SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES DE LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS

1. La Comisión Nacional de los Salarios Mínimos deberá contar con un sistema de gestión de seguridad de datos personales que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.

   El referido sistema de gestión deberá cumplir con los estándares y mejores prácticas, nacionales e internacionales en materia de gestión de información, que determinen las áreas competentes de la Comisión Nacional de los Salarios Mínimos, para la protección de datos personales.

   Corresponderá a la Unidad de Transparencia, y a las Direcciones de Sistemas, de Coordinación de la Información, de Administración de Riesgos, de Control Interno y de Seguridad, en el ámbito de sus respectivas atribuciones, llevar a cabo, de manera coordinada y en conjunto con las unidades administrativas del Banco, el diseño, la implementación y la mejora continua del sistema de gestión de seguridad de datos personales, con base en las necesidades institucionales.

   La elaboración y actualización periódica del documento de seguridad previsto en el artículo 35 de la LGPDPPSO estará a cargo, de manera coordinada, de la Unidad de Transparencia, las Direcciones de Coordinación de la Información, de Administración de Riesgos y de Control Interno, con la participación de las unidades administrativas del Banco. En dicho documento deberán mencionarse, además, las medidas de seguridad implementadas para a protección de los datos personales.

2. La Unidad de Transparencia dirigirá, en coordinación con la Dirección de Coordinación de la Información y la Dirección de Administración de Riesgos, las gestiones necesarias para que las unidades administrativas del Banco actualicen el inventario de datos personales y sistemas de tratamiento, de modo que se complemente, cuando menos, con la información prevista en el artículo 58 de los Lineamientos Generales. Lo anterior, conforme al plan de trabajo que al efecto se establezca.

Para la actualización del inventario de datos personales y sistemas de tratamiento, el personal de las unidades administrativas del Banco deberá proporcionar a la Unidad de Transparencia la información que esta les solicite, relacionada con los Activos de Información, y participar en las reuniones de trabajo a las que se les convoque con el mismo propósito.

La información recabada será parte del Inventario de Activos de Información recabada será parte del inventario de Activos de Información del Banco, cuya custodia estará a cargo de la Dirección de Coordinación.

3. Las unidades administrativas del Banco, en coordinación con la Dirección de Administración de Riesgos, realizarán la identificación y documentación de los procesos que involucren el tratamiento de datos personales, incluyendo los roles y responsabilidades, así como la cadena de rendición de cuentas de los servidores públicos que participen en los mismos.

4. La Dirección de Coordinación de la Información, deberá proponer a este Comité los criterios específicos y mecanismos para la gestión, control y cumplimiento de los plazos aplicables para el bloqueo y supresión de datos personales.

5. Las unidades administrativas del Banco, en coordinación con la Dirección de Administración de Riesgos, deberán llevar a cabo los análisis de riesgos y de brecha, previstos en el artículo 33, fracciones IV y V, de la LGPDPPSO, considerando, cuando menos, lo previsto en los artículos 60 y 61 de los Lineamientos Generales, respectivamente. A tal efecto, en las correspondientes metodologías de análisis de impacto a la información y evaluación de riesgos no financieros, los datos personales se clasificarán por categorías, considerando el riesgo inherente de estos en los sistemas de tratamiento.

En caso de que se presente una vulneración a la seguridad de los datos personales en posesión del Banco, el titular de la unidad administrativa involucrada, o quien actúe en su suplencia en caso de ausencia conforme al Reglamento Interior del Banco de México, deberá dar aviso inmediato a la Dirección de Administración de Riesgos para que ésta lleve a cabo el correspondiente registro en la bitácora de vulneraciones a la seguridad de los datos personales a que se refiere el artículo 39 de la LGPDPPSO. Asimismo, deberá dar aviso a la Unidad de Transparencia, y deberá remitir un informe dirigido al Comité de Transparencia en el que indique, cuando menos lo siguiente:

a) La naturaleza incidente, particularmente si considera que afecta de forma significativa los derechos patrimoniales o morales del titular.

   Se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de manera enunciativa mas no limitativa, con sus bienes muebles o inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

   Se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa mas no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físico, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

b) Las circunstancias de tiempo, modo y lugar en la que la vulneración haya ocurrido.
c) Las categorías y el número aproximado de titulares afectados.
d) Los sistemas de tratamiento y datos personales comprometidos.
e) La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.

f) Una propuesta sobre las medidas que los titulares de los datos comprometidos, en su caso, podrían adoptar para proteger sus intereses.
g) Las acciones correctivas que haya llevado a cabo, y las que en su caso sugiera implementar.
h) Las recomendaciones dirigidas al titular.
i) Los medios a través de los cuales los titulares, en su caso, podrían obtener más información al respecto.

Para los efectos de este numeral, de manera enunciativa mas no limitativa, se entenderá por vulneración de seguridad:

i. La pérdida o destrucción no autorizada;
ii. El robo, extravío o copia no autorizada;
iii. El uso, acceso o tratamiento no autorizado, o
iv. El daño, la alteración o modificación no autorizada.

La Dirección de Administración de Riesgos deberá llevar a cabo la actualización a la bitácora de vulneraciones a la seguridad de datos personales.

Una vez que la Unidad de Transparencia reciba noticia de alguna vulneración de seguridad de los datos personales, a través del secretario o Pro Secretario de este Comité de Transparencia convocará a los miembros del mismo a una sesión extraordinaria con carácter urgente, a efecto de que puedan tomar las determinaciones correspondientes en el ámbito de sus atribuciones, y se coordine la instrumentación de las acciones previstas en la LGPDPPSO y los Lineamientos Generales.

6. La Dirección de Control Interno, deberá llevar a cabo el seguimiento del monitoreo de la seguridad de los datos personales, con base en los mecanismos que las unidades administrativas del Banco tengan implementados para estos efectos, así como en la información que deban

proporcionarle a esa Dirección. Dicho monitoreo tendrá como propósito conocer periódicamente el estado de control, con la finalidad de obtener seguridad razonable sobre el funcionamiento del sistema de gestión de seguridad de datos personales, así como de las acciones de mejora continua que se lleven a cabo.

La Unidad de Auditoría, en el ámbito de su competencia, deberá verificar a través de auditorías, la aplicación de los criterios para el manejo, mantenimiento, seguridad y protección de los datos personales que estén en posesión de las unidades administrativas del Banco.

El resultado de las actividades de monitoreo y verificación previstas en este numeral deberán ser informadas a este Comité de Transparencia, a efecto de que esté en posibilidad de actuar en el ámbito de sus atribuciones. El informe previsto en este párrafo será presentado sin perjuicio de la información que la Dirección de Control Interno y la Unidad de Auditoría deban reportar a otros Órganos Colegiados, tales como el Comité de Seguimiento al Sistema de Control Interno o el Comité de Auditoría.

7. Las Direcciones de Control Interno, de Recursos Humanos y de Recursos Materiales, así como cualquier otra unidad administrativa competente, deberán continuar promoviendo en el ámbito de sus respectivas atribuciones, la formalización de compromisos y el establecimiento de cláusulas de confidencialidad, como mecanismos de control para que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de estos, y que dicha obligación subsista aún después de finalizar sus relaciones con el Banco.

8. La Unidad de Transparencia deberá presentar anualmente ante este Comité de Transparencia, el programa que prevea la capacitación del personal en materia de protección de datos personales, considerando sus

roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

9. La información que resulte del sistema de gestión de seguridad de datos personales deberá ser considerada como insumo para el diseño y adecuación de políticas, procedimientos, roles y responsabilidades, programa de capacitación u otros elementos requeridos para la mejora continua de la gestión de la información en el Banco.