



COMITÉ GARANTE DEL BANCO DE MÉXICO

RESOLUCIÓN BANXC2618594

Referencia: Solicitud con folio 420030700111526

Sujeto obligado recurrido: Banco de México

Sesión: 25/26

Ciudad de México, a veinticinco de septiembre de dos mil veintiséis

Síntesis de la decisión: Este Comité Garante confirma la respuesta emitida por el sujeto obligado, debido a que, del análisis efectuado, se concluyó que era procedente la reserva de la información de instituciones financieras afectadas por ciberataques durante el periodo 2019 a 2026, en términos del artículo 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la Información Pública. Además, respecto del desglose de la cantidad anual de ciberataques reportados entre el 2012 y el 2018, se verificó que el sujeto obligado realizó una búsqueda exhaustiva, razonable y con criterio amplio, sin identificar expresión documental que atendiera lo solicitado ni advertir obligación normativa de contar con esa información. Finalmente, se validó que el resto de la información estaba disponible en una fuente de acceso público en formatos abiertos, tal y como se encuentra disponible.

Índice temático

I. Resultandos	2
II. Considerandos.....	6
II.1 Competencia.....	6
II.2 Cuestiones previas	6
II.3 Análisis del caso concreto	8
III. Decisión.....	33

IV. Resolutivos 34

En sesión del veinticinco de septiembre de dos mil veintiséis, el Comité Garante de este Instituto Central resuelve el recurso de revisión **BANXC2618594**, y determina **CONFIRMAR** la respuesta emitida con motivo de la solicitud de información con folio 420030700111526, en virtud de los siguientes:

I. Resultandos

1. **Presentación de la solicitud.** El primero de junio de dos mil veintiséis, a través de la Plataforma Nacional de Transparencia (en adelante “PNT”), una persona requirió, desde 2012 y hasta la fecha en que presentó su solicitud, en formato editable, lo siguiente:

1. La cantidad anual de ciberataques reportados al Banco de México, desglosada por institución financiera de la banca privada del país y los daños económicos que se informaron.
2. Respecto de cada ciberataque reportado, precisar lo siguiente:
 - a. Fecha en que ocurrió
 - b. Nombre de la institución financiera
 - c. Tipo de ciberataque
 - d. Autor del ciberataque.
 - e. Cantidad de usuarios afectados
 - f. Monto económico del daño ocasionado
 - g. Si la institución financiera tuvo que pagar algún monto para recuperar la información o por otro concepto. En su caso, precisar el monto y a quién se le pagó
 - h. Duración de las afectaciones del ciberataque

Al respecto, la persona adjuntó un escrito libre que contiene la solicitud de información antes referida.

2. **Respuesta a la solicitud.** El veintinueve de junio de dos mil veintiséis, por medio de la PNT, el sujeto obligado notificó su respuesta mediante un oficio sin número, de la misma fecha, a través del cual hizo del conocimiento de la persona solicitante lo siguiente:

- **Requerimientos 1 (cantidad de ciberataques reportados) y 2, incisos a. (fecha en que ocurrió el ciberataque), c. (tipo de ciberataque) y f. (monto del daño ocasionado):** Únicamente se cuenta con información pública del 2019 al 2026, disponible en la subsección “Respuesta a incidentes en el sector financiero”, del micrositio de ciberseguridad del Banco de México, proporcionando un hipervínculo para su consulta. Para el periodo previo al 2019, no se localizaron registros y tampoco se advirtió obligación normativa de contar con dicha información.
- **Requerimientos 2, incisos d. (autor del ciberataque), e. (cantidad de usuarios afectados), g. (si se tuvo que cubrir algún monto para recuperar información o por otro concepto) y h. (duración de las afectaciones):** Derivado de una búsqueda exhaustiva, razonable y con criterio amplio en sus archivos institucionales no se identificó información o expresión documental que atienda lo requerido, y tampoco se advirtió la obligación normativa de contar con ello.
- **Requerimiento 2, inciso b. (identificación de la institución financiera afectada):** La Dirección de Ciberseguridad del Banco de México clasificó la información con fundamento en el artículo 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la Información Pública, al considerar que su divulgación podría: i) afectar la efectividad de las medidas adoptadas en relación con las políticas en materia del sistema financiero del país; ii) poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y iii) obstruir la prevención de delitos. Esta determinación fue confirmada por el Comité de Transparencia mediante su resolución del veinticinco de junio de dos mil veintiséis.

Finalmente, identificó el apartado “Sistema Financiero”, sección “Estabilidad financiera” y subsección “Ciberseguridad”, del portal de “Ciberseguridad” de la página de internet del Banco de México, donde puede consultarse información relacionada con la seguridad de la información en el sistema financiero y la estrategia de ciberseguridad de dicho Instituto Central; así como diversas referencias de interés en materia de ciberseguridad.

A su respuesta, el sujeto obligado adjuntó las siguientes documentales:

- Oficio sin número, del veintidós de junio de dos mil veintiséis, suscrito por el Director de Ciberseguridad y dirigido al Comité de Transparencia, ambos del

sujeto obligado, a través del cual se solicitó confirmar la clasificación de la información relativa a la identificación de las entidades o intermediarios financieros de los cuales se tiene conocimiento que han sufrido ciberataques, entre el uno de enero de dos mil diecinueve y el uno de junio de dos mil veintiséis.

- Documento que contiene la prueba de daño relativa a la clasificación de la identificación de las entidades o intermediarios financieros de los cuales el Banco de México tiene conocimiento que han sufrido ciberataques.
- Resolución del veinticinco de junio de dos mil veintiséis, emitida por el Comité de Transparencia del sujeto obligado, a través de la cual se confirmó la clasificación como reservada de la información antes señalada.

3. **Recurso de revisión.** El veintiuno de julio de dos mil veintiséis, mediante la PNT, la persona solicitante interpuso el presente recurso de revisión por considerar que: i) se clasificó la información del **requerimiento 2, inciso b.** (nombres de las instituciones financieras de la banca privada afectadas por un ciberataque) que, desde su punto de vista, es pública y su divulgación no genera una afectación legal u operativa; ii) no se atendió la temporalidad solicitada en los **requerimientos 1** (cantidad de ciberataques reportados) y **2**, respecto de los **incisos a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque), **d.** (autor del ciberataque), **e.** (cantidad de usuarios afectados) y **f.** (monto del daño ocasionado), pues sólo se proporcionó información del periodo 2019 a 2026, pero se omitió incluir información del resto de la temporalidad solicitada, es decir, del 2012 al 2018; y iii) no se ofreció la información en formatos abiertos, es decir, la posibilidad de descargar la información en archivos en formato Excel.

La persona recurrente adjuntó escrito libre que contiene su recurso de revisión.

4. **Radicación y admisión.** El veinticuatro de julio de dos mil veintiséis, se dictó proveído mediante el cual se radicó y registró el expediente en que se actúa en el Libro de Gobierno de la Dirección de Control Interno del Banco de México. En ese mismo acuerdo, se admitió a trámite el recurso de revisión, en términos del artículo 153, fracciones I, II y IV, de la Ley General de Transparencia y Acceso a la Información Pública, lo cual se notificó a las partes el tres de agosto de dos mil veintiséis.

5. **Alegatos del sujeto obligado.** El doce de agosto de dos mil veintiséis, el sujeto obligado remitió un oficio sin número, de la misma fecha, por medio del cual, presentó sus alegatos en los que argumentó lo que a su interés convino en defensa

de su respuesta a la solicitud materia del presente recurso de revisión BANXC2618594, e invocó la causal de sobreseimiento que consideró se actualizaba.

6. Recepción de alegatos. El diecisiete de agosto de dos mil veintiséis, se tuvo por presentado, en tiempo y forma, al sujeto obligado formulando alegatos; manifestando lo que a su derecho convino, y por admitidas las probanzas ofrecidas, consistentes en la instrumental de actuaciones y la presuncional en su doble aspecto, legal y humana.

7. Cierre de instrucción. El catorce de septiembre de dos mil veintiséis, al no existir diligencias pendientes por desahogar, se emitió el acuerdo por medio del cual se declaró cerrada la instrucción, quedando el expediente en estado de resolución.

8. Calendario de días inhábiles de la Autoridad Garante. Con el propósito de preservar los principios de certeza y seguridad jurídica, así como los derechos procesales de las personas inconformes y de los sujetos obligados, el Comité Garante del Banco de México aprobó, en sesión de diecisiete de diciembre de dos mil veinticinco, la *Disposición por la que se establece el calendario oficial de días inhábiles de la Autoridad Garante del Banco de México para el año 2026, para efectos de los actos y procedimientos previstos en la Ley General de Transparencia y Acceso a la Información Pública, así como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, la cual fue publicada el veinticuatro de diciembre de dos mil veinticinco en el Diario Oficial de la Federación.

En términos del numeral Primero de la citada Disposición, se determinaron como días inhábiles para la Autoridad Garante del Banco de México, para el dos mil veintiséis, además de sábados y domingos, los siguientes: del jueves 1° al martes 6 de enero, lunes 2 de febrero, lunes 16 de marzo, del miércoles 1° al viernes 3 de abril, viernes 1° y martes 5 de mayo, del lunes 27 al viernes 31 de julio, miércoles 16 de septiembre, lunes 2 y lunes 16 de noviembre y del lunes 21 al jueves 31 de diciembre.

En consecuencia, en esos días se suspenden los plazos y términos inherentes a la recepción, tramitación, sustanciación y resolución, entre otros, de los medios de impugnación en materia de acceso a la información pública establecidos en la Ley General de Transparencia y Acceso a la Información Pública.

De acuerdo con lo anterior, a la fecha de emisión de la presente resolución, se actualizaron como días inhábiles, sábados y domingos, así como del veintisiete al

treinta y uno de julio de dos mil veintiséis, y el dieciséis de septiembre de la misma anualidad.

En atención a que no existe diligencia pendiente de desahogo y que, en términos del artículo 30 Bis, fracción XXV, del Reglamento Interior del Banco de México, la Dirección de Control Interno, a través de la Unidad Garante, proveyó a este Comité Garante la información necesaria para resolver el recurso de revisión **BANXC2618594**; incluyendo el proyecto para su análisis y resolución, en términos de los siguientes:

II. Considerandos

II.1 Competencia

Este Comité Garante del Banco de México es competente para conocer y resolver el presente recurso de revisión, con fundamento en los artículos 6°, párrafo cuarto, apartado A, fracciones IV y VIII, y 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos; 1° de la Ley del Banco de México; 4° Ter y 31 Ter, párrafos segundo y sexto, fracción I, del Reglamento Interior del Banco de México; así como 1°, 3°, fracción V, 4°, 8°, 35, fracción II, 144, 148, 153, y 154, de la Ley General de Transparencia y Acceso a la Información Pública.

II.2 Cuestiones previas

En relación con lo dispuesto por el artículo 158 de la Ley General de Transparencia y Acceso a la Información Pública, el sujeto obligado argumentó que, en el caso concreto, se actualizaba la hipótesis prevista en la fracción V del mismo artículo, conforme a la cual será desechado por improcedente el recurso de revisión cuando se impugne la veracidad de la información proporcionada.

Al respecto, el artículo 159, fracción IV, de la citada Ley General, dispone que el recurso de revisión será sobreseído en todo o en parte, cuando, una vez admitido, aparezca una causal de improcedencia como la antes mencionada.

En ese contexto, y dado que de actualizarse la hipótesis de improcedencia invocada por el sujeto obligado podría derivar en el sobreseimiento del presente medio de impugnación, a continuación, se realizará su estudio de manera preliminar al examen de fondo.

A través de su oficio de alegatos, el sujeto obligado refiere que el presente medio de impugnación es improcedente, al estimar que las manifestaciones de la persona solicitante impugnan la veracidad de la atención a su solicitud con folio 420030700111526, pues en ese acto señaló que *“...proporcionó información que se encuentra incompleta, a pesar de que todos los datos que le fueron requeridos se encuentran en su posesión, por tratarse de información que resulta de su plena competencia; no obstante, varios de los puntos solicitados no fueron atendidos satisfactoriamente...”*, con lo cual sostiene implícitamente que la respuesta emitida supuestamente no es verdadera, cuando en su momento, se le explicó que tras una búsqueda exhaustiva, razonable y con criterio amplio en los archivos institucionales del Banco Central no se identificó información o expresión documental que atienda el requerimiento **2**, incisos **d.** (autores de los ciberataques) y **e.** (cantidad de usuarios afectados), y tampoco se observó obligación normativa de contar con ello. Lo anterior, sin perder de vista que, el actuar de los sujetos obligados se rige por el principio de buena fe.

Al respecto, tras revisar las constancias que integran el expediente en que se actúa, este Comité Garante advierte que las manifestaciones de la persona solicitante no buscan impugnar la veracidad de la información y calificar de falsa la respuesta proporcionada por el sujeto obligado, sino que a través de las mismas y en aplicación de la suplencia de la queja prevista en el artículo 148 de la Ley General de Transparencia y Acceso a la Información Pública, controvierte, entre otros aspectos, la inexistencia de la información solicitada en el requerimiento **2**, incisos **d** (autores de los ciberataques) y **e** (cantidad de usuarios afectados), al considerar que dicha información forma parte de sus competencias y, consecuentemente, la posee en sus archivos.

En ese sentido, respecto de la inconformidad presentada contra la atención a los puntos previamente identificados, es claro que se actualiza el supuesto previsto en la fracción II del artículo 145 de la Ley General de Transparencia y Acceso a la Información Pública, que prevé la procedencia del recurso de revisión contra la inexistencia de la información solicitada.

Así, toda vez que el agravio al que alude el sujeto obligado en su oficio de alegatos se relaciona con una de las causales de procedencia enlistadas en la Ley de la materia, específicamente contra la inexistencia de la información solicitada, dichas manifestaciones no pueden traducirse en la impugnación de la veracidad de la información, pues el propio marco normativo aplicable faculta a las personas solicitantes a interponer un recurso de revisión en dicho supuesto, a efecto de que este Comité Garante analice si la respuesta se llevó a cabo conforme a los

parámetros previstos en Ley General de la materia y, en su caso, determinar si es procedente.

De esta manera, frente a lo expuesto por el sujeto obligado durante la sustanciación del recurso de revisión, las manifestaciones de la persona solicitante no actualizan la hipótesis de improcedencia enlistada en el artículo 158, fracción V, en relación con el diverso 159, fracción IV, ambos de la Ley General de la materia; por el contrario, es procedente su análisis en los términos previamente identificados.

Adicionalmente, del estudio de las constancias que integran el expediente del presente recurso de revisión, no se aprecia que se actualice algún otro supuesto de improcedencia o sobreseimiento en términos de los artículos 158 y 159 de la Ley General de Transparencia y Acceso a la Información Pública.

Por tanto, a continuación, se analizará de fondo el presente asunto.

II.3 Análisis del caso concreto

La presente resolución se centrará en determinar si la respuesta emitida por el sujeto obligado en atención a la solicitud con folio 420030700111526 cumple con las disposiciones de la Ley General de Transparencia y Acceso a la Información Pública.

Para tal efecto, resulta pertinente precisar los elementos esenciales del caso, es decir, la solicitud presentada, la respuesta emitida, los agravios formulados y los alegatos expresados por el sujeto obligado.

a. Solicitud. Para el periodo comprendido de 2012 a la fecha en que presentó la solicitud, la persona solicitante requirió en formato editable lo siguiente:

- 1.** La cantidad anual de ciberataques reportados, desglosada por institución financiera de la banca privada del país y los daños económicos que se informaron.
- 2.** Respecto de cada ciberataque reportado, precisar lo siguiente:
 - a.** Fecha en que ocurrió
 - b.** Nombre de la institución financiera
 - c.** Tipo de ciberataque
 - d.** Autor del ciberataque

- e. Cantidad de usuarios afectados
- f. Monto económico del daño ocasionado
- g. Si la institución financiera tuvo que pagar algún monto para recuperar la información o por otro concepto. En su caso, precisar el monto y a quién se le pagó
- h. Duración de las afectaciones del ciberataque

b. Respuesta a la solicitud. Con la atención proporcionada por la Dirección de Ciberseguridad, adscrita a la Dirección General de Contraloría y Administración de Riesgos del Banco de México, el sujeto obligado señaló lo siguiente:

- **Requerimientos 1 (cantidad de ciberataques reportados) y 2, incisos a. (fecha en que ocurrió el ciberataque), c. (tipo de ciberataque) y f. (monto del daño ocasionado):** Únicamente se cuenta con información pública del 2019 al 2026, disponible en la subsección “Respuesta a incidentes en el sector financiero”, del micrositio de ciberseguridad del Banco de México, proporcionando un hipervínculo para su consulta. En cuanto al resto del periodo que también fue solicitado, no se localizaron registros y tampoco se advirtió obligación normativa de contar con dicha información.
- **Requerimientos 2, incisos d. (autor del ciberataque), e. (cantidad de usuarios afectados), g. (si se tuvo que cubrir algún monto para recuperar información o por otro concepto) y h. (duración de las afectaciones):** Derivado de una búsqueda exhaustiva, razonable y con criterio amplio en sus archivos institucionales no se identificó información o expresión documental que atienda lo requerido, y tampoco se advirtió la obligación normativa de contar con ello.
- **Requerimiento 2, inciso b. (identificación de la institución financiera afectada):** Clasificó la información con fundamento en el artículo 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la Información Pública, al considerar que con su divulgación podría: i) afectar la efectividad de las medidas adoptadas en relación con las políticas en materia del sistema financiero del país; ii) poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y iii) obstruir la prevención de delitos. Esta determinación fue confirmada por el Comité de Transparencia mediante su resolución del veinticinco de junio de dos mil veintiséis, anexa al oficio de respuesta junto con la respectiva prueba de daño.

Finalmente, identificó el apartado “Sistema Financiero”, sección “Estabilidad financiera” y subsección “Ciberseguridad”, del portal de “Ciberseguridad” de la página de internet del Banco de México, donde puede consultarse información relacionada con la seguridad de la información en el sistema financiero y la estrategia de ciberseguridad de dicho Instituto Central; así como diversas referencias de interés en materia de ciberseguridad.

c. Motivo de inconformidad. En aplicación de la suplencia de la queja prevista en el artículo 148 de la Ley General de Transparencia y Acceso a la Información Pública, la persona solicitante interpuso el presente recurso de revisión contra: i) la clasificación de la información requerida mediante el **contenido 2, inciso b.** (identificación de la institución financiera afectada); ii) la inexistencia de la información materia de los **contenidos 1** (cantidad de ciberataques reportados) y **2, incisos a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque), **d.** (autores de los ciberataques), **e.** (cantidad de usuarios afectados) y **f.** (monto del daño ocasionado) para el periodo comprendido entre el 2012 y el 2018; y iii) la entrega de información en un formato inaccesible para la persona recurrente, pues no se priorizó la entrega de la información en formatos abiertos, como es el Excel.

En ese sentido, de la lectura de las manifestaciones expuestas en el recurso de revisión, se aprecia que no se expresó inconformidad alguna relacionada con la información proporcionada en atención a los **requerimientos 1** (cantidad de ciberataques reportados) y **2, incisos a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque), **d.** (autores de los ciberataques), **e.** (cantidad de usuarios afectados) y **f.** (monto del daño ocasionado), del 2019 al 2026.

Asimismo, la persona recurrente tampoco expresó inconformidad con la atención al **contenido 2, incisos g.** (si la institución financiera tuvo que pagar algún monto para recuperar la información o por otro concepto) y **h.** (duración de las afectaciones del ciberataque) para todo el periodo identificado en la solicitud.

Por ello, este Comité Garante determina que dichas actuaciones del sujeto obligado no serán objeto de estudio en el presente Considerando, por tratarse de actos consentidos tácitamente, al no haber sido controvertidos dentro del plazo legal; motivo por el cual la respuesta quedó firme.

Resultan aplicables por analogía las jurisprudencias con rubros *ACTOS CONSENTIDOS TÁCITAMENTE*¹ y *REVISIÓN EN AMPARO. LAS CONSIDERACIONES NO IMPUGNADAS DE LA SENTENCIA DEBEN DECLARARSE FIRMES*². La primera establece que se presumen consentidos, “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”. La segunda dispone que “cuando alguna consideración de la sentencia impugnada afecte a la recurrente y ésta no expresa agravio en su contra, tal consideración debe declararse firme”.

d. Alegatos del sujeto obligado. Al ser notificado de la admisión del recurso de revisión, en síntesis, el sujeto obligado sostuvo lo siguiente:

- Derivado de una búsqueda exhaustiva, razonable y con criterio amplio en los archivos institucionales del Banco de México, considerando la totalidad de la información con que se cuenta, no se identificó expresión documental alguna que atienda lo requerido, ni la obligación normativa de poseer dicha información para el periodo anterior al 2019, de manera que no resultó necesaria la declaración formal de inexistencia, de conformidad con el artículo 141 de la Ley General de Transparencia y Acceso a la Información Pública.
- Se justificó que la identificación de las entidades o intermediarios financieros que han sufrido ciberataques entre el uno de enero de dos mil diecinueve y el uno de junio de dos mil veintiséis, es reservada en términos del artículo 112, fracciones IV y VII de la Ley General de la materia. Lo anterior, toda vez que su divulgación podría generar una afectación reputacional a la entidad aludida, mediante un impacto moral o económico con alcance hasta sus clientes, así como alertar a individuos o grupos con intenciones maliciosas a focalizar nuevos ataques e intentar aprovecharse de la posible situación de vulnerabilidad.
- La información localizada para el periodo del 2019 al 2026 se proporcionó como obra en sus archivos, sin necesidad de elaborar documentos adicionales para atender las solicitudes, de conformidad con el artículo 131, párrafo primero, de la Ley General de Transparencia y Acceso a la Información Pública. Lo anterior, debido a que el derecho de acceso a la información se satisface con la entrega

¹ Tesis VI.2o. J/21, emitida en la novena época, por el Segundo Tribunal Colegiado en Materia Común del Sexto Circuito, publicada en la Gaceta del Semanario Judicial de la Federación en agosto de 1995, tomo II, página 291, número de registro 204707.

² Tesis 1a./J. 62/2006, aprobada por la Primera Sala de la Suprema Corte de Justicia de la Nación, publicada en la Gaceta del Semanario Judicial de la Federación en septiembre de 2006, tomo XXIV, página 185, número de registro 174177.

de la información con la que cuenta el sujeto obligado, en el formato en que lo tenga, lo cual no implica la obligación de elaborar documentos *ad hoc*.

Lo descrito se desprende de las constancias que obran en el expediente, así como de las pruebas ofrecidas por el sujeto obligado, las cuales fueron debidamente admitidas. Estas consisten, respectivamente, en la instrumental de actuaciones, y la presuncional, en su doble aspecto, legal y humano. Pruebas a las que se les concede valor probatorio en términos de esta resolución.

Expuestas las posturas de las partes, a continuación, se analizará la legalidad de la respuesta impugnada a la luz de los agravios formulados por la persona solicitante, con el propósito de determinar si el sujeto obligado garantizó o no el ejercicio de su derecho de acceso a la información pública.

Conforme a lo previamente expuesto, en el recurso de revisión BANXC2618594 se controvertió la clasificación de una parte de la información requerida, la inexistencia de otros contenidos de la solicitud y que no se ofreció la información en formatos abiertos. Razón por la cual, a continuación, se realizarán los respectivos estudios.

Análisis de la clasificación de la información solicitada mediante el requerimiento 2, inciso b.

De conformidad con los artículos 1º, primer párrafo, y 6º, párrafo cuarto, apartado A, fracciones I y IV, de la Constitución Política de los Estados Unidos Mexicanos, toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijan las leyes.

Así, dado que el derecho de acceso a la información puede limitarse por razones de interés público o seguridad nacional, corresponde a la legislación secundaria desarrollar los supuestos específicos en que procede tal restricción.

A fin de tutelar el interés público como límite constitucionalmente válido al acceso a la información pública, el artículo 112 de la Ley General de la materia establece las hipótesis bajo las cuales determinada información debe ser clasificada como reservada.

Teniendo en cuenta que dichas limitantes al derecho de acceso a la información restringen el principio de máxima publicidad, es necesario justificar de manera fundada y motivada las razones por las cuales el riesgo de perjuicio que supondría la divulgación, supera el interés público general de que se difunda. Así, conforme al artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, para el caso de la información reservada está prevista la inclusión de una prueba de daño que justifique su procedencia, a través de la cual se haga un ejercicio de ponderación entre la divulgación de la información y el perjuicio que su publicidad podría ocasionar al interés protegido por la norma.

En el caso concreto, el sujeto obligado señaló que la identificación de las entidades o intermediarios financieros que han sufrido ciberataques, y que se hicieron de conocimiento de dicho sujeto obligado, tiene el carácter de información reservada en términos del artículo 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la Información Pública, pues su divulgación podría: i) afectar la efectividad de las medidas adoptadas en relación con las políticas en materia del sistema financiero del país; ii) poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y iii) obstruir la prevención de delitos.

Así, para sostener que la divulgación de la información implica un riesgo de perjuicio real, demostrable e identificable, mediante su prueba de daño, el sujeto obligado manifestó lo siguiente:

- Aún cuando las entidades o intermediarios financieros hayan recuperado en su totalidad su operación cotidiana después de un ciberataque, al ser del conocimiento público su estado de vulnerabilidad o indefensión, puede generar desconfianza entre sus clientes beneficiando a sus competidores al captar los clientes que hubiera perdido esa institución, lo cual podría ocasionar un desequilibrio en el sistema financiero.
- Al conducirse las instituciones financieras con estándares similares de seguridad de la información, la vulnerabilidad por la que una entidad fue afectada, puede facilitar que otras sufran ataques similares, a través del uso de métodos en los que se haya identificado su efectividad.
- La identificación de instituciones con antecedentes de ciberataques permite identificar brechas de seguridad en los componentes vulnerables del entorno tecnológico interconectado del sistema financiero. Lo anterior, toda vez que

gran parte de las instituciones del sector financiero deben cumplir con regulaciones y estándares comunes, reflejándose en el uso de tecnologías y medidas de seguridad semejantes. Además, aquellas que están recuperándose de un incidente también tendrían que ocuparse de no recibir otros ataques de terceros hostiles.

- Podría generar un incumplimiento en las obligaciones de participantes afectados en un sistema de pagos, propiciando que incumplan con sus respectivas obligaciones y otros obtengan una ventaja indebida de esta situación, lo cual afectaría el sistema financiero al ocasionar distorsiones en la estabilidad de las operaciones de esas instituciones y en el mercado.
- La identificación de las instituciones podría incentivar a terceros para aplicar metodologías comunes y realizar un ataque-defensa con el propósito de obtener más información como son las especificaciones técnicas en materia de seguridad, el proceso de continuidad operativa y de contingencia, y, en general, información relacionada con su infraestructura informática. De esta manera, identificar brechas en la operación de los participantes o potenciales vulnerabilidades podrían ser utilizadas por otros participantes o personas para diseñar estrategias operativas o tecnológicas que podrían afectar la infraestructura de la entidad y su operación, así como facilitar que terceros logren acceder a información financiera o personal y modifiquen los datos que se procesan en ellas, lo cual podría tener implicaciones directas sobre los usuarios, otras instituciones financieras, incluyendo los participantes del sistema de pagos o bien, contra el propio Banco de México.
- Los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar los sistemas. Una de las formas más comunes de vulnerar los sistemas es la recopilación de manera gradual de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o interrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes.
- Un ataque cibernético que vulnere la operación de las tecnologías de la información y de comunicaciones de las instituciones del sistema financiero o del propio sistema de pagos, sin importar la duración de la interrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y el patrimonio de los usuarios.

- Se obstruiría la prevención de delitos informáticos contra estas instituciones y sus clientes, máxime que se expondrían elementos relativos a posibles investigaciones iniciadas ante las autoridades competentes.
- Proporcionar esta información no aporta un beneficio mayor a la transparencia y la rendición de cuentas que sea compatible con el perjuicio que implicaría el hecho de divulgarla, lo cual permitiría obtener una ventaja indebida sobre otros participantes del sistema y menoscabar la efectividad de estas medidas implementadas en el sistema financiero, así como planear y perpetrar ataques cibernéticos dirigidos específicamente a las instituciones financieras, teniendo como resultado la sustracción de información, incluyendo datos personales de sus usuarios y operaciones realizadas, así como la alteración en órdenes de transferencia entre las cuentas bancarias de los participantes o de sus clientes.

Expuesto lo anterior, este Comité Garante advierte que la prueba de daño del sujeto obligado señala que conceder el acceso a los nombres de las instituciones financieras que han reportado al Banco de México algún ciberataque, implica una afectación en la efectividad de las medidas implementadas en el sistema financiero, poniendo en riesgo su funcionamiento, a la estabilidad de los mercados, incluyendo los sistemas de pagos, ocasionada por la ventaja indebida que podrían adquirir determinadas instituciones financieras y terceros, así como la posibilidad que otras instituciones sufran ataques similares, por la repetición de los métodos en los que se haya identificado la efectividad del ataque, en virtud de que las instituciones del sector financiero cumplen con regulaciones y estándares comunes, en el uso de tecnologías y medidas de seguridad.

De esta manera, a continuación se analizan las causales de reserva invocadas por el sujeto obligado, a efecto de verificar si subsisten las razones que justificaron la clasificación de la información.

Artículo 112, fracción IV de la Ley General de Transparencia y Acceso a la Información Pública

En la referida fracción IV, del artículo 112, se prevé que puede clasificarse como reservada la información cuya divulgación pueda **afectar la eficacia de las medidas adoptadas en relación con las políticas monetaria, cambiaria o del sistema financiero nacional; poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o la del**

propio sistema financiero del país; comprometer la seguridad en la provisión de moneda nacional; o incrementar el costo de las operaciones financieras realizadas por los sujetos obligados del sector público federal.

Al respecto, el Vigésimo Segundo, fracciones I y III, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas³ (en adelante “Lineamientos Generales”), disponen que para clasificar cierta información como reservada en términos del artículo 112, fracción IV, de la Ley General de la materia, es necesario acreditar el vínculo entre su difusión y el menoscabo a 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; o se otorgue una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos.

Con el propósito de identificar el bien jurídico tutelado por la causal que se estudia, cabe señalar que el artículo 28, párrafo séptimo, de la Constitución Política de los Estados Unidos Mexicanos, establece que el Estado contará con un banco central autónomo en el ejercicio de sus funciones y en su administración, cuyo objetivo prioritario consiste en procurar la estabilidad del poder adquisitivo de la moneda nacional, fortaleciendo con ello la rectoría del desarrollo nacional. Esta disposición permite advertir que la estabilidad monetaria constituye un objetivo de relevancia constitucional cuya consecución requiere preservar la capacidad institucional, operativa y técnica del Banco de México para adoptar y ejecutar eficazmente las medidas necesarias para su cumplimiento.

Asimismo, el párrafo octavo del propio artículo 28 constitucional dispone que el Banco Central, en los términos que establezcan las leyes y con la intervención que corresponda a las autoridades competentes, tiene atribuciones para 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. De esta manera, dicho precepto vincula directamente al Banco de México con la regulación de los sistemas cambiario y financiero y no sólo con la adopción formal de disposiciones en esas materias, sino también con asegurar su observancia.

³ Publicados en el Diario Oficial de la Federación el 15 de abril de 2016, con modificaciones posteriores publicadas el 29 de julio de 2016 y el 18 de noviembre de 2022 en el mismo medio de difusión oficial. Aplicables al caso concreto, en términos del Quinto Transitorio, párrafo tercero, del Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución en materia de simplificación orgánica, publicado en el Diario Oficial de la Federación el 20 de diciembre de 2024.

En congruencia con lo anterior, el artículo 2° de la Ley del Banco de México dispone que ese Instituto Central tiene por finalidad proveer a la economía del país de moneda nacional; que en la consecución de esa finalidad debe procurar, como objetivo prioritario, la estabilidad del poder adquisitivo de dicha moneda; y que también le corresponde promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.

Por su parte, el artículo 3°, fracciones I, II, III y IV, del mismo ordenamiento atribuye al Banco de México, entre otras, 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 de este, así como fungir como asesor del propio Gobierno Federal en materia económica, particularmente financiera.

En ese sentido, el objetivo jurídicamente tutelado por las fracciones I y III del Vigésimo Segundo de los Lineamientos generales de clasificación y desclasificación consiste en preservar la capacidad efectiva del Banco de México para cumplir, de manera continua, íntegra, segura y eficaz, sus objetivos y funciones en los ámbitos monetario, cambiario, financiero y de sistemas de pagos; así como evitar la generación de situaciones que otorguen una ventaja indebida a determinados participantes del sector y se generen distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos.

En el caso concreto, el interés de la persona recurrente consiste en conocer los nombres de las instituciones financieras de la banca privada que han reportado ciberataques al Banco de México.

Al respecto, de los argumentos expuestos por el sujeto obligado para justificar la reserva de esta información destaca la posible afectación a las instituciones afectadas por algún ciberataque, otras entidades, usuarios y, en general, a la instrumentación y efectividad de las medidas implementadas en el sistema financiero del país, incluyendo los sistemas de pagos, pues la divulgación de esta información facilitaría que terceros utilicen metodologías, estrategias o tecnologías que puedan afectar su infraestructura y operación, así como emprender alguna acción para acceder a información financiera o personal, modificar los datos que procesan o, incluso, dejarlos sin funcionar adecuadamente; máxime que podría generarse una ventaja indebida entre los participantes del sector, ocasionando una distorsión en la estabilidad de los mercados.

En ese sentido, parte de los objetivos prioritarios del Banco de México son el fortalecimiento de la rectoría del desarrollo nacional del Estado, promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.

Por ello, de conformidad con el artículo 36 de la Ley del Banco de México los intermediarios financieros deben suministrar al propio Banco Central la información que éste les requiera sobre sus operaciones, incluso respecto de alguna o algunas de ellas en lo individual, los datos que permitan estimar su situación financiera y, en general, aquélla que sea útil al Banco para proveer el adecuado cumplimiento de sus funciones.

Por su parte, los artículos 19 y 20 de la Ley de Sistemas de Pagos establecen que el Banco de México supervisa y vigila a los administradores de los sistemas y de los sistemas de pagos, para procurar su correcto funcionamiento. Esta supervisión tiene por objeto evaluar los riesgos a que estén sujetos, sus sistemas de control y los mecanismos adoptados en caso de incumplimiento, así como la calidad de administración.

Y, en relación con la materia de la solicitud, la disposición 13a. de la Circular 13/2017 “Sistemas de pagos administrados por el Banco de México”, establece que los participantes (instituciones financieras) en un sistema de pagos deben observar permanentemente los requisitos técnicos, operativos, de seguridad informática y de gestión de riesgos operacionales necesarios para propiciar el buen funcionamiento de ese sistema, lo cual implica realizar verificaciones periódicas al cumplimiento de los requisitos en materia de atención de incidentes de seguridad informática en sus canales electrónicos.

Asimismo, las disposiciones 2a., fracciones I y XXXVI, y 46a. de la Circular 14/2017 “Reglas del Sistema de Pagos Electrónicos Interbancarios”; 2a., fracción I y 42a. de la Circular 4/2016 “Reglas del Sistema de Pagos Interbancarios”; y el anexo 1 de la Circular número 4/2014 “Cámaras de compensación para pagos con tarjetas”, establecen que las instituciones financieras están sujetas a obligaciones en materia de seguridad de la información, las cuales incluyen la detección, gestión y reporte de incidentes. Por ello, deben implementar procedimientos y mecanismos a seguir para la atención de incidentes de seguridad informática en su infraestructura, que comprendan la identificación, contención, adecuada recolección y resguardo de evidencias.

Además, los participantes en los sistemas de pagos administrados por el Banco de México tienen el deber de comunicarle al propio Banco la detección de incidentes, amenazas y ataques de seguridad informática que afecten o puedan obstaculizar el adecuado funcionamiento de dichos sistemas de pagos y de los servicios financieros.

En ese contexto, las instituciones financieras utilizan sistemas tecnológicos y operativos interconectados para el desarrollo de sus actividades, cuya seguridad, disponibilidad y continuidad es esencial para la prestación de sus servicios financieros, de manera que, las medidas de seguridad no son mecanismos aislados, sino que forman parte de la capacidad de las instituciones y autoridades para identificar amenazas y adoptar medidas de prevención y mitigación para evitar nuevos ataques cibernéticos.

Así, conocer qué instituciones financieras han recibido ciberataques, forma parte de la supervisión de intermediarios y entidades financieras que tiene encomendada el sujeto obligado, de manera que se trata de información vinculada con los sistemas, procesos y servicios informáticos cuya seguridad y funcionamiento se pretende proteger, así como con la efectividad de las medidas implementadas en los sistemas monetario, cambiario, financiero y de la operación de los sistemas de pagos del país.

Si bien los nombres de las instituciones financieras son de conocimiento público, en el caso concreto este dato está asociado a incidentes de seguridad ocurridos en sus sistemas e infraestructura informáticas que son el conducto para realizar sus operaciones y prestar servicios financieros, incluyendo la interacción con otras entidades en el sistema financiero del país y su participación en sistemas de pagos.

Así, la información requerida puede utilizarse para analizar y ejecutar ataques dirigidos no solo a una institución con antecedentes de afectación, sino al resto de entidades, incrementando la capacidad de terceros para explotar vulnerabilidades conocidas, realizar actos de ingeniería social, o diseñar ataques más focalizados que eleven el riesgo de interrupciones en las operaciones de esas instituciones, lo cual puede repercutir en el funcionamiento de todo el sistema financiero.

Lo anterior, teniendo en cuenta que este sector se encuentra interconectado para el desarrollo de sus actividades, lo cual implica que la interrupción o afectación en las operaciones de un participante puede generar efectos en terceros, más cuando existen relaciones operativas, financieras o de pagos que requieran una continuidad en su funcionamiento.

Cabe señalar que los nombres de las instituciones que reportan estos incidentes, también reflejan las decisiones estratégicas adoptadas sobre la administración de sus riesgos tecnológicos, la implementación de controles de seguridad y la protección de información que da sustento a su actividad económica, lo cual además de colocarlos en desventaja frente a terceros del mismo sector, está relacionado con las medidas de protección tecnológica y las capacidades de respuesta ante incidentes de seguridad informática, y facilita que terceros identifiquen debilidades operativas o estrategias para planear futuros ataques con otras entidades.

Lo anterior, sin perder de vista que en los reportes de estabilidad financiera que divulga el sujeto obligado, es posible consultar información relacionada con incidentes de seguridad informática ocurridos en el sistema financiero nacional que le fueron reportados; en los que únicamente se menciona al tipo de entidad (por ejemplo: Banco 1, Banco 2, Sociedad Financiera Popular 1), mes, descripción general, servicios afectados, monto por afectación a clientes y a la propia entidad⁴, sin que se pueda identificar el nombre específico de la institución que presentó el incidente de seguridad informática.

En ese sentido, divulgar el nombre de las instituciones afectadas facilitaría que terceras personas asocien información dispersa en fuentes de acceso público, y puedan obtener un conocimiento más preciso sobre las vulnerabilidades, infraestructura y detalles tanto técnicos como operativos de dichas entidades. Con ello, se incrementaría el riesgo en la seguridad y continuidad de las operaciones y servicios financieros, así como la pérdida de ventaja competitiva frente a competidores, ocasionando un desequilibrio en el desarrollo del sistema financiero del país.

Además, al replicarse estas vulnerabilidades en diversos agentes del sistema financiero, podrían generarse ventajas indebidas en el mercado, una volatilidad injustificada de capital y riesgos en la continuidad de los servicios financieros.

Ante tales circunstancias, de conformidad con el artículo 107 de la Ley General de Transparencia y Acceso a la Información Pública, este Comité Garante estima que se acredita la prueba de daño expuesta por el sujeto obligado, ya que la divulgación de los nombres de las instituciones financieras que reportaron al Banco de México

⁴ A manera de ejemplo, puede consultarse un ejemplo de reporte de incidentes cibernéticos en: <https://www.banxico.org.mx/sistema-financiero/d/%7BE2B17A77-A650-4BC7-2783-11F5F3EFA2E5%7D.pdf>

que sufrieron ciberataques, representaría un riesgo real, demostrable e identificable de perjuicio al interés público.

Lo anterior, debido a que conocer el nombre de aquellas instituciones bancarias que han tenido vulneraciones en materia de ciberseguridad, puede ocasionar que terceros realicen nuevas acciones con el fin de aprovecharlas, ampliando este daño a otras instituciones interconectadas en el sistema financiero, así como ocasionando mayores daños o la interrupción de servicios y operaciones.

Asimismo, el riesgo de perjuicio supera el interés público general de conocer la información, pues debe prevalecer temporalmente la protección de la información requerida, con el propósito de conservar la efectividad en las medidas implementadas en el sistema financiero, incluyendo los sistemas de pagos, lo cual propicia el buen funcionamiento y la estabilidad en el sistema financiero en su conjunto.

Finalmente, la reserva constituye una medida proporcional, idónea y necesaria, al ser el medio menos restrictivo para evitar el daño identificado, sin implicar una restricción absoluta o definitiva al derecho de acceso a la información, ya que únicamente subsiste mientras permanezcan las causas que le dieron origen.

En consecuencia, la reserva temporal de la información solicitada resulta justificada, ya que busca preservar la efectividad de las medidas adoptadas en relación con las políticas en materia del sistema financiero; así como evitar la generación de situaciones que otorguen una ventaja indebida a determinados participantes del sector y se generen distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos.

Artículo 112, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública

De conformidad con el artículo 112, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, y el Vigésimo Sexto de los Lineamientos Generales, se podrá clasificar como información reservada aquella que obstruya la prevención o persecución de los delitos.

Para el supuesto de que se obstruya la prevención de delitos, es necesario que la información solicitada se vincule con la afectación de las acciones implementadas por las autoridades competentes para evitar su comisión, así como menoscabar o limitar la capacidad de las autoridades para tal efecto.

De conformidad con las Directrices para la prevención del delito del Consejo Económico y Social de las Naciones Unidas⁵, “la expresión ‘prevención del delito’, engloba las estrategias y medidas encaminadas a reducir el riesgo de que se produzcan delitos y sus posibles efectos perjudiciales para las personas y la sociedad, incluido el temor a la delincuencia, y a intervenir para influir en las múltiples causas.”

En ese sentido, el objetivo del bien tutelado en dicha causal de clasificación, son las estrategias o acciones dirigidas a evitar, impedir o reducir la comisión de delitos, en este caso, vinculados con la difusión de los nombres de las instituciones financieras que han sufrido ciberataques.

Al respecto, en los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4 y 211 bis 5, del Código Penal Federal; y 112 Quater, fracciones I y II, 112 Sextus de la Ley de Instituciones de Crédito, se regulan diversas conductas relacionadas con el delito de acceso ilícito a sistemas y equipos informáticos, como es la modificación, destrucción o pérdida de información contenida en los mismos, así como el acceso, alteración o modificación del funcionamiento de los equipos o medios electrónicos del sistema bancario mexicano.

De esta manera, la prevención de delitos asociados con incidentes de seguridad de la información, requiere la ejecución de acciones destinadas a identificar, contener y contrarrestar amenazas. Así, salvaguardar los nombres de las instituciones financieras afectadas puede garantizar la eficacia de estas medidas, al evitar que terceros reconozcan patrones de actuaciones y modifiquen sus estrategias para realizar ataques cibernéticos exitosos.

Además, como se mencionó previamente, a partir de esta información es posible que terceros realicen acciones de ataque-defensa con el propósito de obtener más información, como son las especificaciones técnicas en materia de seguridad informática, procesos de continuidad operativa o de contingencia y, en general, información relacionada con su infraestructura informática. A partir de ello, se identificarían brechas en la operación de los participantes o potenciales vulnerabilidades que podrían ser utilizadas por los perpetradores para diseñar estrategias para afectar la infraestructura de la entidad y su operación, así como

⁵ Disponible para su consulta en:
https://www.unodc.org/pdf/compendium/compendium_2006_es_part_03_01.pdf

acceder a información financiera o personal y/o modificar los datos que se procesan en ellas.

El veinticuatro de mayo de dos mil dieciocho, la otrora Procuraduría General de la República (hoy Fiscalía), otras autoridades y algunas asociaciones gremiales financieras de México formalizaron las Bases de Coordinación en Materia de Seguridad de la Información⁶ cuya finalidad es definir un mecanismo de coordinación para dar respuesta efectiva a incidentes de seguridad de la información en el sector financiero. Además, en ese mismo instrumento se estableció la creación de un Grupo de Respuesta a Incidentes (GRI) encargado de coordinar acciones de respuesta a los incidentes que les reporten las instituciones, del cual forma parte el Banco de México.

En ese sentido, ante el incremento sostenido de ataques informáticos en el sector financiero es que se ha establecido una coordinación entre diversas autoridades a fin de robustecer e implementar medidas más efectivas que eviten la comisión del delito de acceso ilícito a sistemas y equipos de informática.

De conformidad con lo anterior, este Comité Garante estima que se acredita la prueba de daño expuesta por el sujeto obligado, ya que la divulgación de los nombres de las instituciones financieras que le reportaron haber sufrido ciberataques, representa un riesgo real, demostrable e identificable de perjuicio al interés público, debido a que conocer esta información disminuye la efectividad de los mecanismos destinados a evitar el acceso indebido y la sustracción de información, ya que se conocería qué instituciones podrían tener vulnerabilidades y ser sujetas de nuevos ataques. Incluso, dicha información, vinculada con la información pública disponible sobre los reportes de ciberataques, permitiría focalizar vulnerabilidades por sectores, lo que implicaría proporcionar información que facilitaría que más instituciones financieras sean atacadas, obstruyendo o limitando la capacidad de reacción de las autoridades para evitar este tipo de delitos.

Asimismo, el riesgo de perjuicio supera el interés público general de conocer la información, pues debe prevalecer temporalmente la protección de la información requerida, con el propósito de conservar el éxito de las acciones y estrategias dirigidas a prevenir futuros ataques informáticos y, consecuentemente, la comisión de delitos relacionados con el acceso ilícito a sistemas y equipos de informática.

⁶ Disponibles en: <https://www.banxico.org.mx/sistema-financiero/d/%7BD0502AA8-7721-5C2C-5C8F-05858CBB4AE7%7D.pdf>

Finalmente, la reserva constituye una medida proporcional, idónea y necesaria, al ser el medio menos restrictivo para evitar el daño identificado, sin implicar una restricción absoluta o definitiva al derecho de acceso a la información.

En consecuencia, la reserva temporal de los nombres de instituciones financieras que sufrieron algún incidente de seguridad resulta justificada.

Expuesto lo anterior, resulta relevante señalar que de conformidad con los artículos 106, 133 y 139 de la Ley General de Transparencia y Acceso a la Información Pública, cuando los sujetos obligados determinen la clasificación de documentos, se deberá atender el siguiente procedimiento:

- En el ejercicio del derecho de acceso a la información pública, la Unidad de Transparencia tiene el deber de turnar la solicitud a las áreas que tengan o puedan tener la información.
- Cuando las áreas hayan clasificado la información requerida como reservada o confidencial, deberá remitir la solicitud, así como un escrito en el que funden y motiven dicha clasificación, al Comité de Transparencia, para que dicho órgano colegiado confirme, modifique o revoque la clasificación.
- La resolución correspondiente, además de estar fundada y motivada, también deberá ser notificada a la persona solicitante, dentro de los veinte días hábiles siguientes de recibida la solicitud (en términos de lo previsto por el artículo 134 de la Ley General de la materia).
- El Comité de Transparencia podrá tener acceso a la información que esté en poder del área correspondiente, de la cual se haya solicitado su clasificación.

En el caso concreto, el sujeto obligado remitió el acta de su Comité de Transparencia mediante la cual se confirmó la clasificación invocada por la Dirección de Ciberseguridad en términos del artículo 112, fracciones IV y VII, de la Ley General de Transparencia y Acceso a la Información Pública, la cual fue hecha del conocimiento de la persona recurrente, a través de la resolución del veinticinco de junio de dos mil veintiséis, suscrita por los integrantes del Comité de Transparencia del Banco de México.

Por tanto, este Comité Garante advierte que el sujeto obligado también atendió lo dispuesto por los artículos a los que se ha hecho mención pues, a través de la respuesta impugnada dio cuenta a la ahora parte recurrente de dicha clasificación.

En consecuencia, el agravio de la persona recurrente contra la clasificación de información es **infundado**.

Análisis de la inexistencia de la información solicitada mediante los requerimientos 1, 2, incisos a., c., d., e. y f.

De conformidad con los artículos 6°, párrafo cuarto, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, 3°, fracción IX y 4° de la Ley General de Transparencia y Acceso a la Información Pública, el derecho humano de acceso a la información pública comprende solicitar, investigar, difundir, buscar y recibir información. Asimismo, toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona, en los términos y condiciones previstos en dicha Ley.

Asimismo, los artículos 131, párrafo primero, y 135 del mismo ordenamiento prevén que los sujetos obligados tienen el deber de otorgar los documentos que obren en sus archivos o a aquellos que estén constreñidos a documentar en ejercicio de sus facultades, competencias o funciones, en la modalidad de entrega y, en su caso, de envío elegidos por las personas solicitantes.

Esto último, en el entendido de que el deber de garantizar este derecho humano no implica que los sujetos obligados tienen que emitir pronunciamientos específicos, explicaciones y/o argumentaciones sobre planteamientos particulares, ni elaborar documentos adicionales para atender las solicitudes.

Adicionalmente, de conformidad con los artículos 16, 41, fracciones II y IV, 133, 140 y 141 de la Ley General en la materia, con motivo del ejercicio del derecho de acceso a la información, es necesario observar diversas directrices, mediante un procedimiento de búsqueda, en los términos siguientes:

- La Unidad de Transparencia de cada sujeto obligado está constreñida a realizar un análisis de la información solicitada para que, en atención a la naturaleza de la misma, turne el requerimiento a todas las unidades administrativas con facultades y competencias para su atención.
- La búsqueda debe comprender todos los documentos que obren en los archivos del sujeto obligado y/o que deben generar de conformidad con sus facultades y atribuciones conferidas por mandato de ley, misma que debe ser exhaustiva y razonable para brindar atención a lo requerido.

- En caso de que la información no se encuentre en los archivos del sujeto obligado, aun cuando normativamente existen competencias conforme a las cuales sí debería obrar en aquellos, el Comité de Transparencia analizará el caso, tomará las medidas necesarias para su localización y, en su caso, emitirá una resolución que confirme su inexistencia.
- La resolución debe contener datos que permitan a las personas solicitantes generar certeza de que las condiciones de búsqueda fueron razonables y exhaustivas, exponiendo circunstancias de tiempo, modo y lugar.
- En aquellos casos en que no se advierta obligación o competencia alguna de los sujetos obligados para contar con la información, derivado del análisis de las disposiciones jurídicas aplicables a la materia de la solicitud, y además no se tengan elementos de convicción que permitan suponer que esta debe obrar en sus archivos, o bien, se cuente con atribuciones, pero no se hubiera generado la información, no será necesario que el Comité de Transparencia emita una resolución que confirme su inexistencia.

Expuesto el marco normativo aplicable a la gestión de la solicitud de acceso a la información pública, cabe recordar que, entre otros aspectos, se requirió la cantidad anual de ciberataques reportados al Banco de México durante el periodo del 2012 al 2018, desglosada por cada institución financiera de la banca privada del país y los daños económicos que se informaron (**requerimiento 1**), precisando fecha en que ocurrieron los ciberataques (**requerimiento 2.a.**), tipo (**requerimiento 2.c.**) y autor (**requerimiento 2.d.**) del ciberataque, cantidad de usuarios afectados (**requerimiento 2.e.**) y monto económico del daño ocasionado (**requerimiento 2.f.**).

En respuesta, el sujeto obligado precisó que, tras una búsqueda exhaustiva, razonable y con criterio amplio en sus archivos institucionales no identificó registros, información o expresión documental que atienda los requerimientos antes identificados y tampoco advirtió la obligación normativa de contar con esa información.

En ese sentido, de conformidad con los artículos 1° y 2° de la Ley General de Transparencia y Acceso a la Información Pública, se destaca que entre sus objetivos está garantizar el acceso a la información contenida en los documentos que los sujetos obligados generan, obtienen, adquieren, transforman o conservan con motivo del ejercicio de sus atribuciones y/o actividades, sin importar su fuente.

De esta manera, en cumplimiento con los artículos 4°, 8° y 131 de la Ley General en la materia, y a efecto de atender la solicitud de información previamente identificada, el sujeto obligado activó su procedimiento de búsqueda con el propósito de localizar las expresiones documentales que atendieran lo solicitado en los requerimientos **1** (cantidad de ciberataques reportados) y **2, incisos a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque), **d.** (autores de los ciberataques), **e** (cantidad de usuarios afectados) y **f.** (monto del daño ocasionado) para el periodo del 2012 al 2018.

Así, la solicitud con folio 420030700111526 fue atendida por la Dirección de Ciberseguridad, adscrita a la Dirección General de Contraloría y Administración de Riesgos, por lo que se procede a determinar si dicha área es competente para conocer de la información que es del interés de la persona recurrente.

Al respecto, en términos del artículo 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México es un órgano autónomo, cuyo objetivo prioritario es procurar la estabilidad del poder adquisitivo de la moneda nacional, fortaleciendo con ello la rectoría del desarrollo nacional que corresponde al Estado.

De conformidad con los artículos 1°, 2°, 24 y 26 de la Ley del Banco de México, entre las finalidades del sujeto obligado está la promoción del sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos.

Como parte de sus atribuciones, el Banco Central puede expedir disposiciones cuyo propósito sea 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; sin perjuicio del resto de normatividad que pueda emitir en términos de otras leyes. Las características de las operaciones activas, pasivas y de servicios que realicen las instituciones de crédito, así como las de crédito, préstamo o reporto que celebren los intermediarios bursátiles, se ajustarán a esta regulación que emita el sujeto obligado.

Por su parte, con fundamento en los artículos 1°, párrafo primero, 2°, 4°, 29 Bis y 30 del Reglamento Interior⁷, así como Primero y Segundo del Acuerdo de adscripción de las unidades administrativas, ambos del Banco de México⁸, el sujeto

⁷ Última reforma publicada en el Diario Oficial de la Federación el 19 de noviembre de 2025.

⁸ Última reforma publicada en el Diario Oficial de la Federación el 30 de mayo de 2025.

obligado cuenta con diversas unidades administrativas, entre las que destaca la **Dirección de Ciberseguridad**, adscrita a la Dirección General de Contraloría y Administración de Riesgos, responsable de las siguientes atribuciones:

- Establecer políticas, lineamientos y estrategias institucionales para fortalecer la ciberseguridad, así como todos los sistemas que soportan la operación y procesos.
- Requerir información en materia de seguridad de la información, ciberseguridad, ciberresiliencia e incidentes de ciberseguridad a las entidades e intermediarios financieros o entidades que operen algún sistema del Banco de México o en su interconexión a las infraestructuras de cómputo y telecomunicaciones de este último o bien, en su participación en los Sistemas de Pagos e Infraestructuras de Mercados.
- Definir la política, protocolos y plan de respuesta a incidentes de ciberseguridad, así como coordinar las acciones de respuesta y recuperación a incidentes que afecten al Instituto Central o al sistema financiero.

Teniendo en cuenta la materia de la solicitud origen del recurso de revisión que nos ocupa, es posible advertir que la Unidad de Transparencia del sujeto obligado realizó la gestión ante la unidad administrativa que conforme a sus atribuciones podría contar con la información del interés de la persona recurrente, dado que sus requerimientos están vinculados con la atención a los ciberataques reportados por instituciones financieras al sujeto obligado.

De esta forma, en términos del marco normativo aplicable, es posible advertir que la unidad administrativa antes identificada, esto es, la Dirección de Ciberseguridad es la competente para pronunciarse sobre lo solicitado.

En ese sentido, se deduce que el sujeto obligado atendió en sus términos lo dispuesto en el artículo 133 de la Ley General de Transparencia y Acceso a la Información Pública, conforme al cual, al tramitar las solicitudes, las Unidades de Transparencia deben turnarlas a las áreas competentes que cuenten con la información o estén constreñidas a tenerla de acuerdo con sus facultades, competencias y funciones, a fin de que realicen una búsqueda exhaustiva y razonable de lo requerido.

Ahora bien, en el caso concreto, la persona recurrente se inconformó con la no localización de la información previamente identificada, la cual se relaciona con los

ciberataques reportados al Banco de México por las instituciones financieras de la banca privada del país, durante el periodo del 2012 al 2018.

Respecto del periodo antes identificado, de la revisión al marco normativo aplicable por parte del Comité Garante, con apoyo de la Unidad Garante, no se observa que el sujeto obligado deba contar con esta información en sus archivos, es decir, del 2012 al 2018.

Adicionalmente, de la investigación efectuada por el Comité Garante con apoyo en la Unidad Garante, en el portal de internet del sujeto obligado⁹ y en la red informática en cita, no se localizaron elementos de los que se pueda concluir fehacientemente o presumir, aun indiciariamente, que deba existir en sus archivos la información objeto de los requerimientos **1** (cantidad de ciberataques reportados) y **2, incisos a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque), **d.** (autores de los ciberataques), **e.** (cantidad de usuarios afectados) y **f.** (monto del daño ocasionado) para el periodo del 2012 al 2018.

Ante este panorama, es posible advertir que como resultado de la búsqueda exhaustiva, razonable y con criterio amplio que realizó en sus archivos institucionales el sujeto obligado, la información en comento no fue localizada, por lo que es inconcuso que dichos pronunciamientos brindan certeza jurídica de que no obran en su poder expresiones documentales que atiendan esas peticiones informativas, ya que la respuesta proporcionada adquiere validez en razón de que las actuaciones de los sujetos obligados son congruentes con la buena fe administrativa, en el sentido de que se presumen apegadas a la legalidad y veracidad, salvo prueba en contrario¹⁰.

Asimismo, si bien el acceso a la información pública comprende el derecho fundamental a solicitar, investigar, difundir, buscar y recibir información que se encuentre integrada en documentos que registren el ejercicio de las facultades, funciones y competencias de los sujetos obligados¹¹, no se debe eludir que dicho alcance está condicionado a la existencia de la información; es decir, que la misma sea generada conforme al ejercicio de las facultades, competencias o atribuciones de los sujetos obligados.

⁹ Disponible para su consulta en: www.banxico.org.mx

¹⁰ Jurisprudencia 2ª./J. 77/2006, emitida en la novena época, por la Segunda Sala de la Suprema Corte de Justicia de la Nación, publicada en la Gaceta del Seminario Judicial de la Federación en junio de 2006, tomo XXIII, página 213, número de registro 174897.

¹¹ Artículo 4o. de la Ley General de Transparencia y Acceso a la Información Pública.

Lo anterior, sin perder de vista que en términos del artículo 131 de la Ley General de Transparencia y Acceso a la Información Pública, el deber de los sujetos obligados de conceder el acceso a las expresiones documentales que obran en sus archivos no se extiende a la elaboración de documentos adicionales que atienden las solicitudes en particular, ni emitir pronunciamientos específicos, explicaciones y/o argumentos sobre supuestos hipotéticos.

Además de brindar certeza jurídica sobre el procedimiento de búsqueda que efectuó en sus archivos y su resultado, se considera que es suficiente para tener por satisfecho su derecho de acceso a la información, en la inteligencia que cumplir con una solicitud de tal naturaleza no implica que necesariamente se deba proporcionar la información o documentos solicitados. También se puede satisfacer tal derecho en aquellos casos en que el sujeto obligado llevó a cabo los actos establecidos en la Ley General de Transparencia y Acceso a la Información Pública, para emitir y justificar el sentido de sus respuestas, como ocurre en los casos que se analizan.

Así, como quedó asentado previamente, al analizar el procedimiento de búsqueda que desahogó el sujeto obligado quedó acreditado que: i) la solicitud de información se turnó a la única unidad administrativa con atribuciones para conocer lo requerido (Dirección de Ciberseguridad, adscrita a la Dirección General de Contraloría y Administración de Riesgos); ii) no se identificó obligación o competencia alguna del sujeto obligado para contar con lo solicitado para el periodo del 2012 al 2018; y iii) tampoco se ubicaron elementos que permitan presumir que el sujeto obligado deba poseer las documentales que son del interés de la persona recurrente. Por tanto, el sujeto obligado cumplió con lo previsto en los artículos 131 y 133 de la Ley General de Transparencia y Acceso a la Información Pública.

Adicionalmente, este Comité Garante advierte que no constituye incumplimiento a la normatividad aplicable, que el sujeto obligado no hubiera sometido a consideración de su Comité de Transparencia la inexistencia de la información solicitada en los requerimientos **1 y 2**, incisos **a., c., d., e. y f.**, entre el 2012 y el 2018, pues del análisis a su Reglamento Interior, el Acuerdo de adscripción de sus unidades administrativas y la información que por obligación de transparencia tiene el deber de publicitar al amparo de la Ley en comento, no se desprende disposición alguna que le imponga su posesión y tampoco se observa elemento de convicción que apunte a su existencia.

Por tanto, en el caso que nos ocupa se actualiza el supuesto establecido en el segundo párrafo del artículo 141 de la Ley General de Transparencia y Acceso a la Información Pública; es decir, que no es necesaria la intervención del Comité de

Transparencia para confirmar la declaración de inexistencia de la información requerida mediante la solicitud de información que nos ocupan.

Así, el agravio contra la no localización de la información solicitada en los requerimientos **1** (cantidad de ciberataques reportados) y **2, incisos a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque), **d.** (autores de los ciberataques), **e.** (cantidad de usuarios afectados) y **f.** (monto del daño ocasionado) para el periodo del 2012 al 2018 resulta **infundado**.

Análisis de la entrega de información en un formato inaccesible

De conformidad con el artículo 6º, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, en relación con los diversos 4º y 131 de la Ley General de Transparencia y Acceso a la Información Pública, los sujetos obligados deberán otorgar los documentos que obren en sus archivos o aquellos que estén obligados a documentar, conforme a las características físicas o electrónicas con las que cuenten o del lugar donde se encuentre, sin necesidad de elaborar documentos adicionales para atender las solicitudes de acceso a información.

En la misma línea, la fracción V del artículo 20 del referido ordenamiento establece como obligación de los sujetos obligados promover la generación, documentación y publicación de información en formatos abiertos y accesibles. Aunado a ello, el artículo 12, fracción I, de la misma Ley General dispone que, durante la generación, publicación y entrega de información deberá garantizarse que esta sea accesible, confiable, verificable, veraz, oportuna y atender las necesidades del derecho de acceso a la información de toda persona.

Así, como parte de la actuación que los sujetos obligados deben procurar al garantizar el derecho de acceso a la información es su accesibilidad, es decir, que efectivamente pueda consultarse sin barreras técnicas, físicas o materiales, de modo que la persona solicitante pueda llegar a ella sin dificultad. Dicho de otra manera, la información debe proporcionarse en condiciones que permitan su localización, apertura, lectura, comprensión y aprovechamiento, sin obstáculos técnicos o de disponibilidad.

Lo anterior, representa un estándar mínimo, indispensable y no restrictivo para procurar el ejercicio pleno y efectivo del derecho de acceso a la información pública.

Adicionalmente, el artículo 132 de la Ley General de Transparencia y Acceso a la Información Pública faculta a los sujetos obligados para hacer saber a las personas

solicitantes la fuente, el lugar y la forma en que pueden consultar, reproducir o adquirir aquella información que ya se encuentre disponible al público en medios impresos (tales como libros, compendios, trípticos, archivos públicos) y en formatos electrónicos en Internet o en cualquier otro medio.

En el caso concreto, en relación con los requerimientos **1** (cantidad de ciberataques reportados) y **2**, incisos **a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque) y **f.** (monto del daño ocasionado), el sujeto obligado señaló que únicamente cuenta con información pública del 2019 al 2026, disponible en la subsección “Respuesta a incidentes en el sector financiero”, del micrositio de ciberseguridad del Banco de México, respecto de la cual proporcionó un vínculo electrónico para su consulta.

Al respecto, con apoyo de la Unidad Garante, este Comité Garante procedió a la verificación de dicho hipervínculo, advirtiendo diversos enlaces que remiten a los incidentes cibernéticos ocurridos anualmente en el sistema financiero nacional, del 2019 a 2026. Cada relación contiene los rubros: entidad, fecha, descripción, canal y afectación (millones de pesos).

De esta manera, es dable concluir que la información sí es accesible, pues conforme a las instrucciones proporcionadas por el sujeto obligado es posible acceder a la misma.

Ahora bien, en cuanto a acceder a la información en formatos abiertos, cabe señalar que de conformidad con el artículo 3º, fracción VIII, de la Ley General de la materia, son datos abiertos aquellos digitales públicos que son accesibles en línea, y que pueden ser usados, reutilizados y redistribuidos por cualquier persona. Entre sus características destaca su disponibilidad para la mayor cantidad de personas, que su acceso no requiera una contraprestación; ser actualizados periódicamente y que estén en formatos abiertos. Es decir, que los documentos tengan un conjunto de características y de presentación de la información correspondientes a la estructura lógica utilizada para almacenar datos y facilitar su procesamiento digital, cuyas especificaciones estén disponibles públicamente y permitan el acceso sin restricción de uso por parte de las personas.

De la revisión a la información que el sujeto obligado proporcionó para atender los contenidos **1** (cantidad de ciberataques reportados) y **2**, incisos **a.** (fecha en que ocurrió el ciberataque), **c.** (tipo de ciberataque) y **f.** (monto del daño ocasionado), para el periodo del 2019 al 2026, se advierte que la misma cumple con las características de accesibilidad al estar disponible en una fuente de acceso público donde no se requiere contraprestación alguna.

Además, considerando las características del formato utilizado para publicar la información, se observa que el mismo permite copiar y reutilizar la información.

En ese sentido, en términos del artículo 132 de la Ley General de Transparencia y Acceso a la Información Pública, el sujeto obligado hizo saber a la parte recurrente la fuente, el lugar y la forma en que puede consultar aquella información que se encuentra disponible al público en formatos electrónicos en internet, los cuales son accesibles y se encuentran disponibles en formatos abiertos.

Aunado a lo anterior, si bien la persona recurrente alegó que la información no se proporcionó en formato Excel, lo cierto es que, de conformidad con los artículos 131 y 132 de la Ley General de Transparencia y Acceso a la Información Pública, la garantía del derecho de acceso a la información no se extiende a la elaboración de documentos en formatos específicos, por lo que cumple con su obligación de acceso al remitir a la persona recurrente al lugar en el que se encuentra pública la información, indicando los pasos a seguir para su consulta; máxime que, como quedó de manifiesto, dicha información cumple con las características de accesibilidad y de formatos abiertos.

Así, mediante la respuesta otorgada, se observa que el sujeto obligado informó que parte de la información requerida estaba disponible en una fuente de acceso público, proporcionando el medio idóneo para consultar y obtenerla directamente, tal y como se encuentra disponible.

Lo anterior, toda vez que, si bien en términos del artículo 20, fracción V, de la Ley General de la materia, los sujetos obligados deben promover la generación, documentación y publicación de la información en formatos abiertos y accesibles, lo cierto es que, la exigencia de que esta se proporcione con dicha calidad no debe entenderse como una obligación de generar o procesar información que obra en una fuente de acceso público que, como ocurrió en el caso concreto, se facilitó su acceso mediante un vínculo electrónico.

En consecuencia, el agravio de la persona recurrente contra la entrega de información en formatos abiertos, es **infundado**.

III. Decisión

En atención al estudio previamente efectuado y, toda vez que los agravios de la persona recurrente son **infundados**, en términos del artículo 154, fracción II, de la

Ley General de Transparencia y Acceso a la Información Pública, este Comité Garante considera procedente **CONFIRMAR** la respuesta emitida por el Banco de México en su calidad de sujeto obligado, a la solicitud de información con folio 420030700111526.

Por lo expuesto y fundado en términos de los artículos 35, fracciones I y II, 145, fracciones I, II y VIII, 148, 153, 154, fracción II, 156 y 161, de la Ley General de Transparencia y Acceso a la Información Pública, este órgano colegiado emite los siguientes:

IV. Resolutivos

Primero. Este Comité Garante **CONFIRMA** la respuesta emitida por el Banco de México a la solicitud de información con folio 420030700111526, en su calidad de sujeto obligado, en razón de las consideraciones expuestas y con fundamento en el artículo 154, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública.

Segundo. Se hace del conocimiento de la persona recurrente que, de encontrarse insatisfecha con esta resolución, le asiste el derecho de impugnarla ante el Poder Judicial de la Federación, en términos del artículo 161 de la Ley General de Transparencia y Acceso a la Información Pública.

Tercero. Notifíquese la presente resolución a la persona recurrente y al sujeto obligado a través de los medios designados para tales efectos.

Así lo resolvieron, por unanimidad, la y los integrantes del Comité Garante del Banco de México, en sesión celebrada el veinticinco de septiembre de dos mil veintiséis y firman electrónicamente en términos del artículo 10 del Reglamento Interior del Banco de México, junto con su secretaria.

ERIK MAURICIO SÁNCHEZ MEDINA
Presidente

NORA BRENDA REYES RODRÍGUEZ
Integrante suplente

RODOLFO SALVADOR LUNA DE LA TORRE
Integrante

MARÍA ELENA MÉNDEZ SÁNCHEZ
Secretaria

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
25/09/2026 14:53:07	MARIA ELENA MENDEZ SANCHEZ	f442a414755519398eabcea890c49e0d4d3fd6dac7fb4489d51b178bdf6a5266
25/09/2026 15:24:25	NORA BRENDA REYES RODRIGUEZ	3a5c0495aba8ae0f0ed4b451a7e8c7a546bc9637124b20df9845f7b06fa845d5
25/09/2026 15:32:52	RODOLFO SALVADOR LUNA DE LA TORRE	ab8258a49b3b05637e1463bda77a8b432c75d4ab759f8dca984fdb2543c7755b
25/09/2026 17:29:10	ERIK MAURICIO SANCHEZ MEDINA	cdb9ba84b6be6f81fc3c5b4d27d26bceff6aa470db822e64f0f239509c7315f9d