SEMARNAT

SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

RESOLUCIÓN NÚMERO 400/2018 DEL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES (SEMARNAT) DERIVADA DE LA SOLICITUD DE INFORMACIÓN CON NÚMERO DE FOLIO 0001600345718

ANTECEDENTES

I. El 10 de septiembre de 2018 la Unidad de Transparencia de la SEMARNAT recibió a través de la Plataforma Nacional de Transparencia y, posteriormente, turnó a la **Dirección General de Informática y Telecomunicaciones (DGIT),** la siguiente solicitud de acceso a información con número de folio **0001600345718:**

> *"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. Ordenado por Número de serie, de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada equipo. b. Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso a. c. Forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP (por sus siglas en ingles Internet protocol) privada en la red (de forma manual o por medio del Protocolo de Configuración Dinámica de Host DHCP, por sus siglas en ingles Dynamic Host Configuration Protocol). d. Domicilio actual en donde se encuentra físicamente cada equipo..."* ***(Sic)***

II. Con fecha 8 de octubre de 2018, la Unidad de Transparencia notificó, a través del Oficio **SEMARNAT/UCPAST/UT/2897/18**, la siguiente **respuesta**:

> *"La Dirección General de Informática y Telecomunicaciones (DGIT), le anexa la información solicitada informa 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. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado***

ROUTER

SITIO	*TIPO SITIO*	*EQUIPO*	*FABRICANTE*	*NUMERO DE PARTE*	*NUMERO DE SERIE*
SEMARNAT DEL GUERRERO	*REMOTO*	*ROUTER*	*HUAWEI*	*AR1220E*	*2102350DQJDMH10 00025*
SEMARNAT AGUASCALIENTES	*REMOTO*	*ROUTER*	*HUAWEI*	*AR1220E*	*2102350DQJDMGB0 00086*
SEMARNAT DEL BCS	*REMOTO*	*ROUTER*	*HUAWEI*	*AR1220E*	*2102350DQJDMGB0 00091*
SEMARNAT DEL CAMPECHE	*REMOTO*	*ROUTER*	*HUAWEI*	*AR1220E*	*2102350DQJDMGB0 00108*
SEMARNAT DEL CHIAPAS	*REMOTO*	*ROUTER*	*HUAWEI*	*AR1220E*	*2102350DQJDMGB0 00097*
					...

...

a y b. Nombre aquéllas Personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada Equipo.

Las contraseñas son administradas por la Dirección de Infraestructura Tecnológica, la cual pertence a la Dirección General de Informática y Telecomunicaciones de la SEMARNAT. Esto en el ejercicio de sus facultades de acuerdo al artículo 37 del ReglqmentoInterior de la SEMARNAT.

c. Forma en que cada equipo obtiene o asigna, segun sea el caso, la dirección IP (por sus siglas en inglés Internet Protocol) privada en la red (de forma manual o por medio del Protocolo de Configuración Dinámica de host DHCP) por sus siglas en ingles Dynamic Host Configuration Protocol)

Todo el equipamiento DE COMPUTO se conecta mediante DHCP:
Para las oficinas centrales a través del CORE y Delegaciones y Regionales a través de los switches y Router

4. Domicilio actual en dónde se encuentra físicamente cada equipo
Para el equipo de computo, routers y access point anexo la relacion de los domicilios.

Sitios Centrales:

	CIUDAD	SITIO	DOMICILIO
1	CD.MX	EJÉRCITO NACIONAL (SEDE)	Av. Ejército Nacional No. 223 Esq. Lago Xochimilco, Col Anáhuac I Sección, Delegación Miguel Hidalgo C.P. 11320, Ciudad de México
2	CD.MX	CONAGUA (DATA CENTER)	Av de los Insurgentes Sur 2416, Copilco Universidad, Coyoacán, C.P. 04360
3	CD.MX	INEGI	Héroes De Nacozari Sur 2301 Pisos 1 Fracc. Jardines Del Parque, Ags.
4	CD.MX	EDIFICIO VIVEROS	Progreso No.3. Col Del Carmen Coyoacán C.P. 04100 México D.F.
5	CD.MX	PARQUE SAN ANTONIO	Avenida Central No. 300 Col La Carola Delegación Álvaro Obregón C.P. 01180
			....

'..." (Sic)

III. Con fecha 23 de octubre de 2018, la Unidad de Transparencia recibió a través del Sistema de Gestión de Medios de Impugnación (**SIGEMI**), el **acuerdo** emitido por el Secretario de Acuerdos y Ponencia de Acceso a la Información, a través del cual admitió a trámite el **Recurso de Revisión** radicado con el número de expediente **RRA 7336/18,** toda vez que acreditó los requisitos contenidos en los artículos 147, 148, 149 y 156 fracción I de la LFTAIP.

IV. Con fecha 21 de octubre de 2018, el solicitante interpuso recurso de revisión ante ese Instituto, los motivos de su **queja** del mencionado recurso son los siguientes:

> ***"El sujeto Obligado entrega información que no corresponde con lo peticionado en la solicitud 0001600345718: esto por lo que hace a los incisos a) y b) del numeral 1" (Sic).***

V. Con fecha 23 de octubre de 2018, y con el fin de atender el Recurso de Revisión mencionado en el punto III, la Unidad de Transparencia lo turnó a la Unidad Administrativa **DGIT** para atender el citado Recurso admitido por el INAI.

VI. Que mediante el oficio número **Oficio Número DGIT/513/370/18,** del 31 de octubre de 2018, la **DGIT** informó al Presidente de del Comité de Transparencia de la SEMARNAT que la información *es* susceptible de ser clasificada como **INFORMACIÓN RESERVADA por un cinco años**, y continuar dicha reserva si prevalecen las casusas de la misma. Lo anterior de conformidad con lo establecido por **artículos 104 y 113 fracción V** de la Ley de General de Transparencia y Acceso a la Información Pública (**LGTAIP**); el artículo **110 fracción V** de la Ley Federal de Transparencia y Acceso a la Información Pública (**LFTAIP**), así como del **vigésimo tercero y trigésimo tercero** de los **Lineamientos Generales** en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, conforme al cuadro que se describe a continuación:

"...

DESCRIPCIÓN DE LO QUE SE CLASIFICA COMO RESERVADA	*MOTIVO*	*FUNDAMENTO LEGAL*
"Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)" *(Sic)*	***Debido a que la información solicitada, si llegara a ser entregada o divulgada, puede poner en RIESGO LA VIDA, SEGURIDAD, O SALUD DE UNA PERSONA FÍSICA.***	*Artículos **104 y 113 fracción V** de la **Ley de General** de Transparencia y Acceso a la Información Pública.* ***Artículo 110 fracción V de la Ley Federal** de Transparencia y Acceso a la Información Pública.* ***Vigésimo tercero y trigésimo tercero de los Lineamientos** Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.*

..." (Sic)

Asimismo, de conformidad con los **artículos 104** y **113 fracciones V de la LGTAIP** la **DGIT** mencionó en el oficio número **Oficio No. DGIT/513/370/18** la manera en que se acredita los elementos de la prueba de daño y el **vigésimo tercero y trigésimo tercero,** de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para las Versiones Públicas con los supuestos siguientes:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;

Daño real: *La divulgación de la información puede resultar en una brecha de seguridad informática para la SEMARNAT, ya que al ser identificables los servidores públicos que resguardan la información sensible y estratégica, pone en riesgo la seguridad de la institución, así como la identificación, susceptibilidad e integridad de las propias personas responsables de dicha confidencialidad.*

Daño demostrable: *Dar a conocer al solicitante los nombres de las personas físicas que resguardan las claves, permisos informáticos, credenciales administrativas, privilegios de superusuario, root, contraseñas de administrador de los equipos mencionados de la dependencia, pone en riesgo su vida, integridad y seguridad.*

Daño identificable: *Hacer pública la información solicitada podría generar mal uso de la misma, pues al ser identificables los servidores públicos que resguardan información de alta seguridad, generaría un daño identificable y potencial a la vida, seguridad e integridad de su persona, así como abrir la posibilidad de que los requirentes tengan la capacidad de acceder a las claves de administrador o superusuario, acceso a los equipos y sistemas institucionales, es decir, un riesgo inminente a la seguridad informática de la SEMARNAT, acceso a expedientes, información sensible, reservada o confidencial y, por ende, poner en riesgo datos personales de los ciudadanos que utilizan los servicios de la Secretaría.*

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda;

Poner a disposición la información solicitada, implica un riesgo inminente y pone en peligro la integridad y seguridad de las personas físicas responsables de resguardar esta información, ya que al revelar sus nombres, son susceptibles de ser objetivos clave en el caso de un ataque cibernético a la institución, por ser estos servidores públicos depositarios de las *"contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)"*, facilitarían el acceso a la infraestructura de la dependencia por cualquier medio remoto o local, poniendo en riesgo la información estratégica, reservada, confidencial, los sistemas informáticos, servidores, redes y datos personales de los ciudadanos que usan los servicios de la SEMARNAT.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio,

La información solicitada no aporta interés público a la ciudadanía, ya que forma parte de la funciones inherentes a la Dirección General de Informática y Telecomunicaciones (DGIT) y, asimismo la SEMARNAT debe cumplir con el artículo 3, fracción XXIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que establece que los sujetos obligados deben garantizar las medidas de seguridad técnicas, "acciones y mecanismos

que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento", asimismo "prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados". Esta información solo debe ser de conocimiento interno y no aporta ningún beneficio al ponerla a disposición del público, además de que se deben proteger los nombres de las personas responsables de resguardar las "contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)" pues es de mayor importancia estratégica y seguridad el reservarla.

Asimismo, de conformidad con el trigésimo tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, se justifican los siguientes elementos:

I. Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;

Artículos 104 y 113 fracción V de la Ley de General de Transparencia y Acceso a la Información Pública.
Artículo 110 fracción V de la Ley Federal de Transparencia y Acceso a la Información Pública.
Vigésimo tercero y trigésimo tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y, por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;

El beneficio asociado a la atención de la solicitud de información es inexistente, pues es mayor el daño potencial a la seguridad de las personas que resguardan la información y a la vulnerabilidad de los sistemas informáticos de la SEMARNAT que el interés público de conocerla. De proporcionar la información, se estarían colocando en riesgo a las personas físicas involucradas en la seguridad informática de la Secretaría, lo que podría generar canales de comunicación e identificación de los responsables de su resguardo, vulnerabilidad a su persona, riesgo de la información protegida y acceso a toda la información y redes internas de esta dependencia. Se considera que el interés de un tercero no es mayor a la obligación que se tiene de actuar conforme a derecho, y es mayor la responsabilidad de garantizar la protección de la información (datos personales, secreto industrial, información clasificada, confidencial, sensible o estratégica que ahí se almacena), así como la seguridad informática de la dependencia.

III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate;

La difusión de la información solicitada podría poner en riesgo inminente la seguridad informática de la dependencia y la integridad física o amenaza a las personas que los resguardan, por lo que es mayor la responsabilidad de garantizar la protección de la información (datos personales, secreto industrial, información clasificada, confidencial, sensible o estratégica que ahí se almacena), así como la seguridad informática de la SEMARNAT.

IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;

En la sección de la prueba de daño, se mencionan los riesgos y daños reales, demostrables e identificables.

V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y

Circunstancias de modo:

Al ser parte inherente a las funciones de la DGIT, la difusión de la información solicitada, es decir el "nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)", vulneraría la integridad física o amenaza a las personas que la resguardan, facilitaría el acceso e identificación de responsables y transgrediría la protección de la información almacenada en los servidores (datos personales, secreto industrial, información clasificada, confidencial, sensible o estratégica) y la seguridad informática la Semarnat.

Circunstancias de tiempo:

La información deberá reservarse por un periodo de cinco años, y continuar dicha reserva si prevalecen las casusas de la misma.

Circunstancias de lugar del daño:

Debido a las facilidades de la tecnología, el daño puede ser realizado dentro o fuera de las instalaciones de la SEMARNAT.

VI. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.
Los demás puntos indicados en la citada solicitud de información se proporcionaron en su momento, a excepción del "inciso a", es decir, el "nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada equipo", por las razones arriba indicadas.

De conformidad con el vigésimo tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, será necesario acreditar un vínculo, entre la persona física y la información que pueda poner en riesgo su vida, seguridad o salud:

Revelar la información sobre las personas responsables de las contraseñas de administración de los equipos de la SEMARNAT pone en riesgo su vida, integridad física y seguridad al ser identificables y hacer públicos sus datos. Adicionalmente, los solicitantes, aplicando los conocimientos técnicos necesarios y contando con las claves de acceso, pueden poner en inminente riesgo la seguridad de toda la información y los sistemas informáticos de la dependencia, así como de sus equipos de cómputo.

CONSIDERANDO

I. Que este Comité de Transparencia es competente para confirmar, modificar o revocar la clasificación de información que realicen los titulares de las Áreas de la SEMARNAT, en los términos que establecen los artículos 65, fracción II; 102, primer párrafo; 140, segundo párrafo y segundo párrafo del Segundo Transitorio de la LFTAIP; 44, fracción II; 103, primer párrafo; 137 segundo párrafo y Tercero Transitorio de la LGTAIP; así como el vigésimo quinto de los Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública.

II. Que la fracción del artículo 113 de la LFTAIP y el primer párrafo del artículo 116 de la LGTAIP establecen que se considera información confidencial la que contiene datos personales concernientes a una persona física identificada o identificable.

III. Que el primer párrafo del artículo 117 de la LFTAIP y el primer párrafo del artículo 120 de la LGTAIP establecen que para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información.

IV. Que en la fracción I del Trigésimo Octavo de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas publicado en el Diario Oficial de la Federación, el 15 de abril del 2017, se establece que se considera como información confidencial, los datos personales en términos de la norma aplicable.

V. Que el sujeto obligado deberá acreditar la aplicación de la prueba de daño, de conformidad con el **artículo 104** de la LGTAIP, así como el **trigésimo tercero** de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas

VI. Que en los **artículos 113 fracción V** de la LGTAIP y **110 fracción V** de la LFTAIP, de conformidad con el **vigésimo tercero** de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Publicas establecen como información reservada, aquella **que pueda poner en riesgo la vida, seguridad o salud de una persona física.**

VII. Que en el oficio número **DGIT/513/370/18**, la **DGIT** informó al Presidente del Comité de Transparencia, los motivos y fundamentos para considerar que la información solicitada se encuentra **RESERVADA**, mismos que consisten en:

*"**Debido a que la información solicitada, si llegara a ser entregada o divulgada, puede poner en RIESGO LA VIDA, SEGURIDAD, O SALUD DE UNA PERSONA FÍSICA.**" (Sic)*

VIII. De conformidad con lo previsto en el **artículo 104 de la LGTAIP la DGIT** justificó los siguientes elementos de prueba de daño:

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.

IX. *Que el **trigésimo tercero** de los Lineamientos generales en materia de clasificación y desclasificación de la Información, así como para la elaboración de versiones públicas establece que para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General, los sujetos obligados atenderán lo siguiente.*

I. Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;

II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y, por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;

III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate,

IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;

V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y

VI. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés

público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.

La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. No se considerará que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad".

X. Que la **DGITR** acreditó lo previsto en el **Vigésimo tercero Fracción V** de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, con la finalidad de acreditar, un vínculo entre la persona física y la información que pueda **poner en riesgo su vida, seguridad o salud.**

XI. Al respecto, este Comité considera que la **DGIT**, motivó y justificó la existencia de prueba de daño conforme a lo dispuesto en el **ARTÍCULO 104 DE LA LGTAIP**, por los motivos y fundamentos que a continuación se detallan:

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;

Este Comité, considera que la DGIT justificó el presente elemento, con base en lo siguiente:

Daño real: *La divulgación de la información puede resultar en una brecha de seguridad informática para la SEMARNAT, ya que al ser identificables los servidores públicos que resguardan la información sensible y estratégica, pone en riesgo la seguridad de la institución, así como la identificación, susceptibilidad e integridad de las propias personas responsables de dicha confidencialidad.*

Daño demostrable: *Dar a conocer al solicitante los nombres de las personas físicas que resguardan las claves, permisos informáticos, credenciales administrativas, privilegios de superusuario, root, contraseñas de administrador de los equipos mencionados de la dependencia, pone en riesgo su vida, integridad y seguridad.*

Daño identificable: *Hacer pública la información solicitada podría generar mal uso de la misma, pues al ser identificables los servidores públicos que resguardan información de alta seguridad, generaría un daño identificable y potencial a la vida, seguridad e integridad de su persona, así como abrir la posibilidad de que los requirentes tengan la capacidad de acceder a las claves de administrador o superusuario, acceso a los equipos y sistemas institucionales, es decir, un riesgo inminente a la seguridad informática de la SEMARNAT, acceso a expedientes, información sensible, reservada o confidencial y, por ende, poner en riesgo datos personales de los ciudadanos que utilizan los servicios de la Secretaría.*

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda;

Este Comité, considera que la **DGIT** justificó el presente elemento, con base en lo siguiente:

Poner a disposición la información solicitada, implica un riesgo inminente y pone en peligro la integridad y seguridad de las personas físicas responsables de resguardar esta información, ya que al revelar sus nombres, son susceptibles de ser objetivos clave en el caso de un ataque cibernético a la institución, por ser estos servidores públicos depositarios de las "contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)", facilitarían el acceso a la infraestructura de la dependencia por cualquier medio remoto o local, poniendo en riesgo la información estratégica, reservada, confidencial, los sistemas informáticos, servidores, redes y datos personales de los ciudadanos que usan los servicios de la SEMARNAT.

III. La limitación se adecúa al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio:

Este Comité, considera que la **DGIT** justificó el presente elemento, con base en lo siguiente:

La información solicitada no aporta interés público a la ciudadanía, ya que forma parte de la funciones inherentes a la Dirección General de Informática y Telecomunicaciones (DGIT) y, asimismo la SEMARNAT debe cumplir con el artículo 3, fracción XXIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que establece que los sujetos obligados deben garantizar las medidas de seguridad técnicas, "acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento", asimismo "prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados". Esta información solo debe ser de conocimiento interno y no aporta ningún beneficio al ponerla a disposición del público, además de que se deben proteger los nombres de las personas responsables de resguardar las "contraseñas administrativas o su equivalente

(permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)" pues es de mayor importancia estratégica y seguridad el reservarla.

De igual manera, este Comité considera que la **DGIT** demostró los elementos previstos en el **vigésimo tercero** de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, mismos que quedaron acreditados como a continuación se indica:

Revelar la información sobre las personas responsables de las contraseñas de administración de los equipos de la SEMARNAT pone en riesgo su vida, integridad física y seguridad al ser identificables y hacer públicos sus datos. Adicionalmente, los solicitantes, aplicando los conocimientos técnicos necesarios y contando con las claves de acceso, pueden poner en inminente riesgo la seguridad de toda la información y los sistemas informáticos de la dependencia, así como de sus equipos de cómputo.

Asimismo, de conformidad con el **trigésimo tercero** de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, se justifican los siguientes elementos:

I. Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;

Este Comité considera que se expresa la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, de la siguiente manera:

Artículos 104 y 113 fracción V de la Ley de General de Transparencia y Acceso a la Información Pública.
Artículo 110 fracción V de la Ley Federal de Transparencia y Acceso a la Información Pública.
Vigésimo tercero y trigésimo tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y, por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;

Este Comité considera que se acredita que el riesgo de perjuicio rebasa el interés público protegido por la reserva, de la siguiente manera:

> *El beneficio asociado a la atención de la solicitud de información es inexistente, pues es mayor el daño potencial a la seguridad de las personas que resguardan la información y a la vulnerabilidad de los sistemas informáticos de la SEMARNAT que el interés público de conocerla. De proporcionar la información, se estarían colocando en riesgo a las personas físicas involucradas en la seguridad informática de la Secretaría, lo que podría generar canales de comunicación e identificación de los responsables de su resguardo, vulnerabilidad a su persona, riesgo de la información protegida y acceso a toda la información y redes internas de esta dependencia. Se considera que el interés de un tercero no es mayor a la obligación que se tiene de actuar conforme a derecho, y es mayor la responsabilidad de garantizar la protección de la información (datos personales, secreto industrial, información clasificada, confidencial, sensible o estratégica que ahí se almacena), así como la seguridad informática de la dependencia.*

III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate;

Este Comité considera que se acredita el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado, de la siguiente manera:

> *La difusión de la información solicitada podría poner en riesgo inminente la seguridad informática de la dependencia y la integridad física o amenaza a las personas que los resguardan, por lo que es mayor la responsabilidad de garantizar la protección de la información (datos personales, secreto industrial, información clasificada, confidencial, sensible o estratégica que ahí se almacena), así como la seguridad informática de la SEMARNAT.*

IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;

Este Comité considera que se acreditó que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable, de la siguiente manera:

En la sección de la prueba de daño, se mencionan los riesgos y daños reales, demostrables e identificables.

V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y

Este Comité considera que se acreditaron las circunstancias de modo, tiempo y lugar del daño, de la siguiente manera:

Circunstancias de modo:

Al ser parte inherente a las funciones de la DGIT, la difusión de la información solicitada, es decir el "nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.)", vulneraría la integridad física o amenaza a las personas que la resguardan, facilitaría el acceso e identificación de responsables y transgrediría la protección de la información almacenada en los servidores (datos personales, secreto industrial, información clasificada, confidencial, sensible o estratégica) y la seguridad informática la Semarnat.

Circunstancias de tiempo:

La información deberá ***reservarse por un periodo de cinco años****, y continuar dicha reserva si prevalecen las casusas de la misma.*

Circunstancias de lugar del daño:

Debido a las facilidades de la tecnología, el daño puede ser realizado dentro o fuera de las instalaciones de la SEMARNAT.

I. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información;

Este Comité considera que se eligió la opción de excepción al acceso a la información menos restrictiva, de la siguiente manera:

Los demás puntos indicados en la citada solicitud de información se proporcionaron en su momento, a excepción del "inciso a", es decir, el "nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada equipo", por las razones arriba indicadas". ***(Sic)***

Por lo anterior, este Comité estima procedente la reservada, en virtud de que se actualiza el supuesto previsto en el artículo 113, fracción V de la LGTAIP y el artículo 110, fracción V de la LFTAIP; acorde a los elementos para la prueba de daño previstos en el artículo 104 de la LGTAIP y en los vigésimo tercero y trigésimo tercero de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas.

RESOLUTIVOS

PRIMERO. - Derivado del análisis lógico-jurídico se **confirma** la clasificación de **INFORMACIÓN RESERVADA** señalada en el **Antecedente VI**, de conformidad con lo expuesto en la parte Considerativa de la presente Resolución, por los motivos mencionados en el oficio **DGIT/513/370/18** de la **DGIT**, por un **periodo de cinco años, y continuar dicha reserva si prevalecen las casusas de la misma**. Lo anterior de conformidad con lo establecido por **artículos 104 y 113 fracción V** de la Ley de General de Transparencia y Acceso a la Información Pública; el artículo **110 fracción V** de la Ley Federal de Transparencia y Acceso a la Información Pública, así como del **vigésimo tercero y trigésimo tercero** de los **Lineamientos Generales** en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, conforme al cuadro que se describe a continuación.

SEGUNDO. - Se instruye a la Unidad de Transparencia para notificar la presente Resolución a la Titular de la **DGIT**, al solicitante, así como al INAI como parte del cumplimiento de la Resolución del Recurso de Revisión **RRA 7336/18**.

Así lo resolvió el Comité de Transparencia de la Secretaría de Medio Ambiente y Recursos Naturales el 31 de octubre de 2018.

M.A.P. Jaime García García
Presidente del Comité de Transparencia de la
Secretaría de Medio Ambiente y Recursos Naturales

Mtra. Luz María García Rangel
Suplente del Titular del Órgano Interno de Control en la
Secretaría de Medio Ambiente y Recursos Naturales

Lic. Jorge Legorreta Ordorica
Titular de la Unidad de Transparencia de la
Secretaría de Medio Ambiente y Recursos Naturales