Comité de Transparencia
Cuarta Sesión Extraordinaria
Asunto: **Resolución de versión pública.**
Solicitud de información 4220700007420.
Cumplimiento al RRA 06533/20
Ciudad de México, 25 de septiembre de 2020.

RESOLUCIÓN DERIVADA DE LA CUARTA SESIÓN EXTRAORDINARIA DE 2020 DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN NACIONAL DE ARBITRAJE MÉDICO

VISTOS: Para resolver el procedimiento de acceso a la información requerida mediante la solicitud al rubro citada, con base en los siguientes:

ANTECEDENTES

I. Con fecha 11 de septiembre de 2020, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), notificó a través de la Plataforma Nacional de Transparencia, la resolución del recurso de revisión 06533/20, mediante la cual **modificó** la respuesta otorgada por la Comisión Nacional de Arbitraje Médico, instruyéndola para el efecto que:

> *"...proporcione al particular la versión pública de su documento de seguridad, testando únicamente lo relativo al plan de trabajo que contiene, además, el análisis de riesgo y brecha del documento de seguridad, lo anterior con fundamento en el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; entregando las restantes secciones íntegras, incluyendo el inventario de datos personales.*
>
> *Asimismo, deberá someter dicha clasificación a su Comité de Transparencia para su aprobación, entregando a la persona inconforme el acta en la que consta dicha circunstancia.*

RESUELVE

PRIMERO.- *Con fundamento en lo que establece el artículo 157 fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública, se* ***MODIFICA*** *la respuesta emitida por la Comisión Nacional de Arbitraje Médico.*

> ***SEGUNDO.-*** *Con fundamento en los artículos 157, párrafo segundo de la Ley Federal de Transparencia y Acceso a la Información Pública, se instruye a la Comisión Nacional de Arbitraje Médico para que en un término no mayor a diez días hábiles, contados a partir del día hábil siguiente al de su notificación, cumpla con la presente resolución, y en términos del artículo 159, párrafo segundo, de la misma Ley informe a este Instituto sobre su cumplimiento."*
>
> (Sic)

II. El 14 de septiembre de 2020, el Secretariado Técnico del Comité de Transparencia, notificó la resolución recaída al medio de impugnación antes citado a la Dirección General de Difusión e Investigación y Encargo de la Dirección General de Calidad e Informática.

III. En cumplimiento a la referida resolución que emitió el INAI, la Dirección General de Difusión e Investigación y Encargo de la Dirección General de Calidad e Informática del 11 de septiembre de 2020, manifestó lo siguiente:

> *"...el Documento de Seguridad de la Comisión Nacional de Arbitraje Médico (CONAMED), en lo conducente a las secciones relativas al* ***Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo****, es susceptible de clasificarse como* ***reservado****, de conformidad con el artículo 110, fracción VII de la Ley Federal de Transparencia y acceso a la Información Pública y al Vigésimo Sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas; de manera que, con el hecho de divulgar la información requerida, se podría evitar la comisión de determinadas conductas delictivas contempladas en la ley penal vigente.*
>
> *Lo anterior, en el entendido de que, en los rubros del documento de seguridad antes invocados se detallan las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en el tratamiento, como pueden ser, hardware, software, personal del ente Responsable, los lugares donde se establecen las medidas de seguridad existentes y su cotejo respecto a las faltantes, por lo que su difusión potencializa*

el nivel de vulnerabilidad de las medidas de seguridad de los datos personales que posee la Comisión Nacional de Arbitraje Médico, lo cual podría derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros, previstos en los artículos 211 bis-1 al 211 bis-7 del código punitivo aludido.

Así, la divulgación del documento de seguridad, en lo referente al Plan de Trabajo, Análisis de Riesgo y Análisis de Brecha, incrementaría sustancialmente la posibilidad de que agentes externos a la Institución cometan algún ilícito, al vulnerar las medidas de seguridad que posee, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, facilitando que personas expertas en informática perturben las medidas de seguridad de los datos personales que posee éste órgano desconcentrado de la Secretaría de Salud.

En ese sentido, proporcionar las partes referidas del documento de seguridad podría obstruir la prevención de potenciales delitos informáticos de los sistemas en donde se efectúa el tratamiento de datos, ya que en este documento se describe detalladamente el tipo, ubicación y volumetría de los equipos así como sus características, tipo de puertos, protocolos de autentificación y de administración, sistema operativo, tipo de procesamiento, estándares de los equipos instalados en la CONAMED, limitando así la capacidad de la autoridad para evitar la comisión de delitos informáticos, vulnerando la seguridad de la información e infringiendo el contenido de lo establecido en el "Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información" (MAAGTICSI) en su capítulo IV de "Disposiciones para la seguridad de la información" Sección I de "Seguridad de la información", esto mediante los siguientes potenciales ataques dirigidos:

- *Ataques DDoS: Las siglas vienen de su nombre en inglés Distributed Denial of Service, es decir, denegación distribuida de servicio. Este tipo de ataque consiste en saturar la red con peticiones que hagan más lento al servidor y consuma más recursos por cada conexión. La forma más común de realizar un*

DDoS es a través de una red de bots, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.

- *Ataque DMA: ataque de acceso directo a memoria y permite que determinados dispositivos tengan acceso a la memoria del sistema de otro dispositivo. Este tipo de ataque aprovecha que los puertos DMA no usan la autenticación y control de acceso para la seguridad del contenido y trata de adquirir dicha información a través del acceso directo a una parte o la totalidad del espacio de direcciones de memoria física en la computadora, evitando todos los mecanismos de seguridad del sistema operativo o cualquier pantalla de bloqueo, robando así datos o claves criptográficas, instalar o ejecutar spyware y otros exploits, o modificar el sistema para permitir puertas traseras u otro malware.*

- *Eavesdropping: intercepción del tráfico de red, esto se consigue mediante el monitoreo de los paquetes que circulan por la red utilizando diversas herramientas como los Sniffers que pueden colocarse en alguna estación de trabajo o en el router, para obtener el contenido de datos en la búsqueda de cualquier tipo de información.*

- *Spoofing: técnica que consiste en falsificar a una entidad de confianza para que el usuario entregue información de acceso en una comunicación.*

Ahora bien, la divulgación de estos rubros representa un riesgo real, demostrable e identificable en perjuicio significativo del interés público, puesto que de exponerse implica la posible comisión del delito de acceso ilícito a sistemas y equipos de informática, descrito en los artículos 211 bis-1 al 211 bis-7 del Código Penal Federal, que a la letra señalan:

"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática el Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por

un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Bajo este tenor, se estima que entregar las partes relacionadas con el análisis de riesgo, análisis de brecha y el plan de trabajo, contenidos en el documento de seguridad, vulneraría los sistemas en donde se efectúa el tratamiento de datos, ya que se describe detalladamente los sistemas informáticos en donde se almacenan y procesan los datos personales como bases de datos, directorios, páginas web de

registro, lo que vulneraría la seguridad de la información de la Comisión Nacional de Arbitraje Médico.

Asimismo, el resguardo cobra importancia si se considera que una eventual divulgación implicaría conocer, copiar, modificar, destruir o provocar la pérdida de información, así como un daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado a la información personal de los Titulares de los datos. De manera que, revelar la información solicitada generaría daños inmediatos e inminentes, toda vez que daría a los particulares y/o delincuencia organizada, una oportunidad de conocer e incluso vulnerar datos importantes, las características de la tecnología y seguridad entre datos que, proporcionarlos radicaría en una flagrante violación de preceptos legales que ameritan sanciones por parte de las autoridades correspondientes.

En ese sentido, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo parcial del documento de seguridad contiene, el plan de trabajo, el análisis de riesgo y de brecha que implica llevar a cabo acciones de prevención de diversos delitos tipificados en el Código Penal Federal, lo cual cobra toral importancia si se considera que dichas conductas implican vulnerar las medidas de seguridad de los datos personales que se poseen.

Además, el resguardo de la información solicitada representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la reserva consiste en prevenir las conductas tipificadas en el Código Penal Federal, consistentes en acceso no autorizado a los sistemas, robos de información de expedientes médicos, suplantación de identidades, mismas que de llevarse a cabo podrían permitir la realización de diversos ataques a la infraestructura tecnológica y de sistemas que lo integran, con la consecuencia directa de la violación al principio de responsabilidad.

Por consiguiente, la difusión de dichos elementos del Documento de Seguridad incrementa significativamente la posibilidad de que terceras personas expertas en informática vulneren las medidas de seguridad, accediendo de forma no autorizada a los sistemas de datos que no son públicos, perturben las medidas de seguridad de los datos personales contenidas en el Sistema Integral de Gestión Ciudadana (SIGC) y Archivo de Trámite (Expedientes), por lo tanto, se

estima procedente su reserva, de conformidad con el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública."

(Sic)

IV. la Dirección General de Difusión e Investigación y Encargo de la Dirección General de Calidad e Informática, ha puesto a disposición del particular la versión pública del Documento de Seguridad de la Comisión Nacional de Arbitraje Médico.

V. La información suprimida en la versión pública, remitida para la atención del cumplimiento de la resolución, consiste en el **plan de trabajo, el análisis de riesgo y el análisis de brecha.**

VI. Con la respuesta de la unidad administrativa citada en antecedentes, este Comité de Transparencia procede a valorar lo manifestado.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para conocer y resolver el presente procedimiento de acceso a la información, de conformidad con lo dispuesto por los artículos 44, fracción II de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 65, fracción II, 97, párrafo sexto, 98, fracción I y 102 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).

SEGUNDO. Que en términos del artículo 97, párrafo tercero, de la LFTAIP; 100 LGTAIP; numerales Cuarto, Quinto y Noveno de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas; y los Lineamientos para la Organización y Conservación de los Archivos los titulares de las Áreas, entendiendo a estas últimas como aquellas previstas en el Reglamento Interior, estatuto orgánico respectivo o equivalente, son responsables de clasificar la información, al ser la instancia encargada de la producción de los documentos en el ámbito de sus atribuciones y los conocedores de la misma, al ser éstas las que están en posibilidad de identificar de acuerdo a las actividades que llevan a cabo, si cuentan o no con la información que da cumplimiento a las obligaciones de transparencia y si ésta es susceptible de ser información clasificada, por lo cual, la Dirección General de Difusión e Investigación y Encargo de la Dirección General de Calidad e Informática, y el generador de la información, así como el enlace designado para tales efectos, son estrictamente responsables de la elaboración y revisión de la versión pública con

los respectivos formatos y leyendas de clasificación la información en términos de las disposiciones aplicables.

TERCERO. La Dirección General de Difusión e Investigación y Encargo de la Dirección General de Calidad e Informática, clasificó como reservada la información descrita en el Antecedente IV por un periodo de cinco años, con fundamento en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública; y 97, 98 fracción II, 100, 108 y 110, fracción VII, la Ley Federal de Transparencia y Acceso a la Información Pública, y el numeral vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

CUARTO. En el presente considerando se analizará la procedencia de la clasificación reservada respecto a la información antes señalada, con fundamento en los preceptos legales antes invocados.

Al respecto, los preceptos de la LGTAIP prevén lo siguiente:

> *"Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:*
> ...
> *VII.* ***Obstruya la prevención o persecución de los delitos****;*
> ..."

Por su parte, los preceptos de la LFTAIP citados establecen:

> *"**Artículo 97.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
> *En el proceso de clasificación de la información, los sujetos obligados observarán, además de lo establecido en el Título Sexto de la Ley General, las disposiciones de la presente Ley.*
> *Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en la Ley General y la presente Ley.*
> *Los sujetos obligados deberán aplicar, de manera restrictiva y limitada, las excepciones al derecho de acceso a la información previstas en el presente Título y deberán acreditar su procedencia, sin ampliar las excepciones o supuestos de reserva o confidencialidad previstos en las leyes, de conformidad con lo establecido en la Ley General.*

Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen documentos o expedientes como reservados, ni clasificar documentos antes de dar respuesta a una solicitud de acceso a la información.
La clasificación de información reservada se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño."
*"**Artículo 98.** La clasificación de la información se llevará a cabo en el momento en que:*
II. Se determine mediante resolución de autoridad competente, o;
..."
*"**Artículo 100.** Al clasificar información con carácter de reservada es necesario, en todos los casos, fijar un plazo de reserva."*
*"**Artículo 108.** Cuando un documento contenga partes o secciones reservadas o confidenciales, los sujetos obligados, para efectos de atender una solicitud de información, deberán elaborar una Versión Pública en la que se testen las partes o secciones clasificadas, indicando su contenido de manera genérica y fundando y motivando su clasificación.*
*"**Artículo 110**. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación.*
...
VII. Obstruya la prevención o persecución de los delitos;
..."

Finalmente, el numeral Vigésimo sexto del Acuerdo establece lo siguiente:

"Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.
Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:
I. La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;
II. Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y

> *III. Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal."*
>
> (Sic)

De conformidad con lo anterior, se advierte que podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.
Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:

> *III. Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal.*

En ese sentido, los documento de seguridad en lo referente al Plan de Trabajo, Análisis de Riesgo y Análisis de Brecha, son susceptibles de clasificarse como reservados de conformidad con el artículo 110, fracción VII de la Ley Federal de la materia, conforme al lineamiento Vigésimo Sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Lo anterior, en el entendido de que en rubros se detallan las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en el tratamiento, como pueden ser, hardware, software, personal del responsable, además se establecen las medidas de seguridad existentes contra las faltantes, por lo que su difusión potencializa el nivel de vulnerabilidad de las medidas de seguridad de los datos personales que posee la CONAMED, lo cual podría derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros, previstos en los artículos 211 bis-1 al 211 bis-7 del código punitivo aludido.

Asimismo, el resguardo cobra importancia si se considera que una eventual divulgación implicaría conocer, copiar, modificar, destruir o provocar la pérdida de

información, así como un daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado a la información personal de los Titulares de los datos.

De manera que, revelar la información solicitada generaría daños inmediatos e inminentes, toda vez que daría a los particulares y/o delincuencia organizada, una oportunidad de conocer e incluso vulnerar datos importantes, las características de la tecnología y seguridad entre datos que, proporcionarlos radicaría en una flagrante violación de preceptos legales que ameritan sanciones por parte de las autoridades correspondientes.

En ese sentido, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo de parte de los Documentos de Seguridad contienen, el plan de trabajo, el análisis de riesgo y de brecha que implica llevar a cabo acciones de prevención de diversos delitos tipificados en el Código Penal Federal, lo cual cobra importancia si se considera que dichas conductas implican vulnerar las medidas de seguridad de los datos personales que se poseen.

Además, el resguardo de la información solicitada representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la reserva consiste en prevenir las conductas tipificadas en el Código Penal Federal, consistentes en acceso no autorizado a los sistemas, robos de información de expedientes médicos, suplantación de identidades, mismas que de llevarse a cabo podrían permitir la realización de diversos ataques a la infraestructura tecnológica y de sistemas que lo integran, con la consecuencia directa de la violación al principio de responsabilidad.

Por consiguiente, la difusión del Documento de Seguridad incrementa significativamente la posibilidad de que terceras personas expertas en informática vulneren las medidas de seguridad, accediendo de forma no autorizada a los sistemas de datos que no son públicos, perturben las medidas de seguridad de los datos personales contenidas en los expedientes clínicos de los pacientes, por lo tanto, se estima procedente su reserva, de conformidad con el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

En atención a lo descrito, este órgano colegiado, con fundamento en los preceptos legales invocados, **CONFIRMA** la clasificación de información como reservada de la documentación requerida por el particular, descrita en líneas anteriores, por un periodo de cinco años.

Por lo antes expuesto, este Comité de Transparencia,

R E S U E L V E

PRIMERO. Se confirma la clasificación de la información como reservada hecha valer por la Dirección General de Difusión e Investigación y Encargo de la Dirección General de Calidad e Informática, por un periodo de **cinco años**; en términos del considerando **CUARTO** de este documento.

SEGUNDO. Publíquese la presente resolución en el sitio de Internet de esta Dependencia.

TERCERO. Notifíquese al solicitante, a través del Sistema de Solicitudes de Información Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, la presente resolución.

CUARTO. El particular podrá interponer el recurso de revisión previsto por los artículos 142 y 143 de la LGTAIP, en concordancia con lo establecido en los artículos 147 y 148 de la LFTAIP.

Así, por unanimidad de votos lo resolvieron los integrantes del Comité de Transparencia de la Comisión Nacional de Arbitraje Médico.

LIC. JUAN ANTONIO OROZCO MONTOYA
PRESIDENTE DEL COMITÉ DE TRANSPARENCIA

LIC. JUAN LÓPEZ MARTÍNEZ
RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS E INTEGRANTE DEL COMITÉ DE TRANSPARENCIA

LIC. JAIME GENARO LÓPEZ VELA,
TITULAR DEL ÓRGANO INTERNO DE CONTROL