ACUERDO MEDIANTE EL CUAL SE APRUEBA LA INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY DE CIBERSEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES PARA LA CIUDAD DE MÉXICO.

Acordado en Sesión Ordinaria celebrada el **veintiséis de marzo de dos mil veinticinco**, por **unanimidad** de votos, de los integrantes del Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, conformado por las Comisionadas y los Comisionados Ciudadanos, que firman al calce, ante Miriam Soto Domínguez, Secretaria Técnica, de conformidad con lo dispuesto en el artículo 15, fracción IX del Reglamento Interior de este Instituto, para todos los efectos legales a que haya lugar.

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
64bab33d32780b8156a0064185365ed(

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ
COMISIONADA PRESIDENTA

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
17eedcefffcfb8f599e2dd43115d3f12

JULIO CÉSAR BONILLA GUTIÉRREZ
COMISIONADO CIUDADANO

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
49c3322f9fae81f8a527961bf6a8deed

MARÍA DEL CARMEN NAVA POLINA
COMISIONADA CIUDADANA

MIRIAM SOTO DOMÍNGUEZ
SECRETARIA TÉCNICA

Este documento fue firmado electrónicamente. La firma CDMX tendrá validez en el documento digital.

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
04b4409fc95a0c7d80f5f9fa93704c8c

ACUERDO MEDIANTE EL CUAL SE APRUEBA LA INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY DE CIBERSEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES PARA LA CIUDAD DE MÉXICO.

CONSIDERANDO

1. Que el artículo 116, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos (Constitución Federal), prevé que, en las Constituciones de las Entidades Federativas, se establecerá la creación de organismos autónomos, especializados, imparciales y colegiados, responsables de garantizar los derechos de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, conforme a los principios y bases establecidos por el artículo 6°, párrafo segundo de la Constitución Federal.

2. Que de conformidad con lo establecido en los artículos 46, Apartado A, inciso d) y 49 de la Constitución Política de la Ciudad de México (Constitución local); 37, primer párrafo de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (Ley de Transparencia) y 78 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados de la Ciudad de México (Ley de Datos), el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (Instituto) es un Órgano Autónomo, de carácter especializado, independiente, imparcial y colegiado, con personalidad jurídica y patrimonio propio, cuenta con plena autonomía técnica, de gestión y financiera, con capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, funcionamiento y resoluciones; es responsable de garantizar el cumplimiento de la Ley de Transparencia, dirigir y vigilar el ejercicio de los Derechos de Acceso a la Información y la Protección de Datos Personales, conforme a los principios y bases establecidos por el artículo 6º párrafo segundo y 16 de la Constitución Federal; y demás preceptos aplicables de la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia) y la propia Ley de Transparencia.

3. Que el artículo 79, fracción XVII de la Ley de Datos refiere que el Instituto, entre otras, tendrá las atribuciones establecer en su ámbito de competencia, políticas y lineamientos para el manejo, tratamiento y protección de los sistemas de datos personales que estén en posesión de sujetos obligados, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley de Datos.

4. Que de acuerdo con lo establecido en el artículo 62 de la Ley de Transparencia, el Pleno de este Instituto es el órgano superior de dirección que tiene la responsabilidad de vigilar el cumplimiento de las disposiciones constitucionales y legales en materia de transparencia, acceso a la información y protección de datos personales en la Ciudad de México.

Calle de La Morena No. 865, Local 1, "Plaza de la Transparencia", Col. Narvarte Poi
C.P. 03020, Alcaldía Benito Juárez, Ciudad de México.
Teléfono: 55 56 36 21 20

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
04b4409fc95a0c7d80f5f9fa93704c8c

5. Que de acuerdo con lo establecido en los artículos 57, párrafo primero; 67, inciso a) de la fracción II; y, 71, fracción XVIII, de la Ley de Transparencia, el Instituto podrá en todo momento presentar iniciativas de leyes o decretos ante el Congreso de la Ciudad de México en las materias de su competencia; en ese sentido, el Pleno del Instituto cuenta con la facultad, en materia regulatoria, de aprobar dichas iniciativas de leyes o decretos, para después presentarlas al Poder Legislativo Local, por conducto de su Comisionada Presidenta.

6. Que el veintisiete de febrero de dos mil diecinueve, el Pleno de este órgano garante aprobó su Reglamento Interior mediante acuerdo 0313/SO/27-02/2019; el cual es de observancia general y obligatoria para las unidades administrativas y personal del Instituto, que tiene por objeto establecer normas que regulan el funcionamiento y operación de la estructura orgánica para el correcto ejercicio de sus atribuciones.

7. Que de conformidad con lo señalado en los artículos 9 y 10 del Reglamento Interior del Instituto de Transparencia, Acceso a la Información, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (Reglamento interior), el Pleno del Instituto funcionará y tomará sus decisiones de manera colegiada ajustándose al principio de igualdad entre sus integrantes, siendo la autoridad frente a las Comisionadas y Comisionado en su conjunto y en lo particular, sus resoluciones son obligatorias para éstos, aunque estén ausentes o sean disidentes al momento de tomarlas. Las decisiones y resoluciones se adoptarán por mayoría simple. En caso de empate, la Comisionada Presidenta resolverá con voto de calidad en términos de lo señalado por el artículo 63 de la Ley de Transparencia.

8. Que de conformidad con el artículo 14, fracción XVI, es atribución de las Comisionadas y los Comisionados Ciudadanos proponer a la Comisionada Presidenta asuntos para integrarlos en el orden del día, en los términos del Reglamento de Sesiones del Pleno del Instituto, y de conformidad con el artículo 7 Fracciones IV, V y VI del Reglamento de Sesiones del Pleno de este Instituto, corresponde a las Comisionadas y Comisionados remitir previamente a las demás personas integrantes del Pleno, a la Secretaría Técnica, y en su caso a las Unidades Administrativas, los proyectos que serán sometidos a consideración del Pleno, así como someter a consideración del Pleno cualquier asunto de la competencia del Instituto e instruir a la persona titular de la Secretaría Técnica, la inclusión, retiro o diferimiento de asuntos en el proyecto de orden del día, de conformidad con la Ley de Transparencia, el Reglamento Interior y este Reglamento de Sesiones.

Calle de La Morena No. 865, Local 1, "Plaza de la Transparencia", Col. Narvarte Poi
C.P. 03020, Alcaldía Benito Juárez, Ciudad de México.
Teléfono: 55 56 36 21 20

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
04b4409fc95a0c7d80f5f9fa93704c8c

9. Que de conformidad con los numerales 5, 6, 7 y 8 de los Considerandos de este acuerdo, la Comisionada Presidenta Laura Lizette Enríquez Rodríguez presenta la **"INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY DE CIBERSEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES PARA LA CIUDAD DE MÉXICO''** para ser presentada ante el Poder Legislativo de la Ciudad de México, por su conducto en calidad de Presidenta del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México

Por las consideraciones y fundamentos anteriormente expuestos, el Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México emite el siguiente:

ACUERDO

PRIMERO. Se aprueba la **''INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY DE CIBERSEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES PARA LA CIUDAD DE MÉXICO''**, misma que se integra al presente acuerdo como **ANEXO ÚNICO**, formando parte integral del mismo.

SEGUNDO. Se aprueba la presentación de la **''INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY DE CIBERSEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES PARA LA CIUDAD DE MÉXICO''** ante el Poder Legislativo de la Ciudad de México, por conducto de la Comisionada Presidenta del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, **Mtra. Laura Lizette Enríquez Rodríguez**.

TERCERO. El presente Acuerdo entrará en vigor el día de su aprobación por el Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

CUARTO. Se instruye a la Secretaría Técnica para que el presente Acuerdo sea incorporado al portal de Internet del Instituto.

Calle de La Morena No. 865, Local 1, "Plaza de la Transparencia", Col. Narvarte Poi
C.P. 03020, Alcaldía Benito Juárez, Ciudad de México.
Teléfono: 55 56 36 21 20

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
04b4409fc95a0c7d80f5f9fa93704c8c

Ley de Ciberseguridad en materia de Protección de Datos Personales para la Ciudad de México

Exposición de motivos

Los avances de la transformación digital a nivel mundial y el uso de nuevas tecnologías, como es el caso la inteligencia artificial, ha traído grandes beneficios para mejorar la calidad de vida de las personas y mejorar las economías de los países; sin embargo, también representa nuevos riesgos para garantizar la confianza en el entorno digital.

El *Global Cybersecurity Outlook 2025. Insight Report, January 2025*[1] del *World Economic Forum*, refiere que el sector público se ha visto afectado de manera desproporcionada, ya que el 38% de los encuestados informaron de una resiliencia insuficiente en este sector, en comparación con el 10% de las organizaciones medianas y grandes del sector privado. Además de que esta desigualdad se extiende a la fuerza laboral cibernética, ya que el 49% de las organizaciones del sector público indican que carecen del talento necesario para cumplir sus objetivos de ciberseguridad. Lo cual, sumado a los avances en inteligencia artificial y la sofisticación de los ciberataques, plantean riesgos como el acceso no autorizado que podrían conducir a violaciones a la privacidad y un posible uso indebido de los datos personales.

A nivel de país, el *National Cyber Security Index (NCSI)*[2], índice global en tiempo real que mide el grado de preparación de los países para prevenir las amenazas cibernéticas y gestionar los incidentes cibernéticos, identifica que entre las amenazas cibernéticas fundamentales se encuentra la violación de la confidencialidad de los datos y para el caso de México a enero de 2024 le otorgó un 38.33% de cumplimiento sobre 100%, considerando su total cumplimiento en el indicador de protección de datos personales al contar con una legislación en la materia y una autoridad supervisora pública para su aplicación; sin embargo, aún no cumple con otros indicadores ya que no cuenta con un marco normativo en materia de ciberseguridad.

Por otra parte, el *Índice de Desarrollo Digital Estatal (IDDE) 2024* del Centro México Digital[3], que ofrece una visión completa del nivel de desarrollo digital y los avances de cada entidad, ubica a la Ciudad de México en primer lugar, y resalta un puntaje de 100% respecto del indicador de digitalización de trámites, lo cual inevitablemente tiene aparejado retos en materia de ciberseguridad, caracterizado por un aumento exponencial en la frecuencia y sofisticación de ciberataques, tales como ransomware, robo masivo de datos personales, phishing, denegación de servicio distribuida (DDoS) y ataques a infraestructuras críticas, que no sólo comprometen la seguridad de sistemas esenciales para la operatividad gubernamental, sino también generan brechas de datos personales que hacen vulnerables a las personas y lesionan el ejercicio de sus derechos.

---

[1] *Global Cybersecurity Outlook 2025. Insight Report, January 2025* del Foro Económico Mundial, elaborado en colaboración con Accenture, examina las tendencias de ciberseguridad que afectarán a las económicas y sociedades en el próximo año.

[2] https://ncsi.ega.ee/country/mx/

[3] El IDDE utiliza una metodología estadística de índices compuestos que agrupa 71 variables en 12 subpilares y 3 pilares principales: 1) Infraestructura, 2) Digitalización de las personas y la sociedad y 3) Innovación y adopción tecnológica en las empresas.

Ante este panorama, la presente Ley de Ciberseguridad en Materia de Protección de Datos Personales para la Ciudad de México, tiene como objetivo fortalecer las capacidades técnicas, operativas y de gestión de incidentes vinculados a la protección de datos personales; la resiliencia y capacidades de prevención en su tratamiento indebido; promover la ciberseguridad y fomentar la generación de talento, para el fortalecimiento de la confianza digital; así como difundir una cultura de ciberseguridad entre los sujetos obligados y los titulares de los datos personales.

Lo anterior a fin de reforzar las obligaciones que ya establecen tanto la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México como los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, respecto del deber de seguridad, sobre todo respecto de los incidentes que potencialmente pudieran llevar a una vulneración de datos personales.

En este sentido se establecen que los sujetos obligados deberán designar a una persona responsable que coordine las acciones de ciberseguridad, así como contar con una Estrategia de Ciberseguridad, un Sistema de Gestión de Seguridad de la Información que integre los documentos de seguridad de cada uno de los sistemas de datos personales, el deber de capacitar, certificar y fomentar la profesionalización de sus servidores públicos en materia de ciberseguridad; así como de fomentar una cultura de ciberseguridad y mejores prácticas, entre otras.

También le otorga al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFOCDMX), la facultad de solicitar a los sujetos obligados que hayan sufrido una vulneración de datos personales, un dictamen pericial en materia informática, que le permita determinar las condiciones en las que ésta se dio a fin de emitir recomendaciones técnicas y administrativas en materia de protección de datos personales, así como orientar al sujeto obligado respecto de las medidas correctivas y preventivas que resulten necesarias.

De manera adicional, se establece que el INFOCDMX coordinará las acciones en materia de cultura de ciberseguridad entre los sujetos obligados y los titulares de los datos personales; desarrollará acciones de concientización, difusión y fomento de la ciberseguridad para la población de la Ciudad de México e impulsará la adopción de programas de capacitación, certificación y profesionalización de las habilidades, conocimientos y capacidades de los sujetos obligados en materia de ciberseguridad.

Estas medidas buscan fortalecer la confianza digital de la población de la Ciudad de México y ser un referente de la protección de los datos personales para la construcción de un gobierno electrónico seguro. La privacidad y la seguridad de la información no son meros desafíos técnicos, sino pilares esenciales de la confianza institucional y la salvaguarda de la dignidad de las personas en la era digital. Por ello, esta ley se erige como un instrumento indispensable para garantizar el derecho fundamental a la protección de datos personales y la seguridad en el ciberespacio.

Ley de Ciberseguridad en materia de Protección de Datos Personales para la Ciudad de México

TÍTULO PRIMERO
DISPOSICIONES GENERALES
Capítulo Único

Artículo 1. La presente Ley es de orden e interés público en la Ciudad de México y tiene por objeto establecer las bases, principios y requisitos en materia de ciberseguridad a fin de robustecer el cumplimiento de los deberes de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en la Ciudad de México.

Son sujetos obligados por esta Ley, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, partidos políticos, fideicomisos y fondos públicos de la Ciudad de México.

Artículo 2. La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, la Constitución Política de la Ciudad de México, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, la Ley de Archivos de la Ciudad de México y demás normatividad aplicable, favoreciendo en todo momento, la protección más amplia para las personas físicas.

Artículo 3. Son objetivos de esta ley:

I. Establecer directrices para fortalecer las capacidades técnicas, operativas y de gestión de incidentes de los sujetos obligados, vinculados a la protección de datos personales ante las amenazas en el ciberespacio, así como fortalecer su resiliencia;
II. Fortalecer las capacidades de prevención en el tratamiento indebido de datos personales en posesión de los sujetos obligados;
III. Promover la ciberseguridad entre los sujetos obligados y fomentar la generación de talento, para el fortalecimiento de la confianza digital;
IV. Difundir una cultura de ciberseguridad entre los sujetos obligados y los titulares de los datos personales.

Artículo 4. Además de las definiciones establecidas en el artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, artículo 6 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y 4 de la Ley de Archivos de la Ciudad de México, para los efectos de esta ley se entenderá por:

I. **Activo:** Cualquier recurso, sistema, infraestructura o elemento tecnológico utilizado para el tratamiento de datos personales según el nivel de riesgo y sensibilidad, tanto por el responsable, encargado o terceros;
II. **Amenaza**: cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones del sujeto obligado;
III. **Ciberseguridad:** conjunto de herramientas, políticas, conceptos de seguridad, controles de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para

proteger los activos de información de los sujetos obligados y los usuarios en el ciberentorno;

IV. **Confidencialidad:** atributo que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados;

V. **Controles de seguridad de la información**: las medidas de seguridad establecidas para preservar la confidencialidad, integridad y disponibilidad de los activos de información del sujeto obligado contra las amenazas latentes o existentes y, que coadyuvan en la gestión de riesgos inherentes a su uso de acuerdo con lo establecido en el sistema de gestión de seguridad de datos personales de dicho sujeto obligado;

VI. **Comité Interno de Ciberseguridad**: instancia a la que hace referencia el artículo 12 de la presente Ley;

VII. **Disponibilidad:** atributo que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado;

VIII. **Estándares técnicos:** conjunto de especificaciones, directrices, y requisitos técnicos diseñados para proteger sistemas, redes, aplicaciones, datos e infraestructuras contra amenazas y vulnerabilidades a los que están expuestos los sujetos obligados;

IX. **Estrategia de Ciberseguridad:** Documento que integra el conjunto de políticas, procedimientos, tecnologías, mecanismos y acciones que el sujeto obligado establece para proteger sus activos en el cumplimiento de los deberes de seguridad y confidencialidad en materia de protección datos personales;

X. **Gestión de riesgos**: empleo de técnicas y procedimientos para el seguimiento continuo del estado de ciberseguridad de la información del sujeto obligado que implique el tratamiento de datos personales;

XI. **Incidente (seguridad de la información):** corresponde al evento o serie de eventos de seguridad de la información no deseados o inesperados, que pueda comprometer las funciones esenciales del sujeto obligado y/o comprometer la confidencialidad, integridad o disponibilidad de los datos personales;

XII. **Instituto:** Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México;

XIII. **Integridad:** atributo que consiste en que la información no ha sido modificada o destruida sin autorización;

XIV. **Ley de Archivos:** La Ley de Archivos de la Ciudad de México;

XV. **Ley de Ciberseguridad:** La Ley de Ciberseguridad en materia de Protección de Datos Personales para la Ciudad de México;

XVI. **Ley de Datos:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;

XVII. **Ley de Transparencia:** Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;

XVIII. **Lineamientos:** Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;

XIX. **Riesgo:** posibilidad de ocurrencia de un incidente de ciberseguridad (la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias de este);

XX. **Seguridad de la Información**: la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma mediante la adopción de aspectos técnicos, organizacionales y humanos;

XXI. **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de políticas, procedimientos, directrices y recursos que están diseñados para gestionar

y proteger la información dentro del sujeto obligado. El objetivo de un SGSI es garantizar la **confidencialidad**, **integridad** y **disponibilidad** de la información mediante la aplicación de un enfoque basado en la gestión del riesgo, controlando las amenazas y vulnerabilidades que puedan afectarla;

XXII. **TIC:** Tecnologías de la Información y la Comunicación;

XXIII. **Vulnerabilidad**: debilidad presente en un activo de información que potencialmente permitirá que una amenaza impacte de manera negativa, con posibles afectaciones para la seguridad del a información dentro del sujeto obligado.

TÍTULO SEGUNDO
DE LOS PRINCIPIOS Y DEBERES
Capítulo Único

Artículo 5. Además de los principios y deberes establecidos en los Capítulos I y II del Título Segundo de la Ley de Datos, Capítulo II de la Ley de Transparencia y 5 de la Ley de Archivos, para los efectos de esta ley se observarán los siguientes principios generales:

I. **Control de daños:** frente a un ciberataque o a un incidente de ciberseguridad que comprometa datos personales, los sujetos obligados deben adoptar las medidas necesarias para evitar su escalada o posible propagación a otros sistemas informáticos;

II. **Cooperación:** para resolver los incidentes de ciberseguridad que comprometan datos personales, deberán prevalecer la cooperación con el Instituto y, si es necesario, cooperar entre diversos sectores u otros sujetos obligados, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios;

III. **Seguridad en el ciberespacio:** los sujetos obligados deben otorgar especial protección a las redes y sistemas informáticos que traten datos personales;

IV. **Respuesta responsable:** en la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques que comprometan datos personales, los sujetos obligados no podrán llevar a cabo ni apoyar operaciones ofensivas;

V. **Seguridad de la información:** además de las medidas de seguridad técnicas establecidas en la Ley de datos y demás normatividad en la materia, los sujetos obligados deben adoptar las medidas técnicas de seguridad de la información que consideren necesarias, incluyendo el cifrado, a fin de salvaguardar los datos personales que trate; y

VI. **Seguridad y privacidad por defecto y desde el diseño**: los sistemas informáticos, aplicaciones y tecnologías de la información que diseñen, usen o implementen los sujetos obligados que incluya algún tratamiento de datos personales, deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos que se procesan.

Artículo 6. Los sujetos obligados atenderán los siguientes deberes generales en materia de ciberseguridad:

I. **Contar con una Estrategia de Ciberseguridad,** que contendrá los elementos establecidos en el artículo 16 de esta Ley y deberá incluir un enfoque de gestión de riesgos y protección de datos personales;

II. **Designar a una persona responsable de coordinar las acciones de ciberseguridad**, el cual deberá al menos tener el mismo nivel del Oficial de

Protección de Datos Personales, el cual tendrá las funciones establecidas en el artículo 11 de la presente Ley;

III. **Establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de Información (SGSI)**, que integre los documentos de seguridad de cada uno de los sistemas de datos personales, en los términos de los lineamientos que para ese efecto se publiquen;

IV. **Reportar incidentes de seguridad,** en los que se haya configurado alguna vulneración de las establecidas en el artículo 31 y 33 de la Ley de Datos, 59 y 60 de los Lineamientos o el artículo 7 fracción II de la presente Ley;

V. **Capacitar y certificar a los servidores públicos en materia de ciberseguridad**, así como concientizar a cualquier persona involucrada en la prestación de servicios contratados por el sujeto obligado;

VI. **Fomentar una cultura de ciberseguridad y mejores prácticas en materia de seguridad de la información**, entre los sujetos obligados y los titulares de los datos personales; y

VII. **Fomentar la profesionalización en materia de ciberseguridad** para los servidores públicos de los sujetos obligados.

Artículo 7. En adición al artículo anterior, los sujetos obligados atenderán los siguientes deberes específicos en materia de seguridad de la información:

I. **Seguridad de la información,** además de lo establecido en el artículo 65 de la Ley de Archivos para garantizar la confidencialidad, integridad y disponibilidad de la información, el sujeto obligado deberá establecer un Sistema de Gestión de Seguridad de Información (SGSI) alineado con las mejores prácticas y estándares internacionales en materia de seguridad de la información;

II. **Seguridad en el tratamiento de datos personales**, en adición a lo establecido en los artículos 31 y 33 de la Ley de Datos, así como el 59 y 60 de los Lineamientos, el sujeto obligado deberá notificar al Instituto cuando cualquier incidente en los sistemas o infraestructuras que potencialmente pudieran llevar a una vulneración de datos personales.

Artículo 8. Cuando el Instituto tenga conocimiento de que se ha llevado a cabo alguna vulneración de seguridad establecida en el artículo 31 de la Ley de Datos o artículo 7 fracción II de la presente Ley de Ciberseguridad, deberá:

I. Solicitar al sujeto obligado que haya sufrido la vulneración, un peritaje informático emitido por alguna autoridad competente o tercero certificado, en los términos de los lineamientos que para dichos efectos se emitan, a fin de determinar las condiciones bajo las cuales se dio la vulneración.

   El peritaje informático tendrá como objetivo determinar las circunstancias, alcance y posibles responsables de la vulneración, y servirá como insumo para que el Instituto pueda:

   a) Emitir recomendaciones técnicas y administrativas en materia de protección de datos personales; y
   b) Orientar al sujeto obligado respecto de las medidas correctivas y preventivas que resulten necesarias.

II. El sujeto obligado deberá implementar, en el plazo y términos que determine el Instituto, las medidas recomendadas para mitigar el impacto de la vulneración y

prevenir incidentes futuros, informando de manera documentada sobre el cumplimiento de dichas medidas.

III. En caso de que del peritaje informático se desprendan indicios que pudieran derivar en alguna sanción administrativa, existencia de un delito o la posible comisión de éste en el tratamiento indebido de datos personales, el Instituto deberá dar vista al Órgano Interno de Control del sujeto obligado, a fin de que proceda conforme a lo dispuesto por las leyes aplicables.

La información derivada de los puntos anteriores, deberán clasificarse y desclasificarse en los términos de la Ley de Transparencia, las leyes específicas y las demás disposiciones jurídicas que resulten aplicables.

TÍTULO TERCERO
DE LAS ATRIBUCIONES DEL INSTITUTO EN MATERIA DE CIBERSEGURIDAD
Capítulo Único

Artículo 9. El Instituto tendrá las siguientes atribuciones, en materia de ciberseguridad para la protección de los datos personales:

I. Coordinar y orientar a los sujetos obligados en materia de ciberseguridad para el cumplimiento de la presente Ley de Ciberseguridad;
II. Coordinar y fomentar las acciones en materia de cultura de ciberseguridad entre los sujetos obligados y los titulares de los datos personales;
III. Solicitar a los sujetos obligados que se cuenten con un peritaje informático en los casos en que haya sufrido alguna de vulneración de datos personales;
IV. Desarrollar acciones de concientización, difusión y fomento de la ciberseguridad para la población de la Ciudad de México;
V. Fomentar la participación social en materia del derecho a la ciberseguridad y la cultura de ciberseguridad;
VI. Impulsar, participar y fomentar la creación de redes, foros o alianzas en materia de ciberseguridad, integradas por diferentes actores, público, privado, academia, sociedad civil y población en general;
VII. Colaborar en el establecimiento de estándares, lineamientos y directrices aplicables en materia de ciberseguridad;
VIII. Impulsar la adopción de programas de capacitación, certificación y profesionalización de las habilidades, conocimientos y capacidades de los sujetos obligados y de la población en general, en materia de ciberseguridad;
IX. Celebrar convenios de colaboración con autoridades federales, estatales, asociaciones locales, nacionales e internacionales, organizaciones públicas, privados y academia para el cumplimiento de los objetivos de la presente Ley;
X. Establecer premios, estímulos y reconocimientos en materia de buenas prácticas en ciberseguridad, para los sujetos obligados y para la población en general;
XI. Participar en foros locales, nacionales e internacionales, en materia de ciberseguridad; y
XII. Colaborar con otros órganos garantes locales, autoridades federales e internacionales para compartir conocimiento y experiencias en materia de ciberseguridad con un enfoque de protección de datos personales.

TÍTULO CUARTO
DE LA PERSONA RESPONSABLE DE COORDINAR LAS ACCIONES DE CIBERSEGURIDAD Y EL COMITÉ INTERNO DE CIBERSEGURIDAD
Capítulo Único

Artículo 10. El sujeto obligado deberá designar una persona especializada en la materia, que será responsable de coordinar las acciones de ciberseguridad de los sistemas e infraestructuras que soportan el tratamiento de los datos personales al interior del sujeto obligado, para asegurar que las acciones en materia de ciberseguridad se encuentran coordinadas y vigentes a fin de dar cumplimiento a los principios y deberes de seguridad y confidencialidad.

Artículo 11. La persona responsable de coordinar las acciones de ciberseguridad tendrá las siguientes funciones:

I. Coordinar a las personas responsables de seguridad de los sistemas de datos personales referidos en el artículo 2 fracción XIII de los Lineamientos.
II. Coordinar la creación e implementación de la Estrategia de Ciberseguridad del sujeto obligado, para lo cual deberá establecer un Comité Interno de Ciberseguridad;
III. Coordinar con el responsable de seguridad de la información, el oficial de protección de datos personales o enlace de protección de datos personales, la elaboración de la evaluación de impacto y el análisis de riesgos relacionados con la seguridad de la información, así como la implementación de medidas para mitigarlos y garantizar la protección de las infraestructuras y sistemas de información, relacionadas con el tratamiento de datos personales en función de su sensibilidad e impacto;
IV. Elaborar propuestas de políticas, conceptos de seguridad, controles de seguridad, directrices, métodos de gestión de riesgos, prácticas idóneas y recomendaciones en materia de ciberseguridad para someterlos a consideración del Comité Interno de Ciberseguridad;
V. Elaborar y someter anualmente la actualización de la Estrategia de Ciberseguridad al titular del sujeto obligado o a quien éste designe, para su aprobación;
VI. Dar seguimiento a la implementación de la Estrategia de Ciberseguridad al interior del sujeto obligado;
VII. Elaborar el informe anual de cumplimiento de la Estrategia de Ciberseguridad del sujeto obligado, el cual deberá presentarse a más tardar la última semana de enero del siguiente ejercicio fiscal;
VIII. Brindar asesoría en materia de ciberseguridad al interior del sujeto obligado;
IX. Elaborar el programa anual de capacitación en materia de ciberseguridad para el sujeto obligado, que deberán someterse a aprobación del Comité Interno de Ciberseguridad y asegurar su cumplimiento;
X. Coordinar las acciones orientadas a fortalecer la cultura de ciberseguridad en el sujeto obligado de manera transversal;
XI. Coordinar, con el apoyo del Comité de Ciberseguridad, la atención y respuesta a incidentes de seguridad que implique o puedan llevar a una vulneración de datos personales;
XII. Coordinar la investigación respecto a lo establecido en la fracción anterior, así como, proponer acciones para la mitigación de impactos y mejoras para prevenir eventos futuros;
XIII. Gestionar la elaboración del peritaje informático que solicite el Instituto;

XIV. Conocer las prácticas de seguridad y su eficacia, así como proponer mejoras para adaptarse a las nuevas amenazas y cambios en el entorno tecnológico para la protección de datos personales; y
XV. Las demás que establezcan las disposiciones jurídicas aplicables.

Artículo 12. Los sujetos obligados deberán establecer un Comité Interno de Ciberseguridad, que coadyuve en las acciones necesarias para la preparación, detección, respuesta y recuperación de incidentes cibernéticos en los que se vulneren o puedan vulnerarse datos personales, así como implementar acciones de mejora continua; el cual estará integrado por:

I. La persona titular del Sujeto Obligado, quien lo presidirá;
II. La persona designada como responsable de coordinar las acciones de ciberseguridad, quien fungirá como Secretario Técnico;
III. La persona designada como oficial de protección de datos personales;
IV. La persona titular del área de tecnologías;
V. La persona titular del área jurídica;
VI. La persona titular de la Unidad de Transparencia;
VII. La persona responsable de la coordinación de archivos;
VIII. La persona titular del área de comunicación;
IX. La persona titular del área de administración y finanzas y
X. Las personas responsables de seguridad de los sistemas de datos personales del sujeto obligado referidos en el artículo 2 fracción XIII de los Lineamientos.

Artículo 13. Entre las funciones que tendrá el Comité Interno de Ciberseguridad se encuentran:

I. Colaborar en la elaboración e implementación de la Estrategia de Ciberseguridad del sujeto obligado en la que se consideren las siguientes fases:
    a) Preparación, en la que se deberá:
        i. Identificar y actualizar los activos de información del sujeto obligado;
        ii. Elaborar y actualizar un Plan de continuidad de TIC con un enfoque de protección de datos personales;
        iii. Integrar un Equipo de Respuesta a Incidentes en los que se hayan vulnerado datos personales;
        iv. Proponer campañas de concientización sobre ciberseguridad vinculado a la protección de datos personales;
    b) Detección, en la que se deberá:
        i. Llevar a cabo una gestión y monitoreo de manera proactiva para identificar incidentes que puedan llevar a una vulneración de datos personales;
        ii. Elaborar el Protocolo de Atención a Incidentes respecto de la protección de datos personales;
    c) Respuesta y recuperación:
        i. Llevar a cabo la contención y mitigación de la amenaza que pudiera vulnerar datos personales con recursos del propio sujeto obligado o externos;
        ii. Llevar a cabo la recuperación de servicios esenciales vinculados al tratamiento de datos personales;
        iii. Desarrollar actividades posts-incidentes que pudieran incluir la presentación de denuncias ante las instancias correspondientes;

d) Actualización y mejora continua:
    i. Analizar y mejorar el Sistema de Gestión en Seguridad de la Información del sujeto obligado;
    ii. Implementar herramientas de monitoreo y detección de incidentes;
    iii. Contar con capacitación especializada continua para los Equipos de Respuesta del Sujeto Obligado.

El Comité Interno de Ciberseguridad podrá ser asistido por un consejo consultivo multisectorial temporal, que estará integrado por consejeros que serán honoríficos, de la siguiente manera: dos representantes del sector privado, dos representantes del sector académico y dos representantes de sociedad civil, el cual atenderá a las reglas de funcionamiento, procedimientos transparentes de designación, temporalidad y renovación que para ello se determinen.

TÍTULO QUINTO
DE LA ESTRATEGIA DE CIBERSEGURIDAD
Capítulo Único

Artículo 14. La Estrategia de Ciberseguridad deberá contemplar un enfoque integral para proteger los activos de información, garantizar la resiliencia frente a amenazas y cumplir con los objetivos organizacionales, así como definir y priorizar las acciones necesarias para minimizar el riesgo del sujeto obligado de sufrir un ataque, así como el impacto de éste en los que pueda configurarse alguna vulneración de datos personales. Para lo cual se requiere entender el entorno de amenazas y aprovechar los recursos con los que cuente.

Artículo 15. En la elaboración de la Estrategia de Ciberseguridad se deberá tener como objetivo asegurar que se toman las medidas necesarias para que el sujeto obligado siga operando a pesar de las amenazas. Para lo cual procurará que sus activos, sistemas o personas, estén protegidos, y sean resilientes en caso de sufrir una vulneración de datos personales, esto con un enfoque proactivo, a fin de minimizar el posible impacto del incidente a las personas titulares de los datos personales y reducir el daño reputacional, a los proveedores, empleados, etc. es decir todos los interesados en general.

Artículo 16. Para elaborar la Estrategia de Ciberseguridad del sujeto obligado, se deberán llevar a cabo las siguientes acciones:

I. Creación del Comité Interno de Ciberseguridad para su redacción;
II. Elaborar un análisis de riesgos considerando lo establecido en el artículo 51 de los Lineamientos, así como el análisis de los escenarios que puedan llevar a vulneraciones de los datos personales o los sistemas de tratamiento en el ciberespacio;
III. Llevar a cabo un análisis de brecha, considerando lo establecido en el artículo 52 de los Lineamientos, así como con la finalidad de conocer el estado de los controles de seguridad implementados frente a los riesgos detectados en la fracción anterior, para lo cual se puede utilizar el marco de ciberseguridad que el Comité Interno de Ciberseguridad determine;
IV. Definir las acciones de ciberseguridad que se determinen, los tiempos, responsabilidades, indicadores y recursos necesarios para su ejecución; y
V. Documentar todas las fases de la estrategia, para su posterior uso o consulta.

TÍTULO SEXTO
DE LA CAPACITACIÓN Y CERTIFICACIÓN
Capítulo I

Artículo 17. El Instituto promoverá un programa de capacitación y certificación en materia de ciberseguridad. La capacitación será obligatoria para todos los sujetos obligados. La certificación será obligatoria particularmente para las personas responsables de coordinar las acciones de ciberseguridad, el Oficial de Protección de Datos Personales, el Director General de TIC u homólogo y los responsables de seguridad de la información referidos en el artículo 2 fracción XIII de los Lineamientos.

Artículo 18. Los sujetos obligados deberán desarrollar las competencias en materia de ciberseguridad, fomentar la cultura de ciberseguridad y fortalecer la capacidad de respuesta ante incidentes y asegurar el cumplimiento de las normas y estándares aplicables de ciberseguridad y seguridad de la información, a través de la capacitación al personal involucrado en el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI) y promover la certificación en la materia.

Artículo 19. La capacitación y certificación en ciberseguridad referida en los artículos 17 y 18 debe basarse en los siguientes principios:

I. **Accesibilidad y equidad**: Asegurar que las oportunidades de formación estén disponibles para todos los servidores públicos de los sujetos obligados y sectores de la sociedad, sin discriminación alguna, promoviendo la inclusión digital y la igualdad de oportunidades;
II. **Relevancia y actualización**: Los programas de capacitación deben estar alineados con las amenazas, tecnologías emergentes y buenas prácticas actuales en ciberseguridad, para que los profesionales, servidores públicos y sociedad puedan adaptarse de manera efectiva a los cambios continuos; e
III. **Inclusión de todos los niveles**: La capacitación debe cubrir desde el nivel básico hasta el avanzado, abarcando tanto a los usuarios finales como a los profesionales de ciberseguridad, y debe adaptarse a las necesidades de diferentes sectores de sujetos obligados, así como público en general.

Artículo 20. El Instituto, en colaboración con entidades educativas, academias, cualquier organización y expertos en ciberseguridad, que acredite su conocimiento; será responsable de diseñar y promover programas de capacitación accesibles y relevantes, con contenidos actualizados que aborden tanto las amenazas cibernéticas presentes y futuras.

Artículo 21. El Instituto, en colaboración con organismos especializados, universidades o academias, establecerá un sistema de certificación de competencias en ciberseguridad, el cual reconocerá a los individuos y sujetos obligados a que cumplan con los estándares de competencia establecidos en materia de ciberseguridad, detección de amenazas y gestión de riesgos, así como áreas de prevención, detección y respuesta ante incidentes cibernéticos, entre otros. El Instituto publicará los lineamientos para el desarrollo e implementación de este sistema de certificación.

Artículo 22. En los lineamientos referidos en el artículo anterior, se establecerán las bases para la creación de un comité independiente que revisará los programas y hará recomendaciones para su mejora, asegurando que sigan siendo relevantes y eficaces; así

como que el sistema de capacitación y certificación se someta a una evaluación periódica para determinar su efectividad y adaptabilidad a las nuevas amenazas y tecnologías.

Artículo 23. El Instituto, en colaboración con los Sujetos Obligados, a través de las personas responsables de coordinar las acciones de ciberseguridad y el Oficial de Protección de Datos Personales, supervisarán que los sujetos obligados implementen programas de capacitación adecuados y que sus servidores públicos reciban la formación pertinente.

Artículo 24. El Instituto, en colaboración con el Gobierno de la Ciudad de México, el Gobierno Federal, entidades privadas u organizaciones internacionales, podrá establecer mecanismos de financiación para facilitar el acceso a la capacitación y certificación en ciberseguridad, especialmente para sujetos obligados. Esto podrá incluir incentivos fiscales, becas de formación y financiamiento para proyectos de investigación en educación en ciberseguridad.

Artículo 25. Los sujetos obligados deberán tomar en cuenta que, al momento de contratar soluciones tecnológicas, infraestructura, aplicaciones o servicios relacionados con el tratamiento de datos personales, los proveedores, encargados o terceros, cuenten con estándares técnicos y certificaciones en materia de seguridad de la información y privacidad, que sean pertinentes, idóneas y actualizadas, reconocidas nacional e internacionalmente.

Capítulo II
DE LA COORDINACIÓN Y PROMOCIÓN DE LA CIBERSEGURIDAD ENTRE LOS SUJETOS OBLIGADOS

Artículo 26. Con la finalidad de promover la cultura de ciberseguridad y fomentar la colaboración y responsabilidad compartida entre los sujetos obligados y actores del sector público, academia, expertos y sociedad civil, el Instituto impulsará la creación de una Alianza por la Ciberseguridad de la Ciudad de México, que tendrá por objetivo promover la colaboración entre diferentes actores para la construcción de la ciberseguridad en la Ciudad de México.

TÍTULO SÉPTIMO
DE LAS SANCIONES
Capítulo Único

Artículo 27. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la observancia de los principios establecidos en el artículo 5 de la presente Ley;
II. No documentar todas las fases de la Estrategia de Ciberseguridad, incluyendo su informe de cumplimiento;
III. No contar con un Sistema de Gestión de Seguridad de la Información;
IV. No reportar al Instituto los incidentes de ciberseguridad que pudieran llevar a una vulneración de datos personales conforme a lo establecido en el artículo 31 y 33 de la Ley de Datos, así como al artículo 7 fracción II de la presente Ley;

V. La falta de atención a la solicitud del Instituto, del dictamen pericial en materia informática forense, a fin de determinar las condiciones bajo las cuales se dio la vulneración;
VI. No implementar las medidas recomendadas por el Instituto para mitigar el impacto de la vulneración y prevenir incidentes futuros, así como no informar de manera documentada sobre el cumplimiento de dichas medidas;
VII. La falta de designación de la persona responsable de la coordinación de las acciones de ciberseguridad; y
VIII. No llevar a cabo las acciones de detección establecidas en el artículo 13, fracción I, inciso b), incluyendo el Protocolo de atención a incidentes respecto de la protección de datos personales.

Las causas de responsabilidad previstas en las fracciones III a la VI, así como la reincidencia de las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

En caso de que la presunta infracción hubiere sido cometida por algún integrante de algún partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.

Las sanciones de carácter económico que se deriven del incumplimiento de las acciones descritas no podrán ser cubiertas con recursos públicos.

Artículo 28. Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.

Artículo 29. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto en el artículo 27 de esta Ley**,** son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Artículo 30. En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto deberá remitirá a la autoridad competente, junto con la denuncia correspondiente, un expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.
La autoridad que conozca del asunto deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción al Instituto.

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la

adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.

Asimismo, deberá integrar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto tenga conocimiento de los hechos.

TRANSITORIOS

Primero. La presente Ley entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

Segundo. El Titular de cada sujeto obligado designará a una persona responsable de la coordinación de las acciones en materia de ciberseguridad y deberá notificarlo al Instituto para su registro a más tardar dentro de los 30 días hábiles a partir de la entrada en vigor de la presente Ley.

Tercero. El Instituto deberá emitir los lineamientos a que se refieren los artículos 8 fracción I y 21 de la presente Ley y publicarlos en la Gaceta Oficial de la Ciudad de México, a más tardar 365 días posteriores a la entrada en vigor de la presente Ley.

Cuarto. Los sujetos obligados contarán con 120 días hábiles a partir de la entrada en vigor de la presente Ley para establecer un Sistema de Gestión en Seguridad de la Información, haber aprobado su Estrategia de Ciberseguridad y el Protocolo de Atención a incidentes respecto de la protección de datos personales.

Quinto. En un plazo 365 días, contados a partir de la entrada en vigor de la presente Ley, los sujetos obligados deberán establecer su Programa Anual de Ciberseguridad.

Sexto. El Instituto proporcionará un programa de capacitación para todos los sujetos obligados, enfocado en el cumplimiento de las nuevas disposiciones legales. Este programa de capacitación será anual y permanente.

Séptimo. La implementación de la presente Ley, se encuentra sujeta a la disponibilidad presupuestal, humana y material que para tal efecto tenga el Instituto y los sujetos obligados.

Congreso de la Ciudad de México, a los ___ días del mes de _____ de dos mil veinticinco.