RESOLUCIÓN DEL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA EJECUTIVA DEL SISTEMA NACIONAL ANTICORRUPCIÓN CON MOTIVO DE LA DECLARACIÓN DE CLASIFICACIÓN REALIZADA POR LA UNIDAD DE SERVICIOS TECNOLÓGICOS Y PLATAFORMA DIGITAL NACIONAL (USTPDN), RELATIVA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA CON NÚMERO DE FOLIO 331637022000231.

ANTECEDENTES

I. El 04 de mayo de 2015, se publicó en el Diario Oficial de la Federación la Ley General de Transparencia y Acceso a la Información Pública (**LGTAIP**).

II. El 27 de mayo de 2015 se publicó en el Diario Oficial de la Federación el "Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de combate a la corrupción", mediante el cual se reformó, entre otros, el artículo 113 constitucional, instituyéndose el Sistema Nacional Anticorrupción (**SNA**) como la instancia de coordinación entre las autoridades de todos los órdenes de gobierno competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de recursos públicos.

III. El 15 de abril de 2016, se publicó en el Diario Oficial de la Federación los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas (**Lineamientos**).

IV. El 09 de mayo de 2016, se publicó en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública (**LFTAIP**).

V. El 18 de julio de 2016, se publicó en el Diario Oficial de la Federación el Decreto del Titular del Poder Ejecutivo Federal, por el que se expidió la Ley General del Sistema Nacional Anticorrupción (**LGSNA**) cuyo artículo 24 dispone la creación de un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio, con autonomía técnica y de gestión, con sede en la Ciudad de México, denominado Secretaría Ejecutiva del Sistema Nacional Anticorrupción (**SESNA**).

VI. El artículo Cuarto transitorio de la Ley General del Sistema Nacional Anticorrupción (**LGSNA**) establece que la **SESNA** debía iniciar sus operaciones, a más tardar a los sesenta días siguientes a la sesión de instalación del Comité Coordinador del **SNA**.

VII. El día 04 de abril de 2017 se instaló el Comité Coordinador del **SNA**.

Viaducto presidente Miguel Alemán Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

VIII. El día el 27 de junio de 2022, en la Primera Sesión Extraordinaria del Órgano de Gobierno de la **SESNA** del mismo año, fue nombrado el nuevo Secretario Técnico, persona servidora pública con funciones de dirección de esta Secretaría, como las demás que le confiere la **LGSNA**.

IX. Con fecha del 03 de octubre de 2022 fue presentada la **solicitud de acceso a la información pública** con número de folio **331637022000231** a través del Sistema de Solicitud de Acceso a la Información de la Plataforma Nacional de Transparencia, misma que se transcribe a continuación:

> *"**Descripción clara de la solicitud de información***
> "Podrían responder a la pregunta: ¿Cómo previene la dependencia ataques de cibernéticos y/o hackeo? -Solicito información y registro acerca de los intentos de ciberataques, hackeo o filtración de información que la dependencia ha sufrido del 2012 a la fecha. -Solicito las auditorías realizadas en materia de evaluación de ciberseguridad realizadas en la dependencia -Solicito información sobre los softwares, programas o medidas de protección de ciberseguridad en su dependencia, así como las fechas en que comenzaron a utilizarse, sus actualizaciones. -Igualmente, solicito información sobre capacitaciones recibidas de 2012 a la fecha en torno a ciberseguridad a elementos de su dependencia." *(SIC)*.

X. El 03 de octubre de 2022, la **Unidad de Transparencia** turnó la solicitud a la **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)** por ser la unidad administrativa competente para dar respuesta.

XI. El 18 de octubre de 2022, la **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)** dio respuesta a la solicitud 331637022000231, argumentando lo siguiente:

> "**-Podrían responder a la pregunta: ¿Cómo previene la dependencia ataques de cibernéticos y/o hackeo?**
> La dependencia se apega al marco regulatorio ISO 27001 con el objetivo de disminuir los riesgos mediante la implementación de un Sistema de Gestión de la Seguridad de la Información y la implementación de acciones clave como:
>
> - Diagnostico integral de seguridad
> - Evaluación y tratamiento de riesgos
> - Gobierno de la seguridad de la información

Viaducto presidente Miguel Alemán Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo. C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

-Solicito información y registro acerca de los intentos de ciberataques, hackeo o filtración de información que la dependencia ha sufrido del 2012 a la fecha.

La institución fue creada en 2017 y de esa fecha al día de hoy, la institución no ha tenido brechas de ciberseguridad

-Solicito las auditorías realizadas en materia de evaluación de ciberseguridad realizadas en la dependencia

No se han realizado auditorías en la materia. Sin embargo, la SESNA ha realizado un diagnóstico de seguridad para detectar y atender cualquier posible vulnerabilidad tanto de la institución como de las plataformas tecnológicas que maneja. Este estudio fue realizado por un tercero por lo que los datos que contiene son de carácter reservado.

-Solicito información sobre los softwares, programas o medidas de protección de ciberseguridad en su dependencia, así como las fechas en que comenzaron a utilizarse, sus actualizaciones.

La información específica sobre software, programas y medidas de protección de ciberseguridad se considera de carácter reservado al contener información sensible como versiones específicas de software y configuraciones, motivo por el cual no es posible compartir esta información, sin embargo, se comunica que la SESNA cuenta con mecanismos y estrategias de seguridad que ayudan a disminuir el riesgo y la posibilidad de un ataque, se mencionan algunas estrategias a continuación:

- Gestión activa de bots
- Políticas de respaldo
- OAuth 2.0
- Web Aplication Firewall
- Firewalls perimetrales
- Sistemas de detección de intrusos
- Sistema de filtrado de contenido
- Política de contraseñas seguras
- Captchas
- Aplicación de actualizaciones y parches
- VPN's
- Antivirus
- Certificados SSL
- Escaneo de vulnerabilidades

-Igualmente, solicito información sobre capacitaciones recibidas de 2012 a la fecha en torno a ciberseguridad a elementos de su dependencia.

Viaducto presidente Miguel Alemán Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

La institución fue creada en 2017 y de esa fecha al día de hoy, el personal de la institución no ha recibido, por parte de la SESNA, capacitación en materia de ciberseguridad.

Al respecto, me permito **solicitar se someta a consideración del comité de Transparencia la reserva de la información del punto 3 y 4 debido a que incluye información que se considera reservada, lo anterior con fundamento en el artículo 110 fracción VII y VIII de la LGTAIP.**

Prueba de Daño

En virtud de lo antes mencionado, **se considera que, al revelar** la información solicitada referente **en materia de evaluación de ciberseguridad realizadas en la dependencia** e **información sobre los softwares, programas o medidas de protección de ciberseguridad,** trata de características técnicas muy específicas de la infraestructura tecnológica (versiones específicas de software y configuraciones, sistemas y equipos de informática), dando a conocer las vulnerabilidades y los planes de remediación que la SESNA contempla para su mitigación; la cual contiene información sensible que al darlos a conocer revelarían elementos que de ser utilizados de una manera malintencionada, ponen en riesgo la integridad de la información y los sistemas de esta Secretaría propiciando que **se cause un daño presente, probable y específico**, revelando elementos que pudieran ser usados para intentar vulnerar nuestros controles de seguridad.

La infraestructura tecnológica (sistemas y equipos de informática), así como los mecanismos de seguridad informática de la SESNA, minimizan posibles riesgos para mantener la confidencialidad, integridad y disponibilidad de la información resguardada de la institución, la cual es considerada como sensible, **toda vez que dicha información es utilizada para** mantener a salvo la información de la institución por lo cual; el proporcionar la información de configuración de dicha infraestructura podría ser usada para facilitar el acceso de un tercero a la red institucional, **lo cual propicia la vulneración de** lo que culminaría en un riesgo al sistema interno de la institución, consumándose con ello el delito de acceso ilícito a sistemas y equipos de informática, motivo por el cual no es posible compartir esta información, lo anterior con fundamento en el **artículo 110 fracción VII de la Ley Federal de Transparencia y acceso a la información pública (LFTAIP)**."

XII. Por lo antes expuesto, se solicita que, se someta a consideración del Comité de Transparencia de la **SESNA**, esta clasificación, a efecto de que dicho órgano colegiado confirme la clasificación de la información relativa a la **evaluación de ciberseguridad realizada en la dependencia e información sobre los softwares, programas o medidas de protección de ciberseguridad**, con fundamento en el

Viaducto presidente Miguel Aleman Valdés, Núm. 105, Col. Escandon Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

artículo 110 fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), por considerarse reservada por un plazo de **tres años.**

XIII. En esa tesitura, este Comité de Transparencia procede a valorar las manifestaciones expuestas por la **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)**, de conformidad con los siguientes:

C O N S I D E R A N D O S

Primero.- El Comité de Transparencia de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción es competente en términos de los artículos 43 y 44, fracción II de la Ley General de Transparencia y Acceso a la Información Pública y Sexagésimo segundo de los *Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas,* para confirmar, modificar o revocar las determinaciones que en materia de clasificación de la información realicen los titulares de las áreas de los sujetos obligados y aprobar las versiones públicas elaboradas para el cumplimiento de las obligaciones de transparencia establecidas en los Títulos Quinto de la **LGTAIP** y Tercero de la **LFTAIP**.

Al respecto es importante señalar que el artículo 97 de la **LFTAIP** dispone que:

> ***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.*
>
> *(...)*
>
> *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.*
>
> *(...)*

Segundo. – La **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)** ha realizado un **diagnóstico de seguridad para detectar y atender cualquier posible vulnerabilidad tanto de la institución como de las plataformas**

Viaducto presidente Miguel Aleman Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

tecnológicas que maneja. Este estudio fue realizado por un tercero por lo que los datos que contiene son de carácter reservado y por otra parte **al revelar** la información solicitada referente **en materia de evaluación de ciberseguridad realizadas en la dependencia** e **información sobre los softwares, programas o medidas de protección de ciberseguridad,** trata de características técnicas muy específicas de la infraestructura tecnológica (versiones específicas de software y configuraciones, sistemas y equipos de informática), dando a conocer las vulnerabilidades y los planes de remediación que la SESNA contempla para su mitigación; la cual contiene información sensible que al darlos a conocer revelarían elementos que de ser utilizados de una manera malintencionada, ponen en riesgo la integridad de la información y los sistemas de esta Secretaría propiciando que **se cause un daño presente, probable y específico**, revelando elementos que pudieran ser usados para intentar vulnerar nuestros controles de seguridad.

Tercero. - La información reservada por la **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)** es la referente a:

- **Diagnóstico de seguridad para detectar y atender cualquier posible vulnerabilidad tanto de la institución como de las plataformas tecnológicas que maneja.**

- **Información sobre los softwares, programas o medidas de protección de ciberseguridad.**

Cuarto. - La clasificación de la información testada tiene fundamento en los artículos 97 (ya transcrito) y 110, fracción VII de la **LFTAIP**, que se reproducen para mayor referencia:

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;

(...)

En el caso, también resulta aplicable el Vigésimo sexto de los Lineamientos *Generales en*

Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas:

> ***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 imitar la capacidad de las autoridades para evitar la comisión de delitos.*
>
> *(...)*

Por su parte, para la aplicación de la prueba de daño, el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública (**LGTAIP**), determina 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.*

Quinto. - La información clasificada por la **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)** como reservada de acuerdo con los siguientes argumentos:

> ***"Prueba de Daño***
>
> - En virtud de lo antes mencionado, **se considera que, al revelar** la información solicitada referente **en materia de evaluación de ciberseguridad realizadas en la dependencia** e **información sobre los softwares, programas o medidas de protección de ciberseguridad,** trata de características técnicas muy específicas de la infraestructura tecnológica (versiones específicas de software y configuraciones,

Viaducto presidente Miguel Aleman Valdés, Núm. 105, Col. Escandon Seccion 1, Alcaldia Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

sistemas y equipos de informática), dando a conocer las vulnerabilidades y los planes de remediación que la SESNA contempla para su mitigación; la cual contiene información sensible que al darlos a conocer revelarían elementos que de ser utilizados de una manera malintencionada, ponen en riesgo la integridad de la información y los sistemas de esta Secretaría propiciando que **se cause un daño presente, probable y específico**, revelando elementos que pudieran ser usados para intentar vulnerar nuestros controles de seguridad.

- La infraestructura tecnológica (sistemas y equipos de informática), así como los mecanismos de seguridad informática de la SESNA, minimizan posibles riesgos para mantener la confidencialidad, integridad y disponibilidad de la información resguardada de la institución, la cual es considerada como sensible, **toda vez que dicha información es utilizada para** mantener a salvo la información de la institución por lo cual; el proporcionar la información de configuración de dicha infraestructura podría ser usada para facilitar el acceso de un tercero a la red institucional, **lo cual propicia la vulneración de** lo que culminaría en un riesgo al sistema interno de la institución, consumándose con ello el delito de acceso ilícito a sistemas y equipos de informática, motivo por el cual no es posible compartir esta información, lo anterior con fundamento en el **artículo 110 fracción VII de la Ley Federal de Transparencia y acceso a la información pública (LFTAIP)**."

En ese orden de ideas y de conformidad con los elementos con que cuenta éste Comité de Transparencia, determina la información relativa a la **evaluación de ciberseguridad y la información sobre los softwares, programas o medidas de protección de ciberseguridad** son de carácter reservado con fundamento en el artículo 110, fracción VII de la LFTAIP, lo anterior en razón que la difusión de las mismas podría menoscabar o limitar la capacidad de este sujeto obligado para evitar la comisión de delitos e incluso propiciar la comisión de los mismos máxime que en esas secciones se establece la manera en la cual está resguardada la información de la institución, así como su protección y las áreas de oportunidad que tiene este sujeto obligado en la salvaguarda de sus **archivos electrónicos ante los casos recientes de hackeo a instancias gubernamentales.**

Al respecto, se considera correcta la valoración de la **Unidad de Servicios Tecnológicos y Plataforma Digital Nacional (USTPDN)** respecto a la relevancia de reservar la información antes mencionada para salvaguardar la capacidad de funcionamiento de este sujeto obligado.

En conclusión, se considera que las **Medidas de Seguridad Informática** de los sistemas de la SESNA incluyendo la Plataforma Digital Nacional es información de carácter reservada,

Viaducto presidente Miguel Alemán Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

en consecuencia, son susceptibles de ser clasificados como reservada de conformidad con lo establecido en el artículo 110, fracción VII de la **LFTAIP**.

Sexto. - Por lo que hace el plazo de reserva, la **Unidad de Transparencia** estimó **tres años**, por lo que este Órgano Colegiado atendiendo a las circunstancias de modo, tiempo y lugar, se considera procedente el periodo señalado para la reserva a partir del **19 de octubre 2022**, fecha en que el Comité de Transparencia de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción confirmó dicho plazo.

De esta manera, se cumple con lo establecido en el artículo 100 de la **LFTAIP**, que señala lo siguiente:

> ***Artículo 100****. Al clasificar información con carácter de reserva es necesario, en todos los casos, fijar un plazo de reserva.*

Séptimo. - Derivado de los argumentos expresados, este Órgano Colegiado considera que fue agotado el procedimiento establecido en el artículo 140 de la **LFTAIP**, mismo que es citado para mayor precisión:

> ***Artículo 140.*** *En caso de que los sujetos obligados consideren que los Documentos o la información requerida deban ser clasificados, deberá seguirse el procedimiento previsto en el Capítulo I del Título Séptimo de la Ley General, atendiendo además a las siguientes disposiciones:*
>
> ***I.*** *Confirmar la clasificación;*
> ***II.*** *Modificar la clasificación y otorgar total o parcialmente el acceso a la información, y*
> ***III.****Revocar la clasificación y conceder el acceso a la información.*
>
> *El Comité de Transparencia podrá tener acceso a la información que esté en poder del Área correspondiente, de la cual se haya solicitado su clasificación.*
>
> *La resolución del Comité de Transparencia será notificada al interesado en el plazo de respuesta a la solicitud que establece el artículo 135 de la presente Ley.*

Con base en lo anteriormente expuesto y con fundamento en lo dispuesto por los artículos 64, 65, fracción II, 97, 100, 110, fracción VII; y 140 de la **LFTAIP**; 104 de la **LGTAIP**; el Vigésimo

Viaducto presidente Miguel Aleman Valdés, Núm. 105, Col. Escandón Seccion 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

sexto de los **Lineamientos**, este Comité de Transparencia por unanimidad emite la siguiente:

R E S O L U C I Ó N

PRIMERO.- En términos del artículo 140, fracción I de la **LFTAIP,** se **CONFIRMA** la **clasificación de la información como reservada** de la información relativa a: **evaluación de ciberseguridad y la información sobre los softwares, programas o medidas de protección de ciberseguridad** considerando que se relacionan con el **Documento de Seguridad SESNA 2022** y el **Documento de Seguridad de la Plataforma Digital Nacional 2022 cuyas versiones públicas fueron aprobadas en la Décima sesión Extraordinaria de este Comité el pasado 29 de junio de 2022.**

SEGUNDO. - Se confirma que el periodo de reserva sea por tres años, en términos de los señalado en el Considerando SEXTO de la presente resolución.

TERCERO. - **NOTIFÍQUESE** copia de la presente resolución a la persona solicitante, a través de la vía elegida al presentar la solicitud de acceso a la información pública.

CUARTO. - Publíquese la presente resolución en el sitio de internet de este sujeto obligado.

QUINTO.- Se hace del conocimiento de la persona solicitante, que de conformidad con lo dispuesto en los artículos 142 y 143 de la Ley General de Transparencia y Acceso a la Información Pública, 147 y 148 de la Ley Federal de Transparencia y Acceso a la Información Pública, podrá interponer, por sí mismo o a través de su representante, de manera directa o por escrito, o por medios electrónicos, recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (**INAI**) o ante esta Unidad de Transparencia, dentro de los 15 días hábiles siguientes a la fecha de la notificación de la respuesta, medio de impugnación que deberá contener los requisitos previstos en el artículo 149 de la Ley Federal mencionada.

Así lo resolvieron, los integrantes del Comité de Transparencia de la **SESNA**, el día 19 de octubre de 2022.

Viaducto presidente Miguel Aleman Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx

LIC. RICARDO BAEZA SANTANA
Titular de la Unidad de Transparencia
Presidente del Comité de Transparencia

LIC. AIDA GUADALUPE MORENO NEYRA
Suplente del Responsable del Área
Coordinadora de Archivos

MTRA. MÓNICA VARGAS RUIZ
Titular del Órgano Interno de Control en la
Secretaría Ejecutiva del Sistema Nacional
Anticorrupción

Viaducto presidente Miguel Aleman Valdés, Núm. 105, Col. Escandón Sección 1, Alcaldía Miguel Hidalgo, C.P. 11800, CDMX. Tel. +52 55 5131 5645 www.sesna.gob.mx