito de su competencia, el cumplimiento de la presente Ley.

Capítulo V

De la Fiscalía Especializada en Delincuencia Cibernética

Artículo 41. La Fiscalía General del Estado contará con una Fiscalía Especializada en Delincuencia Cibernética, como autoridad con capacidades técnicas, encargada de la investigación de hechos que puedan constituir delitos en contra de la ciberseguridad del Estado, en términos de la legislación correspondiente.

La Fiscalía Especializada en Delincuencia Cibernética contará con un equipo multidisciplinario con especialización legal, técnica y económica en la materia. La Ley Orgánica de la Fiscalía General del Estado establecerá la estructura y atribuciones con las que contará.

Artículo 42. Para ser titular de la Fiscalía Especializada en Delincuencia Cibernética se deberán cumplir los requisitos siguientes:

I. Ser ciudadano mexicano, en pleno goce de sus derechos civiles y políticos;

II. Tener cuando menos veintinueve años cumplidos al día de su designación;

III. Gozar de buena reputación y no haber sido condenado por delito doloso que amerite pena de prisión;

IV. Contar con título y cédula profesional expedidos legalmente;

V. Acreditar contar con conocimientos legales en materia de ciberseguridad y de TIC necesarios para el ejercicio del cargo;

VI. Contar, al menos, con cuatro años de experiencia en el servicio público, y

VII. Los demás requisitos que la legislación correspondiente establezca.

TÍTULO CUARTO

DE LAS POLÍTICAS EN MATERIA DE CIBERSEGURIDAD

Capítulo I

De la Política General de Ciberseguridad

Artículo 43. El Estado contará con una política general de ciberseguridad, en la cual se establecerán los controles mínimos necesarios a efecto de cumplir con las finalidades previstas en el artículo segundo de la presente Ley.

La Oficina de Ciberseguridad realizará todas las gestiones, acciones y requerimientos necesarios a las Autoridades para la elaboración de la política prevista en el presente artículo.

En la elaboración de la política general de ciberseguridad participarán, al menos, un representante de los Poderes Ejecutivo, Legislativo y Judicial, así como de los órganos constitucionales autónomos. En caso de no lograr un consenso, cada poder y entidad autónoma emitirá su propia política general de ciberseguridad, la cual será obligatoria para todas sus autoridades adscritas.

La política general de ciberseguridad será de observancia obligatoria para todas las Autoridades, sus servidores públicos y prestadores de servicios.

Capítulo II

De las Políticas Sectoriales de Ciberseguridad

Artículo 44. El Estado podrá contar con políticas sectoriales de ciberseguridad, las cuales establecerán obligaciones específicas de acuerdo con las necesidades del sector gubernamental o público que corresponda.

Las Unidades de Ciberseguridad serán las responsables de analizar la pertinencia de emitir políticas sectoriales de Ciberseguridad.

La política sectorial de ciberseguridad será obligatoria para las Autoridades del sector correspondiente.

TÍTULO QUINTO

DEL ÍNDICE, INFORMES Y EJERCICIOS EN MATERIA DE CIBERSEGURIDAD PARA LA MEJORA CONTINUA

Capítulo I

Del Índice de Ciberseguridad

Artículo 45. El Estado de San Luis Potosí contará con un índice que mida y evalúe las capacidades de ciberseguridad de las Autoridades. Las Autoridades están obligadas a tomar en consideración los resultados del índice a efecto de mejorar sus capacidades en materia de seguridad cibernética.

Todas las Autoridades están obligadas a proporcionar la información y documentos necesarios, así como a brindar las facilidades necesarias para la elaboración del índice.

Las Autoridades son responsables de la veracidad de la información proporcionada para la elaboración del índice.

El Índice será publicado en la página de Internet de la Oficina de Ciberseguridad.

Capítulo II

De los informes anuales en materia de Ciberseguridad

Artículo 46. Las Unidades de Ciberseguridad deberán elaborar y rendir un informe anual en materia de Ciberseguridad que será presentado a su titular de la Autoridad y remitirá copia a la Oficina de Ciberseguridad.

La Oficina de Ciberseguridad establecerá los rubros que deberá contener el informe previsto en este artículo y elaborará un reporte con el contenido de los informes que le sean remitidos, el cual presentará a los Poderes Ejecutivo y Legislativo del Estado dentro de los tres primeros meses de cada año.

Artículo 47. La Oficina de Ciberseguridad elaborará y rendirá un informe anual sobre su actuar, que será presentado al titular del Poder Ejecutivo y al Poder Legislativo.

Capítulo III

De los Ejercicios en materia de Ciberseguridad

Artículo 48. Las Autoridades podrán realizar ejercicios controlados en materia de ciberseguridad a efecto de identificar vulnerabilidades y subsanar áreas de oportunidad.

TÍTULO SEXTO

DE LOS PROVEEDORES TECNOLÓGICOS EXTERNOS

Capítulo I

De los Proveedores en materia de Ciberseguridad

Artículo 49. Todos los proveedores de soluciones tecnológicas en materia de Ciberseguridad del Estado deberán acreditar experiencia y contar, al menos, con una certificación vigente en la materia, emitida por una entidad reconocida.

Todo proveedor que no acredite lo establecido en el párrafo anterior no podrá ser contratado por las Autoridades.

Capítulo II

De los Proveedores de TIC

Artículo 50. Todos los proveedores de TIC del Estado deberán acreditar que sus TIC cuentan con controles o especificaciones en materia de Ciberseguridad y, de ser el caso, que cumplen con lo previsto en el artículo 289 de la Ley Federal de Telecomunicaciones y Radiodifusión.

Todo proveedor que no acredite lo establecido en el párrafo anterior no podrá ser contratado por las Autoridades.

Capítulo III

De las Garantías para el Estado

Artículo 51. Todos los proveedores en materia de Ciberseguridad y de TIC deberán garantizar, según corresponda, que sus productos y servicios contribuirán en el cumplimiento de las finalidades previstas en el artículo segundo de la presente Ley.

Artículo 52. Todo contrato, convenio u equivalente, mediante el cual se formalice la prestación de servicios en materia de ciberseguridad y de TIC deberá establecer sanciones y procedimientos claros en caso de incumplimiento por parte de los proveedores.

Las sanciones serán proporcionales a los daños que se puedan causar.

Todo proveedor que no acepte por escrito el contenido del presente artículo no podrá ser contratado por las Autoridades.

Artículo 53. Todo contrato, convenio u equivalente, mediante el cual se formalice la prestación de servicios en materia de ciberseguridad y de TIC deberá establecer obligaciones a los proveedores de entrega de información y documentos de manera inmediata sobre los servicios prestados, así como sanciones y procedimientos claros en caso de incumplimiento por parte de los proveedores.

Las sanciones serán proporcionales a los daños que se puedan causar.

Todo proveedor que no acepte por escrito la obligación prevista en el presente artículo no podrá ser contratado por las Autoridades.

Artículo 54. De ser aplicable, todo contrato, convenio u equivalente, mediante el cual se formalice la prestación de servicios en materia de ciberseguridad y de TIC deberá establecer obligaciones relativas a respaldo y borrado seguro de información.

Artículo 55. Todas las Autoridades deberán de contar con un listado de sus proveedores en materia de ciberseguridad y de TIC.

TÍTULO SÉPTIMO

DE LA OBLIGACIÓN DE COOPERACIÓN

Capítulo Único

Artículo 56. Todas las Autoridades están obligadas a cooperar con la Oficina de Ciberseguridad, así como a brindar la información, soportes y documentos que sean necesarios y que estén relacionados con el cumplimiento de la presente Ley, en los formatos y plazos establecidos. Los requerimientos de información podrán ser a través de medios electrónicos.

En caso de incumplimiento a la obligación prevista en el párrafo anterior, el titular de la Oficina de Ciberseguridad notificará de manera directa al titular de la Autoridad para el inmediato cumplimiento del requerimiento de información. En caso de que persista el incumplimiento, se dejará constancia de ello y se notificará a la Autoridad Investigadora para el inicio de los procedimientos de ley.

Los incumplimientos previstos en al párrafo anterior, serán públicos en la página electrónica de la Oficina de Ciberseguridad.

TÍTULO OCTAVO

DE LA INFORMACIÓN EN MATERIA DE CIBERSEGURIDAD

Capítulo Único

Artículo 57. La información en materia de Ciberseguridad que ponga en riesgo las finalidades previstas en el artículo segundo de la presente Ley tendrá el carácter de reservada.

Las Autoridades en materia de ciberseguridad y personal adscrito estarán sujetos a responsabilidad en los casos de divulgación de la información en su posesión derivado del ejercicio de sus atribuciones.

Artículo 58. La política general de ciberseguridad establecerá los registros de eventos de TIC que serán conservados, su plazo de conservación y demás aspectos relevantes que se consideren necesarios para ello.

TÍTULO NOVENO

DE LA ASISTENCIA Y COOPERACIÓN NACIONAL E INTERNACIONAL

Capítulo Único

Artículo 59. La Oficina de Ciberseguridad podrá solicitar asistencia a entidades nacionales e internacionales a efecto de desarrollar recursos humanos especializados en el Estado en materia de ciberseguridad.

Artículo 60. Las Autoridades de ciberseguridad por sí, o a través de las autoridades competentes, y dentro del marco legal aplicable, podrán cooperar y compartir información con otras autoridades estatales, federales e internacionales en asuntos de ciberseguridad.

TÍTULO DÉCIMO

DE LAS RESPONSABILIDADES EN MATERIA DE CIBERSEGURIDAD

Capítulo Único

Artículo 61. Todo acto u omisión de servidores públicos y prestadores de servicios de las Autoridades que incumpla la presente Ley o tenga por objeto o efecto contravenir o poner en riesgo las finalidades previstas en el artículo segundo de la presente Ley constituirá una falta administrativa grave en términos del artículo 50 de la Ley de Responsabilidades Administrativas para el Estado y Municipios de San Luis Potosí.

Las conductas previstas en el presente artículo se investigarán y sancionarán en términos de la legislación prevista en el párrafo anterior, sin perjuicio de las responsabilidades de otra naturaleza a que haya lugar.

TÍTULO DÉCIMO PRIMERO

DE LAS DELITOS EN CONTRA DE LA CIBERSEGURIDAD DEL ESTADO

Capítulo Único

Artículo 62. Al que sin autorización y por cualquier medio reduzca o provoque la reducción en el rendimiento, en la capacidad, en la efectividad o en el funcionamiento de una red, sistema, página web, aplicación, dispositivo, equipo de cómputo o cualquier otra tecnología de la información y comunicación utilizada o en posesión de las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización vigente al momento de la ejecución de la conducta.

Artículo 63. Al que sin autorización y por cualquier medio interrumpa o provoque la interrupción o la pérdida de la capacidad para usar una red, sistema, página web, aplicación, dispositivo, equipo de cómputo o cualquier otra tecnología de la información y comunicación utilizada o en posesión de las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Artículo 64. Al que sin autorización introduzca o provoque la introducción por cualquier medio de programas de cómputo o códigos informáticos en redes, sistemas, páginas web, aplicaciones, dispositivos, equipos de cómputo o en cualquier otra tecnología de la información y comunicación que afecten la disponibilidad, integridad, autenticidad, confidencialidad o no repudio de la información utilizada o en posesión de las Autoridades o confidencialidad de sus comunicaciones, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización vigente al momento de la ejecución de la conducta.

Artículo 65. Al que sin autorización y por cualquier medio utilice privilegios, credenciales, nombres de usuarios o contraseñas para acceder a información o a las tecnologías de la información y comunicación en posesión de las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización vigente al momento de la ejecución de la conducta.

Artículo 66. Al que sin autorización y por cualquier medio monitoree una tecnología de la información y comunicación o intercepte información soportada, procesada o transmitida en una tecnología de la información y comunicación utilizada o en posesión de las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Artículo 67. Al que sin autorización y por cualquier medio modifique, elimine o provoque la modificación o eliminación de información, bases de datos o archivos almacenados, procesados o transmitidos en las tecnologías de la información y comunicación utilizadas o en posesión de las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Artículo 68. Al que sin autorización y por cualquier medio modifique o provoque la modificación de la configuración de los controles de ciberseguridad en las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Artículo 69. Al que sin autorización y por cualquier medio divulgue o provoque la divulgación, comparta gratuitamente, intercambie o comercialice información o bases de datos en posesión de las Autoridades, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Artículo 70. Al que sin autorización y por cualquier medio firme cualquier tipo de documento electrónico o mensaje de datos utilizando un certificado digital de firma electrónica o digital del que no sea titular, se le impondrán de tres meses a tres años de prisión y de quinientas a tres mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Artículo 71. Al que genere, divulgue, comparta gratuitamente, intercambie, comercialice u obtenga información por cualquier medio para cometer los delitos previstos en los artículos 62, 63, 64, 65, 66, 67, 68, 69 y 70 de la presente ley, se le impondrán de seis meses a diez años de prisión y de quinientas a cinco mil veces el monto de la unidad de medida y actualización, vigente al momento de la ejecución de la conducta.

Transitorios

Artículo Primero. El presente decreto entrará en vigor al día hábil siguiente a su publicación en el Periódico Oficial del Estado.

Artículo Segundo. En un plazo no mayor a sesenta días naturales a partir de la entrada en vigor del presente decreto, el titular del Ejecutivo del Estado deberá realizar las modificaciones correspondientes a su estructura orgánica a efecto de contar con la autoridad a que se refiere el artículo 29 de la presente Ley y deberá emitir su reglamento interno, el cual deberá incluir al EIRIC.

Artículo Tercero. En un plazo no mayor a sesenta días naturales a partir de la entrada en vigor del presente decreto, los titulares de las Autoridades deberán realizar las modificaciones correspondientes a sus estructuras orgánicas o equivalentes a efecto de contar con las unidades a que se refiere el artículo 35 de la presente Ley.

Artículo Cuarto. En un plazo no mayor a sesenta días naturales a partir de la entrada en vigor del presente decreto, la autoridad competente deberá publicar el instrumento de creación de la fiscalía a la que se refiere el artículo 41 de la presente Ley.

Artículo Quinto. En un plazo de dos años contado a partir de la entrada en vigor del presente decreto, el titular de la Oficina de Ciberseguridad presentará al titular del Ejecutivo del Estado y al Poder Legislativo un informe en el que analice la pertinencia de mejorar las capacidades en materia de ciberseguridad mediante la creación de una agencia estatal en la materia, entidad que contará, al menos, con las facultades y atribuciones de la Oficina de Ciberseguridad.

Artículo Sexto. Dentro de un plazo no mayor a quince días naturales a partir de su creación, las Unidades de Ciberseguridad deberán dar cumplimiento a lo previsto en el artículo 21 de la presente Ley y notificarlo a la Oficina de Ciberseguridad.

Artículo Séptimo. Dentro de un plazo no mayor a ciento ochenta días naturales contados a partir de su creación, las Unidades de Ciberseguridad deberán emitir el dictamen previsto en el artículo 5, fracción VII, de la presente Ley respecto de las TIC que estén siendo utilizadas por las Autoridades al momento de la entrada en vigor de la presente Ley y enviarlo a la Oficina de Ciberseguridad.

Artículo Octavo. Concluidos los plazos previstos en los artículos segundo y tercero transitorios anteriores, la Oficina de Ciberseguridad contará con un plazo de ciento ochenta días naturales para emitir la política a que se refiere el artículo 43 de la presente Ley.

Artículo Noveno. Se derogan todas aquellas disposiciones legales que se opongan al presente decreto.

[Término de la iniciativa]
****

Conclusiones

La presente iniciativa tiene como finalidad que las Autoridades del Estado de San Luis Potosí y sus municipios comiencen su andar en un andamiaje básico, dinámico, prospectivo, basado en un marco legal, institucional y coordinado a efecto de adentrarse en los grandes y complejos retos que ya representan las amenazas a la ciberseguridad. De no hacerlo o posponerlo, continuará la predisposición gubernamental a ser más vulnerables a las amenazas cibernéticas y, como consecuencia, tendrán que hacer frente a las responsabilidades que ello conlleva.

Observen la oportunidad, comiencen el análisis, discutan ampliamente, enriquezcan el proyecto con su experiencia y aprueben la presente iniciativa, en beneficio de todos, y tengan en cuenta lo siguiente:

> La seguridad pública en nuestro entorno tangible y la seguridad cibernética tienen un común denominador, ambas son realmente complejas, la diferencia es que sólo en una de ellas hemos generado un marco legal, experiencia y capacidades.

En mi calidad de ciudadano potosino interesado por la mejora del Estado de San Luis Potosí, cuenten con mi tiempo para la explicación y discusión de este tema que nos compete a todos, al amparo de un parlamento abierto.

Por lo expuesto y con fundamento en los artículos señalados en el inicio de este escrito, solicito a ese Congreso del Estado de San Luis Potosí se den los trámites de ley respecto de esta iniciativa de nueva ley, mediante la cual se expida la "Ley de Ciberseguridad del Estado de San Luis Potosí y sus Municipios".

Acompaño al presente lo siguiente:

Anexo 1. Dispositivo de almacenamiento de datos, el cual contiene el presente escrito en versión digitalizada.
Anexo 2. Datos personales de identificación y contacto, los cuales solicito sean resguardados como información confidencial.

La seguridad cibernética es una causa de interés público que nos compete a todos.

Atentamente

Jonathan López Torres

www.jonathanlopeztorres.org