

Comité de  
Transparencia  
Acta de la Segunda  
Sesión Extraordinaria  
Ciudad de México, 29 de  
junio de 2020.

**ACTA CORRESPONDIENTE A LA SEGUNDA SESIÓN  
EXTRAORDINARIA DE 2020  
DEL COMITÉ DE TRANSPARENCIA DE LA  
COMISIÓN NACIONAL DE ARBITRAJE MÉDICO**

En la Ciudad de México, siendo las doce horas del veintinueve de junio de dos mil veinte, en la sala de juntas de la Subcomisión Jurídica de la Comisión Nacional de Arbitraje Médico, en adelante CONAMED, ubicada en el noveno piso del edificio marcado con el número doscientos cincuenta de la calle Mitla, colonia Vértiz Narvarte, código postal 03600, Alcaldía Benito Juárez, reunidas las personas que a continuación se mencionan, a efecto de celebrar la Segunda Sesión Extraordinaria de 2020 del Comité de Transparencia de la CONAMED.

El licenciado Juan Antonio Orozco Montoya, Subcomisionado Jurídico, Presidente del Comité de Transparencia, en lo sucesivo el Comité, el Doctor Miguel Ángel Lezana Fernández, Director General de Difusión e Investigación y Encargado del despacho de la Dirección General de Calidad e Informática e invitado del Comité, conforme a lo instituido en la Sexta de las Reglas de Funcionamiento, en adelante las Reglas, el licenciado Juan López Martínez, Responsable del Área Coordinadora de Archivos y, en términos de la Sexta de las Reglas, el licenciado Alberto Isaac Hernández Gómez, Secretario Técnico del Comité.

Una vez que los participantes registraron su asistencia, se asienta en la presente acta que de acuerdo al contenido del oficio CONAMED/UDT/199/2020 de fecha 24 de junio de la anualidad que transcurre, que se convocó al titular del Órgano Interno de Control en CONAMED, el pasado 26 de junio a las once horas con treinta minutos, según se desprende del acuse del citado oficio, es decir, con la debida antelación, conforme a la Tercera de las Reglas del Comité, habida cuenta que la naturaleza de la presente sesión es la de extraordinaria, de manera que se cumple con el plazo para convocar a sesión de veinticuatro horas previas a su celebración. Lo anterior, sin que implique óbice el contenido del oficio



número SFP.OIC.CONAMED.TOIC.104.2020 de fecha 26 de junio de 2020, recibido en la Unidad de Transparencia a las diecisiete horas con quince minutos, en cuyo cuerpo el titular del Órgano Interno de Control en CONAMED, Lic. Gibrán Ernesto Silva Basso informó al Comité que, en suplencia suya, había designado a la licenciada Olga Araceli Labastida García, titular del Área de Responsabilidades de ese órgano fiscalizador, para participar en la presente sesión, no obstante, dicha funcionaria no se presentó a ésta segunda sesión extraordinaria.

Asentado lo descrito en el párrafo precedente, habiendo registrado su asistencia los participantes presentes en la lista correspondiente, se verificó el *quórum* legal para llevar a cabo la sesión, por lo que el Presidente del Comité declaró instalada la Segunda Sesión Extraordinaria de 2020 del Comité de Transparencia de CONAMED y dio la bienvenida a los presentes para proceder a dar lectura al siguiente:

#### ORDEN DEL DÍA

1. Lista de asistencia y declaración de quórum.
2. Lectura del Orden del día.
3. El titular de la Dirección General de Difusión e Investigación y Encargado del Despacho de la Dirección General de Calidad e Informática, Dr. Miguel Ángel Lezana Fernández, somete a la consideración y, en su caso, aprobación del Comité de Transparencia de la reserva del Documento de Seguridad de CONAMED, derivado de la solicitud de información con folio 4220700007420.
4. Asuntos generales.

#### DESAHOGO DEL ORDEN DEL DÍA

**PRIMER PUNTO.** Atendidas las formalidades del primer numeral del Orden del Día, se procedió al desahogo del siguiente numeral.

**SEGUNDO PUNTO.** En uso de la voz, el Presidente del Comité de Transparencia hizo referencia a la petición que formula el titular de la Dirección General de Difusión e Investigación y Encargado del Despacho de la Dirección General de Calidad e Informática, Dr. Miguel Ángel Lezana Fernández, para someter a consideración y, en su caso, aprobación del Comité, sobre la reserva de información derivada de la solicitud de información con folio 4220700007420.



En ese sentido, el Dr. Miguel Ángel Lezana Fernández comenzó su participación mencionando que se realizó una búsqueda exhaustiva en los archivos físicos y electrónicos bajo resguardo de la Dirección General de Difusión e Investigación, sin haber localizado el referido documento actualizado conforme a la normatividad aplicable y vigente, de acuerdo a la estructura propia del documento en alusión, con el contenido siguiente:

- Inventario de datos personales y de los sistemas de tratamiento;
- Funciones y obligaciones de las personas que traten datos personales;
- Análisis de riesgos;
- Análisis de brecha;
- Plan de trabajo;
- Mecanismos de monitoreo y revisión de las medidas de seguridad, y
- Programa general de capacitación.

Continuó exponiendo que, en coordinación y apoyo a las unidades administrativas que conforman la Comisión Nacional (CONAMED), respecto al funcionamiento de sus sistemas, el catálogo de los datos personales que recaban, las finalidades, así como también las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen, al igual que las funciones y obligaciones del personal adscrito a dichas unidades y áreas administrativas, que son quienes deciden sobre el tratamiento de datos personales, por lo que éste órgano desconcentrado de la Secretaría de Salud, es responsable de elaborar el multicitado documento de seguridad, el cual mismo que en archivo adjunto se acompaña al presente.

En ese sentido, abordó las razones y motivos a través de los cuales solicitó la reserva de información derivada de la solicitud 4220700007420, citando de forma resumida que, del análisis al contenido del Documento de Seguridad de CONAMED con el fin de cumplir con el requisito (prueba de daño) establecido en los artículos 103 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) y el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), es viable observar que el Documento de mérito contiene datos sensibles, como lo son el estado de salud, diagnósticos clínicos, padecimientos y enfermedades, entre otros, amén de los roles asignados a cada una de las personas que realizan el tratamiento, los cuales deben guardar estricta confidencialidad de la información, y se contemplan distintas medidas de seguridad que permiten





asegurar la confidencialidad, disponibilidad e integridad de la información recabada, así como la criticidad de los mismos y controles existentes, lo cual estriba en que, de darse a conocer tal información, se estarían exponiendo vulnerabilidades potenciales, que pueden ser aprovechadas por un agente interno o externo y ser una amenaza a los sistemas, provocando ya sea la pérdida o destrucción no autorizada, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada, impactando de manera significativa en los titulares de los datos personales que obran en posesión de la Comisión Nacional de Arbitraje Médico. Así dicho, el invocado documento de seguridad posee el carácter de reservado, con fundamento en los artículos 97, 98, 100, 102 y 110, fracciones I, V y VII de la LFTAIP y 103, 104, 106, 113, fracciones I, V y VII, de la LGTAIP; ya que si bien, a través del derecho de acceso a la información, cualquier persona puede tener acceso a la información en posesión de los sujetos obligados, también lo es que existen determinadas restricciones al respecto, mismas que se refieren a la información reservada, pues se fundamenta y motiva, a través de la aplicación de la prueba de daño, la solicitud de clasificación como información reservada, por un plazo de cinco años, de Documento de Seguridad de CONAMED, en razón a que su entrega, puesta a disposición, publicación, difusión, o cualquier acto similar de publicidad implica un daño presente, probable y específico, atendiendo a la naturaleza de la información que contiene.

Prosiguió su exposición señalando que, lo antes vertido, revela que de darse a conocer la información contenida en el Documento de Seguridad, se estaría proporcionando acceso a cuestiones torales como son, el nombre, cargo y adscripción de los Responsables, Encargados y Usuarios de la información tratada, la estructura y descripción de los sistemas de datos personales, la especificación detallada del tipo de datos personales contenidos en el sistema de datos, las funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales, las medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad, entre las que destacan los procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del sistemas de datos personales, la actualización de información contenida en el sistema, los procedimientos de creación de copias de respaldo y de recuperación de los datos, las bitácoras de acciones llevadas a cabo en el sistema, el procedimiento de notificación, gestión y respuesta ante incidentes y el procedimiento para la cancelación de un sistema de datos personales. Por ello, es dable insistir en que, de hacer pública esta información, se estaría dando apertura a conocer la



infraestructura tecnológica y, en su caso, las vulnerabilidades de éste sujeto obligado, incluyendo el nivel de confidencialidad de los activos de información en los sistemas, aplicativos y demás medios tecnológicos de información y comunicaciones, donde reside, viaja y procesa la información específica y estratégica de CONAMED, así como la información relativa a las características específicas y configuraciones de los sistemas y sus medidas de seguridad administrativas, físicas y electrónicas, por lo que potencialmente se estaría ante un escenario que facilitaría la intrusión de agentes externos en los sistemas de los responsables, en los que existen distintos datos personales de diversa índole a través del conocimiento de la información relacionada al análisis de riesgos y de brecha, de las unidades administrativas relacionadas con el sistema de datos, generando un daño inmediato e inminente.

Dio seguimiento a lo aportado al Comité, enfatizando que, el riesgo de daño que supondría la divulgación del Documento de Seguridad de CONAMED, representa inminentemente un riesgo real, demostrable e identificable de perjuicio significativo a la vida, salud, seguridad e integridad física de los titulares de la información, superando el interés público general de que se difunda, toda vez que las afectaciones no solo trastocan diversos aspectos de seguridad de la información de CONAMED, sino que el daño se extiende a otros ámbitos, tales como la política pública en materia de conciliación y arbitraje, la amenaza a la vida y a la salud de las personas, amén de la cuestión de seguridad nacional y que, en caso de ser vulnerados, dicha información podría ser extraída con resultados catastróficos para el País, o más aún, hurtada para fines de lucro, pues se contiene información de personas físicas y morales particulares, domicilios, representaciones, medios de contacto, entre otros, que pueden ser de uso indebido para llegar a aquellas personas que han sido usuarios de los servicios de CONAMED, constituyendo en sí mismo una conducta delictiva, que revelación de la información mencionada expone información personal y sensible de usuarios de CONAMED, al exhibir información, facilitando la contaminación de virus, ataques a las redes de datos por parte de grupos subversivos u organizaciones criminales, pudiendo dar origen a la posible comisión de un delito derivado de la exposición no autorizada, y en caso de ser vulnerada, dicha información podría ser utilizada con resultados catastróficos para el país.

Que ante tales circunstancias, es necesario establecer y mantener medidas de seguridad para la protección de los datos personales de nivel alto, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño,



pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, entre las que destaca la reserva de la información contenida en el Documento de Seguridad, en virtud de que el mismo contiene datos personales relativos a los atributos, permisos y accesos de las cuentas mediante las cuales, los distintos usuarios informáticos de todos los niveles jerárquicos obtienen servicios como correo electrónico e Internet, así mismo, como parte del inventario de datos se incluyen datos personales de índole sensible, es decir, aquellos datos que refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este; por lo que al dar a conocer información de un documento de seguridad se pone en riesgo la integridad de los sistemas de información de éste sujeto obligado, así como afectar directamente a los titulares de los datos personales sujetos de protección, toda vez que divulgando los inventarios, medidas de seguridad existentes, faltantes, amenazas, vulnerabilidades y el volumen de la información, se podrían aplicar métodos tecnológicos para tratar de vulnerar las defensas informáticas existente.

Por otro lado, aseveró que las implicaciones de entregar esta Información, recaen en el hecho de que podría vulnerar la seguridad de la información de esta Comisión Nacional, en virtud de que la apertura de las medidas de seguridad existentes y la evaluación de los riesgos, además de activos clave y sujetos autorizados para su tratamiento, abriría una brecha de seguridad que podría ser explotada por algún agente Interno o externo, accediendo a información no autorizada, entre las que destaca información sumamente sensible, respecto de la cual existe la inherente obligación de proteger conforme a lo establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por lo que atenta contra los principios de seguridad de la Información señalados en tal ley y en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Tomando en cuenta lo anterior, de proporcionar dicha información, algún sujeto o factor externo o interno podrían vulnerar la seguridad de la información e incurrir en la posible comisión de un delito, tal como se ha descrito en el Código Penal Federal, respecto a modificación, destrucción, provocación de pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, su conocimiento sin autorización, obtención, copia sin autorización o utilización contenida en cualquier sistema, equipo o medio de almacenamiento informáticos, bajo cuya óptica, se pone de manifiesto que proporcionar la información de las medidas de seguridad implementadas, se pondría a CONAMED en un punto vulnerable y de máximo riesgo respecto a sus



sistemas de información, lo que daría pauta a la comisión de conductas que la ley penal describe como delitos.

Resumió manifestando que la información descrita en los documentos de seguridad pudiera dar lugar, entre otras, a vulnerabilidades como las siguientes:

- Permitir el acceso ilícito a sistemas y equipos informáticos, intentando la suplantación de los mismos;
- Potenciar la posibilidad de vulnerar la seguridad de la infraestructura tecnológica;
- Poner en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones institucionales;
- Dar a conocer puntos de vulnerabilidad para la seguridad de los sistemas de información
- Revelar aspectos específicos de la operación y funcionamiento de la infraestructura tecnológica;
- Comprometer los registros de cada uno de los usuarios (pacientes y prestadores de servicios);
- Vulnerar los sistemas informáticos, así como la información contenida en éstos;
- Atentar en contra de la infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas;
- Divulgar información sensible que en su conjunto pueda representar un insumo de alta valía para la generación de ataques informáticos, y
- Generar ataques a otras instituciones al ser suplantada la identidad de la infraestructura de cómputo abriendo la posibilidad de un ataque masivo a la Administración Pública.

Siguió su línea argumentativa en el sentido que resulta indispensable la reserva de la información contenida en el documento de seguridad pues, conociendo los datos de referencia, con conocimientos técnicos avanzados se podría suplantar la identidad de usuarios, titulares y responsables de los sistemas, y brindar esta información pudiera generar posibles atacantes que pudieran aprovecharse de posibles vulnerabilidades, así como hacer uso indebido, ilícito y lucrativo; adicionalmente, sostiene que el riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda, ya que el resguardo de los datos contenidos en los distintos documentos de seguridad, implica la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el





Código Penal Federal, lo cual cobra gran relevancia, si se considera que dicha conducta implica 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 información de salud, considerada en términos del artículo 3, fracción X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, como información sensible.

Finalmente declaró que en tales consideraciones y derivado de las razones, motivos y fundamentos expuestos con prelación, por parte de la Dirección General de Difusión e Investigación, así como la Dirección General de Calidad e Informática, solicita al Comité de Transparencia la reserva del multi referido Documento de Seguridad, por un periodo de 5 años, con fundamento en el artículo 110, fracciones I, V y VII de la Ley Federal de Transparencia y Acceso a la Información Pública y 113, fracciones I, V y VII, de la Ley General de Transparencia y Acceso a la Información Pública.

Habiendo escuchado las razones y motivos vertidos para solicitar la reserva de la información inherente al Documento que nos ocupa, mismos que previo a la celebración de la sesión tuvieron oportunidad de conocer y consultar, en términos del artículo 43, párrafo cuarto de la LGTAIP, incluso durante el desarrollo de la sesión, los fundamentos jurídicos para tales efectos, amén de lo instituido en el numeral Quinto, fracción I de las Reglas del Comité de Transparencia de CONAMED, somete a voto de los integrantes la propuesta esgrimida en páginas anteriores, respecto a lo cual, los integrantes presentes del Comité, adoptaron el acuerdo siguiente:

**ACUERDO 01-EXT02/29-06-2020.** Por unanimidad de los integrantes presentes, el Comité de Transparencia de la Comisión Nacional de Arbitraje Médico, en términos de lo dispuesto en los artículos 6°, apartado "A", fracción I; 3°, fracción IV, 23, 24, fracciones I y XIV, 43, párrafos primero, segundo y tercero, 44, fracciones II y IX, 103, 104, 106, fracción I y 113, fracciones I, V y VIII, de la Ley General de Transparencia y Acceso a la Información Pública; 4, fracción I, 5, 11, fracción I, 64, párrafos primero y segundo, 65, fracciones II y IX, 97, 98, fracción I, 100, 102 y 110, fracciones I, V y VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; **CONFIRMA** la clasificación de la información como reservada, hecha valer por la Dirección General de Difusión e Investigación y el Encargo de la Dirección General de Calidad e Informática, por un periodo de 5 años, en razón a que no existe ningún impedimento legal para tal efecto, estimando fundadas y motivadas las

*[Handwritten signatures in blue ink]*







causas por las que se esgrime la prueba de daño para la clasificación de la información, solicitada por la Dirección General de Difusión e Investigación y el Encargo del Despacho de la Dirección General de Calidad e Informática.

TERCER PUNTO. En virtud de no haber más asuntos generales que tratar, el Presidente del Comité de Transparencia dio por concluida la sesión a las trece horas del día de la fecha y con la aprobación de los asistentes se levantó la presente acta para constancia y efectos legales a que haya lugar. Lo anterior, con fundamento en la Octava, fracción V, de las Reglas de Funcionamiento del Comité de Transparencia de la Comisión Nacional de Arbitraje Médico.

Lic. Juan Antonio Orozco Montoya,  
Presidente del Comité de Transparencia  
y Titular de la Unidad de Transparencia.

Lic. Juan López Martínez,  
Responsable del Área Coordinadora de  
Archivos e Integrante del Comité de  
Transparencia.

Lic. Alberto Isaac Hernández Gómez.  
Secretario Técnico del Comité de  
Transparencia.

Dr. Miguel Ángel Lezana Fernández,  
Director General de Difusión e Investigación  
y Encargado del despacho de la Dirección  
General de calidad e Informática

Última hoja correspondiente al Acta de la Segunda Sesión Extraordinaria de 2020 del Comité de Transparencia de la CONAMED, celebrada el veintinueve de junio de dos mil veinte.

