Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

**Sujeto Obligado ante el cual se presentó la solicitud:** Banco de México
**Folio de la solicitud:** 6110000027618
**Número de expediente:** RRA 4770/18
**Comisionado Ponente:** Francisco Javier Acuña Llamas

**Visto** el expediente relativo al recurso de revisión interpuesto ante este Instituto, se procede a dictar la presente resolución con base en los siguientes:

## ANTECEDENTES

I. El **21 de mayo de 2018**, el entonces peticionario presentó una solicitud de acceso a la información, a través de la Plataforma Nacional de Transparencia, mediante la cual requirió al **Banco de México**, lo siguiente:

> **Modalidad preferente de entrega de información:**
> "Entrega por Internet en la PNT"
>
> **Descripción clara de la solicitud de información**:
> "Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: a. Número de serie, de parte y de modelo. b. Marca. c. Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico. d. Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup). e. Si se encuentra activada la tecnología WIFI. f. Seguridad o cifrado implementado en la conexión WIFI (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc). g. Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico."

II. El **14 de junio de 2018**, el **Banco de México** comunicó al entonces solicitante la prórroga para dar respuesta en los siguientes términos:

**a)** Oficio sin número de referencia de **14 de junio de 2018**, emitido por la **Unidad de Transparencia del Banco de México**, a través del cual manifestó lo siguiente:

> "Hacemos referencia a su solicitud identificada con el número de folio **6110000027618**, que hizo llegar a la Unidad de Transparencia del Banco de México, la cual se transcribe a continuación:
>
> *[Se transcribe solicitud de información]*
>
> Al respecto, en términos de los artículos 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; y Vigésimo octavo, de los "Lineamientos que establecen los procedimientos internos de atención a

solicitudes de acceso a la información pública", dados a conocer en el Diario Oficial de la Federación mediante publicación del doce de febrero de dos mil dieciséis, el plazo de veinte días hábiles para notificar la respuesta a las solicitudes de acceso a la información podrá ampliarse hasta por diez días más, siempre y cuando existan razones fundadas y motivadas, las cuales deberán ser aprobadas por el Comité de Transparencia.

En este sentido, nos permitimos informarle que el Comité de Transparencia del Banco de México, en sesión ordinaria 22/2018, del catorce de junio de dos mil dieciocho, resolvió confirmar la ampliación del plazo de respuesta a su solicitud. Al efecto, sírvase encontrar adjunto a la presente, en formato PDF, la resolución del Comité de Transparencia en la que determinó lo anterior.

Asimismo, le informamos que las actas de las sesiones celebradas por dicho órgano colegiado, incluida la que señalamos anteriormente, podrá consultarlas en la página de Internet de este Banco Central, través de la siguiente ruta: http://www.banxico.org.mx -LEY DE TRANSPARENCIA-Comité de Transparencia-Actas del Comité de Transparencia del Banco de México-Actas ordinarias.

No obstante lo anterior, para pronta referencia, adjuntamos la liga donde podrá consultar las referidas actas: http://www.banxico.org.mx/ley-de-transparencia/actas-del-comite-de-transparencia-del-banco-de-mex/actas-ordinarias.html.

La Unidad de Transparencia del Banco de México notifica a usted lo anterior, en ejercicio de las facultades señaladas en los artículos 1, 45, fracciones II, IV y V, 125, párrafo primero, 126, 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 61, fracciones II, IV y V, 126, párrafo primero, 127, 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 80., párrafos primero y tercero, 10, párrafo primero, 31 Bis, fracciones II, IV, V, y XXIX, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción XIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; Quinto, párrafo primero, Séptimo, y Vigésimo octavo, de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", publicados en el Diario Oficial de la Federación el doce de febrero de dos mil dieciséis.

Le informamos que Banco de México es responsable de la protección de los datos personales que recabe, los cuales serán tratados con sujeción a las atribuciones y facultades que la normatividad aplicable le confiere, y para finalidades acordes a estas. Puede consultar nuestros avisos de privacidad en la página de internet (www.banxico.org.mx), en la sección "Ley de Transparencia", subsección "Avisos de Privacidad", o a través de la siguiente liga: http://www.banxico.org.mx/ley-de-transparencia/aviso-privacidad.html."

**b)** Acta del Comité de **14 de junio de 2018**, signada por los **Integrantes del Comité de Transparencia del Banco de México**, a través del cual resolvieron lo siguiente:

"...

**RESUELVE**

**ÚNICO.** Se confirma la ampliación del plazo de respuesta, por diez días hábiles adicionales al plazo original, respecto de la solicitud de acceso a la información citada al rubro, en términos de lo expuesto en 105 considerandos Segundo y Tercero de la presente determinación.

..."

**III.** El **28 de junio de 2018**, el **Banco de México**, a través de la Plataforma Nacional de Transparencia, dio respuesta a la solicitud de información que presentó el entonces solicitante, en los términos siguientes:

"En alcance a la solicitud recibida con No. de Folio **6110000027618**, dirigida a la Unidad de enlace de **BANCO DE MÉXICO (BANXICO)**, el día **21/05/2018**, nos permitimos hacer de su conocimiento que:

Con fundamento en la Ley General de Transparencia y Acceso a la Información Pública, se adjunta la información solicitada:

"Se envia respuesta a la solicitud recibida con No. de Folio 6110000027618"

Archivo: 6110000027618_065.zip

Asimismo, el Sujeto Obligado adjuntó a su respuesta copia simple de las siguientes documentales:

**a)** Oficio sin número de referencia de **28 de junio de 2018**, emitido por la **Unidad de Transparencia del Banco de México**, a través del cual manifestó lo siguiente:

"En atención a su solicitud de acceso a la información, identificada con el número de folio **6110000027618**, recibida a través de la plataforma tecnológica INFOMEX, la cual se transcribe a continuación:

*[Se transcribe solicitud de información]*

Sobre la parte de su solicitud relativa a:

- *Número de serie de los routers y puntos de acceso inalámbricos.*
- *Si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico.*
- *Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup).*
- *Si se encuentra activada la tecnología WIFI.*
- *Seguridad o cifrado implementado en la conexión WIFI. (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc)*

- *Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso de los routers y puntos de acceso inalámbrico.*

Hacemos de su conocimiento que el Comité de Transparencia del Banco de México en sesión ordinaria 24/2018, del veintiocho de junio de dos mil dieciocho, resolvió confirmar la clasificación de la información como reservada. Dicha clasificación se fundamenta y motiva en el oficio presentado por la Dirección General de Tecnologías de la Información que se adjunta en archivo pdf junto con la resolución correspondiente.

De igual manera, le informamos que las actas de las sesiones celebradas por dicho órgano colegiado, incluida la que señalamos anteriormente, podrá consultarlas en la página de Internet de este Banco Central (http://www.banxico.org.mx), a través de la siguiente ruta: LEY DE TRANSPARENCIA>Comité de Transparencia>Actas del Comité de Transparencia del Banco de México> Actas ordinarias. No obstante lo anterior, para pronta referencia, adjuntamos la liga donde podrá consultar las referidas actas: http://www.banxico.org.mx/ley-de-transparencia/actas-del-comite-de-transparencia-del-banco-de-mex/actas-ordinarias.html.

Por otro lado, le informamos lo siguiente:

- Actualmente no se soporta la operación de equipos módem.
- No contamos con un registro documental de los números de parte de los routers y puntos de acceso inalámbrico.
- Las marcas y modelos de los routers y puntos de acceso inalámbrico actualmente en operación se presentan en el Anexo "A".

**ANEXO "A"**

**ROUTERS Y PUNTOS DE ACCESO INALÁMBRICO**

| ROUTERS | | PUNTOS DE ACCESO INALÁMBRICO | |
|---|---|---|---|
| MARCA | MODELO | MARCA | MODELO |
| CISCO | 1921 | CISCO | 5508 AIR-CT5508-K9 |
| CISCO | 2901 | CISCO | AIRONET AIR-CAP2602I-N-K9 |
| CISCO | 2901-VSEC/K9 | CISCO | AIRONET AIR-CAP3702I-N-K9 |
| CISCO | 2911-V/K9 | CISCO | AIRONET AIR-CAP3702E-N-K9 |
| CISCO | 2911-VSEC/K9 | CISCO | AIRONET AIR-CAP3802E-N-K9 |
| CISCO | 2921 | CISCO | AIRONET AIR-CAP3802I-N-K9 |
| CISCO | 2921-V/K9 | CISCO | AIRONET AIR-LAP1142N-A-K9 |
| CISCO | 3925 | CISCO | AP1572EAC |

| | | | |
|---|---|---|---|
| CISCO | 3925-V/K9 | | |
| CISCO | 3945E-V/K9 | | |
| CISCO | 4321 | | |
| CISCO | ASR1001 | | |
| CISCO | ASR1002X | | |
| CISCO | C2951-VSEC/K9 | | |
| CISCO | C2951-V/K9 | | |
| CISCO | C881-K9 | | |
| CISCO | ISR 4331 | | |

Finalmente, si desea participar en nuestra Encuesta de Satisfacción a través de la siguiente liga, http://www.banxico.org.mx/WebEncuestas/Credenciales1.do?tema=UNIDAD_TP&version=16.06, le agradeceremos contestar las cuatro preguntas del cuestionario, ya que sus respuestas nos ayudarán a mejorar nuestros servicios tanto hacia usted como hacia otros usuarios.

La Unidad de Transparencia del Banco de México notifica a usted la presente respuesta a su solicitud de acceso a la información, en ejercicio de las facultades señaladas en los artículos 1, 45, fracciones II, IV y V, 125, párrafo primero, 126, 132, párrafo primero, 137, último párrafo, 142, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 61, fracciones II, IV y V, 126, párrafo primero, 127, 135, párrafo primero, 140, último párrafo, 147, de la Ley Federal de Transparencia y Acceso a la Información Pública; 80., párrafos primero y tercero, 10, párrafo primero, 31 Bis, fracciones II, IV, y V, del Reglamento Interior del Banco de México; Primero, párrafo primero y segundo, fracción XIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; Quinto, párrafo primero, y Séptimo, de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", dados a conocer en el Diario Oficial de la Federación mediante publicación del doce de febrero de dos mil dieciséis.

En términos de lo previsto en el Trigésimo tercero de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", dados a conocer en el Diario Oficial de la Federación mediante publicación del doce de febrero de dos mil dieciséis, le informamos que cuenta con quince días hábiles siguientes a la fecha de la presente notificación, para interponer recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ubicado en avenida Insurgentes Sur 3211, delegación Coyoacán, colonia Insurgentes Cuicuilco, código postal 04530, en la Ciudad de México.

Le recordamos que Banco de México es responsable de la protección de los datos personales que recabe, los cuales serán tratados con sujeción a las atribuciones y facultades que la normatividad aplicable le confiere, y para finalidades acordes a estas. Puede consultar nuestros avisos de privacidad en la página de internet

(www.banxico.org.mx), en la sección "Ley de Transparencia", subsección "Avisos de Privacidad", o a través de la siguiente liga: http://www.banxico.org.mx/ley-de-transparencia/aviso-privacidad.html"

**b)** Oficio número **DGTI-91/2018** de **21 de junio de 2018**, signado por el **Director General de Tecnologías de la Información del Banco de México**, a través del cual comunicó lo siguiente:

"Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000027618, que nos turnó la Unidad de Transparencia el 21 de mayo de 2018, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

*[Se transcribe solicitud de información]*

Sobre el particular, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, sexto y séptimo párrafos, de la Constitución Política de los Estados Unidos Mexicanos; 103, 104, 105, 106, fracción I, 108, último párrafo, y 113, fracciones I y IV de la Ley General de Transparencia y Acceso a la Información Pública; 97, segundo, tercero y sexto párrafos, 98, fracción I, y 110, fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública; 2° y 3°, fracción I, de la Ley del Banco de México; 4, 8, primero y segundo párrafos, 10, 15 Bis 1, 18 Bis, 29 del Reglamento Interior del Banco de México, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Cuarto, párrafo primero, Séptimo, fracción I, y último párrafo, Octavo, párrafos primero al tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, primer y segundo párrafos, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, nos permitimos informarles que **esta unidad administrativa clasifica como reservada la siguiente información**:

- Número de serie de los routers y puntos de acceso inalámbricos.
- Si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico.
- Si se encuentra activada la tecnología WPS (por sus siglas en Ingles Wi-Fi Protected Setup),
- Si se encuentra activada la tecnología WIFI.
- Seguridad o cifrado implementado eh la conexión WIFI.
- Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso de los routers y puntos de acceso inalámbrico.

Lo anterior en virtud de que esta información corresponde a especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México; lo cual se fundamenta y motiva en la prueba de daño que se anexa.

Considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones; se extienden a rangos de

entre diez y quince años, esta información deberá ser reservada, al menos; por cinco años.

Por lo expuesto, solicito atentamente a este Comité de Transparenta confirmar la señalada clasificación de la información realizada por esta unidad administrativa.

Lo anterior con fundamento en los artículos 44, fracción II, III y 137, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 108 y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como eh el Vigésimo quito de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes,

Asimismo; de conformidad con el Décimo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, informamos que el personal que, por la naturaleza de sus atribuciones, tiene acceso a la información clasificada es el siguiente:

| Información clasificada | Personal de la DGTI con acceso a la información clasificada |
|---|---|
| Los números de serie de cada uno de los routers y puntos de acceso inalámbricos. | Gerencia de Telecomunicaciones (Gerente)<br>Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal)<br>Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente)<br>Oficina de Soporte a la Gestión Presupuestal (Todo el personal).<br>Subgerencia de Planeación y Regulación (Todo el personal) |
| • Si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico.<br>• Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup).<br>• Si se encuentra activada la tecnología WIFI.<br>• Seguridad o cifrado implementado en la conexión WIFI.<br>• Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso de los routers y puntos de acceso inalámbrico. | Gerencia de Telecomunicaciones (Gerente)<br>Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal)<br>Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente)<br>Oficina de Soporte a la Gestión Presupuestal (Todo el personal). |

..."

c) Prueba de daño número **DGTI.18 H 4.1** de **21 de junio de 2018**, emitida por el **Director General de Tecnologías de la Información del Banco de México**, a través del cual comunicó lo siguiente:

"**PRUEBA DE DAÑO**

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

**Sujeto Obligado ante el cual se presentó la solicitud:** Banco de México
**Folio de la solicitud:** 6110000027618
**Número de expediente:** RRA 4770/18
**Comisionado Ponente:** Francisco Javier Acuña Llamas

***Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México.***

En términos de lo dispuesto por los artículos 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como con la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", es de clasificarse como información reservada aquella cuya publicación pueda:

a) Comprometer la seguridad nacional;
b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;
c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero, del país;
d) Comprometer la seguridad en la provisión de moneda nacional al país.

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones y de seguridad electrónica, sus configuraciones, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; los análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos; así corno toda información derivada de estas especificaciones que, de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa; es clasificada como reservada.

Cabe aclarar que como parte de las especificaciones de la infraestructura de comunicaciones se incluye lo siguiente:

- Los números de serie de cada uno de los equipos de cómputo, ruteadores (routers) y puntos de acceso inalámbricos, así como las unidades administrativas, conforme al organigrama institucional, que hacen uso de cada uno de estos equipos.
- Información sobre las contraseñas para acceder a la configuración y administración de los ruteadores (routers) y puntos de acceso inalámbrico.
- Información que identifique la configuración o el estado de los puertos de red (identificador de los servicios a los cuales se dirige un paquete de datos determinado) del Banco de México.
- Información relacionada con los protocolos de Internet utilizados.

- Nombre y versiones de los programas utilizados para administrar los cortafuegos (firewall) de red.
- Información sobre las tecnologías de red inalámbrica utilizadas y sus mecanismos de seguridad.

En consecuencia, la referida información es reservada en virtud de lo siguiente:

**La divulgación de la información representa un riesgo de perjuicio significativo al interés público**, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, toda vez que dicho riesgo es:

**1) Real**, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales a realizar acciones hostiles en contra de las tecnologías de la información de este Banco Central.

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, dela Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los artículos 20 y 30 de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de esos procesos.

Al respecto, es importante destacar que los sistemas informáticos y de comunicaciones del Banco de México fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero, por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

En este sentido, el artículo 5, fracción XII, de la ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra la **infraestructura de tecnologías de la información y comunicaciones** del Banco de México.

Asimismo, el artículo décimo séptimo, fracción VIII, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Consecuentemente, pretender atacar o inhabilitar los sistemas del Banco, representa una amenaza a la seguridad nacional, ya que publicar la información que se solicita, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del Banco de México, Banco Central del Estado México, por mandato constitucional.

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

En consecuencia, se actualiza la causal de reserva prevista en el artículo 113, fracción I, de la LGTAIP, ya que la divulgación de la información referida compromete la seguridad nacional, al posibiliter la destrucción, inhabilitación o sabotaje de la infraestructura de carácter estratégico con la que opera el Banco de México.

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el

acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.) y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, individuos con propósitos delincuencia les pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 20 de la ley del Banco de México.

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad; la substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales; la corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los, sistemas de pagos.

Por lo anterior, mantener la reserva de las especificaciones de la infraestructura de tecnologías de la información y comunicaciones, que soportan en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos,

considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**.

Por tanto, se actualiza la causal de reserva prevista en el artículo 113, fracción IV, de la LGTAIP, toda vez que la divulgación de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

**2) Demostrable**, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Por citar sólo un ejemplo, considérese el proyecto Metasploit. Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier .sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades

incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS.

- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva.
- De acuerdo canta Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado Un malweare instalado en un equipo de cómputo, el cual logró obtener credencial.es y acceso para generar mensajes fraudulentos en el sistema SWIFT; los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.
- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIH; Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos.
- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas.
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)". Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TOaS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.
- Además de los ataques tradicionales y comunes de usurpación de direcciones MAC, el posible rastreo de equipos móviles empleando esta dirección, hace que no, solase pueda identificar cuando estos equipos se conectan a redes Wi-Fi, sino que además se pudiera estar siguiendo a la persona que lo usa, ocurriendo lo mismo con solo proporcionar el número telefónico de un celular, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto.
- Respecto a la adopción del protocolo para la comunicación en Internet "IPv6", el cual permite la comunicación entre los diferentes elementos de la red y nuestra propia computadora o dispositivo móvil, existen indicios de que los agentes malintencionados han comenzado las pruebas y la investigación de "IPv6" basados en métodos de ataque 000512 (Denial of service -

Denegación del servicio), el cual provoca que un servicio o recurso en una red de computadoras sea inaccesible a usuarios legítimos.

- El conocer el nombre y la versión del programa que administra los cortafuegos o "firewalls" (dispositivos para bloquear los accesos no autorizados ,a una red de computadoras, permitiendo al mismo tiempo comunicaciones autorizadas), puede llevar a conocer las vulnerabilidades de estos dispositivos, las cuales inclusive se llegan a publicar en páginas de Internet.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red? (cuyas especificaciones de fabricación, y por consiguiente posibles vulnerabilidades se pueden obtener indirectamente a través de sus números de serie accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group"), ¿qué puertos de comunicaciones usan? (Si se encuentran abiertos o inactivos), ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?; etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque; si ésta se divulgara directamente bajo la forma de información pública.

Por otro lado, el uso de la tecnología "WiFi", que permite la interconexión inalámbrica de dispositivos electrónicos (computadoras, teléfonos, etc), ya Sea entre ellos o hacia Internet, puede implicar riesgos importantes, ya que sin los adecuados mecanismos de seguridad, terceros pueden acceder a estas redes sin autorización, con la posibilidad de acceder y controlar los dispositivos "WiFi", tales como los ruteadores (o "routers" en inglés) encargados de encaminar los datos trasmitidos entre diferentes redes o subconjuntos de dispositivos, con tan solo conocer su identificador en la red. Por otro lado, el acceso no autorizado a un dispositivo "WiFi" permite supervisar y registrar toda la información que se trasmite a través de éste.

Dentro del uso de redes inalámbricas; el estándar "WPS" (WiFi Protected Setup) define diversos mecanismos para configurar una red local inalámbrica apoyados en el sistema de seguridad conocido como "WPA2" (WiFi Protected Access 2 - Acceso Protegido WiFi 2). El conocer los mecanismos de protección utilizados también permitiría a un atacante identificar las vulnerabilidades asociadas a éstos.

A partir de lo mencionado anteriormente, el dar a conocer la unidad, área u órgano del Banco de México que hace uso de cada uno de ruteadores y puntos de acceso inalámbricos, facilitaría direccionar a algún área funcional que sea del interés del atacante cibernético materializar los riesgos recién señalados.

En resumen, de la misma manera que el resto de las especificaciones de tecnologías de la información y telecomunicaciones, el conocimiento de las tecnologías: utilizadas para la comunicación inalámbrica y sus mecanismos de seguridad y cifrado tales como el estándar WPS, y por obvias razones; el uso de contraseñas para acceder a fas dispositivos WiFi, tales como los ruteadores y puntos de acceso inalámbricos, así como las unidades administrativas que hacen uso de esta tecnología, permitiría a un atacante identificar y aprovechar vulnerabilidades asociadas a ellas.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

**3) Identificable**, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others". El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "Oplcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "0 pica rus - Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo.

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operadores por un monto mayor a 270 billones de pesos; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre ellos el Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**; facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

**El riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda**, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero; económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

En consecuencia, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** contenida en los documentos que se clasifican, no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían muy probablemente implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. Con ello, se imposibilitaría al Banco de México cumplir

con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 26, párrafo sexto de la Constitución.

En efecto, **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad; el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

Por lo anterior, el revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiado o monetario del país, la puesta en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

**La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información relativa a **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**. De otra forma, de entregarse la información de dichas especificaciones, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección respecto a su infraestructura de tecnologías de la información y de comunicaciones para cubrirse de los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaría una carrera interminable entre establecer barreras de protección y divulgación de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y deberá mantenerse en esta clasificación por un periodo de cinco años, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones.

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que

coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

En consecuencia, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, 109, 113, fracciones I y IV, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 104, 105, 106, 110, fracciones I y IV, y 111, de la LFTAIP; 146, de la Ley General del Sistema de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 3o. de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, y 29, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes; **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, se ha determinado clasificar como reservada."

**d)** Acta del Comité de Transparencia de **28 de junio de 2018**, signada por los **Integrantes del Comité de Transparencia del Banco de México**, a través de la cual resolvieron lo siguiente:

"...

**RESUELVE**

**ÚNICO.** Se confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresada en la prueba de daño contenida en el oficio precisado en el resultando Quinto de la presente determinación.

..."

**IV.** El **12 de julio de 2018**, se recibió vía la Plataforma Nacional de Transparencia, el recurso de revisión interpuesto por el hoy recurrente en contra de la respuesta emitida por el **Banco de México**, en el cual establece lo siguiente:

"...

**AGRAVIO ÚNICO.- Violación a la garantía de máxima publicidad de la información.**

ARTÍCULOS TRANSGREDIDOS: 6° DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, 4°, 11 Y 12 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, 3° DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Inicialmente es oportuno señalar que por disposición del artículo 6° constitucional, el derecho fundamental de acceso a la información deberá interpretarse en función del principio de máxima publicidad. Asimismo, en atención a lo establecido en el artículo 1 ° constitucional y en la Ley reglamentaria del artículo 6° del mismo ordenamiento, en todo momento debe prevalecer la protección más amplia para la persona.

El principio de máxima publicidad enunciado en los artículos 11 y 12 de la Ley General de Transparencia y Acceso a la Información Pública (en lo subsecuente referida como Ley General), vincula a todo sujeto obligado a efecto de que permita el acceso y entregue todo tipo información generada, obtenida, adquirida, transformada o en su defecto se encuentre en su posesión; con exclusión de aquella que por disposición de Ley actualiza algún supuesto de excepcionalidad.

*[Se transcriben artículos]*

Ahora bien, como se evidenciará a priori en las subsecuentes líneas, la clasificación de información efectuada por el sujeto obligado en atención a la solicitud 6110000027618 transgrede el principio de máxima publicidad de la información. Sin embargo, es de advertirse antes que en función de lo dispuesto en el artículo 20 de la Ley General, la carga de la prueba recae directamente sobre el sujeto obligado.

*[Se transcribe artículo]*

Como se mencionó, el principio de máxima publicidad únicamente puede verse limitado por la actualización de algún supuesto previsto en el régimen de excepciones, es decir, ante la presencia de información clasificada como confidencial o reservada.

Los artículos 113 de la Ley General y 110 de la Ley Federal de Transparencia y Acceso a la Información Pública (en lo subsecuente Ley Federal) establecen que información será considerada como reservada.

*[Se transcriben artículos]*

Ahora bien, la información precisada en la solicitud 6110000027618 no actualiza algún supuesto previsto en los artículos antes transcritos, tal y como lo hace aparentar la clasificación efectuada por el sujeto obligado.

Lo anterior, toda vez que lo peticionado en la solicitud 6110000027618 se trata de información que de ninguna forma compromete la seguridad nacional, la seguridad pública o la defensa nacional; afecta la efectividad de las medidas adoptadas en

relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pone en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; compromete la seguridad en la provisión de moneda nacional al país; y menos aún vulnerar o alterar el normal desarrollo de las funciones desempeñadas por el sujeto obligado.

Sino por el contrario, lo único que permite es corroborar si realmente el sujeto obligado emplea adecuadamente mecanismos o técnicas tendientes a robustecer su seguridad informática, así como la nacional y la pública.

Es importante se tenga en consideración que el número de serie y de parte, son datos que por disposición de los artículos 68 de la Ley Federal y 70 fracción XXXIV de la Ley General, se encuentra abiertos al público; ya que estos deben formar parte de los inventarios de los bienes muebles en posesión o propiedad el sujeto obligado.

*[Se transcriben artículos]*

Inclusive, si alguno de los datos requeridos en la solicitud 6110000027618 pusieran en riesgo la seguridad informática implementada por el sujeto obligado; este Instituto, Caminos y Puentes Federales, las Secretarías de Economía, de Medio Ambiente y Recursos Naturales, el Instituto Mexicano del Seguro Social, el Tribunal Federal de Justicia Administrativa, la Consejería Jurídica del Ejecutivo Federal, el Servicio de Administración Tributaria, la Auditoria Superior de la Federación, no hubiesen entregado datos equivalentes en respuesta a las solicitudes de información pública: 0673800104818, 0912000013718, 0001000063618, 0001600166518, 0064100938518, 3210000027918, 0220000004218, 0610100064118 y 0110000044318, respectivamente; mismas que con fundamento en el penúltimo párrafo del artículo 149 de la Ley Federal, someto a consideración de este Instituto.

En suma, la clasificación efectuada por el sujeto obligado resulta violatoria del principio de máxima publicidad, y en última instancia del derecho fundamental de acceso a la información reconocido constitucional y convencionalmente en beneficio del hoy recurrente; ya que como se argumentó en líneas anteriores, lo requerido en la solicitud 6110000027618 no actualiza algún supuesto de reserva previsto en la Ley Federal o en la Ley General.

**PRUEBAS**

**A.** Con fundamento en el artículo 20 de la Ley General, de aplicación supletoria a la Ley Federal, atentamente solicito se aplique la reversión de la carga de la prueba al sujeto obligado, es decir, se le requiera para que pruebe la reserva de la información precisada en la solicitud de información pública número 6110000027618.

*[Se transcriben artículos]*

**B.** La instrumental de actuaciones y la presuncional en su doble aspecto, en todo lo que me favorezca.

**PUNTOS PETITORIOS**

Por lo antes expuesto y fundado atentamente solicito:

**I.** Tenerme por interpuesto en tiempo y forma el presente recurso.
**II.** Tenerme por señalado como único y exclusivo medio para recibir notificaciones el correo electrónico indicado.
**III.** Aplicar la suplencia de la queja al presente recurso.
**IV.** Revocar o en su caso modificar la respuesta del sujeto obligado, con la finalidad de que se me entregue la información pública solicitada, conforme a los términos y criterios precisados originalmente; y en el supuesto de no poderse entregar bajo la modalidad de entrega elegida, manifiesto conformidad para que se realice vía correo electrónico señalado en la presente."

**V**. El **12 de julio de 2018**, el Comisionado Presidente **Francisco Javier Acuña Llamas** de este Instituto asignó el número de expediente **RRA 4770/18**, al recurso de revisión y con base en el sistema aprobado por el Pleno, fue recaído a la Ponencia a su cargo para los efectos del artículo 156, fracción I de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**VI**. El **01 de agosto de 2018**, el Secretario de Acuerdos y Ponencia de Acceso a la Información[1], adscrito a la Oficina del Comisionado Ponente, **acordó la admisión** del recurso de revisión interpuesto por el hoy recurrente en contra del **Banco de México**, en cumplimiento con lo establecido en el artículo 156, fracción I de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**VII**. El **06 de agosto de 2018**, se notificó al **Banco de México**, a través de la *Herramienta de Comunicación*, la admisión del recurso de revisión, otorgándole un plazo de siete días hábiles a partir de dicha notificación, para que manifestara lo que a su derecho conviniera, ofreciera pruebas y formulara alegatos, dando cumplimiento al artículo 156, fracciones II y IV de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**VIII**. El **15 de agosto de 2018**, se recibió en este Instituto a través de la Herramienta de Comunicación, los **alegatos** por parte del **Banco de México**, a través de los cuales remitió las siguientes documentales:

Oficio sin número de referencia de **15 de agosto de 2018**, firmado por el **Gerente de Análisis y Promoción de Transparencia y por el Subgerente de Análisis Jurídico y Promoción de Transparencia, ambos de la Unidad de**

[1] De conformidad con lo dispuesto por el numeral Tercero, fracción VII del *Acuerdo mediante el cual se confieren funciones a los Secretarios de Acuerdos y Ponencia para coadyuvar con los Comisionados Ponentes en la sustanciación de los medios de impugnación competencia del Instituto, establecidos en la Ley General de Transparencia y Acceso a la Información Pública y en la Ley Federal de Transparencia y Acceso a la Información Pública*, publicado en el *Diario Oficial de la Federación* el 25 de agosto de 2016.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

**Sujeto Obligado ante el cual se presentó la solicitud:** Banco de México
**Folio de la solicitud:** 6110000027618
**Número de expediente:** RRA 4770/18
**Comisionado Ponente:** Francisco Javier Acuña Llamas

**Transparencia del Banco de México**, a través del cual comunicaron lo siguiente:

"...

**III. CONTESTACIÓN A LOS AGRAVIOS**

En la atención de la solicitud de acceso a la información materia del presente informe, identificada con el número de folio **6110000027618**, el Banco de México actuó en estricto apego a las disposiciones constitucionales, legales y reglamentarias que rigen la materia, así como con total respeto a los derechos humanos del solicitante.

Los agravios expresados por el recurrente son infundados, tal como se destaca a continuación:

En los agravios, el recurrente aduce que la clasificación de la información efectuada por este Banco Central viola la *"garantía de máxima publicidad de la información"*, pues considera que en el caso concreto no se actualizan los supuestos de clasificación previstos en los artículos 113 de la LGTAIP y 110 de la LFTAIP.

Lo argumentado por el recurrente es infundado, toda vez que contrario a lo que aduce, en el presente caso quedó plenamente acreditado, a través de la prueba de daño respectiva, que se actualizan las causales de clasificación previstas en los artículos 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), y la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas. Esto, en razón de que se demostró que la divulgación de la información clasificada puede: comprometer la seguridad nacional; afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, y comprometer la seguridad en la provisión de moneda nacional al país.

Al respecto, deben destacarse los siguientes aspectos que fueron debidamente expuestos y comprobados a través de la prueba de daño mencionada:

**a.** La divulgación de la información clasificada comprometería la seguridad nacional, ya que posibilitaría la destrucción, inhabilitación o sabotaje de la infraestructura de carácter estratégico y prioritaria, involucrada en los procesos de emisión de billetes y acuñación de moneda a nivel nacional (lo anterior comprende el diseño de billetes, el manejo de insumos para su fabricación y manufactura, así como los actos correspondientes al traslado y custodia de efectivo, valores y metales preciosos, y el almacenamiento, abastecimiento, canje, retiro, reproducción, destrucción y entrega de signos monetarios).

De igual forma, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y la economía nacional en su conjunto.

**b.** Dicho riesgo es real, dado que la difusión de la información referida haría posible que personas o grupos de ellas, con intenciones delictivas, llevaran a cabo acciones hostiles en contra de las tecnologías de la información de este Banco Central utilizadas, entre otras funciones, para cumplir la relacionada con el objetivo prioritario de proveer de moneda nacional a la economía del país, y en consecuencia afectarán un **área estratégica del Estado mexicano**.

En efecto, debe tenerse presente que, en términos del artículo 28, párrafo sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, la acuñación de moneda y emisión de billetes constituyen **áreas estratégicas del Estado mexicano**, funciones que son ejercidas de manera exclusiva por el Banco de México.

**c.** En ese sentido, los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo.

Al respecto, es preciso mencionar que las tecnologías de la información y comunicaciones con las que el Banco de México cuenta, son herramientas necesarias e indispensables para la consecución de las finalidades y funciones que por mandato constitucional y legal tiene encomendadas este Banco Central, entre las que se encuentran las relacionadas con la finalidad de proveer de moneda nacional a la economía del país.

**d.** En efecto, los sistemas informáticos y de comunicaciones del Banco de México fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero. En particular, dichos sistemas son utilizados para cumplir con la función del Banco de México en las áreas estratégicas relacionadas con la finalidad de proveer de moneda nacional a la economía del país. Por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

**e.** En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

**f.** A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra, como se ha dicho, la infraestructura de tecnologías de la información y comunicaciones del Banco de México utilizadas, entre otras funciones, para cumplir su función constitucional en las áreas estratégicas relacionadas con la finalidad de proveer de moneda nacional a la economía del país.

**g.** Asimismo, la fracción VIII del Lineamiento Décimo séptimo de los *Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*, señala que se considera como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

**h.** Consecuentemente, el riesgo de que por la divulgación de información se ataquen o inhabiliten los sistemas del Banco Central, representa una amenaza a la seguridad nacional, pues posibilitaría la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico del mismo, como lo es la que se utiliza para cumplir con las funciones constitucionales del Banco de México en las áreas estratégicas relacionadas con la finalidad de proveer de moneda nacional a la economía del país.

**i.** En efecto, proporcionar las especificaciones de la infraestructura de tecnologías de la información y comunicaciones (como es el caso de los números de serie de los routers y puntos de acceso inalámbricos; si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico; si se encuentra activada la tecnología WPS (por sus siglas en inglés Wi-Fi Protected Setup); si se encuentra activada la tecnología WIFI, seguridad o cifrado implementado en la conexión WIFI; así como conforme al organigrama estructural, unidades áreas u órganos que hacen uso de los routers y puntos de acceso inalámbricos) indudablemente facilitaría que terceros logren acceder a información utilizada por el Banco de México para cumplir su función en las áreas estratégicas relacionadas con la finalidad de proveer de moneda nacional a la economía del país; así como acceder información financiera o personal y modificar los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

j. A mayor abundamiento, debe destacarse que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se basan en (1) descubrir y aprovechar vulnerabilidades, mediante el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

k. Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.) y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar (como es el caso de los números de serie de los routers y puntos de acceso inalámbricos; si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico; si se encuentra activada la tecnología WPS (por sus siglas en inglés Wi-Fi Protected Setup); si se encuentra activada la tecnología WIFI, seguridad o cifrado implementado en la conexión WIFI; así como conforme al organigrama estructural, unidades áreas u órganos que hacen uso de los routers y puntos de acceso inalámbricos) individuos con propósitos delincuencia les pueden llevar a cabo un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

l. Sea cual fuere el origen o motivo del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, la actualización de ese riesgo podría conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 20. de la Ley del Banco de México.

m. De materializarse los riesgos descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; aspectos relacionados con el diseño y fabricación de billete; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos.

Asimismo, podría sustraerse información de política monetaria o cambiaria, previo a sus informes programados, o bien ocasionarse su alteración o interrupción en las fechas de su publicación, lo cual igualmente afectaría las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales.

**n.** Con lo anterior, también se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo, se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

**o.** Por lo anterior, mantener la reserva de las especificaciones de la infraestructura de tecnologías de la información y comunicaciones, que soportan en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

**p.** El riesgo referido es además **demostrable**, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como lo es la relacionada con la finalidad de proveer de moneda nacional a la economía del país.

**q.** Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Al respecto, en la prueba de daño que sustentó la clasificación que nos ocupa, se citaron diversos ejemplos, debidamente documentados, de ataques cibernéticos perpetrados con base en información sobre las especificaciones de infraestructuras tecnológicas.

**r.** De igual modo, el riesgo que se generaría en caso de que la información clasificada se divulgara es identificable.

En efecto, tal como se expuso en la prueba de daño que sustentó la clasificación, el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Al respecto, se puede mencionar que durante 2016 y 2017, nuestros registros

indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

**s.** En relación con lo anterior, en la referida prueba de daño se refirió que lo anterior no es ajeno a la banca mundial, la cual es continuamente asediada por grupos denominados "hacktivistas", y se citaron casos concretos registrados en diversos medios, de los que se acompañó evidencia documental.

**t.** Asimismo, en la referida prueba de daño se refirió, para dimensionar de manera más clara las consecuencias que un eventual ataque informático dirigido al Banco de México podría generar, que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto mayor a 270 billones de pesos; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

**u.** Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de las especificaciones de la infraestructura de tecnologías de la información y comunicaciones, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

**v.** Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre ellos el propio Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

**w.** Asimismo, se destacó que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder

adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

**x.** Por contrapartida, dar a conocer información como la solicitada por el recurrente (los números de serie de los routers y puntos de acceso inalámbricos; si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico; si se encuentra activada la tecnología WPS (por sus siglas en inglés Wi-Fi Protected Setup); si se encuentra activada la tecnología WIFI, seguridad o cifrado implementado en la conexión WIFI; así como conforme al organigrama estructural, unidades áreas u órganos que hacen uso de los routers y puntos de acceso inalámbricos) no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

**y.** En relación con lo anterior, debe insistirse en que un ataque exitoso a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendría implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. De resultar exitosos tales ataques, se imposibilitaría al Banco de México cumplir con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 28, párrafo sexto de la Constitución.

**z.** A mayor abundamiento, debe hacerse hincapié en que la información que pretende obtener el ahora recurrente no satisface un interés público, pues no se relaciona con la rendición de cuentas o el uso de recursos. Así, al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste. Como se ha dicho, revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

**aa.** Por otra parte, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información solicitada, la cual nada tiene que ver con la rendición de cuentas o el ejercicio de recursos públicos.

**bb.** Asimismo, de entregarse la información solicitada, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección respecto a su infraestructura de tecnologías de la información y de comunicaciones para cubrirse de los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaría una carrera interminable entre establecer barreras de protección y divulgación de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

**cc.** Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer las especificaciones de la infraestructura de tecnologías de la información y comunicaciones generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en dar a conocer dicha información.

**dd.** Adicionalmente, y en relación con lo manifestado por el recurrente, quien infundadamente cuestiona la clasificación realizada, debe señalarse que los números de serie de los equipos de cómputo quedan registrados en las bases de datos de los fabricantes de los equipos, ya que además de ser utilizados como un identificador de control durante el periodo de garantía para fines de soporte técnico, los proveedores pueden contar con información más específica y detallada de cada equipo vendido con respecto a las especificaciones dadas a conocer a sus compradores e inclusive publicada en Internet.

Considerando que el número de serie constituye un identificador único asociado a un dispositivo durante su proceso de manufactura. El dar a conocer los números de serie de cada uno de los equipos de cómputo, routers y puntos de acceso inalámbricos del Banco de México, facilitaría que terceros identifiquen posibles vulnerabilidades asociadas a estos equipos, con las consecuentes afectaciones que pudieran suscitarse, que van desde el acceso a información financiera o personal, la modificación de los datos que se procesan en ellos o, incluso, dejar fuera de operación a los sistemas de información del Banco.

Por lo que, no divulgar los números de serie asociados a estos dispositivos es en sí una medida básica de seguridad, ya que continuamente se publican vulnerabilidades asociadas a los números de serie de distintas tecnologías.

A continuación se hace referencia al caso donde al obtenerse el número de serie de un router, aprovechando una vulnerabilidad asociada, con este número de serie se pueden obtener, tanto el nombre de usuario, como la contraseña del administrador del router y aprovechar otras vulnerabilidades asociadas. La información fue obtenida de internet en el vínculo: https://www.cvedetails.com/cve/CVE-2016-10175/ (Anexo Ocho)

Asimismo, de contar con la información solicitada, personas que tuvieran intención de atacar los sistemas del Banco de México tomarían ventaja, por ejemplo, si obtuvieran información de otras fuentes sobre debilidades o

defectos de fabricación de ciertos equipos, lo cual les permitiría acceder con mayor facilidad a estos y sustraer información, alterarla, o causar un daño disruptivo.

**ee.** Por otra parte, debe destacarse que contrario a lo aducido por el recurrente, es falso que el Banco de México, en su carácter de sujeto obligado, deba documentar los "números de serie y de parte" de los equipos de cómputo bajo su posesión o propiedad, o que estos deban integrar el inventario de bienes muebles previsto en la fracción XXXIV del artículo 70 de la LGTAIP.

En relación con lo anterior, es importante considerar que el contenido del referido inventario no es caprichoso o indeterminado. Se encuentra sujeto a los lineamientos técnicos emitidos por el Sistema Nacional de Transparencia, al igual que el resto de la información correspondiente a las obligaciones de transparencia.

Al respecto, el artículo 61 de la LGTAIP, establece:

*[Se transcribe artículo]*

En tales términos, la información que debe publicarse en cumplimiento a la obligación de transparencia prevista en la citada fracción XXXIV del artículo 70 de la LGTAIP, está definida por los Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia (Lineamientos técnicos generales).

Al respecto, debe destacarse que en el formato y criterios relativos a la aludida fracción XXXIV del artículo 70 de la LGTAIP, de los mencionados Lineamientos técnicos generales, no se establece que el número de serie o el número de parte de los equipos de cómputo, o de algún otro bien mueble, deba integrar el inventario previsto en la misma. Únicamente se requiere en dichos Lineamientos, la descripción del bien (en general), lo cual se hace debidamente, dando a conocer la marca y modelo del bien respectivo.

**ff.** A mayor abundamiento, y en relación con los riesgos de dar a conocer si se usan contraseñas para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico, de la misma manera que para cualquier equipo de cómputo, permitiría a un atacante identificar y aprovechar vulnerabilidades asociados a estos equipos.

Los ruteadores y otros dispositivos de red son blancos principales para ser atacados, aprovechando vulnerabilidades mediante las cuales se logra acceder con privilegios de administrador mediante contraseñas simples implantadas en el código fuente (hard-coded password), o porque no se cambian las contraseñas de administración configuradas de fábrica. Un ejemplo de estas amenazas se describe en la siguiente página:

https://securelist.com/threat-intelligence-report-for-the-telecommunications-industry/75846/ (Anexo Nueve).

**gg.** Por otro lado, dar a conocer si se encuentra activada la tecnológia WIFI, la seguridad o cifrado implementado en la conexión WIFI, así como si se encuentra activada la tecnologia WPS (por sus siglas en inglés Wi-Fi Protected Setup), es nuevamente, coadyuvar a facilitar la posibilidad de un ataque, ya que el uso de la tecnología "WiFi", que permite la interconexión inalámbrica de dispositivos electrónicos (computadoras, teléfonos, etc.), ya sea entre ellos o hacia Internet, puede implicar riesgos importantes, ya que sin los adecuados mecanismos de seguridad, terceros pueden acceder a estas redes sin autorización, con la posibilidad de acceder y controlar los dispositivos "WiFi", tales como los ruteadores (o "routers" en inglés) encargados de encaminar los datos trasmitidos entre diferentes redes o subconjuntos de dispositivos, con tan solo conocer su identificador en la red. Por otro lado, el acceso no autorizado a un dispositivo l/WiFi/l permite supervisar y registrar toda la información que se trasmite a través de éste.

Asimismo, dentro del uso de redes inalámbricas, el estándar "WPS" (WiFi Protected Setup) define diversos mecanismos para configurar una red local inalámbrica apoyados en el sistema de seguridad conocido como "WPA2" (WiFi Protected Access 2 - Acceso Protegido WiFi 2). El conocer los mecanismos de protección utilizados también permitiría a un atacante identificar las vulnerabilidades asociadas a éstos, y facilitaría el éxito en sus posibles ataques.

La descripción de cómo se pueden aprovechar las vulnerabilidades asociadas a los diferentes aspectos de la configuración de la tecnologia WiFi, cuando esta se llega a utilizar, se describen en la siguiente página de Internet: https://www.krackattacks.com/ (Anexo Diez).

**hh.** En cuanto a dar a conocer, conforme el organigrama estructural, las unidades administrativas que hacen uso de los routers y puntos de acceso inalámbrico, facilitaría direccionar a algún área funcional que sea del interés del atacante cibernético materializar los riesgos recién señalados.

A este respecto, expertos en el tema de seguridad, como Offensive Security consideran que la obtención de información de especificaciones como: ¿qué equipos componen la red? (cuyas especificaciones de fabricación, y por consiguiente posibles vulnerabilidades se pueden obtener indirectamente a través de sus números de serie accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, ¿qué puertos de comunicaciones usan? (Si se encuentran abiertos o inactivos), ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información seria mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

La información referente al tema de recopilación de información se puede consultar en la siguiente página:

https://www.offensivesecurity.com/metasploit-unleashed/information-gathering/ (Anexo Once).

En resumen, de la misma manera que el resto de las especificaciones de tecnologías de la información y telecomunicaciones, el conocimiento de las tecnologías utilizadas para la comunicación inalámbrica y sus mecanismos de seguridad y cifrado tales como el estándar WPS, y por obvias razones, el uso de contraseñas para acceder a los dispositivos WiFi, tales como los ruteadores y puntos de acceso inalámbricos, así como las unidades administrativas que hacen uso de esta tecnología, permitiría a un atacante identificar y aprovechar vulnerabilidades asociadas a ellas.

Atento a lo anterior, es evidente que, contrario a lo aducido por el recurrente, en el presente caso se clasificó debidamente la información relativa a: Los números de serie de los routers y puntos de acceso inalámbricos; si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico; si se encuentra activada la tecnología WPS (por sus siglas en inglés Wi-Fi Protected Setup); si se encuentra activada la tecnología WIFI, seguridad o cifrado implementado en la conexión WIFI; así como conforme al organigrama estructural, unidades áreas u órganos que hacen uso de los routers y puntos de acceso inalámbricos, al actualizarse las causales de clasificación previstas en los artículos 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como con la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*.

## IV. PRUEBAS

A fin de acreditar las manifestaciones vertidas por esta Unidad de Transparencia, se ofrecen los siguientes medios de prueba:

1. **La DOCUMENTAL PÚBLICA.** Consistente en copia certificada de la solicitud de acceso a la información identificada con el número de folio 6110000027618. Se acompaña como Anexo Uno.

2. **La DOCUMENTAL PÚBLICA.** Consistente en copia certificada de la evidencia del turno interno de la solicitud 6110000027618. Se acompaña como Anexo Dos.

3. **La DOCUMENTAL PÚBLICA.** Consistente en copia certificada del oficio DGTI- 78/2018, mediante el cual la Dirección General de Tecnologías de la Información del Banco de México sometió a la consideración del Comité de Transparencia la confirmación de la ampliación plazo de respuesta de la solicitud de referencia. Se acompaña como Anexo Tres.

4. **La DOCUMENTAL PÚBLICA.** Consistente en la resolución mediante la cual el Comité de Transparencia del Banco de México confirmó la determinación de ampliación del plazo de respuesta. Se acompaña como Anexo Cuatro.

5. **La DOCUMENTAL PÚBLICA.** Consistente en el oficio DGTI-91/2018, mediante el cual la Dirección General de Tecnologías de la Información solicitó al Comité de Transparencia del Banco de México confirmar la clasificación de la información, relativa a la solicitud de acceso a la información 6110000027618. Se acompaña como Anexo Cinco.

6. **La DOCUMENTAL PÚBLICA.** Consistente en copia certificada del acta de la sesión ordinaria 24/2018, de veintiocho de junio de dos mil dieciocho, con sus respectivos anexos M y N. Se acompaña como Anexo Seis.

   Los referidos documentos también pueden ser consultados en la página de Internet de este Banco Central (http://www.banxico.org.mx), a través de la siguiente ruta: LEY DE TRANSPARENCIA> Comité de Transparencia> Actas del Comité de Transparencia del Banco de México > Actas ordinarias, o mediante la siguiente liga: http://www.banxico.org.mx/ley-de-transparencia/actas-del-comite-de-transparencia-del-banco-de-mex/actas-ordinarias.html

   Asimismo, se puede acceder directamente al acta mencionada a través de la siguiente liga: http://transparencia.banxico.org.mx/documentos/%7B4F62831D-0E82-C8D1-9F46-790868417757%7D.pdf

7. **La DOCUMENTAL PÚBLICA.** Consistente en copia certificada de la respuesta notificada por la Unidad de Transparencia del Banco de México, relativa a la solicitud de acceso a la información 6110000027618. Se acompaña como Anexo Siete.

8. **La DOCUMENTAL.** Consistente en impresión de la página "CVE Details". Se acompaña como Anexo Ocho.

9. **La DOCUMENTAL.** Consistente en impresión de la página "SecureList". Se acompaña como Anexo Nueve.

10. **La DOCUMENTAL.** Consistente en impresión de la página "Key Reinstallation Attacks". Se acompaña como Anexo Diez.

11. **La DOCUMENTAL.** Consistente en impresión de la página "Offensive Security". Se acompaña como Anexo Once.

12. **La INSTRUMENTAL DE ACTUACIONES.** Consistente en todo lo actuado en el presente recurso en lo que favorezca al Banco de México.

13. **La PRESUNCIONAL.** En su doble aspecto legal y humano, en todo aquello que favorezca al Banco de México.

Por lo anteriormente expuesto y fundado,

**A ESE H. COMISIONADO PONENTE,** atentamente pedimos se sirva:

**PRIMERO.** Tenernos por presentados en nuestro respectivo carácter de Gerente de Análisis y Promoción de Transparencia y Subgerente de Análisis Jurídico y Promoción de Transparencia, del Banco de México, desahogando en tiempo y forma la vista que se mandó dar al Banco de México mediante auto de primero de agosto de dos mil dieciocho, notificado en esa misma fecha.

**SEGUNDO.** Tener por hechas las manifestaciones señaladas en el presente escrito, y por ofrecidas, admitidas y desahogadas, las pruebas que se relacionan en el apartado correspondiente.

**TERCERO.** Por las razones expuestas en el cuerpo de este escrito confirmar el acto impugnado."

Al efecto, el Sujeto Obligado adjuntó a su escrito de alegatos, las documentales listadas del numeral 1 al 11 de su apartado de pruebas.

**IX**. El **13 de septiembre de 2018**, la Secretaria de Acuerdos y Ponencia de Datos Personales, adscrita a la Oficina del Comisionado Ponente, dictó acuerdo por medio del cual se **amplió el plazo de resolución**; lo anterior, de acuerdo con lo establecido en el artículo 151 de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**X**. El **19 de septiembre de 2018**, se notificó al ahora recurrente mediante estrados[2], en términos del artículo 159 de la *Ley Federal de Transparencia y Acceso a la Información* Pública, la admisión del recurso de revisión, informándole sobre su derecho de manifestar lo que a su derecho convenga, ofrecer todo tipo de pruebas y presentar alegatos, dentro del término de siete días hábiles contados a partir de dicha notificación, de conformidad con lo establecido en el artículo 156, fracciones II y IV de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**XI**. El **20 de septiembre de 2018**, se notificó al **Banco de México** y al ahora recurrente el acuerdo de ampliación respectivo.

**XII**. El **05 de octubre de 2018**, la Secretaria de Acuerdos y Ponencia de Datos Personales, adscrita a la Oficina del Comisionado Ponente, dictó acuerdo por medio del cual se **decretó el cierre de instrucción** en el medio de impugnación

[2] La notificación se realizó por estrados toda vez que el 06 de agosto de 2018 el correo electrónico enviado para tales efectos fue devuelto y, posteriormente el 18 de septiembre de 2018, la pieza postal fue devuelta por el Servicio Postal Mexicano.

que nos ocupa; lo anterior, de acuerdo con lo establecido en el artículo 156, fracción VI de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**XIII**. El **08 de octubre de 2018**, se notificó al **Banco de México**, a través de la Herramienta de Comunicación, el acuerdo de cierre de instrucción descrito en el antecedente inmediato anterior.

**XIV**. El **08 de octubre de 2018**, se notificó al hoy recurrente mediante estrados, en términos del artículo 159, fracción II de la *Ley Federal de Transparencia y Acceso a la Información Pública,* el referido acuerdo de cierre de instrucción.

**XV**. A la fecha de la presente determinación no se recibió alegatos por parte del hoy recurrente.

## CONSIDERANDOS

**PRIMERO**. El Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es competente para conocer respecto del presente asunto, de conformidad con lo previsto en el artículo 6o, Apartado A, fracción VIII, de la *Constitución Política de los Estados Unidos Mexicanos*; los artículos 41, fracción II, 146, 150 y 151, y los Transitorios Primero y Quinto de la *Ley General de Transparencia y Acceso a la Información Pública*, publicada en el *Diario Oficial de la Federación* el 05 de mayo de 2016; así como lo dispuesto en los artículos 21, fracción II, 146, 151,156 y 157 y los Transitorios Primero y Quinto de la *Ley Federal de Transparencia y Acceso a la Información Pública*, publicada en el *Diario Oficial de la Federación* el 09 de mayo de 2016; así como el artículo 18, fracciones V, XIV y XVI del *Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, publicado en el *Diario Oficial de la Federación* el 17 de enero de 2017.

**SEGUNDO**. El entonces peticionario presentó una solicitud de acceso a la información ante el **Banco de México**, por virtud de la cual requirió, eligiendo como modalidad de Entrega a través del portal, de cada uno de los Modems, Routers (rúters) o Puntos de acceso inalámbricos, lo siguiente:

**a.** Número de serie, de parte y de modelo.
**b.** Marca.
**c.** Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico.

**d.** Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup).
**e.** Si se encuentra activada la tecnología WIFI.
**f.** Seguridad o cifrado implementado en la conexión WIFI (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc).
**g.** Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico"

En respuesta a la solicitud de acceso, el **Banco de México** a través de la **Dirección General de Tecnologías de la Información** comunicó lo siguiente:

- Entregó un listado de los Routers y Puntos de acceso inalámbrico, mismo que contiene la Marca y Modelo.

- Determinó que la información de los **contenidos de información a)**, **c)**, **d)**, **e)**, **f)** y **g)** es clasificada en términos de lo establecido en el artículo 110 fracciones I y IV de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

- El Comité de Transparencia confirmó la clasificación referida.

Inconforme, el hoy recurrente presentó un recurso de revisión, a través del cual señaló como agravio su inconformidad contra la clasificación decretada por el Sujeto Obligado, además ofreció como medio de prueba la instrumental de actuaciones y la presuncional en su doble aspecto.

Establecido lo anterior, resulta dable hacer mención que el hoy recurrente no se inconformó respecto de la respuesta proporcionada por el Sujeto Obligado al **contenido de información b)**, esto es, la marca y modelo de cada uno de los Modems, Routers (rúters) o Puntos de acceso inalámbricos.

En vista de lo anterior, se considera como **actos consentidos** de manera tácita y, por ende, no formara parte del estudio que se realice en la presente resolución.

Sirve de apoyo al anterior razonamiento, la jurisprudencia y tesis aislada que se citan a continuación:

"No. Registro: 204,707
**Jurisprudencia**
Materia(s): Común
Novena Época

Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
II, Agosto de 1995
Tesis: VI.2o. J/21
Página: 291

**ACTOS CONSENTIDOS TÁCITAMENTE.** Se presumen así, para los efectos del amparo, los actos del orden civil y administrativo, que no hubieren sido reclamados en esa vía dentro de los plazos que la ley señala.

SEGUNDO TRIBUNAL COLEGIADO DEL SEXTO CIRCUITO.
Amparo en revisión 104/88. Anselmo Romero Martínez. 19 de abril de 1988. Unanimidad de votos. Ponente: Gustavo Calvillo Rangel. Secretario: Jorge Alberto González Álvarez.
Amparo en revisión 256/89. José Manuel Parra Gutiérrez. 15 de agosto de 1989. Unanimidad de votos. Ponente: Gustavo Calvillo Rangel. Secretario: Humberto Schettino Reyna.
Amparo en revisión 92/91. Ciasa de Puebla, S.A. de C.V. 12 de marzo de 1991. Unanimidad de votos. Ponente: Gustavo Calvillo Rangel. Secretario: Jorge Alberto González Álvarez.
Amparo en revisión 135/95. Alfredo Bretón González. 22 de marzo de 1995. Unanimidad de votos. Ponente: Gustavo Calvillo Rangel. Secretario: José Zapata Huesca.
Amparo en revisión 321/95. Guillermo Báez Vargas. 21 de junio de 1995. Unanimidad de votos. Ponente: Gustavo Calvillo Rangel. Secretario: José Zapata Huesca."

"No. Registro: 219,095
**Tesis aislada**
Materia(s): Común
Octava Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación
IX, Junio de 1992
Tesis:
Página: 364

**CONSENTIMIENTO TÁCITO DEL ACTO RECLAMADO EN AMPARO. ELEMENTOS PARA PRESUMIRLO.** Atento a lo dispuesto en el artículo 73, fracción XII, de la Ley de Amparo, el juicio constitucional es improcedente contra actos consentidos tácitamente, reputando como tales los no reclamados dentro de los plazos establecidos en los artículos 21, 22 y 218 de ese ordenamiento, excepto en los casos consignados expresamente en materia de amparo contra leyes. Esta norma jurídica tiene su explicación y su fundamento racional en esta presunción humana: cuando una persona sufre una afectación con un acto de autoridad y tiene la posibilidad legal de impugnar ese acto en el juicio de amparo dentro de un plazo perentorio determinado, y no obstante deja pasar el término sin presentar la demanda, esta conducta en tales circunstancias revela conformidad con el acto. En el ámbito y para los efectos del amparo, el razonamiento contiene los hechos conocidos siguientes: a) Un acto de autoridad; b) Una persona afectada por tal acto;

c) La posibilidad legal para dicha persona de promover el juicio de amparo contra el acto en mención; d) El establecimiento en la ley de un plazo perentorio para el ejercicio de la acción; y e) El transcurso de ese lapso sin haberse presentado la demanda. Todos estos elementos deben concurrir necesariamente para la validez de la presunción, pues la falta de alguno impide la reunión de lo indispensable para estimar el hecho desconocido como una consecuencia lógica y natural de los hechos conocidos. Así, ante la inexistencia del acto de autoridad faltaría el objeto sobre el cual pudiera recaer la acción de consentimiento; si no hubiera una persona afectada faltaría el sujeto de la acción; si la ley no confiere la posibilidad de ocurrir en demanda de la justicia federal, la omisión de tal demanda no puede servir de base para estimar la conformidad del afectado con el acto de autoridad, en tanto no pueda encausar su inconformidad por ese medio; y si la ley no fija un plazo perentorio para deducir la acción de amparo o habiéndolo fijado éste no ha transcurrido, la no presentación de la demanda no puede revelar con certeza y claridad la aquiescencia del acto de autoridad en su contenido y consecuencias, al subsistir la posibilidad de entablar la contienda.

CUARTO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.
Amparo en revisión 358/92. José Fernández Gamiño. 23 de marzo de 1992. Unanimidad de votos. Ponente: Mauro Miguel Reyes Zapata. Secretaria: Aurora Rojas Bonilla.
Amparo en revisión 421/92. Rodolfo Aguirre Medina. 19 de marzo de 1992. Unanimidad de votos. Ponente: Leonel Castillo González. Secretario: J. Jesús Contreras Coria.
Amparo en revisión 704/90. Fernando Carvajal. 11 de octubre de 1990. Unanimidad de votos. Ponente: Leonel Castillo González. Secretario: Jaime Uriel Torres Hernández.
Octava Época, Tomo VI, Segunda Parte-1, página 113."

Una vez admitido a trámite el presente medio de impugnación y notificadas que fueron las partes, en la etapa recursiva, el Sujeto Obligado reiteró los términos de su respuesta inicial y, además ofreció como medio de prueba siete documentales públicas, cuatro documentales, la instrumental de actuaciones y la presuncional en su doble aspecto.

Ahora bien, respecto a las documentales ofertadas por el Sujeto Obligado debe decirse que al ser pruebas documentales se les valora en términos de lo dispuesto por el siguiente criterio emitido por el Poder Judicial de la Federación:

"Novena Época
Instancia: Pleno
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo: III, Abril de 1996
Tesis: P. XLVII/96
Página: 125

**PRUEBAS. SU VALORACIÓN CONFORME A LAS REGLAS DE LA LÓGICA Y DE LA EXPERIENCIA, NO ES VIOLATORIA DEL ARTÍCULO 14**

> **CONSTITUCIONAL (ARTÍCULO 402 DEL CÓDIGO DE PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL).** El Código de Procedimientos Civiles del Distrito Federal, al hablar de la valoración de pruebas, sigue un sistema de libre apreciación en materia de valoración probatoria estableciendo, de manera expresa, en su artículo 402, que los medios de prueba aportados y admitidos serán valorados en su conjunto por el juzgador, atendiendo a las reglas de la lógica y de la experiencia; y si bien es cierto que la garantía de legalidad prevista en el artículo 14 constitucional, preceptúa que las sentencias deben dictarse conforme a la letra de la ley o a su interpretación jurídica, y a falta de ésta se fundarán en los principios generales del derecho, no se viola esta garantía porque el juzgador valore las pruebas que le sean aportadas atendiendo a las reglas de la lógica y de la experiencia, pues el propio precepto procesal le obliga a exponer los fundamentos de la valoración jurídica realizada y de su decisión."

En el caso concreto, se tiene que las **pruebas documentales** ofrecidas por el Sujeto Obligado, se tienen por desahogadas dada su propia y especial naturaleza, toda vez que se trata de **documentales públicas**.

Por lo que hace a las **documentales privadas**, dado que el Sujeto Obligado no las perfeccionó, se les da valor de indicio.

Por lo que hace a la prueba **presuncional en su doble aspecto legal y humano** ofertada por las partes, se trata de la consecuencia lógica y natural de los hechos conocidos, y probados al momento de hacer la deducción respectiva.

Ahora bien, por lo que hace a la **instrumental de actuaciones** ofrecida por las partes, éstas revisten el carácter de documentos públicos que forman parte de las constancias que obran en el expediente en que se actúa, por lo que las exhibidas oportuna y formalmente serán tomadas en consideración al momento de analizar y resolver la *litis* planteada.

Derivado de lo anterior, la presente resolución tendrá por objeto analizar la reserva decretada por parte del **Banco de México**. Lo anterior, de conformidad con lo establecido en la *Ley Federal de Transparencia y Acceso a la Información Pública* y demás disposiciones aplicables.

**TERCERO**. En el presente considerando, se analizará el agravio hecho valer por el hoy recurrente, contra la clasificación decretada por el Sujeto Obligado.

En este sentido, resulta dable recordar que el ahora recurrente solicitó al **Banco de México**, entre otras cosas, y de cada uno de los Modems, Routers (rúters) o Puntos de acceso inalámbricos, lo siguiente:

**a.** Número de serie y de parte.

**c.** Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico.
**d.** Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup).
**e.** Si se encuentra activada la tecnología WIFI.
**f.** Seguridad o cifrado implementado en la conexión WIFI (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc).
**g.** Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico"

En respuesta a la solicitud de acceso, el **Banco de México** a través de la **Dirección General de Tecnologías de la Información** comunicó que la información de los **contenidos de información a), c), d), e), f)** y **g)** es clasificada en términos de lo establecido en el artículo 110 fracciones I y IV de la *Ley Federal de Transparencia y Acceso a la Información Pública*. Lo anterior fue confirmado por el Comité de Transparencia.

Establecido lo anterior y, para un mejor desarrollo de la presente determinación, se llevará a cabo el análisis individual de cada uno de los supuestos de clasificación invocados por el Sujeto Obligado.

- **Análisis de la causal de reserva prevista en la fracción I del artículo 110 de la *Ley Federal de Transparencia y Acceso a la Información Pública*.**

En este sentido, el **Banco de México** manifestó que la divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto.

Así las cosas, para determinar la procedencia de la reserva invocada por el Sujeto Obligado, es menester traer a colación lo establecido en la *Constitución Política de los Estados Unidos Mexicanos*[3], en la *Ley de Seguridad Nacional*[4] y en la *Ley General del Sistema Nacional de Seguridad Pública*[5]; mismas que, en lo que interesa, señalan lo siguiente:

**Constitución Política de los Estados Unidos Mexicanos**

"**Artículo 28...**
El Estado tendrá un banco central que será autónomo en el ejercicio de sus funciones y en su administración. Su objetivo prioritario será procurar la estabilidad del poder adquisitivo de la moneda nacional, fortaleciendo con ello la rectoría del desarrollo nacional que corresponde al Estado. Ninguna autoridad podrá ordenar al banco conceder financiamiento. El Estado contará con un fideicomiso público denominado Fondo Mexicano del Petróleo para la Estabilización y el Desarrollo, cuya Institución Fiduciaria será el banco central y tendrá por objeto, en los términos que establezca la ley, recibir, administrar y distribuir los ingresos derivados de las asignaciones y contratos a que se refiere el párrafo séptimo del artículo 27 de esta Constitución, con excepción de los impuestos.

No constituyen monopolios las funciones que el Estado ejerza de manera exclusiva, a través del banco central en las áreas estratégicas de acuñación de moneda y emisión de billetes. El banco central, en los términos que establezcan las leyes y con la intervención que corresponda a las autoridades competentes, regulará los cambios, así como la intermediación y los servicios financieros, contando con las atribuciones de autoridad necesarias para llevar a cabo dicha regulación y proveer a su observancia. La conducción del banco estará a cargo de personas cuya designación será hecha por el Presidente de la República con la aprobación de la Cámara de Senadores o de la Comisión Permanente, en su caso; desempeñarán su encargo por periodos cuya duración y escalonamiento provean al ejercicio autónomo de sus funciones; sólo podrán ser removidas por causa grave y no podrán tener ningún otro empleo, cargo o comisión, con excepción de aquéllos que actúen en representación del banco y de los no remunerados en asociaciones docentes, científicas, culturales o de beneficencia. Las personas encargadas de la conducción del banco central, podrán ser sujetos de juicio político conforme a lo dispuesto por el artículo 110 de esta Constitución.
..."

**Ley de Seguridad Nacional**

"**Artículo 5.-** Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:
...

[3] Para consulta en http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf
[4] Visible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf
[5] Consultable en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP_260617.pdf

> **XII.** Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.
> ..."

**Ley General del Sistema Nacional de Seguridad Pública**

> "**Artículo 146.-** Para efectos de esta Ley, se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional."

De los ordenamientos legales transcritos es posible advertir que, por mandato constitucional, el Estado tendrá un banco central -denominado **Banco de México**- que será autónomo en el ejercicio de sus funciones, así como, en su administración.

En este orden, el **Banco de México** tiene como objetivo prioritario, procurar la estabilidad del poder adquisitivo de la moneda nacional, fortaleciendo con ello la rectoría del desarrollo nacional que corresponde al Estado.

De igual forma, la Constitución establece que no constituyen monopolios las funciones que el Estado ejerza de manera exclusiva, a través del banco central en las **áreas estratégicas de acuñación de moneda y emisión de billetes**.

Ahora bien, entre las funciones con las que cuenta el **Banco de México**, se encuentra la de **regular los cambios, así como la intermediación y los servicios financieros**, contando con las atribuciones de autoridad necesarias para llevar a cabo dicha regulación y proveer a su observancia.

En este orden de ideas, es claro que el **Banco de México realiza actividades de carácter estratégico**, por lo que la infraestructura necesaria para hacerlo también lo es; por tanto, el Estado promulgó la *Ley de Seguridad Nacional*, misma que prevé las amenazas a la Seguridad Nacional del país, y en donde se establecen los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico.

Por último, de la *Ley General del Sistema Nacional de Seguridad Pública*, se desprende que se consideran como instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la *Constitución Política de los Estados Unidos Mexicanos*.

Establecido lo anterior, toca ahora citar el artículo 110, fracción I, de la *Ley Federal de Transparencia y Acceso a la Información Pública*, mismo que prevé lo siguiente:

> "**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:
>
> **I.** Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
>
> ..."

Por su parte, la *Ley General de Transparencia y Acceso a la Información Pública*, establece lo siguiente:

> "**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:
>
> **I.** Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
>
> ..."

Concatenado con lo anterior, los *Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas*[6], prevén lo siguiente:

> "**Décimo séptimo.** De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando:
>
> ...
>
> **VIII.** Se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, así como la indispensable para la provisión de bienes o servicios públicos de agua potable, de emergencia, vías generales de comunicación o de cualquier tipo de infraestructura que represente tal importancia para el Estado que su destrucción o incapacidad tenga un impacto debilitador en la seguridad nacional;
>
> ..."

De lo anterior, es posible advertir que **la información podrá considerarse clasificada como reservada, cuando la misma comprometa la seguridad nacional** o aquella que al difundirse actualice o potencie un riesgo o amenaza a la seguridad nacional, esto es, **cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario**, así como, la indispensable para la provisión de bienes o servicios públicos de agua potable, de emergencia, vías generales de

[6] Para consulta en http://dof.gob.mx/nota_detalle.php?codigo=5433280&fecha=15/04/2016

comunicación o de cualquier tipo de infraestructura que represente tal importancia para el Estado.

En este sentido, no pasa desapercibido para quien resuelve, que el Sujeto Obligado, a través de su Comité de Transparencia, validó la prueba de daño que sustenta la clasificación de la información en estudio, y la cual ratificó a través de la exposición de sus alegatos, al motivar la reserva de la información, **desarrollando la prueba de daño, tal como lo establece el artículo 104, de la *Ley en la Materia***, estableciendo con ello, la afectación que causaría a la seguridad nacional, la entrega y publicidad de la información requerida; argumentos que se traen a colación y los cuales versan en los siguientes términos:

**1) Real**, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales a realizar acciones hostiles en contra de las tecnologías de la información de este Banco Central.

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la *Constitución Política de los Estados Unidos Mexicanos*, el **Banco de México** tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los artículos 20 y 30 de la *Ley del Banco de México*, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el **Banco de México** ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de esos procesos.

Al respecto, es importante destacar que los sistemas informáticos y de comunicaciones del **Banco de México** fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero, por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

En este sentido, el artículo 5, fracción XII, de la *Ley de Seguridad Nacional* establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la *Ley General del Sistema Nacional de Seguridad Pública* dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra la **infraestructura de tecnologías de la información y comunicaciones** del **Banco de México**.

Asimismo, el artículo 17, fracción VIII, de la citada legislación, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Consecuentemente, pretender atacar o inhabilitar los sistemas del Banco, representa una amenaza a la seguridad nacional, ya que publicar la información que se solicita, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del **Banco de México**, Banco Central del Estado México, por mandato constitucional.

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del **Banco de México**.

**2) Demostrable**, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo.

Expertos en el tema de seguridad, como Offensive Security consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red? (cuyas especificaciones de fabricación, y por consiguiente posibles vulnerabilidades se pueden obtener indirectamente a través de sus números de serie accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group"), ¿qué puertos de comunicaciones usan? (Si se encuentran abiertos o inactivos), ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por otro lado, el uso de la tecnología "WiFi", que permite la interconexión inalámbrica de dispositivos electrónicos (computadoras, teléfonos, etcétera), ya sea entre ellos o hacia Internet, puede implicar riesgos importantes, ya que sin los adecuados mecanismos de seguridad, terceros pueden acceder a estas redes sin autorización, con la posibilidad de acceder y controlar los dispositivos "WiFi", tales como los ruteadores (o "routers" en inglés) encargados de encaminar los datos trasmitidos entre diferentes redes o subconjuntos de dispositivos, con tan solo conocer su identificador en la red. Por otro lado, el acceso no autorizado a un dispositivo "WiFi" permite supervisar y registrar toda la información que se trasmite a través de éste.

Dentro del uso de redes inalámbricas, el estándar "WPS" (WiFi Protected Setup) define diversos mecanismos para configurar una red local inalámbrica apoyados en el sistema de seguridad conocido como "WPA2" (WiFi Protected Access 2 - Acceso Protegido WiFi 2). El conocer los mecanismos de protección utilizados también permitiría a un atacante identificar las vulnerabilidades asociadas a éstos.

Por tanto, el dar a conocer la unidad, área u órgano del **Banco de México** que hace uso de cada uno de ruteadores y puntos de acceso inalámbricos, facilitaría direccionar a algún área funcional que sea del interés del atacante cibernético materializar los riesgos recién señalados.

En resumen, de la misma manera que el resto de las especificaciones de tecnologías de la información y telecomunicaciones, el conocimiento de las tecnologías utilizadas para la comunicación inalámbrica y sus mecanismos de seguridad y cifrado tales como el estándar WPS, y por obvias razones, el uso de contraseñas para acceder a los dispositivos WiFi, tales como los ruteadores y puntos de acceso inalámbricos, así como las unidades administrativas que

hacen uso de esta tecnología, permitiría a un atacante identificar y aprovechar vulnerabilidades asociadas a ellas.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central, impidiéndole cumplir sus funciones establecidas en la *Ley del Banco de México*, así como aquello que le fue conferido por mandato constitucional.

**3) Identificable**, puesto que el **Banco de México** se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el **Banco de México** es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**; facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

**El riesgo de perjuicio que supondria la divulgación de la información solicitada, supera el interés público general de que se difunda**, ya que el Interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero; económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

En consecuencia, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** contenida en los documentos que se clasifican, no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían muy probablemente implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. Con ello,

se imposibilitaría al Banco de México cumplir con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 26, párrafo sexto de la Constitución.

En efecto, **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad; el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

Por lo anterior, el revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

En consecuencia, este Instituto advierte que el sujeto obligado argumenta que el proporcionar la información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones que fue solicitada por el particular, representa un riesgo real, demostrable e identificable para el Estado, pues se estarían dando elementos cuya suma, facilitan la vulnerabilidad de sus actividades estratégicas, encomendadas constitucionalmente, relacionadas con la acuñación de moneda y emisión de billetes.

Asimismo, destaca que el riesgo de perjuicio que se supondría la divulgación, supera el interés público general de que se difunda, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, lo cual precisa de la conservación de la infraestructura de carácter estratégico y prioritario, y supera el interés público para conocerse, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, prevalece la protección de las funciones del **Banco de México** con carácter estratégico, que por mandato constitucional tiene.

Asimismo, durante la etapa recursiva el **Banco de México** agregó lo siguiente:

El riesgo es real, dado que la difusión de la información referida haría posible que personas o grupos de ellas, con intenciones delictivas, llevaran a cabo acciones hostiles en contra de las tecnologías de la información de este Banco Central utilizadas, entre otras funciones, para cumplir la relacionada con el

objetivo prioritario de proveer de moneda nacional a la economía del país, y en consecuencia afectarán un área estratégica del Estado mexicano.

El riesgo referido es además demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como lo es la relacionada con la finalidad de proveer de moneda nacional a la economía del país.

El riesgo también es identificable, pues el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Al respecto, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

En vista de lo anterior, se estima que la publicidad de la información solicitada, facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México; lo cual se traduce efectivamente, en una vulnerabilidad latente de la infraestructura estratégica.

En consecuencia, la protección de la información solicitada, sí permite disminuir las probabilidades de ataques a la infraestructura estratégica del sujeto obligado, y coadyuva a mantener la seguridad en los sistemas que se administran en el Banco de México para el sano desarrollo de la economía.

Por los motivos expuestos, se advierte que con la divulgación de la información clasificada por el sujeto obligado, sí se posibilita la destrucción, inhabilitación o sabotaje de su infraestructura de carácter estratégico por mandato constitucional, lo cual permite concluir que en la especie, se actualiza la causal de reserva prevista en la fracción I del artículo 110 de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

- **Análisis de la causal de reserva prevista en la fracción IV del artículo 110 de la *Ley Federal de Transparencia y Acceso a la Información Pública*.**

En ese contexto normativo, el artículo 110, fracción IV de la *Ley Federal de Transparencia y Acceso a la Información Pública*, prevé lo siguiente:

"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

...

**IV.** Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;

..."

Por su parte, los *Lineamientos Generales* prevén lo siguiente:

"**Vigésimo Segundo.** Podrá clasificarse la información como reservada con fundamento en lo previsto en el artículo 113, fracción IV de la Ley General, cuando se acredite un vínculo entre su difusión y alguno de los siguientes supuestos:

I. Se menoscabe la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto;
II. Se comprometan las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos;

..."

En esta tesitura, se trae a colación la iniciativa que contenía el proyecto de decreto por el que se expediría la *Ley General de Transparencia y Acceso a la Información Pública*, para conocer las referencias mencionadas en la Ley de la materia vigente; sobre la causal de clasificación invocada, la cual dispone lo siguiente:

"...

**Reserva financiera, económica y monetaria**

Actualmente, la fracción III del artículo 13 de la actual Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, establece que aquella información cuya **difusión pueda dañar la estabilidad financiera, económica o monetaria del país**, podrá clasificarse como reservada; por ello, en congruencia a lo anterior, es necesario analizar y ponderar la inclusión también de la estabilidad financiera y económica, además de la monetaria, como mecanismos para proteger el interés público y la seguridad nacional del Estado, en cumplimiento a lo dispuesto por la fracción I del apartado A del artículo 6° Constitucional.

> La Ley Modelo de Acceso a la Información Administrativa de la Organización de los Estados Americanos (OEA), señala en la fracción III y IV de artículo 7 que una solicitud de información puede ser rechazada cuando pueda afectar intereses públicos preponderantes; cuando se trate de información que pudiera afectar el funcionamiento del sistema bancario o financiero; así como cuando se trate información cuya revelación pueda causar perjuicios económicos.
>
> Asimismo, la Ley Modelo Interamericana sobre Acceso a la Información también de la OEA, dispone en su numeral 41 que las autoridades públicas **pueden rechazar el acceso a la información** cuando el acceso genere un riesgo claro, probable y específico de un daño significativo, a la habilidad del Estado para manejar la economía y a legítimos intereses financieros de la autoridad pública, en razón de que se trata de intereses públicos.
>
> Por otra parte, los países con las mayores calificaciones de transparencia, de acuerdo con la Encuesta de Presupuesto Abierto 2012, publicada por el International Budget Partnership, reconocen en su legislación que información en materia financiera, económica y monetaria que debe ser reservada; por ejemplo: Nueva Zelandia, Sudáfrica, Reino Unido, Suecia, Noruega, Francia, Estados Unidos, Corea del Sur, República Checa, Rusia, Eslovenia, Brasil y Alemania.
>
> Ahora bien para estas Comisiones Dictaminadoras, **revelar la información en materia de política monetaria y cambiaria** podría ocasionar reacciones prematuras en inversionistas o agentes económicos que podrían derivar en serias afectaciones a la economía, incluso irreversibles, **en caso que la información se revele de manera inoportuna**. Asimismo, de revelar información sobre administración de reservas de activos internacionales, las instituciones y agentes financieros que ofrezcan los instrumentos de inversión respectivos podrían tomar ventaja de dicha información, ante lo cual se podrían elevar los costos de transacción para el Banco Central o reducir las oportunidades de inversión de dichos activos.
> ..."

Si bien la transcripción anterior se refiere a la iniciativa del decreto de la *Ley General de Transparencia y Acceso a la Información Pública*, lo cierto es que tanto en ésta, como en la *Ley Federal de Transparencia y Acceso a la Información Pública* se contiene la misma causal de clasificación.

En ese sentido, en el decreto se establece que en la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* se incluía una reserva financiera, económica y monetaria, por lo que era necesario analizar si en la nueva ley de la materia debía incluirse una causal de clasificación de la información como la anteriormente existente para que se contemplaran, como mecanismos para proteger el interés público y la seguridad nacional del Estado, en cumplimiento a lo dispuesto por la fracción I del apartado A del artículo 6 de la *Constitución Política de los Estados Unidos Mexicanos*.

Al respecto, se concluyó que la **Información en materia de política monetaria y cambiaria** podría ocasionar reacciones prematuras en inversionistas o agentes económicos que podrían derivar en serias afectaciones a la economía, incluso irreversibles, **en caso que la información se revelara de manera inoportuna**.

Asimismo, se estableció que de revelarse **información sobre administración de reservas de activos internacionales**, **las instituciones** y agentes financieros que ofrezcan los instrumentos de inversión respectivos **podrían tomar ventaja de dicha información**, ante lo cual **se podrían elevar los costos de transacción para el Banco Central o reducir las oportunidades de inversión de dichos activos**.

Bajo los argumentos previos **se hizo necesario incluir en la Ley de Transparencia la clasificación de información financiera económica y monetaria, que en la *Ley Federal de Transparencia y Acceso a la Información Pública* se contiene en el artículo 110, fracción IV.**

Dicho lo previo, se puede colegir que los términos contenidos en el artículo 110, fracción IV de la *Ley de la Materia* se encuentran encaminados a **salvaguardar la política monetaria, que pueda afectar las medidas adoptadas en relación con los diferentes intermediarios y mercados financieros, o que ponga en riesgo la estabilidad de los controladores de riesgo y liquidez**.

Además, que debe menoscabarse la efectividad de las medidas implementadas en los sistemas financieros; comprometerse las acciones encaminadas a proveer a la economía del país de moneda nacional; se otorgue una ventaja indebida, generando distorsiones en la estabilidad de los mercados, o generarse incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan.

De tales circunstancias, los requisitos que se deben cumplir, de conformidad con los *Lineamientos Generales*, corresponden a **aspectos monetarios, económicos, de mercados financieros o de sistemas de pagos.**

Ahora bien, debe puntualizarse que la causal en estudio plantea **términos económicos** como: **sistema financiero**, **instituciones financieras**, **sistemas de pagos, política cambiaria y política monetaria.**

Luego entonces, resulta necesario analizar dichos términos, con el objeto de dilucidar los elementos que permiten a los sujetos obligados clasificar bajo la presente causal de reserva.

Al respecto, y en relación con el término **sistema financiero**, en el portal de internet del **Banco de México** se menciona que desempeña un papel central en el funcionamiento y desarrollo de la economía. Está integrado principalmente por diferentes intermediarios y mercados financieros, a través de los cuales una variedad de instrumentos moviliza el ahorro hacia sus usos más productivos. Los bancos son quizá los intermediarios financieros más conocidos, puesto que ofrecen directamente sus servicios al público y forman parte medular del sistema de pagos. Sin embargo, en el sistema financiero participan muchos otros intermediarios y organizaciones que ofrecen servicios de gran utilidad para la sociedad.[7]

Con relación a las **instituciones financieras**, en el mismo portal se señala que son las que controlan los riesgos de crédito y de liquidez evaluando la capacidad y disposición de pago de los posibles usuarios de financiamiento, creando reservas para enfrentar contingencias, incrementando constantemente el número de depositantes, y compaginando los montos y plazos de los créditos a otorgar con la disponibilidad de recursos.[8]

Por lo que hace a los **sistemas de pagos**, el **Banco de México** señala que están constituidos por un conjunto de instrumentos, procedimientos y normas para transferir recursos financieros entre sus participantes. Dichos sistemas son indispensables para que el sistema financiero funcione eficientemente. Algunos de ellos son especialmente críticos ya que, si su diseño no es adecuado, pueden magnificar la transmisión de problemas de liquidez de un participante a los demás y perturbar la estabilidad del sistema financiero. Por estas razones, uno de los objetivos del **Banco de México** es propiciar el buen funcionamiento de los sistemas de pago del país.[9]

En relación con la **Política cambiaria en México**, el **Banco de México** establece que es responsabilidad de la Comisión de Cambios, la cual está integrada por funcionarios tanto de la Secretaría de Hacienda y Crédito Público como del Banco de México. La Comisión puede reunirse, en todo momento, a solicitud del Secretario de Hacienda y Crédito Público o del Gobernador del Banco de México. Las resoluciones de la Comisión se toman por mayoría de votos, siendo necesario el voto favorable de por lo menos uno de los representantes de la Secretaría de Hacienda.

[7] http://www.banxico.org.mx/divulgacion/sistema-financiero/sistema-financiero.html.
[8] Idem.
[9] Idem.

A finales de 1994, la Comisión de Cambios acordó que el régimen cambiario en México fuera flexible. El tipo de cambio flexible se determina libremente y obedeciendo únicamente a las fuerzas del mercado.[10]

La **Política Monetaria** es el conjunto de acciones que el Banco de México lleva a cabo para influir sobre las tasas de interés y las expectativas inflacionarias del público, a fin de que la evolución de los precios sea congruente con el objetivo de mantener un entorno de inflación baja y estable. Al procurar el objetivo de mantener un entorno de inflación baja y estable, el **Banco de México** contribuye a establecer condiciones propicias para el crecimiento económico sostenido y, por lo tanto, para la creación de empleos permanentes[11].

Ahora bien, con la finalidad de correlacionar los aspectos normativos antes precisados, con las actividades que realiza el **Banco de México** y con ello, poder determinar si se actualiza la causal de reserva en estudio, resulta importante precisar que la Ley del Banco de México en su artículo 2 establece que el sujeto obligado tendrá por **finalidad proveer a la economía del país de moneda nacional**. En la consecución de esta finalidad tendrá como **objetivo** prioritario **procurar la estabilidad del poder adquisitivo** de dicha moneda. Serán también **finalidades** del Banco **promover** el sano **desarrollo** del **sistema financiero** y propiciar el buen funcionamiento de **los sistemas de pagos**.

Por su parte, el artículo 3 de la ley en comento, establece el catálogo de las funciones a cargo del **Banco de México**, tales como:

> **I.** Regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos;
> **II.** Operar con las instituciones de crédito como banco de reserva y acreditante de última instancia;
> **III.** Prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo;
> **IV.** Fungir como asesor del Gobierno Federal en materia económica y, particularmente, financiera;
> **V.** Participar en el Fondo Monetario Internacional y en otros organismos de cooperación financiera internacional o que agrupen a bancos centrales, y
> **VI.** Operar con los organismos a que se refiere la fracción V anterior, con bancos centrales y con otras personas morales extranjeras que ejerzan funciones de autoridad en materia financiera.

[10] Idem
[11] http://www.banxico.org.mx/politica-monetaria-e-inflacion/

El artículo 4 del citado ordenamiento establece que corresponderá privativamente al **Banco de México** emitir billetes y ordenar la acuñación de moneda metálica, así como poner ambos signos en circulación a través de las operaciones que esta Ley le autoriza realizar.

Los actos que está facultado a realizar el Banco de México, en términos del artículo 7 de la ley, corresponden a:

**I.** Operar con valores;
**II.-** Otorgar crédito al Gobierno Federal, a las instituciones de crédito, así como al organismo descentralizado denominado Instituto para la Protección al Ahorro Bancario;
**III.** Otorgar crédito a las personas a que se refiere la fracción VI del artículo 3o.;
**IV.** Constituir depósitos en instituciones de crédito o depositarias de valores, del país o del extranjero;
**V.** Adquirir valores emitidos por organismos financieros internacionales o personas morales domiciliadas en el exterior, de los previstos en la fracción II del artículo 20;
**VI.** Emitir bonos de regulación monetaria;
**VII.** Recibir depósitos bancarios de dinero del Gobierno Federal, de entidades financieras del país y del exterior, de fideicomisos públicos de fomento económico y de los referidos en la fracción XI siguiente, de instituciones para el depósito de valores, así como de entidades de la administración pública federal cuando las leyes así lo dispongan;
**VIII.** Recibir depósitos bancarios de dinero de las personas a que se refiere la fracción VI del artículo 3o.;
**IX.** Obtener créditos de las personas a que se refiere la fracción VI del artículo 3o. y de entidades financieras del exterior, exclusivamente con propósitos de regulación cambiaria; así como constituir cauciones en efectivo o con valores respecto de las operaciones financieras que celebre con dichos sujetos conforme a la presente Ley, derivadas de la administración de la reserva de activos internacionales;
**X.** Efectuar operaciones con divisas, oro y plata, incluyendo reportos;
**XI.** Actuar como fiduciario cuando por ley se le asigne esa encomienda, o bien tratándose de fideicomisos cuyos fines coadyuven al desempeño de sus funciones o de los que el propio Banco constituya para cumplir obligaciones laborales a su cargo, y
**XII.** Recibir depósitos de títulos o valores, en custodia o en administración, de las personas señaladas en las fracciones VII y VIII anteriores. También podrá recibir depósitos de otros efectos del Gobierno Federal.

El artículo 12 de la ley establece que el sujeto obligado será el responsable de llevar una cuenta corriente a la Tesorería de la Federación, ciñendo su actuar a realizar cargos o abonos a esta cuenta mediante instrucción directa del Tesorero y a cargar la cuenta para atender el servicio de la deuda interna del Gobierno Federal.

El artículo 14 establece que el **Banco de México** realiza operaciones con las instituciones de crédito, y otorga financiamientos, mediante el otorgamiento de crédito o a través de la adquisición de valores, que sólo podrán tener por finalidad la regulación monetaria; así, de acuerdo con el artículo 17, los bonos de regulación monetaria que emita el **Banco de México**, serán títulos de crédito nominativos o al portador y tendrán las demás características que el Banco fije, debiendo mantenerse depositados en administración en el propio Banco, cuando éste así lo determine.

Por su parte, el artículo 15 establece que el **Banco de México** contará con una reserva de activos internacionales, que tendrá por objeto coadyuvar a la estabilidad del poder adquisitivo de la moneda nacional mediante la compensación de desequilibrios entre los ingresos y egresos de divisas del país; que de conformidad con el artículo 20, las divisas consisten en billetes y monedas metálicas extranjeros, depósitos bancarios, títulos de crédito y toda clase de documentos de crédito, sobre el exterior y denominados en moneda extranjera, así como, en general, los medios internacionales de pago.

Asimismo, el artículo 24 de la ley en alusión, establece que el **Banco de México** podrá expedir disposiciones en términos de la presente Ley, solamente cuando tengan por propósito la regulación monetaria o cambiaria, el sano desarrollo del sistema financiero, el buen funcionamiento del sistema de pagos, o bien, la protección de los intereses del público; esto sin perjuicio de las demás disposiciones que los preceptos de otras leyes faculten al Banco a expedir en las materias ahí señaladas. Al expedir sus disposiciones, el Banco deberá expresar las razones que las motivan.

En síntesis, es dable afirmar que las funciones del sujeto obligado se pueden englobar en la acuñación de moneda y emisión de billetes, así como regular su emisión; regular los cambios, intermediación, servicios financieros, sistemas de pago; fungir como banco se reserva y acreditante de última instancia, prestar servicios de tesorería al Gobierno Federal, y fungir como asesor del Gobierno Federal en materia económica y financiera.

Además, se encarga de operar con valores; otorgar créditos al Gobierno Federal, a las instituciones de crédito, así como al organismo descentralizado

denominado Instituto para la Protección al Ahorro Bancario y a otros; constituir depósitos en instituciones de crédito o depositarias de valores; adquirir valores emitidos por organismos financieros internacionales o personas morales; emitir bonos de regulación monetaria; recibir depósitos bancarios de dinero del Gobierno Federal; efectuar operaciones con divisas, oro y plata, incluyendo reportos; recibir depósitos de títulos o valores, en custodia o en administración, entre otros.

Este cúmulo de funciones, se pueden englobar como funciones encaminadas a la consecución de sus objetivos, consistentes en proveer a la economía del país de moneda nacional, así como procurar la estabilidad del poder adquisitivo de dicha moneda y promover el sano desarrollo del sistema financiero y de los sistemas de pagos.

Luego entonces, en primer lugar es dable afirmar que el sujeto obligado sí realiza funciones a partir de las cuales genera información susceptible de clasificación bajo la causal en alusión, por lo que su divulgación puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país, además de que las funciones sustantivas del Banco de México, también se encaminan a:

- Implementar la **Política Monetaria** del país, mediante acciones que permitan mantener una inflación baja y estable, necesarios para el crecimiento económico sostenido del país.

- Forma parte de la Comisión de Cambios, la cual establece la **Política cambiaria en México**, y actúa en atención a las directrices que esta comisión emite.

- Su objetivo principal es mantener estable el **Sistema Financiero** del país, por lo que cuenta con facultades de supervisión a los intermediarios financieros, y de imposición de sanciones por incumplimiento a las disposiciones normativas que regulan al sistema en comento.

Una vez precisado lo anterior, conviene aludir a las manifestaciones que el sujeto obligado realizó mediante la prueba de daño entregada en respuesta inicial, mismas que se presentan a continuación:

Es un riesgo **real**, pues los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras,

aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas.

Estos ataques se fundamentan en:

> (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y
>
> (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez éstos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 20 de la *Ley del Banco de México*.

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad; la substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales; la corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los, sistemas de pagos.

Por lo anterior, mantener la reserva de las especificaciones de la infraestructura de tecnologías de la información y comunicaciones, que soportan en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de las especificaciones de la infraestructura de tecnologías de la información y comunicaciones.

El riesgo es **demostrable**, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo.

Expertos en el tema de seguridad, como Offensive Security consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red? (cuyas especificaciones de fabricación, y por consiguiente posibles vulnerabilidades se pueden obtener indirectamente a través de sus números de serie accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group"), ¿qué puertos de comunicaciones usan? (Si se encuentran abiertos o inactivos), ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta

tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por otro lado, el uso de la tecnología "WiFi", que permite la interconexión inalámbrica de dispositivos electrónicos (computadoras, teléfonos, etcétera), ya sea entre ellos o hacia Internet, puede implicar riesgos importantes, ya que sin los adecuados mecanismos de seguridad, terceros pueden acceder a estas redes sin autorización, con la posibilidad de acceder y controlar los dispositivos "WiFi", tales como los ruteadores (o "routers" en inglés) encargados de encaminar los datos trasmitidos entre diferentes redes o subconjuntos de dispositivos, con tan solo conocer su identificador en la red. Por otro lado, el acceso no autorizado a un dispositivo "WiFi" permite supervisar y registrar toda la información que se trasmite a través de éste.

Dentro del uso de redes inalámbricas, el estándar "WPS" (WiFi Protected Setup) define diversos mecanismos para configurar una red local inalámbrica apoyados en el sistema de seguridad conocido como "WPA2" (WiFi Protected Access 2 - Acceso Protegido WiFi 2). El conocer los mecanismos de protección utilizados también permitiría a un atacante identificar las vulnerabilidades asociadas a éstos.

Por tanto, el dar a conocer la unidad, área u órgano del **Banco de México** que hace uso de cada uno de ruteadores y puntos de acceso inalámbricos, facilitaría direccionar a algún área funcional que sea del interés del atacante cibernético materializar los riesgos recién señalados.

En resumen, de la misma manera que el resto de las especificaciones de tecnologías de la información y telecomunicaciones, el conocimiento de las tecnologías utilizadas para la comunicación inalámbrica y sus mecanismos de seguridad y cifrado tales como el estándar WPS, y por obvias razones, el uso de contraseñas para acceder a los dispositivos WiFi, tales como los ruteadores y puntos de acceso inalámbricos, así como las unidades administrativas que hacen uso de esta tecnología, permitiría a un atacante identificar y aprovechar vulnerabilidades asociadas a ellas.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central,

impidiéndole cumplir sus funciones establecidas en la *Ley del Banco de México*, así como aquello que le fue conferido por mandato constitucional.

El riesgo es **identificable**, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre ellos el Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**; facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

Con base en lo anterior y, concatenando con las funciones que realiza el Sujeto Obligado, es dable afirmar que éstas se realizan mediante la infraestructura tecnológica con la que cuenta, misma que fue clasificada.

Así, el daño que generaría la divulgación de la información, puede sustentarse en el hecho de que esta permite abrir espacios de vulnerabilidad a sus sistemas informáticos a través de los cuales realiza las funciones encomendadas constitucionalmente y a través de la *Ley del Banco de México*, pues, tal como lo manifestó el sujeto obligado, tales funciones están sujetas a la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos.

Es por ello, que la divulgación de la información generaría un menoscabo en la implementación de las determinaciones adoptadas en relación con los sistemas financiero, cambiario y monetario del país, pues una intromisión que derive en la obtención de datos relacionados con las decisiones del Sujeto Obligado, podría cambiar el rumbo de la toma de decisiones en cuanto a las políticas que se pretendieran adoptar, toda vez que debe recordarse, los sistemas informáticos y de comunicaciones del **Banco de México** fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero, por lo que, en caso de que las mismas no puedan implementarse, a causa de intromisiones en los instrumentos que sirven para tal efecto, es claro que se generaría un detrimento en su implementación.

Además, proporcionar la información solicitada, también facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

Debe tenerse en cuenta, que derivado de la naturaleza del Sujeto Obligado, y con motivo de las funciones que desempeña, no es una suposición el hecho de que sea blanco de ataques, pues tal como lo precisó el sujeto obligado, los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas.

En el caso en específico, el Sujeto Obligado ha registrado durante 2016 y 2017, un promedio de **700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.**

Así, la divulgación de la información solicitada, facilita por un lado, que se adviertan y aprovechen vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y con ello, se tome ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

La materialización de dichas actividades, puede conllevar a una afectación real en:

- La interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad;
- La substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas del país y de otros participantes internacionales;
- La corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

De manera adicional, la divulgación de la información solicitada, también puede implicar afectaciones que comprometan las acciones encaminadas a proveer a la economía del país de moneda nacional, pues debe recordarse que por mandato constitucional el sujeto obligado realiza las actividades estratégicas de acuñación de monedas y emisión de billetes.

Al respecto, y de una revisión al portal electrónico del sujeto obligado[12], se desprende que los billetes mexicanos se fabrican en la Fábrica de Billetes de Banco de México. El Banco también ordena la acuñación de las monedas mexicanas a la Casa de Moneda de México y pone a ambos en circulación por todo el territorio nacional.

En dicho portal también se precisa que para iniciar el proceso de fabricación, se debe conocer con anticipación la cantidad de billetes y monedas. Para ello, el **Banco de México** toma en cuenta las denominaciones que se requieren en todo

[12] http://www.banxico.org.mx/divulgacion/billetes-y-monedas/participacion-del-banco-mexic.html

el país, la cantidad de billetes y monedas que el público prefiere usar en lugar de otros medios de pago (cheques, tarjetas de débito, etc.), los costos de fabricación, y la cantidad de billetes que deben ser reemplazados. En el caso de las monedas, también resulta importante considerar el costo de los metales que se utilizan.

La información sobre la cantidad de billetes y monedas que se pondrán a circular cada año, se dá a conocer oportunamente tanto a la Fábrica de Billetes del Banco de México como a la Casa de Moneda de México para que programen sus actividades.

Finalmente, se precisa que el **Banco de México** distribuye los billetes y monedas a lo largo del país a través de oficinas propias y de algunos bancos comerciales. De igual forma, el retiro de los billetes y monedas de la circulación se realiza bajo el mismo esquema, con dicho retiro, se cierra su ciclo de vida.

En este sentido, es claro que la información solicitada, configura la infraestructura tecnológica del sujeto obligado que funge como herramienta para la implementación de acciones relativas al diseño de billetes, al manejo de insumos para su fabricación y manufactura, así como a los actos correspondientes al traslado y custodia de efectivo, valores y metales preciosos, y al almacenamiento, abastecimiento, canje, retiro, reproducción, destrucción y entrega de signos monetarios, por lo que su protección permite evitar intromisiones en el buen curso de la provisión de moneda en el país, y evita que se dañe la estabilidad del poder adquisitivo de dicha moneda.

Por todo lo anterior, es de concluir que la información solicitada por el ahora recurrente debe clasificarse como información reservada con fundamento en la fracción IV del artículo 110 de la *Ley Federal de Transparencia y Acceso a la Información Pública*, toda vez que su divulgación sí puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país, así como comprometer la seguridad en la provisión de moneda nacional al país.

Por otra parte, el artículo 99 de la *Ley Federal de Transparencia y Acceso a la Información Pública*, así como el Trigésimo Cuarto de los *Lineamientos Generales*, establecen que la información clasificada podrá permanecer con tal carácter, hasta por un **periodo de cinco años**, y que tal información podrá ser desclasificada: **a)** cuando se extingan las causas que dieron origen a su clasificación; **b)** cuando expire el plazo de clasificación; **c)** cuando exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información; **d)** cuando el

Comité de Transparencia considere pertinente la desclasificación de conformidad con el Título cuarto del mismo ordenamiento, o **e)** cuando se trate de información que esté relacionada con violaciones graves a derechos humanos o delitos de lesa humanidad.

De esta manera, el sujeto obligado a través de la sesión celebrada el dieciséis de mayo de dos mil dieciocho, emitió la resolución mediante la cual su Comité de Transparencia confirmó la clasificación de la información, con fundamento en las fracciones I y IV del artículo 110 de la *Ley Federal de Transparencia y Acceso a la Información Pública*, por un plazo de reserva **5 años**, el cual se considera adecuado, misma que fue notificada al solicitante, dado que, se estima que es el tiempo que el equipo de cómputo del sujeto obligado tiene como vida útil.

En virtud de lo anterior, el agravio del particular relativo a la clasificación de la información es **INFUNDADO**, ya que resultó procedente la reserva invocada por el Sujeto Obligado.

En virtud de lo anterior, con fundamento en el artículo 157, fracción II de la *Ley Federal de Transparencia y Acceso a la Información Pública*, este Instituto considera procedente **CONFIRMAR** la respuesta emitida por el **Banco de México**.

Finalmente, en los mismos términos se resolvió el recurso de revisión **RRA 3634/18**, de la ponencia del Comisionado Carlos Alberto Bonnin Erales, mismo que se votó por mayoría el 15 de agosto de 2018.

Por lo expuesto y fundado, el Pleno de este Instituto:

## R E S U E L V E

**PRIMERO.-** Con fundamento en lo que establece el artículo 157, fracción II de la *Ley Federal de Transparencia y Acceso a la Información Pública*, se **CONFIRMA** la respuesta emitida por el Sujeto Obligado, en los términos de los considerandos de la presente resolución.

**SEGUNDO.-** Con fundamento en el artículo 159 de la *Ley Federal de Transparencia y Acceso a la Información Pública*, notifíquese la presente resolución al recurrente en la dirección señalada para tales efectos, y a través

de la Plataforma Nacional de Transparencia, al Comité de Transparencia del Sujeto Obligado, a través de su Unidad de Transparencia.

**TERCERO.-** Se hace del conocimiento del hoy recurrente que, en caso de encontrarse insatisfecho con la presente resolución, le asiste el derecho de impugnarla ante el Poder Judicial de la Federación, con fundamento en lo previsto en el primer párrafo del artículo 158 de la *Ley General de Transparencia y Acceso a la Información Pública* y 165 de la *Ley Federal de Transparencia y Acceso a la Información Pública*.

**CUARTO.-** Háganse las anotaciones correspondientes en los registros respectivos.

Así, lo resolvieron por mayoría y firman, los Comisionados del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Francisco Javier Acuña Llamas, Carlos Alberto Bonnin Erales, Blanca Lilia Ibarra Cadena, María Patricia Kurczyn Villalobos, Rosendoevgueni Monterrey Chepov y Joel Salas Suárez con voto disidente, siendo ponente el primero de los mencionados, en sesión celebrada el 09 de octubre de 2018, ante Hugo Alejandro Córdova Díaz, Secretario Técnico del Pleno.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

**Sujeto Obligado ante el cual se presentó la solicitud:** Banco de México
**Folio de la solicitud:** 6110000027618
**Número de expediente:** RRA 4770/18
**Comisionado Ponente:** Francisco Javier Acuña Llamas

**Francisco Javier Acuña Llamas**
Comisionado Presidente

**Carlos Alberto Bonnin Erales**
Comisionado

**Blanca Lilia Ibarra Cadena**
Comisionada

**María Patricia Kurczyn Villalobos**
Comisionada

**Rosendoevgueni Monterrey Chepov**
Comisionado

**Joel Salas Suárez**
Comisionado

**Hugo Alejandro Córdova Díaz**
Secretario Técnico del Pleno

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

**Sujeto obligado**: Banco de México
**Folio de la solicitud:** 6110000027618
**Expediente:** RRA 4770/18
**Comisionado Ponente:** Francisco Javier Acuña Llamas

**Voto disidente del Comisionado Joel Salas Suárez, elaborado con fundamento en el artículo 18, fracciones XII y XV del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, respecto de la resolución del recurso de revisión número RRA 4770/18, interpuesto en contra del Banco de México, votado en la sesión plenaria de fecha 09 de octubre de 2018.**

En relación con el presente recurso de revisión, la mayoría de mis colegas integrantes del Pleno de este Instituto, determinaron procedente CONFIRMAR la respuesta del Banco de México.

Sin embargo, emito el presente voto disidente, ya que no estoy de acuerdo con **las causales de reserva analizadas para la clasificación de los datos, consistentes en número de serie y de parte; si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico; si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup); si se encuentra activada la tecnología WIFI; seguridad o cifrado implementado en la conexión WIFI (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc); conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico.**

Lo anterior, en **virtud de que se analizaron las fracciones I y IV del artículo 110** de la Ley Federal de Transparencia y Acceso a la Información Pública para reservar dichos datos, siendo que, desde mi perspectiva, para el caso de mérito, **se tuvo que haber reservado dicha información únicamente en términos de la fracción VII del artículo 110** de dicho ordenamiento.

A efecto de explicar lo anterior, resulta conveniente recordar que los términos contenidos en el artículo 110, fracción I de la Ley de la materia se encuentran encaminados a salvaguardar aquella información que comprometa la seguridad nacional, la seguridad pública o la defensa nacional, cuando se obstaculicen o bloqueen las actividades de inteligencia o contrainteligencia y cuando se revelen normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional; así como cuando se ponga en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público.

En ese tenor, en el asunto concreto, el Banco de México, indicó que proporcionar los datos requeridos por el particular implicaría revelar información que podría ser

aprovechada para vulnerar instalaciones estratégicas y pretender atacar o inhabilitar los sistemas del sujeto obligado, lo que representa una amenaza a la seguridad nacional, ya que se posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico.

No obstante, el Banco de México, no identificó y precisó, por cada uno de los datos reservados, el riesgo que generaría su divulgación de conformidad con la fracción I del artículo 110 de la Ley referida. En virtud de lo anterior, no se estima de qué forma dar a conocer los datos relativos de interés del particular pudiera quebrantar la unidad de la Federación, poner en riesgo la gobernabilidad democrática, la generación y actividades de inteligencia para la seguridad nacional, intervenir en las acciones para evitar la interferencia extranjera, dificultar las estrategias o acciones para combatir la delincuencia organizada en la comisión de los delitos contra la seguridad de la nación, se bloqueen acciones tendientes a prevenir o combatir epidemias o enfermedades exóticas, se difundan las actas o documentos generados en las sesiones del Consejo de Seguridad Nacional, se entreguen datos con información de actividades autorizadas por resolución judicial o de intervención a comunicaciones privadas.

Así pues, se puede concluir que **los datos reservados por el sujeto obligado es información que no está relacionada con acciones encaminadas a actualizar o potencializar un riesgo o amenaza a la seguridad nacional.** Por lo tanto, **no resultaba procedente la reserva de lo peticionado, con fundamento en lo dispuesto en el artículo 110, fracción I** de la Ley Federal de Transparencia y Acceso a la Información Pública.

Ahora bien, por lo que se refiere a la reserva de la información conforme a lo dispuesto en el artículo 110, fracción IV de la Ley Federal de la materia, resulta conveniente recordar que los términos contenidos en dicho ordenamiento se encuentran encaminados a salvaguardar la política monetaria que pueda afectar las medidas adoptadas en relación con los diferentes intermediarios y mercados financieros, o que ponga en riesgo la estabilidad de los controladores de riesgo y liquidez.

En ese tenor, en el asunto concreto, el Banco de México, indicó que proporcionar los datos requeridos por el particular implicaría revelar aspectos técnicos trascendentales de la seguridad, configuración y equipos de cómputo que componen la red de la institución con la que se podría afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país. Igualmente, el sujeto obligado manifestó que se puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y que, en consecuencia, se puede comprometer la seguridad en la provisión de moneda nacional al país.

No obstante, el Banco de México no precisó de qué forma la divulgación de dichos contenidos de información podrían:

I) Menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto;
II) Comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos;
III) Otorgar una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos, o
IV) Generar el incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones que pueda afectar seriamente al sistema financiero.

Es decir, bajo los argumentos esgrimidos por el sujeto obligado no se advierte que se actualicen las fracciones referidas que, de conformidad con el Vigésimo segundo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, deben de acreditarse y demostrar un vínculo con la información de la que obre el asunto para considerar que se actualice la reserva bajo la fracción IV del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

De tal forma, se puede concluir que **la información reservada por el Banco de México, no está relacionada con acciones encaminadas a proveer a la economía del país de moneda nacional, procurando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos;** pues se trata **de datos relativos a las características de las computadoras en posesión del ente obligado, así como al uso de la tecnología WIFI.**

Bajo tales consideraciones, no resulta procedente la reserva de lo peticionado, con fundamento en lo dispuesto en el artículo 110, fracción IV de la Ley Federal de Transparencia y Acceso a la Información Pública.

No obstante, **tomando en cuenta la naturaleza de la información** y los argumentos esgrimidos por el sujeto obligado, considero que **sí se actualiza la causal de reserva establecida en la fracción VII del artículo 110** de la Ley Federal de Transparencia y Acceso a la Información Pública.

Al respecto, de la normativa aplicable a la fracción de mérito es posible desprender que como información **reservada** podrá clasificarse aquella cuya publicación obstruya la **prevención o persecución de los delitos**. Además, para que pueda acreditarse que la información requerida pudiera "obstruir la **prevención** de los delitos", debe vincularse a la **afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos**.

En función de lo anterior, en el caso particular se señalaron como argumentos para negar el acceso a la información, el hecho de que su difusión implicaría dar a conocer la información de la infraestructura tecnológica, así como información relativa a las características específicas y configuraciones de las que disponen los equipos de cómputo utilizados por parte del sujeto obligado, misma que serviría como base para cualquier intento de penetración exitoso a los sistemas internos del sujeto obligado conllevando la afectación de su infraestructura informática y haciéndola susceptible de diversos tipos de ciberataques.

Sin embargo, en relatadas condiciones, con la intención de evidenciar la premisa que se ha señalado, primero es necesario apuntar que la **prevención y persecución son conceptos diferentes** pues, en el asunto que nos ocupa, el primero se refiere a **evitar la comisión de delitos**, mientras que el segundo se invoca **una vez constituida la conducta ilícita**.

A mayor abundamiento, "por definición la palabra ***prevención*** hace referencia a medidas y acciones dispuestas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso para reducir sus efectos sobre la población (...) Por consiguiente, "prevención del delito" no es más que tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito."[1]

Desde el punto de vista criminológico, **prevenir** es "conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse porque ésta se estima inconveniente."[2]

Bajo tales consideraciones, cabe recordar que, de las manifestaciones vertidas por el Banco de México, se advierte que la negativa de acceso a la información se motiva en

[1] "¿Qué es la Prevención del Delito?" Municipio de Poncitlán, Jalisco. Disponible para su consulta en http://www.poncitlan.gob.mx/prevenciondeldelito/2546-que-es-la-prevencion-del-delito.html [Fecha de consulta: 25/10/2017]
[2] Romo Medina, Miguel. *Criminología y Derecho*. Universidad Nacional Autónoma de México, México. 2003. p. 66.

pretender **evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas de informática**.

Al respecto, el *Código Penal Federal*, en sus artículos 211 BIS 1, 211 BIS 2 y 211 BIS 7, disponen que, comente el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del **Estado**, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

De esta forma, se colige que **con la publicidad de dichos datos se generaría un riesgo potencial para la infraestructura tecnológica del Banco de México** ya que puede ser utilizado para propiciar **ataques informáticos de diversa índole**.

Con base en lo anterior, **el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información**, ya **que el resguardo de los datos requeridos** por el solicitante **implican la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal**, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática.

Asimismo, la **limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**, toda vez que **la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática), misma que de llevarse a cabo podría permitir la realización de diversos **ataques** a la infraestructura tecnológica y de sistemas del sujeto obligado, los cuales podrían traer como consecuencia la **inoperatividad** de sus funciones, por un periodo indeterminado.

Por todo lo anterior, se advierte que **difundir** la información requerida **incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito**, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado e infraestructura tecnológica, conociendo con un alto grado de precisión la información técnica referente a sus equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

En esa tónica, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, pues se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la autoridad obligada, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática **perturben el sistema de la infraestructura tecnológica** del Banco de México y ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un **estado vulnerable** la información que en el ente obligado se contiene, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información; resultando, por lo tanto, **procedente su reserva**, de conformidad con el precepto jurídico que se analiza y no con la clasificación aludida por el sujeto obligado en la respuesta a la solicitud de acceso a la información.

A partir de los razonamientos vertidos, formulo el presente voto disidente en relación con la determinación adoptada por la mayoría del Pleno de este Instituto, en tanto que, desde mi perspectiva, no se actualiza la reserva en términos del artículo 110, fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública, sino que se debió modificar la respuesta del sujeto obligado a efecto de que confirmara la reserva de la información de conformidad con la fracción VII, del mismo numeral.

**Respetuosamente**

**Joel Salas Suárez**
**Comisionado**