BANOBRAS

BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C

SISTEMAS DE SUPERVISIÓN Y VIGILANCIA

- INTRODUCCIÓN

La operación y funcionamiento de Banobras se realiza en estricto apego al marco legal aplicable y a las sanas prácticas y usos bancarios, buscando alcanzar dentro de los sectores encomendados al prestar el servicio de banca y crédito, los objetivos de carácter general señalados en el artículo 4o de la Ley de Instituciones de Crédito, que le permiten planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales, tomando en consideración la normatividad aplicable en la materia, así como las políticas establecidas como parte del Sector Bancario.

En ese sentido, de conformidad con lo establecido en el Programa de Protección de Datos Personales; las Políticas Internas para la Gestión y Tratamiento de los Datos Personales y el Documento de Seguridad, Banobras da cumplimiento a dicha obligación, que se complementa con lo establecido en el presente documento.

- AMBITO DE APLICACIÓN

El Sistema de Supervisión y Vigilancia resulta aplicable para las personas servidoras públicas de Banobras que, en el ejercicio de sus atribuciones, obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, manejen, aprovechen, divulguen, transfieran o dispongan datos personales.

- MARCO JURIDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.

- SISTEMAS DE SUPERVISIÓN Y VIGILANCIA

El presente Sistema de Supervisión y Vigilancia se compone de los siguientes elementos:

A. Monitoreo y supervisión;
B. Actuación ante vulneraciones a la seguridad de los datos personales, y
C. Auditorías en materia de datos personales.

En ese sentido, se procede a señalar en qué consiste cada uno de los elementos mencionados.

A. Monitoreo y supervisión

La Gerencia Ejecutiva de Enlace con el INAI y la Dirección de Seguridad de la Información, ejecutarán el monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

I. Monitoreo. Se remitirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la siguiente encuesta:

	Sí	No
1. Se tienen definidas las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales.	☐	☐
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión.	☐	☐
3. Se comunica a cada servidor público sus funciones, obligaciones y cadena de mando en relación con el tratamiento de datos personales que efectúa.	☐	☐
4. Se ha elaborado el inventario de datos personales con los siguientes elementos: • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • La descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.	☐	☐
5. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente: • La obtención de los datos personales; • El almacenamiento de los datos personales; • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales.	☐	☐
6. Se ha realizado un análisis de riesgo.	☐	☐
7. Se ha realizado un análisis de brecha.	☐	☐
8. Se monitorean y revisan de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.	☐	☐

II. Supervisión. Se analizarán las encuestas recibidas, de manera concreta, aquellos puntos en los que se hubiera señalado “No” como respuesta, para emitir las recomendaciones que se estimen pertinentes, para su valoración por parte de las áreas correspondientes.

B. Actuación ante vulneraciones a la seguridad de los datos personales

Se deberán monitorear y revisar las vulneraciones que se presenten de los datos personales, como pueden ser:

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.

En caso de que algún área detecte una vulneración a los datos personales que le den tratamiento, deberá informar a la Dirección de Seguridad de la Información y a la Gerencia Ejecutiva de Enlace con el INAI, lo siguiente:

a) Circunstancias de modo, tiempo y lugar en que se detectó la vulneración.
b) Tratamiento de Datos Personales en el que se detectó la amenaza.
c) Datos personales involucrados.
d) Datos de identificación y de contacto de la persona servidora pública responsable del tratamiento de los datos personales.
e) Descripción de los controles físicos o electrónicos vulnerados.

La Dirección de Seguridad de la Información y la Gerencia Ejecutiva de Enlace con el INAI, llevarán un seguimiento sobre las vulneraciones que se hayan materializado y que hayan sido reportadas por las áreas. Asimismo, revisarán la vulneración reportada y analizarán la factibilidad de proponer alguna medida correctiva o preventiva, en conjunto con el área correspondiente, que permita atender la vulneración que corresponda.

Lo anterior, sin perjuicio de la notificación que se debe realizar al titular de los datos personales, así como al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en términos de lo dispuesto por los artículos 67 y 68 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

C. Auditorías en materia de datos personales

Se deberá contar con auditorías para revisar la eficacia y eficiencia en la protección de los datos personales y las medidas de seguridad establecidas para tales efectos, pudiendo ser de carácter internas o externas, que permitan identificar de forma ordenada las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.

En el aspecto interno, se analizará la factibilidad de incorporar con el área de auditoría interna de Banobras, en su programa anual de trabajo, la implementación de auditorías en materia de seguridad de la información.

Por lo que hace al aspecto externo, Banobras podrá voluntariamente someterse a la realización de auditorías por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la normativa aplicable en la materia.