COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

ACUERDO POR EL QUE SE DETERMINA LA POLÍTICA INTERNA PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES, LOS CRITERIOS PARA ESTABLECER Y MANTENER EL SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES, Y OTRAS POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES

El Comité de Transparencia del Banco de México, con fundamento en los artículos 77 y 78, fracciones I, IV, y V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 4o., párrafos primero y décimo, y 31, fracciones II, V, XVI, y XX, del Reglamento Interior del Banco de México (RIBM), y

CONSIDERANDO

1. Que el 20 de marzo de 2025 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide, entre otras disposiciones, la LGPDPPSO, el cual entró en vigor al día siguiente de dicha publicación.

2. Que en términos del artículo 10 de la LGPDPPSO, en el tratamiento de datos personales los responsables deberán observar, entre otros principios, el de responsabilidad.

Al respecto, de conformidad con el artículo 24, fracción II, de la propia LGPDPPSO, para cumplir con el referido principio de responsabilidad, los sujetos obligados deberán elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización.

3. Que, por otra parte, de conformidad con los artículos 27 y 28 de la LGPDPPSO, para establecer y mantener las medidas de seguridad para la protección de los datos personales, los responsables deben realizar diversas actividades interrelacionadas, las cuales deberán estar documentadas y contenidas en un sistema de gestión.[1]

Adicionalmente, en términos del artículo 29 del mencionado ordenamiento, los responsables deberán elaborar un documento de seguridad, que contenga, al menos, los requisitos previstos en dicho artículo.

4. Que de conformidad con el artículo 77, segundo párrafo, de la LGPDPPSO, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales.

Al respecto, de conformidad con el artículo 78, fracciones I, IV, y V, de la LGPDPPSO, al Comité de Transparencia le corresponden, entre otras funciones:

[1] En términos del art. 28 de la LGPDPPSO: "…se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales…".

a. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales, de conformidad con las disposiciones previstas en esa Ley y en aquellas que resulten aplicables en la materia;

b. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la misma Ley y las disposiciones aplicables en la materia, y

c. Supervisar, en coordinación con las áreas o Unidades Administrativas competentes el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

5. Que, en correlación con las disposiciones de la LGPDPPSO, conforme al artículo 31, fracciones II, V, y XVI, del RIBM, el Comité de Transparencia del Banco de México tiene entre sus atribuciones:

a. Coordinar, supervisar y realizar, de conformidad con las disposiciones aplicables, las acciones necesarias para garantizar en el Banco el derecho a la protección de los datos personales, e instituir los procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los mencionados datos;

b. Establecer aquellos criterios específicos que resulten necesarios para la mejor observancia de las disposiciones en materia de protección de datos personales, y supervisar su aplicación, y

c. Aprobar las políticas, programas, medidas, documentos, controles, mecanismos, procedimientos, esquemas de mejores prácticas, planes de trabajo, informes y demás acciones que las Unidades Administrativas competentes sometan a su consideración a través de la Unidad de Transparencia, para el cumplimiento de los principios y deberes previstos en las disposiciones aplicables al Banco en materia de protección de datos personales.

6. Que de conformidad con lo dispuesto en el artículo 18 Bis, fracción XVII, del RIBM, corresponde a la Dirección de Seguridad y Organización de la Información participar en el diseño, instrumentación y mejora del Sistema de Gestión de Seguridad de Datos Personales.

7. Que, por su parte, en términos de los artículos 79, fracción VII, de la LGPDPPSO y 31 Bis, fracción XXIV, del RIBM, corresponde a la Unidad de Transparencia asesorar a las Unidades Administrativas del Banco en materia de protección de datos personales, y coordinar con estas las acciones que deban implementarse en el Banco para el cumplimiento de los principios y deberes previstos en la propia LGPDPPSO y demás disposiciones aplicables en esa materia.

En consecuencia, este Comité de Transparencia, con fundamento en lo dispuesto por los artículos citados, ha determinado emitir el siguiente:

ACUERDO

Política interna para la gestión y tratamiento de datos personales

PRIMERO. Se determina como política interna para la gestión y tratamiento de los datos personales en el Banco de México la siguiente:

1. En la gestión y el tratamiento de datos personales las personas servidoras públicas del Banco de México deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, conforme a la LGPDPPSO y demás disposiciones aplicables. Las personas servidoras públicas que tengan personal a su cargo, además deberán supervisar el cumplimiento de dichos principios por parte de sus subordinados y adoptar las medidas necesarias para su aplicación.

2. La gestión y el tratamiento de datos personales que lleven a cabo las Unidades Administrativas del Banco de México deberán sujetarse a las facultades y atribuciones que a dicho Banco Central confieren la Ley del Banco de México, el RIBM y las demás disposiciones legales y reglamentarias que regulen su competencia.

3. Los datos personales se gestionarán y tratarán de manera lícita, privilegiando la protección de los intereses de la persona titular y la expectativa razonable de privacidad. En su obtención, las personas servidoras públicas del Banco de México deberán actuar con apego a los principios de legalidad, honradez y lealtad.

4. El tratamiento de datos personales deberá sujetarse al consentimiento de la persona titular, salvo las excepciones previstas en la Ley.

5. Deberá informarse a las personas titulares la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del correspondiente Aviso de privacidad.

6. Las personas titulares de las Unidades Administrativas del Banco de México que recaben datos personales adoptarán las medidas necesarias para procurar que estos sean exactos, completos, correctos y actualizados, a fin de que no se altere su veracidad. Se presumirá que los datos tienen dichas características cuando se recaben directamente de las personas titulares.

7. Únicamente deberán tratarse los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

8. Cuando los datos personales que se recaben hayan dejado de ser necesarios para las finalidades que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, conforme a los procedimientos previstos en la LGPDPPSO y demás disposiciones aplicables. En todo caso, para determinar los plazos de conservación correspondientes, deberán atenderse a las disposiciones aplicables y considerarse los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

9. El tratamiento de los datos personales deberá limitarse al cumplimiento de las finalidades previstas en el correspondiente Aviso de privacidad. Solo podrán tratarse datos personales para finalidades distintas, cuando dicho tratamiento sea conforme a las atribuciones legales del Banco de México, y medie consentimiento de la persona titular, conforme a la LGPDPPSO.

10. Las personas servidoras públicas del Banco de México deberán implementar, cumplir y mantener las medidas de seguridad que determinen las instancias competentes del propio Banco para la protección de los datos personales. Dichas medidas deberán ser establecidas, actualizadas, monitoreadas y revisadas, con base en la metodología definida por las Unidades Administrativas competentes del Banco y los análisis de riesgos respectivos.

11. Las personas servidoras públicas del Banco de México deberán guardar la confidencialidad de los datos personales a los que tengan acceso. Lo anterior, sin perjuicio del cumplimiento de las disposiciones en materia de transparencia y acceso a la información pública.

12. En aquellos casos en que sea necesario clasificar los datos personales, como puede ser para la atención de solicitudes de acceso a la información o para el cumplimiento de las obligaciones de transparencia en las plataformas correspondientes, las personas titulares de las Unidades Administrativas deberán clasificar como confidenciales aquellos datos personales que así lo requieran, según lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y la LGPDPPSO, así como las disposiciones derivadas de tales ordenamientos.

13. Los derechos de las personas titulares en relación con sus datos personales deberán ser respetados por las personas servidoras públicas del Banco de México. El procedimiento para la atención de los derechos de acceso, rectificación, cancelación y oposición (ARCO), deberá llevarse de conformidad con lo dispuesto en la LGPDPPSO y demás disposiciones aplicables.

14. La Unidad de Transparencia establecerá procedimientos para recibir y responder dudas y quejas de las personas titulares de datos personales que sean de fácil acceso y con la mayor cobertura posible.

15. El incumplimiento de los principios y deberes establecidos en la LGPDPPSO serán sancionados de conformidad con lo establecido en dicho ordenamiento. Lo anterior, sin perjuicio de las sanciones del orden civil, penal o de cualquier otro tipo que pudieran derivarse de los mismos hechos.

16. La gestión y el tratamiento de datos personales en el Banco de México estará alineada al marco institucional de gestión y seguridad de la información, así como a la normativa aplicable.

Criterios para establecer y mantener el Sistema de Gestión de Seguridad de Datos Personales

SEGUNDO. El Banco de México 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 Unidades Administrativas competentes del Banco para la protección de datos personales.

Corresponderá a la Unidad de Transparencia, y a las Direcciones de Seguridad y Organización de la Información, de Administración de Riesgos, de Control Interno, de Ciberseguridad 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 29 de la LGPDPPSO estará a cargo, de manera coordinada, entre la Unidad de Transparencia, las Direcciones Generales de Contraloría y Administración de Riesgos y la de Tecnologías de la Información, la Dirección de Seguridad y la Unidad de Auditoria del Banco de México, con la participación de las Unidades Administrativas del Banco que, en su caso, se requiera. En dicho documento se deberá establecer, de manera general, las medidas de seguridad implementadas para la protección de los datos personales.

TERCERO. La Unidad de Transparencia, en coordinación con la Dirección de Seguridad y Organización de la Información y la Dirección de Administración de Riesgos, llevarán a cabo las gestiones necesarias para que las Unidades Administrativas del Banco elaboren el inventario de activos de información; el inventario de datos personales y de los sistemas de tratamiento, en términos del artículo 27, fracción III, de la LGPDPPSO; así como la categorización de los activos de información, prevista en la Norma Administrativa Interna (NAI) "Gestión de la Información".

Para la elaboración de los instrumentos mencionados en el párrafo anterior, el personal de las Unidades Administrativas del Banco deberá proporcionar a la Unidad de Transparencia, Dirección de Seguridad y Organización de la Información y Dirección de Administración de Riesgos, la información que estas les soliciten 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 del Banco, cuya custodia estará a cargo de la Dirección de Seguridad y Organización de la Información.

CUARTO. 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.

QUINTO. La Dirección de Seguridad y Organización de la Información, debe proponer al Comité de Transparencia los criterios específicos y mecanismos para la gestión, control y cumplimiento de los plazos aplicables para el bloqueo y supresión de datos personales.

SEXTO. 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 27, fracciones IV, y V, de la LGPDPPSO. 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, la persona titular de la Unidad Administrativa involucrada, o quien actúe en su suplencia en caso de ausencia conforme al RIBM, 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 33 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, de conformidad con lo previsto en el artículo 35 de la citada Ley:

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

Se entenderá que se afectan los derechos patrimoniales de la persona 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 de la persona titular.

Se entenderá que se afectan los derechos morales de la persona 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 personas titulares afectadas.

d) Los sistemas de tratamiento y datos personales comprometidos.

e) La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.

f) Las recomendaciones acerca de las medidas que las personas 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) Los medios a través de los cuales las personas 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 sea informada respecto de alguna vulneración de seguridad de los datos personales, a través del Secretario o Pro Secretario del 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 demás normatividad aplicable.

SÉPTIMO. La Dirección de Control Interno y la Dirección de Ciberseguridad, deberán llevar a cabo el seguimiento del monitoreo de la seguridad de los datos personales, con base en el esquema previsto en el Anexo Único, y los mecanismos que las Unidades Administrativas del Banco tengan implementados para estos efectos, así como en la información que deban proporcionarle a esas Direcciones. 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, de conformidad con lo dispuesto en el artículo 29 Bis 1, fracción IV, del RIBM.

El resultado de las actividades de monitoreo y verificación previstas en este numeral deberán ser informadas al 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, como lo es el Comité de Riesgos.

OCTAVO. 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.

NOVENO. La Unidad de Transparencia deberá elaborar y someter anualmente ante el Comité de Transparencia, el programa que prevea la capacitación de las personas servidoras públicas del Banco en materia de protección de datos personales, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y su perfil de puestos.

DÉCIMO. 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.

Políticas de protección de datos personales

DÉCIMO PRIMERO. La Dirección de Seguridad y Organización de la Información, deberá considerar, como parte de las normas, lineamientos, prácticas, procedimientos, metodologías, indicadores y herramientas tecnológicas que elabore en ejercicio de sus funciones, la protección de los datos personales en el Banco.

La NAI "Gestión de la Información", establece las responsabilidades del personal del Banco en materia de seguridad de la información y protección de datos personales, incluyendo las funciones y obligaciones de gestión de activos de información, las actividades relacionadas con el inventario de activos de información, el inventario de datos personales y sistemas de tratamiento y la categorización de activos de información, así como los lineamientos de manejo seguro de la misma.

DÉCIMO SEGUNDO. El Comité de Transparencia, a través del Acuerdo que regula la relación del Banco de México con personas encargadas y las transferencias de datos personales, aprobado el pasado 03 de julio de 2025, establece el formato de clausulado que deberá ser incluido en los contratos o instrumentos jurídicos que celebre el Banco de México, con la finalidad de formalizar la transferencia de datos personales y la relación con terceros encargados de tratarlos.

DÉCIMO TERCERO. La Unidad de Transparencia aplicará instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, y establecerá procedimientos para recibir y responder dudas y quejas de las personas titulares de datos personales.

DÉCIMO CUARTO. La Unidad de Transparencia es la encargada de atender y dar seguimiento, con la asesoría de la Dirección Jurídica, a los Recursos de Revisión que promuevan los particulares en materia de acceso a la información y protección de datos personales.

TRANSITORIOS

PRIMERO. El presente Acuerdo entrará en vigor el 03 de octubre de 2025.

SEGUNDO. Se deja sin efectos el "ACUERDO por el que se determinan los criterios para establecer y mantener el Sistema de Gestión de Seguridad de Datos Personales, la política interna de gestión y tratamiento de datos personales, y otras políticas y programas de protección de datos personales", aprobado por este órgano colegiado el 15 de noviembre de 2023.

Así lo determinó por unanimidad de sus integrantes el Comité de Transparencia del Banco de México, el 30 de septiembre de 2025.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Firma electrónica

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

Firma electrónica

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

Firma electrónica

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

ANEXO ÚNICO

ESQUEMA PARA EL SEGUIMIENTO DEL MONITOREO DE LAS MEDIDAS DE SEGURIDAD ADMINISTRATIVAS, FÍSICAS Y TÉCNICAS (TECNOLÓGICAS) DE DATOS PERSONALES

El esquema para el seguimiento del monitoreo de las medidas de seguridad implementadas en las Unidades Administrativas, que la Dirección de Control Interno (DCI) y la Dirección de Ciberseguridad (DCib) llevan a cabo en el ejercicio de sus atribuciones, es un esquema flexible que podrá ajustarse o adaptarse de acuerdo a las necesidades de dichas Unidades, siempre que se dé cumplimiento a las disposiciones que resulten aplicables, el cual deberá observar cuando menos lo que se señala a continuación:

I. El esquema se basa en un cuestionario que la DCI y la DCib proporcionan bienalmente a las Unidades Administrativas de cuyas respuestas se permita conocer el estado de las medidas de seguridad administrativas, físicas y técnicas que tengan implementadas al efecto. En el diseño del cuestionario, la DCI y la DCib podrán solicitar la opinión o participación de la Dirección de Seguridad y Organización de la Información, en el ámbito de sus atribuciones.

Asimismo, la DCI y la DCib podrán realizar la aplicación referida, a través del cuestionario de autodiagnóstico que el grupo de Contralores Internos de Cumplimiento[2] aplica bienalmente a las Unidades Administrativas, relativo a los procesos, riesgos, controles y normatividad relacionados con los procesos a su cargo.

II. Las preguntas del cuestionario en materia de medidas de seguridad físicas y técnicas, serán aplicadas únicamente a las Unidades Administrativas que hayan concluido con el levantamiento del inventario de datos personales y la categorización de los activos de información respectivos, ya que a partir de la información reportada en el mismo, se podrán identificar cambios en los activos de información en los que se gestionan datos personales, y que no hayan sido reflejados en los inventarios respectivos, así como la existencia de amenazas no valoradas, nuevas vulnerabilidades o cambios en su impacto o consecuencias, así como si se han presentado incidentes de seguridad. Por ello, previo a la aplicación de los cuestionarios, el personal de la DCI y la DCib, a través de las Gerencias de Evaluación y Seguimiento de Control, y de Seguimiento, respectivamente, podrán solicitar a la Unidad de Transparencia y/o a la Dirección de Administración de Riesgos, según corresponda, una relación de las Unidades Administrativas que hayan concluido el mencionado inventario y la categorización de sus activos de información.

Por lo que hace a las medidas administrativas, la DCI, a través de la Gerencia de Control Normativo, realizará una serie de preguntas bienales a las Unidades Administrativas que hayan emitido normatividad relacionada con estas medidas, con las cuales se podrá conocer el estado que guarda la misma, así como si requiere de alguna actualización. Para efectos de lo anterior, se podrá tomar como marco de referencia el listado de normatividad que sobre dicho rubro se tiene en el Documento de Seguridad del Banco de México, o la fuente que considere más conveniente

[2] Conforme a lo previsto en el Manual de Procedimiento de Operación "Contralores Internos de Cumplimiento", los **Contralores Internos de Cumplimiento** son un grupo interdisciplinario integrado por el personal de las Gerencias de Riesgos No Financieros, de Evaluación y Seguimiento de Control, y de Control Normativo.

la DCI. Adicionalmente, la Gerencia de Control Normativo, en coordinación con la Unidad de Transparencia, podrán solicitar a las Unidades Administrativas, previo a la aplicación del cuestionario correspondiente, que confirmen si han emitido normatividad adicional.

III. La DCI y la DCib, a través de las Gerencias de Evaluación y Seguimiento de Control, y de Seguimiento, respectivamente, compartirán a las Unidades Administrativas que cuentan con información en el inventario de datos personales del Banco y han categorizado sus activos de información, una serie de preguntas relacionadas con medidas de seguridad físicas y técnicas, las cuales se incluirán en el cuestionario bienal, y de cuyas respuestas se podrá identificar el estado del monitoreo que las propias Unidades Administrativas han realizado a las mencionadas medidas de seguridad (con base en los cambios que se hayan presentado desde la elaboración del respectivo inventario y la categorización de los activos de información).

Por lo que hace a las medidas administrativas, la Gerencia de Control Normativo, con base en las respuestas que las Unidades Administrativas otorguen en el correspondiente cuestionario, identificará si la normatividad relacionada con estas medidas será objeto de alguna modificación y, de ser el caso, tomará nota de la fecha compromiso, misma que se incluirá en el programa de actualización normativa y, en su caso, los aspectos que se modificarán.

IV. La información de las medidas de seguridad físicas y técnicas incluidas en los cuestionarios de autodiagnóstico será compilada y analizada por la DCI y la DCib en un informe, a través de las Gerencias de Evaluación y Seguimiento de Control, y de Seguimiento, respectivamente, para comunicar el resultado de las actividades de monitoreo al Comité de Transparencia, a efecto de que ese órgano colegiado esté en posibilidad de actuar en el ámbito de sus atribuciones. Asimismo, como parte del seguimiento a las medidas de seguridad administrativas, la Gerencia de Control Normativo incluirá en el informe respectivo, los compromisos de actualización de la normatividad relacionada con estas medidas.

Adicionalmente, el mencionado informe se hará del conocimiento de la Unidad de Transparencia, Dirección de Seguridad y Organización de la Información y Dirección de Administración de Riesgos para que programen, en su caso y en el ámbito de su competencia, el asesoramiento a las Unidades Administrativas responsables de la información para mantener actualizado el inventario de datos personales de los activos de información correspondientes. Por su parte, la Unidad de Transparencia, Dirección de Seguridad y Organización de la Información o la Dirección de Administración de Riesgos, podrán solicitar las respuestas de los cuestionarios de autodiagnóstico respectivos.

V. El referido esquema se realizará, sin perjuicio de las actividades que a la Unidad de Auditoría corresponden, para 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.