ACTA DE LA DÉCIMA SÉPTIMA SESIÓN EXTRAORDINARIA DE 2024 DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

El día jueves 30 de mayo de 2024 a las 17:00 hrs, por vía remota, se reunió el Comité de Transparencia de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), a efecto de desarrollar la Décima Séptima Sesión Extraordinaria del año 2024, solicitada por la Unidad de Transparencia, por lo que se dieron cita sus integrantes: la Lic. Elizabeth Araiza Olivares, Directora General de Procedimientos Jurídicos, Defensoría y Tecnologías Financieras, en suplencia de la Mtra. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia, el Lic. Federico Carlos Chávez Osnaya, Titular del Área de Responsabilidades, en suplencia del Mtro. Manuel Juan Corvera Caraza, Titular del Órgano Interno de Control Específico en la CONDUSEF y la Ing. Nancy Candelaria Cortés García, Directora de Gestión y Control Documental, de la Vicepresidencia de Planeación y Administración, asimismo se contó con la asistencia de la Lic. Verónica Meléndez Valdez, Directora de Procedimientos Jurídicos y Tecnologías Financieras y Secretaria Técnica del Comité de Transparencia en suplencia de la Lic. Elizabeth Araiza Olivares.

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

La Lic. Elizabeth Araiza Olivares dio la bienvenida a los Integrantes del Comité de Transparencia a la sesión, agradeciendo su presencia y participación, cediendo el uso de la voz a la Secretaria Técnica, quien enseguida tomó lista de asistencia y verificó la existencia de quórum, advirtiendo que se cumple con el número de Integrantes presentes para sesionar de manera válida.

II.- Aprobación del Orden del Día.

A continuación, la Lic. Elizabeth Araiza Olivares requirió a la Secretaria Técnica dar lectura al Orden del Día; conforme a la instrucción, la Secretaria Técnica informó los puntos enlistados solicitando su aprobación a los Integrantes del Comité, mismos que acordaron emitir el siguiente Acuerdo:

> **CT/CONDUSEF/17ª/SESIÓNEXTRAORDINARIA/01/ACUERDO/2024**: El Comité de Transparencia de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros aprueba el orden del día de la Décima Séptima Sesión Extraordinaria del año 2024.

III.- Desarrollo de la Sesión

La Lic. Elizabeth Araiza Olivares solicitó a la Secretaria Técnica dar lectura a los asuntos a tratar, mismos que se citan a continuación:

- Revisión del **Programa de capacitación en materia de transparencia, acceso a la información, protección de datos personales y temas relacionados del año 2024**, de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), presentado por la **Unidad de Transparencia**, con el objeto de que se apruebe, o en su caso se modifique, a fin de que sea enviado al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y se aplique el mismo a las personas servidoras públicas de esta Comisión Nacional.

- Revisión de la **Política Interna de Protección de Datos Personales en Posesión de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)**, presentado por la **Unidad de Transparencia**, con el objeto de que se apruebe, o en su caso se modifique, a fin de que sea publicado en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

- Revisión de los argumentos lógicos - jurídicos remitidos por la **Unidad de Transparencia**, a fin de que se confirme, modifique o revoque la clasificación de información en su modalidad de reservada del **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF 2020**, a fin de que sea publicado en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

Por consiguiente, la Lic. Elizabeth Araiza Olivares presentó ante el Comité de Transparencia el **PRIMER ASUNTO** a tratar, el cual se indica a continuación:

- Revisión del **Programa de capacitación en materia de transparencia, acceso a la información, protección de datos personales y temas relacionados del año 2024**, de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), presentado por la **Unidad de Transparencia**, con el objeto de que se apruebe, o en su caso se modifique, a fin de que sea enviado al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y se aplique el mismo a las personas servidoras públicas de esta Comisión Nacional.

Por consiguiente, en su calidad de persona facultada para recibir y dar trámite a las solicitudes de Información Pública y 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 los artículos 45, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 61 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 22, fracción I, del Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y como Enlace de Capacitación en Transparencia de la CONDUSEF ante el INAI, en uso de la voz sometió a consideración del Comité de Transparencia lo que a continuación se expone:

En cumplimiento con las obligaciones que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros tiene respecto a la capacitación y actualización de forma permanente a todos sus servidores públicos en materia de Transparencia, Acceso a la Información, Protección de Datos Personales y Archivos, de conformidad con lo dispuesto en los artículos 24, fracción III; 31, fracción X; 42, fracción VII; 44, fracciones V y VI; 53, primer párrafo; y 68, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; 12, fracción III; 30, fracción III; 33, fracción VIII; 35, fracción VII; 84, fracción VII; 89, fracción XXVI; 91, fracción XIV; 92, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 11, fracción III; 21, fracción X; 63, tercer párrafo; 65, fracciones V y VI, de la Ley Federal de Transparencia y Acceso a la Información Pública; la Unidad de Transparencia, a través del Enlace de Capacitación en Transparencia de la CONDUSEF ante el INAI presenta para su aprobación, o en su caso, modificación el **Programa de Capacitación en materia de Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados del año 2024 (PCTAIPDP)**, a fin de que sea enviado al citado Instituto y se aplique el mismo a los servidores públicos de esta Comisión Nacional.

Precisando que la capacitación se realizará en la modalidad presencial a distancia a través de la plataforma denominada Sistema para la Administración de la Capacitación Presencial (SACP) del INAI, en virtud de que la Dirección General de Capacitación del INAI en el Taller de Planeación de la Red por una Cultura de Transparencia en el Ámbito Federal, celebrado el día 24 de abril de 2024, informó que el Centro Virtual de Capacitación en Acceso a la Información y Protección de Datos (CEVINAI) no se encuentra en funcionamiento, toda vez que se encuentra en curso el proceso administrativo para la contratación de almacenamiento de cómputo en la nube, así como para la realización de mejoras con el objeto de que brinde un servicio más eficiente a los usuarios.

Derivado de lo anterior, la capacitación para el presente ejercicio solo se aplicará a las personas servidoras públicas con perfiles específicos de acuerdo al ejercicio de las facultades, funciones y competencias que la normativa les confiera, relacionado con el cupo sujeto a disponibilidad de lugares, conforme a lo siguiente:

A.- Capacitación Básica

- Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública
- Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Introducción a la Ley General de Archivos
- Ética Pública

Personal a capacitar: Nuevos ingresos y promociones a nivel estructura.

B.- Capacitación Especializada

- Aviso de Privacidad

Personal a capacitar: Nuevos ingresos (Enlaces de Transparencia) y personal a nivel estructura de la Vicepresidencia de Unidades de Atención a Usuarios (Directores Generales, Directores de Área Y Titulares de las Unidades de Atención a Usuarios)

- Obligaciones de Transparencia y Carga de Información en el SIPOT
- Fundamentos del Documento de Seguridad en materia de protección de Datos Personales
- Elaboración del Documento de Seguridad

Personal a capacitar: Nuevas designaciones de Enlaces de Transparencia, así como aquellos Enlaces que no los han realizado.

- Clasificación de la Información y prueba de daño

Personal a capacitar: Personas especificas a nivel estructura por ingreso y designación de funciones en la atención de solicitudes de información y carga de información en el Sistema de Portales de Obligaciones de Transparencia (SIPOT)

Al respecto, los Integrantes del Comité de Transparencia revisaron y analizaron la información contenida en el **Programa de Capacitación en materia de Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados del año 2024**, así como las manifestaciones vertidas por el Enlace de Capacitación en Transparencia de la CONDUSEF, resolviendo por unanimidad de votos **APROBAR** el referido programa, a fin de que sea enviado en tiempo y forma al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y se aplique el mismo a los servidores públicos de esta Comisión Nacional, para que se actualicen en los aspectos teóricos, conceptuales y normativos fundamentales y especializados, en materia de transparencia, acceso a la información, protección de datos personales y archivos, con el objetivo que se gestione y aplique la normatividad vigente de manera eficiente y eficaz en la práctica de sus funciones.

Por lo antes expuesto y respecto a lo solicitado por la **Unidad de Transparencia**, el Comité de Transparencia emite el siguiente Acuerdo:

> **CT/CONDUSEF/17ª/SESIÓNEXTRAORDINARIA/02/ACUERDO/2024**: 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 24, fracción III; 31, fracción X; 42, fracción VII; 44, fracciones V y VI; 53, primer párrafo; y 68, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; 12, fracción III; 30, fracción III; 33, fracción VIII; 35, fracción VII; 84, fracción VII; 89, fracción XXVI; 91, fracción XIV; 92 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 11, fracción III; 21, fracción X; 63, tercer párrafo; 65, fracciones V y VI, de la Ley Federal de Transparencia y Acceso a la Información Pública, **APRUEBA** el **Programa de Capacitación en materia de Transparencia, Acceso a la Información, Protección de Datos Personales y temas relacionados** de la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros** para el ejercicio **2024**. En consecuencia se instruye a la Unidad de Transparencia para que se remita el referido programa al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a efecto de que la CONDUSEF cumpla

en tiempo y forma con lo requerido y se aplique el mismo a los servidores públicos de esta Comisión Nacional, para que se actualicen en los aspectos teóricos, conceptuales y normativos fundamentales y especializados, en materia de transparencia, acceso a la información, protección de datos personales y archivos, con el objetivo que se gestione y aplique la normatividad vigente de manera eficiente y eficaz en la práctica de sus funciones.

En otro orden, la Lic. Elizabeth Araiza Olivares presentó ante el Comité de Transparencia el **SEGUNDO ASUNTO** a tratar, el cual se indica a continuación:

- Revisión de la **Política Interna de Protección de Datos Personales en Posesión de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)**, presentado por la **Unidad de Transparencia**, con el objeto de que se apruebe, o en su caso se modifique, a fin de que sea publicado en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

Por consiguiente, en su calidad de persona facultada para recibir y dar trámite a las solicitudes de Información Pública y 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 los artículos 45, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 61 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 22, fracción I, del Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, somete a consideración del Comité de Transparencia la revisión de la **Política Interna de Protección de Datos Personales en Posesión de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)**, con el objeto de que se apruebe, o en su caso se modifique, a fin de que sea publicado en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

Asimismo, señalo que la referida política se elaboró en cumplimiento de lo previsto en el artículo 30, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), normatividad que manifiesta la creación de políticas de protección de datos personales exigibles al interior del responsable de los datos, para dar cumplimiento al principio de responsabilidad establecido por la misma Ley, asi como lo establecido por el artículo 47, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos).

Lo anterior, con el objetivo de garantizar el cumplimiento e incorporación de los principios y deberes respecto a protección de Datos Personales al Interior de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, estableciendo los componentes, procesos y requerimientos que deberán observarse en todo tratamiento de Datos Personales en este sujeto obligado, cuyo ámbito de aplicación será de observancia general y obligatoria para todas las personas servidoras públicas de la CONDUSEF que conforme a sus atribuciones realicen tratamiento de datos personales.

Asimismo, señaló que la citada Política Interna podrá ser actualizada o modificada en cualquier momento en cumplimiento al principio de responsabilidad.

En consecuencia, los integrantes del Comité de Transparencia revisaron y analizaron la **Política Interna de Protección de Datos Personales en Posesión de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros**, propuesta por la Unidad de Transparencia en cumplimiento a lo dispuesto en la LGPDPPSO y los referidos Lineamientos, resolviendo por unanimidad de votos **APROBAR** la emisión y la publicación en el portal electrónico oficial de esta Comisión Nacional, en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley

General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

En cumplimiento con lo anterior, el Comité de Transparencia emite el siguiente Acuerdo, en atención a lo requerido por la **Unidad de Transparencia:**

> **CT/CONDUSEF/17ª/SESIÓNEXTRAORDINARIA/03/ACUERDO/2024:** El Comité de Transparencia de la Comisión Nacional para la Protección y Defensa de los Usuario de Servicios Financieros, de conformidad con lo dispuesto en los artículos 23, 24, fracciones VII y VIII, 43, 44, fracción IX, 68, fracciones II y VI, de la Ley General de Transparencia y Acceso a la Información Pública; 30, fracción II, 83, fracciones I, II, IV y V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 9, 10, 11, fracciones VII y VIII, 16, 64 y 65, fracción IX, de la Ley Federal de Transparencia y Acceso a la Información Pública y 47, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, **APRUEBA** la emisión de la **Política Interna de Protección de Datos Personales en Posesión de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros**. En consecuencia, se instruye a la Unidad de Transparencia para que se publique en el portal electrónico oficial de esta Comisión Nacional, en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materiare, a efecto de que la CONDUSEF cumpla en tiempo y forma con los requerido y se notifique a través de los Enlaces de Transparencia el ámbito de aplicación que será de observancia general y obligatoria para todas las personas servidoras públicas de la CONDUSEF que conforme a sus atribuciones realicen tratamiento de datos personales.

En continuidad con la sesión, la Lic. Elizabeth Araiza Olivares presentó ante el Comité de Transparencia el **TERCER ASUNTO** a tratar, el cual se indica a continuación:

- Revisión de los argumentos lógicos - jurídicos remitidos por la **Unidad de Transparencia**, a fin de que se confirme, modifique o revoque la clasificación de información en su modalidad de reservada del **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF 2020**, a fin de que sea publicado en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

Por consiguiente, en su calidad de persona facultada para recibir y dar trámite a las solicitudes de Información Pública y 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 los artículos 45, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 61 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 22, fracción I, del Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, mediante memorándum número **VJ/UT/029/2024** de fecha 29 de mayo de 2024, somete a consideración del Comité de Transparencia lo siguiente:

Con base en lo establecido en los artículos 3, fracción XXI, 4, 24, fracción VI, 44, fracción II, 100, 101, 104, 106, fracción II, 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 II, 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 II, 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, se solicita se confirme, modifique o revoque la clasificación del **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF 2020** en su modalidad de **RESERVADA**, únicamente respecto a la siguiente información:

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, de ser procedente se apruebe la versión pública de la referida documental para que sea publicada en el portal electrónico oficial de esta Comisión Nacional en el apartado de **"Protección de Datos Personales"** en cumplimiento al referido Programa de Evaluación Anual, conforme los motivos y circunstancias que a continuación se exponen:

La CONDUSEF, como Sujeto Obligado, tiene la obligación de otorgar acceso a los documentos que se encuentren en sus archivos o que esté obligada a documentar de acuerdo con sus facultades, competencias o funciones, en el formato en que el solicitante manifieste, de entre aquellos formatos existentes, conforme a las características físicas de la información o del lugar donde se encuentre y así lo permita, ello en términos de lo previsto en los artículos 129, primer párrafo de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Lo anterior resulta relevante, ya que la información contenida en el **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF** resulta ser de naturaleza pública, toda vez que toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona de conformidad con lo dispuesto en los artículos 6, apartado A, fracción I de la Constitución Política de los Estados Unidos Mexicanos; 3, párrafo primero de la Ley Federal de Transparencia y Acceso a la Información Pública y 4, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública.

Sin embargo, el efectivo acceso a la información en posesión de los sujetos obligados también se encuentra sujeta a un régimen de excepciones que la propia normatividad establece para limitar la publicidad de esta, tal y como lo disponen los artículos 3, párrafo primero de la Ley Federal de Transparencia y Acceso a la Información Pública; 4, párrafo segundo, 11, de la Ley General de Transparencia y Acceso a la Información Pública.

Bajo esa tesitura, el **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF**, contienen información que por su carácter debe ser clasificada como **RESERVADA**, de acuerdo con 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 precisa 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, 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.

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 fundar la clasificación, al citar la fracción y la hipótesis de la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento especifico del presente ordenamiento y cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;*
> *II. Se deberá motivar la clasificación, señalando las circunstancias de modo, tiempo y lugar que acrediten el vínculo entre la difusión de la información y la afectación al interés público o a la seguridad nacional;*
> *III. Se deberán precisar las razones objetivas por las que la apertura de la información generaría un riesgo de perjuicio real, demostrable e identificable al interés jurídico tutelado de que se trate;*
> *IV. Mediante una ponderación entre la medida restrictiva y el derecho de acceso a la información, deberán justificar y probar objetivamente mediante los elementos señalados en la fracción anterior, que la publicidad de la información solicitada generarla un riesgo de perjuicio que supera al interés público de que la información se difunda;*
> *V. Deberán elegir y justificar la opción de excepción al derecho de acceso a la información que menos lo restrinja y que sea adecuada y proporcional para evitar el perjuicio al interés público, evitando siempre que sea posible la reserva absoluta de documentos o expedientes; y*
> *VI. En los casos en que se determine la clasificación total de la información, se deberán especificar en la prueba de daño, con la mayor claridad y precisión posible, los aspectos relevantes de la información clasificada que ayuden a cumplir con el objetivo de brindar certeza al solicitante."*

Por lo que, en cumplimiento con 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 refieren los argumentos lógico - jurídicos respecto a la prueba de daño, a fin de que el Comité de Transparencia de la CONDUSEF, cuente con los elementos necesarios para que confirme, modifique o revoque la clasificación del **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF 2020** como **RESERVADA**, únicamente de los datos antes referidos; en virtud de 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, 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.

Con lo anterior, queda debidamente fundada y motivada la necesidad de la reserva de la información y documentación, en términos de lo dispuesto en la fracción I, de los artículos 113 de la Ley General de Transparencia y Acceso a la Información Pública y 110, de la Ley Federal de Transparencia y Acceso a la Información Pública y en el Lineamiento 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.

Ahora bien, respecto del 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, o bien, hasta que se extingan las causas que dieron origen a su clasificación, toda vez que dicha temporalidad es adecuada y proporcional para la protección del interés público, además de que la reserva constituye una medida temporal de restricción de la información, por lo que, se considera que no es una medida excesiva ni desproporcional, esto atendiendo a lo establecido en los preceptos legales inherentes de la materia, de conformidad con los artículos 101 de la Ley General de Transparencia y Acceso a la Información y 99 de la Ley Federal de Transparencia y Acceso a la Información y Trigésimo Cuarto, de los Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas. Cabe señalar que el periodo de reserva correrá a partir de la fecha en que la que se clasifique la citada información.

Por todo lo antes expuesto, con fundamento en lo establecido en los artículos 3, fracción XXI, 4, 24, fracción VI, 44, fracción II, 100, 101, 104, 106, 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 II, 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 II, 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, se pide al Comité de Transparencia de la CONDUSEF se confirme, modifique o revoque la clasificación del **Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF 2020** en su modalidad de **RESERVADA**, y en su caso se apruebe la versión pública propuesta.

Por consiguiente, los Integrantes del Comité de Transparencia analizaron la motivación y el fundamento dispuesto en el memorándum número **VJ/UT/029/2024** de fecha 29 de junio de 2024, así como las manifestaciones vertidas por la Unidad Administrativa Competente, acreditando con ello, que la información y documentación que contiene el Documento de Seguridad para el Tratamiento de Datos Personales 2020 de esta Comisión Nacional está sujeta a la protección de este Organismo como reservada, de conformidad con los artículos 104, 113 fracción I de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracciónXI de la Ley Federal de Transparencia y Acceso a la Información Pública, en correlación con lo antes referido, el Trigésimo y Trigésimo Tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

Derivado de lo anterior, el Comité de Transparencia resolvió por unanimidad de votos **CONFIRMAR** la clasificación de la información y documentación del Documento de Seguridad para el Tratamiento de Datos Personales 2020 como **RESERVADA**, únicamente respecto a la siguiente información:

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, por el periodo de **5 años**, comprendido del día **30 de mayo del 2024 y hasta el día 30 de mayo del 2029**, o bien, hasta que se extingan las causas que dieron origen a su clasificación.

En consecuencia, se instruye a la Unidad de Transparencia para que se publique el Documento de Seguridad en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

Asimismo, los Integrantes del Comité de Transparencia señalaron que la clasificación de la información y documentación en su modalidad de reservada, así como su conservación, guarda y custodia resulta ser responsabilidad de la Unidad Administrativa Competente, es decir de la **Unidad de Transparencia** de la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.**

Por lo anteriormente expuesto, y en atención a lo requerido por la **Unidad de Transparencia** de la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros**, el Comité de Transparencia a efecto de proveer de legalidad y certeza jurídica dicta el siguiente Acuerdo:

> **CT/CONDUSEF/17ª/SESIÓNEXTRAORDINARIA/04/ACUERDO/2024**: 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 6, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos; 3, fracción XXI, 4, 24, fracción VI, 44, fracción II, 100, 101, 104, 106, fracción II, 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 II, 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 II, 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, a efecto de proveer de legalidad y certeza jurídica **CONFIRMA** la clasificación de la información y documentación contenida en el Documento de Seguridad para el Tratamiento de Datos Personales de la CONDUSEF 2020, por el periodo de 5 años, comprendido del día 30 de mayo del 2024 y hasta el día 30 de mayo del 2029, o bien, hasta que se extingan las causas que

dieron origen a su clasificación. En consecuencia, se instruye a la Unidad de Transparencia para que se publique el Documento de Seguridad en el portal electrónico oficial de esta Comisión Nacional en el apartado de "Protección de Datos Personales" en cumplimiento al Programa de Evaluación Anual 2024, de los sujetos obligados del ámbito público federal, en relación con el desempeño en el cumplimiento de las disposiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable en la materia.

Finalmente, al no haber más asuntos que tratar y agotado el Orden del Día, la Lic. Elizabeth Araiza Olivares dio por concluida la Décima Séptima Sesión Extraordinaria del año 2024 del Comité de Transparencia de la CONDUSEF, siendo las 18:00 horas del día 30 de mayo de 2024.

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

Lic. Elizabeth Araiza Olivares
Directora General de Procedimientos Jurídicos, Defensoría y Tecnologías Financieras.
En suplencia de la Mtra. Elizabeth Ivonne Noriega Aguilar, Vicepresidenta Jurídica y Titular de la Unidad de Transparencia de la CONDUSEF.

Lic. Federico Carlos Chávez Osnaya
Titular del Área de Responsabilidades del Órgano Interno de Control Específico en la CONDUSEF.
En suplencia del Mtro. Manuel Juan Corvera Caraza, Titular del Órgano Interno de Control Específico en la CONDUSEF.

Ing. Nancy Candelaria Cortés García
Directora de Gestión y Control Documental
adscrita a la Vicepresidencia de Planeación y Administración de la CONDUSEF.