# ACTA DE LA DÉCIMA PRIMERA SESIÓN EXTRAORDINARIA DE 2020 DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

El día viernes 03 de julio de 2020, a las 13:30 horas, por vía remota, se reunió el Comité de Transparencia de la CONDUSEF a efecto de desarrollar la Décima Primera Sesión Extraordinaria de 2020, solicitada por la Unidad de Transparencia de esta Comisión Nacional, por lo que se dieron cita sus integrantes: la Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia y la Lic. Ana Clara Fragoso Pereida, Titular del Órgano Interno de Control en la CONDUSEF, así como el Lic. Eduardo Saúl Reyes Gallegos, Director de Planeación y Finanzas adscrito a la Vicepresidencia de Planeación y Administración, designado mediante memorándum VPA/076/2020 de fecha 02 de julio de 2020 para asistir en suplencia por ausencia del C.P. Fernando Enrique Zambrano Suárez, Vicepresidente de Planeación y Administración y encargado de la Dirección de Gestión y Control Documental; adicionalmente participó como invitada a la sesión la Lic. Elizabeth Araiza Olivares, Directora General de Procedimientos Jurídicos, Defensoría y Tecnologías Financieras de la Vicepresidencia Jurídica.

## I.- Declaración de Quórum Legal e Inicio de la Sesión.

La Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia dio la bienvenida a los Integrantes del Comité de Transparencia y a la invitada a la Décima Primera Sesión Extraordinaria, agradeciendo su presencia y participación. Enseguida tomó lista de asistencia y verificó la existencia de quórum, advirtiendo que se satisface el número de Integrantes del Comité que deben estar presentes para sesionar de manera válida.

## II. Aprobación del Orden del Día.

A continuación, la Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia, informó sobre el único asunto a tratar de conformidad con el Orden del Día, siendo este aprobado por los Integrantes del Comité de Transparencia.

## III. Desarrollo de la Sesión

La Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia dio lectura al **ÚNICO ASUNTO** a tratar, el cual se indica a continuación:

- Revisión de los argumentos lógicos - jurídicos presentados por la **Unidad de Transparencia**, a fin de que se confirme, modifique o revoque la Clasificación de la Información como Reservada de la información que obra en el Documento de Seguridad para el Tratamiento de Datos Personales 2020; y en su caso, se autorice la versión pública propuesta del citado documento, para dar atención a la solicitud de información con número de folio **0637000014620**.

En virtud de lo anterior, la Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia informó que mediante memorándum número VJ/UT/037/2020 de fecha 01 de julio de 2020, la Unidad de Transparencia presenta ante los Integrantes del Comité de Transparencia los argumentos lógicos jurídicos, los cuales contienen las razones y circunstancias que fundan y motivan la clasificación de la información como **RESERVADA**, respecto a la información que obra en el **Documento de Seguridad para el Tratamiento de Datos Personales 2020**, solicitado en el folio **0637000014620**, que a la letra indica lo siguiente:

Descripción clara de la solicitud de información.

***"Solicito el documento de seguridad (en su caso, la versión pública) establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. En caso de que la respuesta rebase los límites de carga de la Plataforma Nacional de Transparencia, se requiere se remita al correo electrónico descrito en la solicitud de mérito." (sic)***

En dicho sentido, la Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia dio el uso de la voz a la Lic. Elizabeth Araiza Olivares, Directora General de Procedimientos Jurídicos, Defensoría y Tecnologías Financieras de la Vicepresidencia Jurídica, persona facultada para recibir y dar trámite a las solicitudes de Información Pública, Acceso a Datos Personales, Recursos de Revisión y en todo lo relativo a las obligaciones a cargo de la Unidad de Transparencia, la cual señaló que con base en lo establecido en los artículos 3, fracción XXI, 4, 24, fracción VI, 44, fracción II, 100, 101, 104, 106, fracción I, 108, 111, 113, fracción I y 137 de la Ley General de Transparencia y Acceso a la Información Pública; 3, 11, fracción VI, 65, fracción II, 97, 98, fracción I, 99, 100, 105, 108, 110, fracción I, 111, 118, y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública y Segundo, fracción XVIII, Cuarto, Séptimo, fracción I, Noveno, Décimo Octavo párrafos primero y último, Trigésimo Tercero, Trigésimo Cuarto, Quincuagésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas; Segundo, fracción XXV, Vigésimo Quinto y Vigésimo Sexto de los Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública, la **Unidad de Transparencia** solicita al H. Comité de Transparencia de la CONDUSEF para que, de considerarlo procedente confirme la clasificación de la información como **RESERVADA**, en relación a la información que obra en el **Documento de Seguridad para el Tratamiento de Datos Personales 2020**, respecto a:

1. Nombre, cargo y correo electrónico institucional de los operadores de los sistemas de tratamiento de datos personales referidos en el Documento de Seguridad;
2. Características del lugar físico donde se resguardan los sistemas de tratamiento de datos personales;
3. Medidas de seguridad:
   a) Medidas actuales:
      - Descripción de las medidas actuales.
   b) Análisis de Riesgo:
      - Riesgo/amenaza;
      - Factor de riesgo;
      - Clasificación de factor;
      - Control de factor;
      - Valoración de riesgo:
        - Probabilidad de que ocurra; y
        - Valor.
   c) Identificación del análisis de brecha; y
   d) Plan de Trabajo:
      - Actividad;
      - Evidencia entregable.
4. Diagrama de arquitectura de seguridad en la que es posible apreciar el flujo datos de los sistemas a través de las redes electrónica que interconectan los equipos.

Y en su caso, se autorice y confirme la versión pública del citado **Documento de Seguridad**, a fin de dar atención a la solicitud de información con número de folio **0637000014620,** conforme a los siguientes argumentos lógicos jurídicos expuestos en el memorándum VJ/UT/037/2020 de fecha 01 de julio de 2020, los cuales se indican a continuación:

> *"(...), en virtud de lo previsto en la fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública y a la fracción I, del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, los cuales establecen que podrá clasificarse como **RESERVADA** aquella información cuya publicación comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable; precepto legal que se transcribe para mayor referencia:*
>
> ***Ley General de Transparencia y Acceso a la Información Pública***
>
> ***"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;"*
>
> ***Ley Federal de Transparencia y Acceso a la Información Pública***
>
> ***"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;"*

*En correlación con lo antes referido, el Décimo Octavo primero y último párrafo de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, establece que podrá considerarse como* ***RESERVADA*** *aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, tendientes a preservar y resguardar el ejercicio de los derechos de las personas, así como, aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones, precepto que se transcribe para pronta referencia:*

> ***"Décimo octavo.*** *De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada,* ***aquella que comprometa la seguridad pública, al poner 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.*

*Se pone en peligro el orden público cuando la difusión de la información pueda entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública, menoscabar o dificultar las estrategias contra la evasión de reos; o menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales.*

*Asimismo, podrá considerarse como reservada aquella que* ***revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.****"*

*Con base en lo anterior, se puede precisar que el* ***Documento de Seguridad*** *es un "instrumento que describe en forma detallada las medidas de seguridad implementadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales a cargo del Responsable".*[1]

*Asimismo, el* ***Documento de Seguridad*** *es la* ***"identificación de todas las personas que intervienen en el tratamiento de datos personales a lo largo de su ciclo de vida****"*[2]*. El proceso de identificación se logra mediante el análisis de los procesos de negocio y los tipos de datos personales tratados como parte del flujo de información, por lo que el tratamiento que se les dé a los datos esta en concordancia con los roles y responsabilidades de las personas en su papel de responsable, evitando con ello la asignación no adecuada de privilegios que puede producir que —por error o intencionalmente— se afecte la confidencialidad, integridad o disponibilidad de los datos personales.*

---

[1] **Uciel Fragoso Rodríguez**, 2019, *Diccionario de Protección de Datos Personales*; México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), p. 328.

[2] **Uciel Fragoso Rodríguez**, 2019, *Diccionario de Protección de Datos Personales*; México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), p. 329.

*Por otra parte, el Documento de Seguridad contiene las* ***características del lugar donde se resguardan los sistemas de tratamiento de datos personales*** *los cuales pueden ser soportes físicos y electrónicos, en los cuales se realiza la descripción con detalles sobre las características físicas de la oficina, almacén o bodega donde se resguardan dichos soportes, o bien en el soporte electrónico en donde se albergue la citada información.*

*Ahora bien, el* ***análisis de riesgo*** *en el Documento de Seguridad describe a detalle cómo se implementa el proceso en forma sistemática con una metodología de análisis de riesgo para cada dato personal con un nivel de riesgo inherente asociado, evaluándose los factores ligados a los propios datos, como son: el volumen de los datos y su nivel de riesgo inherente, el número de acceso a los datos y el entorno desde donde se acceden los datos.*

*El proceso de análisis de riesgo implica la identificación del activo a proteger, que en el caso de los datos personales, se identifican los tipos o categorías de los datos personales bajo estudio, después con el proceso para identificar las amenazas que pudieran ocasionar algún daño a los datos, cabe señalar que las amenazas pueden ser internas o externas y pueden tener diferentes orígenes: fenómenos naturales, incidentes, infraestructura tecnológica o de origen humano; las vulnerabilidades o debilidades que se presentan al momento de procesar la información o tratar los datos personales se localizan en los procesos, en la tecnología o en la gente y su nivel de exposición depende de las medidas de seguridad existentes asociadas a cada vulnerabilidad.*

*Con la información recolectada se pueden construir escenarios de riesgo, los cuales prevén situaciones que pueden pasar y que relacionan los componentes del riesgo: activo, amenazas y vulnerabilidades, lo cual permite evaluar la probabilidad de ocurrencia y el impacto que pudiera tener en caso de que dicho escenario de riesgo se materialice.*

*El análisis de riesgo permite llevar a cabo el análisis de brecha, el cual consiste en determinar la diferencia entre las medidas de seguridad existentes y las que faltan para reducir el riesgo hasta un nivel por abajo del establecido por la organización como nivel aceptable, por lo que en su conjunto el análisis de riesgo y el análisis de brecha ayudan a seleccionar las medidas de seguridad aplicables a la protección de los datos personales, cada uno de los mecanismos de seguridad consiste en un control que puede ser del tipo tecnológico, administrativo o de procedimiento y su implementación debe realizarse definiendo un plan de trabajo.*

*El plan de trabajo en el Documento de Seguridad es una parte medular, ya que es donde se detalla las acciones tomadas para implementar las medidas de seguridad, además, se especifican los recursos del tipo económico, humano o de cualquier otra naturaleza que la Comisión Nacional adoptará.*

*En este sentido, se solicita se confirme la clasificación de información como* ***RESERVADA****, referente a la información contenida en el citado Documento de Seguridad cuyos datos se enuncian a continuación:*

1. *Nombre, cargo y correo electrónico institucional de los operadores de los sistemas de tratamiento de datos personales referidos en el Documento de Seguridad;*
2. *Características del lugar físico donde se resguardan los sistemas de tratamiento de datos personales;*
3. *Medidas de seguridad:*
   a) *Medidas actuales:*
      - *Descripción de las medidas actuales.*
   b) *Análisis de Riesgo:*
      - *Riesgo/amenaza;*
      - *Factor de riesgo;*
      - *Clasificación de factor;*
      - *Control de factor;*

- *Valoración de riesgo:*
  - *Probabilidad de que ocurra; y*
  - *Valor.*

c) *Identificación del análisis de brecha; y*

d) *Plan de Trabajo:*
- *Actividad;*
- *Evidencia entregable.*

4. *Diagrama de arquitectura de seguridad en la que es posible apreciar el flujo datos de los sistemas a través de las redes electrónica que interconectan los equipos.*

*Lo anterior, toda vez que es información que compromete la seguridad pública, al poner en peligro las funciones a cargo de la CONDUSEF, tendientes a preservar y resguardar los datos personales de los usuarios de servicios financieros que acuden ante ella a resolver sus controversias. Así como al revelar datos que pudieran ser aprovechados para conocer la capacidad de reacción de la Comisión Nacional ante alguna contingencia, ya que las medidas de seguridad implementadas para proteger los datos personales en esta Comisión Nacional deben ser efectivas y eficientes, mitigando todos los posibles riesgos, en consecuencia, no es posible proporcionar el citado documento sin reservar la información referida.*

*En tal virtud, los artículos 114 de la Ley General de Transparencia y Acceso a la Información Pública y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen que las causales de reserva se deberán fundar y motivar, a través de la aplicación de la prueba de daño, a que se refiere el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, el cual dispone lo siguiente:*

> ***"Artículo 104.*** *En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
>
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio."*

*Asimismo, el artículo* ***Trigésimo tercero*** *de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, establece lo siguiente:*

> ***"Trigésimo tercero.*** *Para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General, los sujetos obligados atenderán lo siguiente:*
>
> *I. Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;*
> *II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;*
> *III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate;*
> *IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;*
> *V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y*

VI. *Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información."*

*En cumplimiento a lo establecido en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, en correlación con el Trigésimo Tercero de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, a continuación se mencionan los argumentos lógico - jurídicos respecto a la prueba de daño, a fin de que el H. Comité de Transparencia de la CONDUSEF, confirme la clasificación de información como* ***RESERVADA****, de los siguientes datos:*

1. *Nombre, cargo y correo electrónico institucional de los operadores de los sistemas de tratamiento de datos personales referidos en el Documento de Seguridad;*
2. *Características del lugar físico donde se resguardan los sistemas de tratamiento de datos personales;*
3. *Medidas de seguridad:*
   a) *Medidas actuales:*
      - *Descripción de las medidas actuales.*
   b) *Análisis de Riesgo:*
      - *Riesgo/amenaza;*
      - *Factor de riesgo;*
      - *Clasificación de factor;*
      - *Control de factor;*
      - *Valoración de riesgo:*
        - *Probabilidad de que ocurra; y*
        - *Valor.*
   c) *Identificación del análisis de brecha; y*
   d) *Plan de Trabajo:*
      - *Actividad;*
      - *Evidencia entregable.*
4. *Diagrama de arquitectura de seguridad en la que es posible apreciar el flujo datos de los sistemas a través de las redes electrónica que interconectan los equipos.*

*Toda vez, que de dar a conocer la información se causaría lo siguiente:*

**1. *Nombre, cargo y correo electrónico institucional de los operadores de los sistemas de tratamiento de datos personales referidos en el documento de seguridad:***

*Dicha información encuadra en el supuesto de clasificación de reserva prevista en la fracción I de los artículos 113 de la Ley General de Transparencia y Acceso a la Información Pública; 110 Ley Federal de Transparencia y Acceso a la Información Pública y Décimo Octavo primero y último párrafo de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, por lo que se proporciona la siguiente prueba de daño:*

I. *La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo a la seguridad de las personas y de la Entidad. La difusión de la información representa un riesgo real en tanto que se facilitaría la identificación de las personas cuyas funciones están encaminadas a preservar la seguridad de los sistemas de tratamiento de datos personales y conocen información sobre los mismos; lo que genera un riesgo demostrable, pues derivado de las funciones operativas que realizan los servidores públicos referidos, la identificación de dichos servidores públicos permitiría la perpetración de actos tendientes a nulificar la efectividad de sus actividades; así como un riesgo identificable, ya que se pondría en riesgo la seguridad de los sistemas de tratamiento de datos personales de la Entidad, toda vez que los servidores públicos*

*asignados para preservar la seguridad conocen de manera detallada las funciones como operadores de los sistemas o como responsables de implementación de nuevas medidas de seguridad.*

II. *El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. Al permitir que se identifique al personal sustantivo que se desempeña como servidor público con funciones de operación y seguridad en los sistemas, se pone en riesgo su seguridad y la de Entidad. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran promover alguna coerción o relación directa con estos servidores públicos, inhibiendo las tareas propias de sus funciones, con el efecto de vulnerar los sistemas de tratamiento de datos personales de esta Comisión Nacional y el interés general de la protección de los datos personales. La limitación de derecho de acceso se justifica a partir del interés público de garantizar la seguridad de las personas que conocen la información sensible frente al beneficio de hacerlos identificables.*

III. *La limitación se adecua al principio de proporcionalidad y representa el menos restrictivo disponible para evitar perjuicio. Resguardar únicamente la información que haga identificable al personal que opera los sistemas referidos o responsable del plan de trabajo, es proporcional frente al derecho de acceso a la información del que gozan todas las personas; esto, pues el resguardo sólo de los datos que podrían poner en riesgo la integridad personal y seguridad de los servidores públicos, así como de los sistemas de tratamiento de datos personales de la Comisión Nacional, por lo que se constituye, que es el medio que menos restringe el acceso a la información. Más aún cuando la limitación se establece con una temporalidad plenamente identificada.*

**2. *Características del lugar donde se resguardan los sistemas de tratamiento de datos personales:***

*Dicha información encuadra en el supuesto de clasificación de reserva prevista en la fracción I de los artículos 113 de la Ley General de Transparencia y Acceso a la Información Pública y 110 Ley Federal de Transparencia y Acceso a la Información Pública y Décimo Octavo primero y último párrafo de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, por lo que se proporciona la siguiente prueba de daño:*

I. *La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo, bajo un riesgo activo de amenazas y vulnerabilidades respecto a la seguridad de la información que obra en la Entidad. La difusión de la información representa un riesgo real en tanto que se facilitaría la identificación de las características del lugar donde se resguardan los sistemas de tratamiento de datos personales los cuales pueden ser soportes físicos y electrónicos, en los cuales se realiza la descripción con detalles sobre las características físicas de la oficina, almacén o bodega donde se resguardan dichos soportes, o bien en el soporte electrónico en donde se albergue la citada información; lo que genera un riesgo demostrable, pues derivado de las funciones operativas que realizan los referidos sistemas se realizaría una identificación de las características del lugar donde se resguardan los citados sistemas, por lo que las medidas de seguridad adoptadas para el resguardo de la información se revelarían, lo que permitiría la perpetración de actos tendientes a nulificar la efectividad de sus propósitos, así como un riesgo identificable, ya que se pondría en riesgo la seguridad de la información que obra en los sistemas de tratamiento de datos personales de la Entidad.*

II. *El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. Al permitir que se identifique las funciones de operación y de seguridad de los sistemas de tratamiento de datos personales, se pone en riesgo su seguridad y la de Entidad. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran promover alguna coerción a los sistemas, inhibiendo las tareas propias de sus funciones, con el efecto de vulnerar los sistemas de tratamiento de datos personales de*

*esta Comisión Nacional y el interés general de la protección de los datos personales. La limitación de derecho de acceso se justifica a partir del interés público de garantizar la seguridad de las personas que conocen la información sensible frente al beneficio de hacerlos identificables.*

III. *La limitación se adecua al principio de proporcionalidad y representa el menos restrictivo disponible para evitar perjuicio. Resguardar únicamente la información que haga las medidas de seguridad adoptadas para salvaguardar el tratamiento de datos personales, es proporcional frente al derecho de acceso a la información del que gozan todas las personas; esto, pues el resguardo sólo de los datos que podrían poner en riesgo la seguridad de los sistemas de tratamiento de datos personales de la Comisión Nacional, por lo que se constituye, que es el medio que menos restringe el acceso a la información. Más aún cuando la limitación se establece con una temporalidad plenamente identificada.*

3. ***Medidas de seguridad: Medidas actuales: Descripción de las medidas actuales; Análisis de Riesgo: Riesgo/amenaza; Factor de riesgo; Clasificación de factor; Control de factor; Valoración de riesgo: Probabilidad de que ocurra y Valor; Identificación del análisis de brecha; y Plan de Trabajo: Actividad; Evidencia entregable:***

*Dicha información encuadra en el supuesto de clasificación de reserva prevista en la fracción I de los artículos 113 de la Ley General de Transparencia y Acceso a la Información Pública y 110 Ley Federal de Transparencia y Acceso a la Información Pública y Décimo Octavo primero y último párrafo de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, por lo que se proporciona la siguiente prueba de daño:*

I. *La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo, bajo un riesgo activo de amenazas y vulnerabilidades respecto a la seguridad de la información que obra en la Entidad. La difusión de la información representa un riesgo real en tanto que se facilitaría la identificación de las medidas de seguridad implementadas para preservar la seguridad de los sistemas de tratamiento de datos personales; lo que genera un riesgo demostrable, pues derivado de las funciones operativas que realizan los referidos sistemas se realizaría una identificación del plan de trabajo y de las medidas de seguridad adoptadas para el resguardo de la información, lo que permitiría la perpetración de actos tendientes a nulificar la efectividad de sus propósitos así como un riesgo identificable, ya que se pondría en riesgo la seguridad de la información que obra en los sistemas de tratamiento de datos personales de la Entidad, toda vez que se revelaría de manera detallada las acciones tomadas para implementar las medidas de seguridad de las funciones y el tratamiento de los sistemas, así como la implementación de nuevas medidas de seguridad aplicables a la protección de los datos personales, que pueden ser del tipo tecnológico, administrativo o de procedimiento.*

II. *El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. Al permitir que se identifique las funciones de operación y de seguridad de los sistemas de tratamiento de datos personales, se pone en riesgo su seguridad y la de Entidad. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran promover alguna coerción a los sistemas, inhibiendo las tareas propias de sus funciones, con el efecto de vulnerar los sistemas de tratamiento de datos personales de esta Comisión Nacional y el interés general de la protección de los datos personales. La limitación de derecho de acceso se justifica a partir del interés público de garantizar la seguridad de las personas que conocen la información sensible frente al beneficio de hacerlos identificables.*

III. *La limitación se adecua al principio de proporcionalidad y representa el menos restrictivo disponible para evitar perjuicio. Resguardar únicamente la información que haga las medidas de seguridad adoptadas para salvaguardar el tratamiento de datos personales, es proporcional frente al derecho de acceso a la información del que gozan todas las*

*personas; esto, pues el resguardo sólo de los datos que podrían poner en riesgo la seguridad de los sistemas de tratamiento de datos personales de la Comisión Nacional, por lo que se constituye, que es el medio que menos restringe el acceso a la información. Más aún cuando la limitación se establece con una temporalidad plenamente identificada.*

4. ***Diagrama de arquitectura de seguridad en la que es posible apreciar el flujo datos de los sistemas a través de las redes electrónica que interconectan los equipos:***

*Dicha información encuadra en el supuesto de clasificación de reserva prevista en la fracción I de los artículos 113 de la Ley General de Transparencia y Acceso a la Información Pública y 110 Ley Federal de Transparencia y Acceso a la Información Pública y Décimo Octavo primero y último párrafo de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas, por lo que se proporciona la siguiente prueba de daño:*

I. *La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo, bajo un riesgo activo de amenazas y vulnerabilidades respecto a la seguridad de la información que obra en la Entidad. La difusión de la información representa un riesgo real en tanto que se facilitaría la identificación de las medidas de seguridad implementadas para preservar la seguridad de los sistemas de tratamiento de datos personales; ya que el diagrama de la arquitectura de seguridad se aprecia el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema; lo que genera un riesgo demostrable, pues derivado de las funciones operativas que realizan los referidos sistemas se realizaría una identificación de las entradas, salidas y repositorios de las medidas de seguridad adoptadas para el resguardo de la información, lo que permitiría la perpetración de actos tendientes a nulificar la efectividad de sus propósitos, así como un riesgo identificable, ya que se pondría en riesgo la seguridad de la información que obra en los sistemas de tratamiento de datos personales de la Entidad, toda vez que se revelaría de manera detallada las acciones tomadas para implementar las medidas de seguridad aplicables a la protección de los datos personales.*

II. *El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda. Al permitir que se identifique las funciones de operación y de seguridad de los sistemas de tratamiento de datos personales, se pone en riesgo su seguridad y la de la Entidad. Lo anterior ante la probabilidad de que personas con pretensiones delictivas pudieran promover alguna coerción a los sistemas, inhibiendo las tareas propias de sus funciones, con el efecto de vulnerar los sistemas de tratamiento de datos personales de esta Comisión Nacional y el interés general de la protección de los datos personales. La limitación de derecho de acceso se justifica a partir del interés público de garantizar la seguridad de las personas que conocen la información sensible frente al beneficio de hacerlos identificables.*

III. *La limitación se adecua al principio de proporcionalidad y representa el menos restrictivo disponible para evitar perjuicio. Resguardar únicamente la información que haga las medidas de seguridad adoptadas para salvaguardar el tratamiento de datos personales, es proporcional frente al derecho de acceso a la información del que gozan todas las personas; esto, pues el resguardo sólo de los datos que podrían poner en riesgo la seguridad de los sistemas de tratamiento de datos personales de la Comisión Nacional, por lo que se constituye, que es el medio que menos restringe el acceso a la información. Más aún cuando la limitación se establece con una temporalidad plenamente identificada."*

Por consiguiente, la Lic. Elizabeth Araiza Olivares, Directora General de Procedimientos Jurídicos, Defensoría y Tecnologías Financieras de la Vicepresidencia Jurídica, persona facultada para recibir y dar trámite a las solicitudes de Información Pública, Acceso a Datos Personales, Recursos de Revisión y en todo lo relativo a las

obligaciones a cargo de la Unidad de Transparencia indicó que de los citados argumentos se desprende que la prueba de daño se comprueba, ya que el equilibrio entre el perjuicio y el beneficio a favor del interés público se ve superado, por tratarse de información específica de datos relacionados con la seguridad de la información en posesión de esta Comisión Nacional.

De igual manera señaló, que el periodo de reserva, se solicita sea de **5 años,** tomando en consideración que dicha temporalidad es adecuada y proporcional para la protección del interés público, atendiendo la naturaleza de la información, de conformidad con los artículos 101 de la Ley General de Transparencia y Acceso a la Información Pública y 99 de la Ley Federal de Transparencia y Acceso a la Información Pública y Trigésimo Cuarto, de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas.

Por todo lo antes expuesto, la Lic. Elizabeth Araiza Olivares, Directora General de Procedimientos Jurídicos, Defensoría y Tecnologías Financieras de la Vicepresidencia Jurídica, persona facultada para recibir y dar trámite a las solicitudes de Información Pública, Acceso a Datos Personales, Recursos de Revisión y en todo lo relativo a las obligaciones a cargo de la Unidad de Transparencia, con fundamento en lo establecido en los artículos 3, fracción XXI, 4, 24, fracción VI, 44, fracción II, 100, 101, 104, 106, fracción I, 108, 111, 113, fracción I y 137 de la Ley General de Transparencia y Acceso a la Información Pública; 3, 11, fracción VI, 65, fracción II, 97, 98, fracción I, 99, 100, 105, 108, 110, fracción I, 111, 118, y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública y Segundo, fracción XVIII, Cuarto, Séptimo, fracción I, Noveno, Décimo Octavo párrafos primero y último, Trigésimo Tercero, Trigésimo Cuarto, Quincuagésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas; Segundo, fracción XXV, Vigésimo Quinto y Vigésimo Sexto de los Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública, solicitó al H. Comité de Transparencia de la CONDUSEF, **confirmar la clasificación de información** como **RESERVADA**, respecto de los siguientes datos:

1. Nombre, cargo y correo electrónico institucional de los operadores de los sistemas de tratamiento de datos personales referidos en el Documento de Seguridad;
2. Características del lugar físico donde se resguardan los sistemas de tratamiento de datos personales;
3. Medidas de seguridad:
    a) Medidas actuales:
        - Descripción de las medidas actuales.
    b) Análisis de Riesgo:
        - Riesgo/amenaza;
        - Factor de riesgo;
        - Clasificación de factor;
        - Control de factor;
        - Valoración de riesgo:
            - Probabilidad de que ocurra; y
            - Valor.
    c) Identificación del análisis de brecha; y
    d) Plan de Trabajo:
        - Actividad;
        - Evidencia entregable.
4. Diagrama de arquitectura de seguridad en la que es posible apreciar el flujo datos de los sistemas a través de las redes electrónica que interconectan los equipos.

Y en su caso autorizar y confirmar la versión pública del **Documento de Seguridad para el Tratamiento de Datos Personales 2020**, para dar atención a la solicitud de información con número de folio **0637000014620.**

Por lo anterior, los Integrantes del Comité de Transparencia revisaron y analizaron la motivación, el fundamento contenido en los argumentos lógicos – jurídicos, así como las manifestaciones vertidas por el área solicitante, resolviendo por unanimidad de votos **CONFIRMAR** la clasificación de la información en su modalidad de **Reservada** de los datos contenidos en el **Documento de Seguridad para el Tratamiento de Datos Personales 2020**, por el plazo de **5 años**, de acuerdo a lo establecido en los artículos 101 de la Ley General de Transparencia y Acceso a la Información Pública y 99 de la Ley Federal de Transparencia y Acceso a la Información Pública y

Trigésimo Cuarto, de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas; así como **AUTORIZAR y CONFIRMAR** la versión pública presentada, a fin de que se de atención en tiempo y forma, respecto a lo solicitado en el folio con número **0637000014620**.

Asimismo, los Integrantes del Comité de Transparencia señalaron que la clasificación de la información en su modalidad de Reservada, la elaboración de la versión pública, así como la conservación, guarda y custodia de la información solicitada y proporcionada resulta ser responsabilidad de la Unidad Administrativa Competente, es decir de la **Unidad de Transparencia** de esta **Comisión Nacional.**

En virtud de lo anteriormente expuesto, los Integrantes del Comité de Transparencia emiten la siguiente resolución:

> **Resolución.** El Comité de Transparencia de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros de conformidad con lo dispuesto en los artículos 3, fracción XXI, 4, 24, fracción VI, 44, fracción II, 100, 101, 104, 106, fracción I, 108, 111, 113, fracción I y 137 de la Ley General de Transparencia y Acceso a la Información Pública; 3, 11, fracción VI, 65, fracción II, 97, 98, fracción I, 99, 100, 105, 108, 110, fracción I, 111, 118, y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública y Segundo, fracción XVIII, Cuarto, Séptimo, fracción I, Noveno, Décimo Octavo párrafos primero y último, Trigésimo Tercero, Trigésimo Cuarto, Quincuagésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas; Segundo, fracción XXV, Vigésimo Quinto y Vigésimo Sexto de los Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública, **CONFIRMA** la Clasificación de la Información como Reservada contenida en el **Documento de Seguridad para el Tratamiento de Datos Personales 2020** y **AUTORIZA y CONFIRMA** la versión pública propuesta por la Unidad de Transparencia. En consecuencia se instruye a la Unidad de Transparencia para que se publique la presente resolución y se le haga del conocimiento al solicitante, a través de la Plataforma Nacional de Transparencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a efecto de dar la atención en tiempo y forma a la solicitud de información de mérito.

Finalmente al no haber más asuntos que tratar, la Lic. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia, dio por concluida la Décima Primera Sesión Extraordinaria del 2020 del Comité de Transparencia de la CONDUSEF, siendo las 14:30 horas del día 03 de julio de 2020.

**INTEGRANTES DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS**

**Lic. Elizabeth Ivonne Noriega Aguilar**
Vicepresidenta Jurídica y Titular de la Unidad de Transparencia.

**Lic. Ana Clara Fragoso Pereida**
Titular del Órgano Interno de Control en la CONDUSEF.

**Lic. Eduardo Saúl Reyes Gallegos**
Director de Planeación y Finanzas de la Vicepresidencia de Planeación y Administración.
Designado para asistir en suplencia por ausencia del C.P. Fernando Enrique Zambrano Suárez, Vicepresidente de Planeación y Administración y encargado de la Dirección de Gestión y Control Documental.