## COMITÉ DE TRANSPARENCIA

## SEGUNDA REUNIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL 2018

En la Ciudad de México, Distrito Federal, siendo las 12 horas del día 20 de julio del año dos mil dieciocho, se reunieron en la sala de juntas de las oficinas que ocupa la Dirección Técnica de la Comisión Nacional de los Salarios Mínimos (CONASAMI), ubicada en el primer piso del edificio marcado con el número catorce de la Avenida Cuauhtémoc, Col. Doctores, Código Postal 06720 de esta Ciudad, los integrantes del Comité de Transparencia de esta Comisión Nacional que enseguida se mencionan:

**INTEGRANTES DEL COMITÉ:** doctor Alfredo Hernández Martínez, Presidente del Comité de Transparencia y Titular de la Unidad de Transparencia; maestra Flor de María Briones Zavala, Titular del Órgano Interno de Control; licenciado Miguel González Ramírez, Director Administrativo y Responsable del Área Coordinadora de Archivos; y licenciada Elvia Pérez Reyes, Directora de Investigación Económica y Coordinadora de los trabajos de la Unidad de Transparencia.

El doctor Hernández inició la sesión agradeciendo a los integrantes del Comité su asistencia y refirió que en esa reunión se estaría al siguiente:

### ORDEN DEL DÍA

1. Lista de Asistencia y comprobación del Quórum.
2. Ratificación del acta de la Primera Sesión Ordinaria del Comité de Transparencia 2018.
3. Pronunciamiento del Comité en relación con la clasificación de información con carácter de reservada, respecto de las siguientes solicitudes de información:

   3.1 Número de folio 1407500004418.
   3.2 Número de folio 1407500004518.

4. Calidad y tiempo en respuestas a solicitudes de información.
5. Asuntos Generales.

### DESARROLLO DE LA SESIÓN

**1. Lista de Asistencia y comprobación del Quórum.**

Se verificó la presencia de los miembros del Comité mediante la firma en la lista de asistencia correspondiente.

El doctor Hernández señaló que existía el quórum necesario para sesionar, por lo que procedió a dar inicio a la reunión convocada. Para ello pidió a la licenciada Pérez Reyes que abordara los temas acordados en el orden del día.

**2. Ratificación del Acta de la Primera Sesión Ordinaria de 2018.**

Los miembros del Comité ratificaron el acta de la Primera Sesión Ordinaria de 2018 del Comité de Transparencia.

**3. Pronunciamiento del Comité en relación con la clasificación de información con carácter de reservada, respecto de las siguientes solicitudes de información:**

**3.1 Número de folio 1407500004418.**

A través de la Plataforma de Nacional de Transparencia (PNT) se recibió la solicitud de información número de folio 1407500004418, en la que se requirió lo siguiente:

*"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los equipos de cómputo en posesión del sujeto obligado: a. Número de serie y de parte. b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña apara acceder a la configuración de la BIOS (siglas en ingles de Basic Input/Output System). e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad, área u órgano que hace uso del equipo de cómputo."*

La Unidad de Transparencia turnó esta solicitud al Departamento de Informática, unidad administrativa competente para atender el requerimiento del particular. El 13 de julio del año en curso, el Departamento de Informática envía la respuesta a la Unidad de Transparencia señalando que "el inciso *a. Número de serie y de parte* corresponde a información reservada" y, en la misma fecha, mediante oficio No. DI/045/2018, solicita al Comité de Transparencia la confirmación de reserva de dicha información, de conformidad con los artículos 110, fracciones V, VIII y XIII de la Ley Federal de Transparencia y Acceso a la Información Pública; 104, fracción I, 106 y 113, fracciones V, VIII y XIII, de la Ley General de Transparencia y Acceso a la Información Pública, por cinco años.

Por lo anterior, este Comité efectuó el siguiente análisis para determinar la procedencia de la reserva de la información.

**Análisis de la solicitud de clasificación de reserva.**

El Departamento de Informática solicita la reserva de "*1. De cada uno de los equipos de cómputo en posesión del sujeto obligado: a. Número de serie y de parte...*" de conformidad con lo dispuesto por el artículo 104 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; y en concordancia con los lineamientos vigésimo tercero, vigésimo séptimo y trigésimo segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas; y la prueba de daño, misma que contiene elementos suficientes para acreditar que la entrega de la información al solicitante causaría un mayor perjuicio a la sociedad e implicaría una vulnerabilidad a las operaciones de la institución, al existir la posibilidad de utilizarla para crear, entre otros, mecanismos o técnicas fraudulentas con lo que se afectaría el interés público y los derechos de terceros.

**La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional.** Al respecto, el Departamento de Informática señala que difundir o hacer del conocimiento público la información solicitada supondría una enorme ventaja para cualquier atacante de la infraestructura de redes de datos, al proporcionarle herramientas para facilitar un ataque a la Entidad, poniendo en riesgo la información sensible contenida tanto en los equipos de cómputo, como la contenida en los servidores que procesan información, lo que supondría el entorpecimiento de su funcionamiento, así como la seguridad de los datos personales confidenciales de los servidores públicos que se encuentran en ciertos equipos de cómputo (tales como: La CURP, RFC, datos familiares, cuentas bancarias, entre otros) infringiendo con ello la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; asimismo, la información contenida en los equipos de las áreas sustantivas de la CONASAMI que sirven de base para los procesos de fijación o revisión de los salarios mínimos general y profesionales; así como a los posibles procesos de responsabilidades que se encontrarían en trámite en el Órgano Interno de Control por quejas, denuncias y faltas de carácter administrativo, entre otros.

La divulgación de la información representa un riesgo real, demostrable e identificable del perjuicio significativo al interés público (fracción I del Artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública).

a) **Riesgo real.** En concordancia con lo antes mencionado, la Entidad realiza esfuerzos para mantener la seguridad de sus equipos y sistemas informáticos, por lo cual permanentemente devenga recursos para contar con un servicio administrado de seguridad informática que previene los ataques mencionados, entre otros, por lo que proporcionar información que facilite un ataque, supone un aumento en la probabilidad de éxito de un atacante informático, poniendo en riesgo la seguridad y la estabilidad de los sistemas informáticos y de las redes de telecomunicaciones de la Entidad, con lo que se violaría el artículo 27 del ACUERDO por el que se modifican las políticas y

disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como del Manual Administrativo de Aplicación General en dichas materias.

b) **Riesgo demostrable.** Es altamente probable y de inminente peligro el proporcionar la información objeto de reserva, toda vez que se materializaría el riesgo que se busca evitar al contar con un servicio de seguridad informática, es decir, evitar efectos negativos en la infraestructura tecnológica de la CONASAMI. Es por ello que actualmente se cuenta con servicios administrados de seguridad informática, como se señala en el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, así como de la Seguridad en la Información, que privilegian la seguridad de los sistemas informáticos y de las redes de telecomunicaciones de la Administración Pública Federal.

c) **Riesgo identificable.** En el caso de la información objeto del presente análisis, el riesgo identificable se refiere al riesgo de un uso mal intencionado de la misma, lo que causaría una vulnerabilidad específica en los sistemas informáticos, equipos y redes de telecomunicaciones de la CONASAMI, pudiendo inhabilitar segmentos de red, identificando ubicación física de los usuarios, intentos de ataque del tipo intrusión, suplantación de identidad, robo de datos y datos personales sensibles de los servidores públicos de la Entidad referidos en la fracción X del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, entre otros.

**El riesgo de perjuicio que supondría la divulgación de la información supera el interés público general de que se difunda.** Toda vez que dicha información no resulta útil a la ciudadanía en general, sino específicamente a especialistas en informática que pueden obtener información a partir de la solicitada como puede ser conocer la ubicación física en tiempo real de cualquiera de los usuarios de los equipos de cómputo; atacar y obtener información de los equipos y redes; conocer información crítica y, en un momento dado, provocar retrasos o dañar sensiblemente las funciones y operación tanto sustantivas como administrativas de la Entidad.

**La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar un perjuicio.** Únicamente se está solicitando reservar la información que puede poner en riesgo la infraestructura tecnológica, los sistemas informáticos y la información que se procesa de la CONASAMI, el resto de información solicitada se proporcionará puntualmente.

Con lo anterior, queda demostrado que subsiste la reserva de la información en términos de lo dispuesto en las fracciones V, VIII y XIII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública y fracciones V, VIII y XIII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en lo dispuesto en los lineamientos vigésimo tercero, vigésimo séptimo y trigésimo segundo de los Lineamientos

Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, y se acredita la reserva temporal de la información señalada por dicha unidad administrativa.
No se omite señalar que se puede ampliar el período de reserva de conformidad con el penúltimo párrafo del artículo 101 de la Ley General de Transparencia y Acceso a la Información Pública y penúltimo párrafo del artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública.

**3.2 Número de folio 1407500004518.**

En la Plataforma de Nacional de Transparencia (PNT) se recibió la solicitud de información número de folio 1407500004518, en la que se requirió lo siguiente:

*"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. Desglosado por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, nombre de los navegadores de Internet que se encuentran instalados en dichos equipos de cómputo. 2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación con el punto anterior. 3. Número de serie o número de parte de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet denominado YANDEX BROWSER. 4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET. 6. Cuáles son las redes sociales oficiales utilizadas como medios de comunicación. 7. Motivos por los cuales son utilizados únicamente las redes sociales a las que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo."*

La Unidad de Transparencia turnó esta solicitud al Departamento de Informática, unidad administrativa competente para atender el requerimiento del particular. El 13 de julio del año en curso, el Departamento de Informática envía la respuesta a la Unidad de Transparencia, señalando que el inciso *1. Desglosado por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado...* y el inciso *9. Por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo*

corresponde a información reservada y, en la misma fecha, mediante oficio No. DI/046/2018, solicita al Comité de Transparencia la confirmación de reserva de dicha información, en términos de lo dispuesto por los artículos 110, fracciones V, VIII y XIII de la Ley Federal de Transparencia y Acceso a la Información Pública; 104, fracción I, 106 y 113, fracciones V, VIII y XIII, de la Ley General de Transparencia y Acceso a la Información Pública, por cinco años. Agregando que en caso de proporcionarse la información solicitada en el punto 1 y punto 9 de la solicitud 147500004518, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con lo siguiente:
*"Requerimiento 1. "Desglosado por el número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado…".*

*La divulgación de números de serie y parte de los equipos que componen la infraestructura de cómputo central y personal representa un riesgo ya que quien posea esta información puede suplantar la identidad de un usuario válido y solicitar al fabricante la generación de tickets de soporte para reemplazo de piezas y/o envío de copias certificadas de los sistemas operativos de los equipos, situación que comprometería la información contenida en los mismos.*

*La vinculación de dicha información con "direcciones MAC de las tarjetas o adaptadores de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo, más los Servidores DNS (Domain Name System)", comprometería la disponibilidad, confidencialidad e integridad de la información de la Entidad, ya que un posible atacante tendría a su alcance todos los elementos necesarios para realizar una suplantación de identidad e ingresar a la red para intentar ataques informáticos que son desde extracción de información, por ejemplo: extracción de datos personales, que por sí misma constituiría una violación a las Leyes General y Federal de Transparencia y Acceso a la Información Pública y a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; denegación de servicio (impedir la operación informática de la Entidad al inhabilitar los servicios); modificación o alteración de información oficial; y publicación o divulgación de información suplantando la identidad de un equipo validado de la Entidad.*

*Requerimiento 9. "Por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo".*

*Proporcionar las direcciones MAC ADDRESS de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que dispone cada equipo de cómputo en la CONASAMI, supone inminentes riesgos en materia de seguridad informática al exponer a la Entidad a diferentes tipos de ataques informáticos, que precisan de dichos datos para llevarse a cabo, como los que se exponen a continuación:*

*El ARP Spoofing (Address Resolution Protocol) es un medio de ataque en el que un tercero no autorizado (hacker), envía mensajes falsificados a una red LAN, el objetivo del ataque es vincular la dirección MAC del equipo con el que se pretende realizar la intrusión, con la*

*dirección IP de un equipo legítimo (o un servidor) en la red (Suplantación de Identidad). Cuando el atacante vincula la dirección MAC a una dirección IP auténtica o válida, el intruso puede hacer una suplantación de identidad y utilizar los aplicativos para reconstruir paquetes de archivos editados en procesadores de texto, o bien, acceder mediante la dirección IP a toda la información que por ella transite, es decir, el intruso se hace pasar ante la red de datos de la organización a la que planea atacar, como un usuario autorizado y válido con permisos de acceso y navegación en la red de la Entidad, teniendo acceso inmediato a datos y recursos informáticos.*

*El ARP Spoofing permite a los atacantes maliciosos interceptar, modificar o incluso retener datos que estén en tránsito. Los ataques de suplantación ARP ocurren en redes de área local que utilizan protocolo de resolución de direcciones (ARP), este tipo de ataques pueden tener efectos graves para la Entidad, ya que, en su nivel más básico, los ataques de suplantación ARP se utilizan para robar información sensible. Cabe señalar que los ataques de suplantación de ARP se utilizan a menudo para facilitar otros ataques como:*

*Ataques de Denegación de Servicio (DoS Denial-of-service attacks).*

*...*

*Secuestro de Sesiones (Session hijacking)*

*...*

*Ataques tipo Hombre en el Medio (Man-in-the-middle Attacks)*

*...*

*Los anteriores son solo algunos ejemplos de los diversos tipos de ataques que pudieran ser facilitados con la divulgación de la información solicitada, ya que con los datos de las direcciones MAC de cada uno de los equipos de cómputo y de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo, los números de serie y parte de los equipos de cómputo proporcionarán los elementos necesarios para dañar la configuración del equipo de cómputo a su alcance.*

*Resulta pertinente precisar que la exposición de la información solicitada compromete los servicios relacionados con la seguridad perimetral, contratados por la CONASAMI, divulgando información que en su conjunto representa un insumo de alta valía para la generación de ataques informáticos, hecho que de materializarse afectaría tanto los servicios que al interior la Entidad provee, así como información y datos personales sensibles de los servidores públicos de la CONASAMI, esto último violentaría lo dispuesto en el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados."*

Por lo anterior, este Comité efectuó el siguiente análisis para determinar la procedencia de la reserva de la información.

**Análisis de la solicitud de clasificación de reserva.**

El Departamento de Informática solicita la reserva de "*1. Desglosado por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado…*" y el inciso "*9. Por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo …*", de conformidad con lo dispuesto por el artículo 104 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; y en concordancia con los lineamientos vigésimo tercero, vigésimo séptimo y trigésimo segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas. De esta forma, procedió a presentar la prueba de daño, la cual contiene, entre otros, los siguientes elementos:

**La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional.** Al respecto, el Departamento de Informática señala que difundir o hacer del conocimiento público la información solicitada supondría una enorme ventaja para cualquier atacante de la infraestructura de redes de datos, al proporcionarle herramientas para facilitar un ataque a la Entidad, poniendo en riesgo la información sensible contenida tanto en los equipos de cómputo, como la contenida en los servidores que procesan información, lo que supondría el entorpecimiento de su funcionamiento, así como la seguridad de los datos personales confidenciales de los servidores públicos (tales como: La CURP, RFC, datos familiares, cuentas bancarias, entre otros) que se encuentran en ciertos equipos de cómputo, infringiendo con esto último la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por lo que es necesario mantener las medidas de seguridad para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, garantizando de esta manera su confidencialidad, integridad y disponibilidad, en términos de los dispuesto en los artículos 31, 32 y 33 de la Ley General de Protección de Datos Personales, en correlación con lo dispuesto en el proceso de organización en su actividad de Seguridad de la Información para proteger la confidencialidad, la integridad y disponibilidad de la información. Asimismo, se vulnera la información sensible contenida en los equipos de las áreas sustantivas de la CONASAMI que sirven de base para los procesos de fijación o revisión de los salarios mínimos general y profesionales; así como a los posibles procesos de responsabilidades que pudieran encontrarse en trámite en el Órgano Interno de Control por quejas, denuncias y faltas de carácter administrativo, entre otros.

La divulgación de la información representa un riesgo real, demostrable e identificable del perjuicio significativo al interés público (fracción I del Artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública).

a) **Riesgo real.** En concordancia con lo antes mencionado, la Entidad realiza esfuerzos para mantener la seguridad de sus equipos y sistemas informáticos, por lo cual

permanentemente devenga recursos para contar con un servicio administrado de seguridad informática que previene los ataques mencionados, entre otros, por lo que proporcionar información que facilite un ataque, supone un aumento en la probabilidad de éxito de un atacante informático poniendo en riesgo la seguridad y la estabilidad de los sistemas informáticos y de las redes de telecomunicaciones de la Entidad, con lo que se violaría el artículo 27 del ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como del Manual Administrativo de Aplicación General en dichas materias.

b) **Riesgo demostrable.** Es altamente probable y de inminente peligro el proporcionar la información objeto de reserva, toda vez que se materializaría el riesgo que se busca evitar al contar con un servicio de seguridad informática, es decir, evitar efectos negativos en la infraestructura tecnológica, de los sistemas informáticos y la información que se procesa de la CONASAMI. Es por ello que actualmente se cuenta con servicios administrados de seguridad informática, como se señala en el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, así como de la Seguridad en la Información, que privilegian la seguridad de los sistemas informáticos y de las redes de telecomunicaciones de la Administración Pública Federal.

c) **Riesgo identificable.** En el caso de la información objeto del presente análisis, el riesgo identificable se refiere al riesgo de un uso mal intencionado de la misma, lo que causaría una vulnerabilidad específica en los sistemas informáticos, equipos y redes de telecomunicaciones de la CONASAMI, pudiendo inhabilitar segmentos de red, identificando ubicación física de los usuarios, intentos de ataque del tipo intrusión, suplantación de identidad, robo de datos y datos personales sensibles de los servidores públicos de la Entidad referidos en la fracción X, del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, entre otros.

**El riesgo de perjuicio que supondría la divulgación de la información supera el interés público general de que se difunda.** Toda vez que dicha información no resulta útil a la ciudadanía en general, sino específicamente a especialistas en informática que pueden obtener información a partir de la solicitada como puede ser conocer la ubicación física en tiempo real de cualquiera de los usuarios de los equipos de cómputo; atacar y obtener información de los equipos y redes; conocer información crítica y, en un momento dado, provocar retrasos o dañar sensiblemente las funciones y operación tanto sustantivas como administrativas de la Entidad.

**La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar un perjuicio.** Únicamente se está solicitando reservar la información que puede poner en riesgo la infraestructura tecnológica, los sistemas

informáticos y la información que se procesa de la CONASAMI, el resto de información solicitada se proporcionará puntualmente.

Adicionalmente, el Departamento de Informática sostiene que no mantiene un registro o archivo de la información sujeta a reserva, toda vez que el proveedor de arrendamiento de los equipos es el propietario y responsable de mantener los resguardos de asignación a cada usuario, así como del mantenimiento y soporte técnico correspondiente, por tanto, la información solicitada no puede difundirse sin el consentimiento previo del propietario, por lo que al no contar con alguna facultad que derive en la elaboración de una relación de los números de serie y direcciones Mac de los equipos de cómputo en posesión de la Comisión Nacional de los Salarios Mínimos, no existe obligación de elaborar documentos *ad hoc* conforme al criterio 03/17 emitido por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Asimismo, el Departamento de Informática invoca "*el criterio sustentado por la Suprema Corte de Justicia de la Nación, Novena Época, publicado en el Semanario Judicial de la Federación y su Gaceta, Tomo XI, abril de 2000, Tesis: P.LX/200, página 74, cuyo rubro y texto es el siguiente: "DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCERO. El derecho la información consagrable en la última parte del artículo XI de la Constitución Federal no es absoluto, sino que, como toda garantía, se haya sujeto a limitaciones o excepciones que sustenten fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales el mencionado derecho no puede ser garantizado indiscriminadamente, sin que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera, así, en cuanto a la seguridad nacional, se tienen normas que por un lado restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daño a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social se cuenta con normas que tienden a proteger la averiguación de los delitos la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados*".

Con lo anterior, queda demostrado que subsiste la reserva de la información en términos de lo dispuesto en las fracciones V, VIII y XIII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública y fracciones V, VIII y XIII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en lo dispuesto en los lineamientos vigésimo tercero, vigésimo séptimo y trigésimo segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se acredita la existencia de un riesgo real, demostrable e

identificable de perjuicio significativo al interés público, así como la reserva temporal de la información señalada por dicha unidad administrativa.

No se omite señalar que se puede ampliar el período de reserva de conformidad con el penúltimo párrafo del artículo 101 de la Ley General de Transparencia y Acceso a la Información Pública y penúltimo párrafo del artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública.
En virtud de lo anterior, con fundamento en lo dispuesto por los artículos 65, fracción II, y 140, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia emite por unanimidad los siguientes Acuerdos.

**ACUERDOS:**

CT/CNSM/004/2018 Se confirma la clasificación de reserva invocada por el Departamento de Informática del **Número de serie y de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado** asociado a la solicitud de información con número de folio 1407500004418, atendiendo los argumentos vertidos en el numeral 3.1 de esta Acta y con fundamento en dispuesto en las fracciones V, VIII y XIII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública y fracciones V, VIII y XIII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en lo dispuesto en los lineamientos vigésimo tercero, vigésimo séptimo y trigésimo segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, por un período de 5 años.

CT/CNSM/005/2018 Se confirma la clasificación de reserva invocada por el Departamento de Informática del **número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado y la dirección MAC (por sus siglas en inglés Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de cómputo por número de serie o número de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado,** asociado a la solicitud de información con número de folio 1407500004518, atendiendo los argumentos vertidos en el numeral 3.2 de esta Acta y con fundamento en dispuesto en las fracciones V, VIII y XIII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública y fracciones V, VIII y XIII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en lo dispuesto en los lineamientos vigésimo tercero, vigésimo séptimo y trigésimo segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, por un período de 5 años.

**4. Calidad y tiempo en respuestas a solicitudes de información.**

En seguimiento al orden del día, la licenciada Pérez Reyes abordó el tema sobre la calidad y tiempo de las respuestas a las solicitudes de información recibidas mediante la Plataforma Nacional de Transparencia, explicando que el INAI emite una calificación que se construye con base en esas variables: calidad y tiempo de respuesta. Por lo anterior, solicitó al doctor Hernández Martínez y al licenciado González Ramírez, en su calidad de Director Técnico y Director Administrativo, respectivamente, instruir a sus áreas administrativas para que se dé respuesta en el menor tiempo posible a las solicitudes de la información que generen y/o posean, cuidando la calidad de las respuestas y que éstas atiendan de manera puntual lo solicitado por el ciudadano.

**4. Asuntos Generales.**

- Protocolo de atención a las solicitudes de información. La licenciada Pérez Reyes presentó a la consideración de los miembros del Comité de Transparencia una nueva versión del Protocolo de atención a las solicitudes de información, mediante el cual se orienta a las unidades administrativas para una atención expedita de las solicitudes de información. Los integrantes del Comité revisarán el documento y harán llegar a la licenciada Pérez Reyes los comentarios o modificaciones que juzguen convenientes.
- Como segundo asunto general, la maestra Briones Zavala y el licenciado González Ramírez señalaron la conveniencia de revisar y, en su caso, actualizar el Reglamento del Comité de Transparencia, a fin de alinear su funcionamiento al marco jurídico vigente. De lo anterior, el Dr. Hernández Martínez tomó debida nota para los efectos procedentes.

Al no haber más asuntos a tratar, el doctor Hernández agradeció la participación y presencia de los miembros del Comité y dio por concluida la reunión a las quince horas del mismo día de su inicio.

| | |
|---|---|
| PRESIDENTE DEL COMITÉ | TITULAR DEL ÓRGANO INTERNO DE CONTROL |
| DR. ALFREDO HERNÁNDEZ MARTÍNEZ<br>DIRECTOR TÉCNICO | MTRA. FLOR DE MARÍA BRIONES ZAVALA |
| RESPONSABLE DEL ÁREA COORDINADORA DE ARCHIVOS | COORDINADORA DE LA UNIDAD DE TRANSPARENCIA |
| LIC. MIGUEL GONZÁLEZ RAMÍREZ<br>DIRECTOR ADMINISTRATIVO | LIC. ELVIA PÉREZ REYES<br>DIRECTORA DE INVESTIGACIÓN ECONÓMICA |