



SEP
SECRETARÍA DE
EDUCACIÓN PÚBLICA

SESIÓN ORDINARIA

ACT/CT/SO/16/07/2019-R

Fecha:	16 de julio de 2019	Lugar:	Donceles No. 100, Colonia Centro Histórico, Alcaldía Cuauhtémoc, Ciudad de México, C.P. 06020
--------	---------------------	--------	---

MIEMBROS DEL COMITÉ DE TRANSPARENCIA

Nombre	Unidad Administrativa	Firma
Lic. Rocío Cuesta Solano.	Titular del Área de Responsabilidades y Suplente del Titular del Órgano Interno de Control en la Secretaría de Educación Pública.	
Lic. Mario Humberto Delgado González.	Responsable del Área Coordinadora de Archivos de la Secretaría de Educación Pública.	
Lic. Cuauhtémoc Rafael Montero Clavel	Director de Procesos Jurisdiccionales y suplente del Titular de la Unidad de Asuntos Jurídicos y Transparencia.	

ASUNTOS Y PUNTOS DE ACUERDO

PUNTO 1.-

ASUNTO QUE SE SOMETE A CONSIDERACIÓN: Confirmación de la clasificación de la información como reservada.



NÚMERO FOLIO: 1100400041319.

I. **Solicitud de acceso a información pública**, misma que se describe a continuación:

“Solicito por este medio el informe final de la Supervisión (auditoría) Realizada al Instituto Tecnológico de Oaxaca durante el mes de Mayo del 2019, los resultados de la misma, así como las conclusiones, recomendaciones y procedimientos administrativos derivados de la misma. El encargado de dicho procedimiento fue el Lic. (...), Director Jurídico del Tecnológico Nacional de México”(SIC).

II. El **Tecnológico Nacional de México (TecNM)** manifestó lo siguiente:

*“En relación al **Instituto Tecnológico de Oaxaca:***

- *Me permito hacer de su conocimiento que, en el Instituto de mérito, no se ha desarrollado una supervisión o auditoría en el mes de mayo de 2019. Sin embargo y en aras de la transparencia le informo que después de realizar una búsqueda exhaustiva en los archivos de este plantel se encontró el Informe Ejecutivo de Revisión Operativa al Instituto Tecnológico de Oaxaca, el cual no es posible proporcionar, toda vez, que el documento en cita forma parte de un proceso deliberativo que aún no termina, motivo por el cual es información clasificada como reservada; a continuación, señalo la prueba de daño:*
- **DOCUMENTO RESERVADO:** *Informes y toda documentación derivada de una revisión operativa llevada a cabo en el Instituto Tecnológico de Oaxaca.*
- **FUNDAMENTO LEGAL:** *Artículos 110, fracción VIII, 97, párrafo sexto;104, 105 párrafo tercero; y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, artículo 113 fracción VIII de la Ley General de Transparencia y Acceso a la Información Pública y el numeral vigésimo séptimo, de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.*
- **MOTIVACION DEL DAÑO:** *No es posible proporcionar la información relativa al informe Ejecutivo de la Revisión Operativa, toda vez que es un proceso que aún no fenece.*



- o **DAÑO PRESENTE:** Se proporcionaría información incompleta o sesgada de un procedimiento que todavía no concluye.
- o **DAÑO PROBABLE:** Entregar la información en los términos solicitados, puede afectar la conducción del procedimiento que aún no fenece.
- o **DAÑO ESPECÍFICO:** Se considera que el entregar la información solicitada por el ciudadano peticionario se estaría divulgando información incompleta o sesgada, de un proceso, que todavía no concluye.
- o Por lo tanto, **el Tecnológico Nacional de México (TecNM.),** solicita a este H. Comité, la confirmación de la clasificación de la información reservada, por un período de 6 meses, debido a que el proceso aun no fenece." (SIC).

Por tanto, el **Tecnológico Nacional de México (TecNM)** solicita a este H. Comité, la confirmación de la clasificación de la información como reservada por seis meses, en lo relativo a los informes y toda documentación derivada de una revisión operativa llevada a cabo en el Instituto Tecnológico de Oaxaca, por los argumentos anteriormente vertidos.

ACUERDO DE COMITÉ: ACT/CT/SO/16/07/2019-R.1.- CON FUNDAMENTO EN EL ARTÍCULO 65, FRACCIÓN II DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, EL COMITÉ DE TRANSPARENCIA DEL TECNOLÓGICO NACIONAL DE MÉXICO (TECNM), CONFIRMA POR UNANIMIDAD LA CLASIFICACIÓN DE LA INFORMACIÓN COMO RESERVADA POR UN PERIODO DE SEIS MESES, EN LO RELATIVO A LOS INFORMES Y TODA DOCUMENTACIÓN DERIVADA DE UNA REVISIÓN OPERATIVA LLEVADA A CABO EN EL INSTITUTO TECNOLÓGICO DE OAXACA, POR LOS ARGUMENTOS ANTERIORMENTE VERTIDOS, CON FUNDAMENTO EN LOS ARTÍCULOS 113, FRACCIÓN VIII; DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA; ASÍ COMO 97, 110, FRACCIÓN VIII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, Y EL NUMERAL VIGÉSIMO SÉPTIMO DE LOS LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN.



PUNTO 2.-

ASUNTO QUE SE SOMETE A CONSIDERACIÓN: Confirmación de la clasificación de la información como reservada.

NÚMERO FOLIO: 0001100194619.

- I. **Solicitud de acceso a información pública**, misma que se describe a continuación:

"Solicito copia simple, en versión pública, de todos los documentos que Unión de Empresarios para la Tecnología en la Educación, A.C. entregó a la Secretaría de Educación Pública, relacionados con el programa "Equipamiento de Aulas", que en el 2012 recibió un donativo de la oficialía mayor de la Secretaría de Educación Pública." (SIC)

- II. La **Unidad de Transparencia** turnó la solicitud a la **Dirección General de Presupuesto y Recursos Financieros (DGPYRF)**, quien solicita la confirmación de la clasificación de la información como reservada parcialmente en los términos siguientes:

*"Toda vez que se recibió solicitud de información con número de folio **0001100194619** en el cual requieren información que debe ser reservada por seguridad de la información, se solicita su intervención a efecto de solicitar al Comité de Transparencia y Acceso a la Información Pública la **RESERVA** de la siguiente información:*

Área: Dirección General de Tecnologías de la información y Comunicaciones.

Nombre del expediente o documento:

Número de serie de cada uno de los equipos de cómputo en posesión de la Secretaría de Educación Pública.

Tema: Seguridad Informática y seguridad de la información

*Momento de la clasificación de la información como reservada: Momento de recibir la solicitud de información pública con número de folio **0001100194619***

Plazo de reserva: Cinco años.

Fecha de inicio de la clasificación: 14 de mayo de 2019.

Fecha de término de la clasificación: 14 de mayo de 2024.



Fundamento legal de la clasificación: Artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública en relación con el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública y Lineamientos Generales en materia de Clasificación y Desclasificación en su artículo Vigésimo Sexto.

Justificación:

Entregar los datos concernientes al número de serie de equipos de cómputo en posesión de la Secretaría de Educación Pública, representa un riesgo de ataque informático, ya que incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado.

En este sentido, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la Secretaría de Educación Públicas, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática perturben el sistema de la infraestructura tecnológica de la Secretaría de Educación Pública, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, por lo tanto, en términos de lo dispuesto por los artículos 106 de la Ley General de Transparencia y Acceso a la Información Pública fracción I, 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, su análogo en el 110, fracciones VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en los Lineamientos Generales en materia de Clasificación y Desclasificación en su artículo Vigésimo Sexto, puede tener la calidad de Información reservada.

Razones y motivos de la clasificación:

En caso de proporcionar dichos números de serie, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar la información requerida:

Proporcionar el número de serie de equipos de cómputo del sujeto obligado, puede ocasionar intrusiones, robo de identidad, afectación en las comunicaciones y por ende un ataque masivo a los equipos de cómputo que se encuentren conectados en la red interna de la Secretaría de Educación Pública y con ello, una afectación en los equipos informáticos y la información contenida en estos.

De esta forma, con la publicidad de los números de serie se generaría un riesgo potencial para la infraestructura tecnológica de la Secretaría de Educación Pública, ya que pueden ser utilizados para la realización de ataques informáticos de diversa índole.

Por lo anterior, y con fundamento en los artículos 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 en los "Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la Elaboración de las Versiones Públicas", en su apartado, Décimo séptimo, último párrafo, Décimo octavo, Décimo noveno y Vigésimo

segundo, fracción I, se procede al correspondiente análisis de la PRUEBA DE DAÑO, en los siguientes términos:

Difundir o hacer del conocimiento público la información solicitada supondría una enorme ventaja para cualquier atacante de sistemas y redes de telecomunicaciones al proporcionarle herramientas para facilitar un ataque a los sistemas de telecomunicaciones con que cuenta la Secretaría poniendo en riesgo la información contenida tanto en los equipos de cómputo como la contenida en los equipos de servidores que procesan información que dependiendo el área de la Secretaría que sea atacado supondría, por ejemplo, un ataque equipos del Órgano Interno de Control o a la Unidad de Asuntos Jurídicos que podría obstruir el seguimiento de procesos administrativos en forma de juicio o entorpecer investigaciones, conocer la ubicación física de una persona identificada o identificable, realizar una suplantación de identidad.

La divulgación de la información relativa a los números de serie de los equipos de cómputo de la Secretaría de Educación Pública representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que se colocaría en estado de vulnerabilidad que permitiría el acceso ilícito de los equipos de cómputo e información contenida en estos.

RIESGO REAL

La divulgación de la información representa un riesgo real ya que de entregarse, se proporcionaría información para llevar a cabo ataques informáticos a los equipos de cómputo y equipos de procesamiento de aplicativos que cuentan con bases de datos con datos personales de ciudadanos usuarios de sistemas y portales web de la Secretaría, en concordancia con lo mencionado, cabe señalar que la SEP realiza esfuerzos para mantener la seguridad de sus equipos y sistemas, por lo cual actualmente 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 y redes de telecomunicaciones de esta Secretaría.

El riesgo de perjuicio que supondría la divulgación de información supera el interés público general de que se difunda, toda vez que la misma 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 atacar y obtener información de los equipos, redes y conocer información crítica.

RIESGO DEMOSTRABLE



En razón de que es altamente probable y de inminente peligro que dar a conocer la información solicitada, materializaría el riesgo que se busca evitar al contar con un servicio de seguridad informática, con lo cual se busca minimizar efectos negativos en la infraestructura tecnológica de la Secretaría, ejemplo de ello es que actualmente se cuenta con un servicio a administrado de seguridad informática y que el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y comunicaciones así como de la Seguridad en la Información privilegia la seguridad en los sistemas y redes de telecomunicaciones de la Administración Pública Federal.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar un perjuicio ya que únicamente se están solicitando reservar los conceptos de información que puede poner en riesgo a la infraestructura tecnológica de la Secretaría.

RIESGO IDENTIFICABLE

En el caso que nos ocupa, el riesgo identificable es el uso que se le dé a la información solicitada puesto que el mal uso de ella causaría una vulnerabilidad específica en los sistemas, equipos y redes de telecomunicaciones de la Secretaría pudiendo inhabilitar segmentos red, identificando ubicación física de los usuarios, intentos de ataque de tipo de intrusión y robo de datos, una posible intervención en la comunicación, la suplantación de equipos de la información que se almacena en el servidor, el detrimento de las instalaciones tecnológicas, el hackeo de los sistemas informáticos.

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectaría severamente el funcionamiento de la infraestructura tecnológica.

Lo anterior resulta relevante, ya que, de la negativa de acceso a la información se motiva en razón de prevenir la comisión de un delito de carácter cibernético que afectaría los equipos informáticos y la información contenida en estos.

Lo anterior en relación con el Código Penal Federal sobre el acceso ilícito a sistemas y equipos de informática dispuesto en los siguientes:

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.



Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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

En este sentido divulgar la información solicitada, permitiría que terceros contaran con los elementos para intentar algún tipo de ataque cibernético para ingresar sin autorización, a todos y cada uno de los equipos de cómputo de esta Secretaría, lo que permitiría la comisión de delitos, como podrían ser los relacionados con el acceso ilícito a sistemas y equipos informáticos, entre otros.

Ahora bien, la divulgación de esta información reservada representa un riesgo real, demostrable e identificable y de perjuicio significativo al interés público, toda vez que al hacerla pública se proveen elementos técnicos que podrían obstruir la prevención de delitos demostrables e identificables, como los de suplantación de identidad y de acceso ilícito a sistemas y equipos informáticos.

*Con base en lo anterior, en este caso particular, **concorre tanto el derecho de acceso a la información como la obligación de los sujetos obligados de clasificar como información reservada aquella que obstruya la prevención o persecución de los delitos**, ambos constituyen fines legítimos, los cuales están consagrados en el artículo 6 de nuestra Constitución Política de los Estados Unidos Mexicanos y normatividad aludidos. De esta forma, al ponderar entre tales derechos **se considera que en este caso concreto debe prevalecer la reserva de la información para no obstaculizar la prevención de delitos**, lo cual tiene sustento en el marco jurídico mencionado.*



De acuerdo con el principio de proporcionalidad, se concluye que la afectación que podría traer la divulgación de la información solicitada es mayor que el interés público de que se difunda, por lo que se considera que en este caso debe prevalecer la reserva, pues ello representa el medio menos restrictivo disponible para evitar un perjuicio a la prevención de delitos demostrables e identificables." (SIC)

Por tanto, la **Dirección General de Presupuesto y Recursos Financieros (DGPYRF)**, solicitan a este H. Comité, la confirmación de la clasificación de la información como reservada parcialmente por un periodo de 05 (cinco) años, en los términos descritos con anterioridad.

ACUERDO DE COMITÉ: ACT/CT/SO/16/07/2019-R.2.- CON FUNDAMENTO EN EL ARTÍCULO 65, FRACCIÓN II DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, EL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, CONFIRMA POR UNANIMIDAD LA CLASIFICACIÓN DE LA INFORMACIÓN COMO RESERVADA PARCIALMENTE POR UN PERIODO DE 05 (CINCO) AÑOS, ATENDIENDO LOS ARGUMENTOS VERTIDOS CON ANTERIORIDAD, Y CON FUNDAMENTO EN LOS ARTÍCULOS 113, FRACCIONES V y VII DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA; ASÍ COMO 110, FRACCIONES V y VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, Y LOS NUMERALES VIGÉSIMO TERCERO, VIGÉSIMO SEXTO TRIGÉSIMO TERCERO Y TRIGÉSIMO CUARTO DE LOS LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN.

PUNTO 3.-

ASUNTO QUE SE SOMETE A CONSIDERACIÓN: Confirmación de la clasificación de la información como reservada.

NÚMERO FOLIO: 0001100194719.

- I. **Solicitud de acceso a información pública**, misma que se describe a continuación:

"Solicito copia simple, en versión pública, de todos aquellos documentos que Unión de Empresarios para la Tecnología en la Educación, A.C. entregó a la Secretaría de Educación Pública para comprobar pagos o gastos relacionados con el programa "Equipamiento de Aulas", que en el 2012 recibió un donativo de la oficialía mayor de la Secretaría de Educación Pública." (SIC)



II. La **Unidad de Transparencia** turnó la solicitud a la **Dirección General de Presupuesto y Recursos Financieros (DGPYRF)**, quien solicita la confirmación de la clasificación de la información como reservada parcialmente en los términos siguientes:

*“Toda vez que se recibió solicitud de información con número de folio **0001100194719** en el cual requieren información que debe ser reservada por seguridad de la información, se solicita su intervención a efecto de solicitar al Comité de Transparencia y Acceso a la Información Pública la **RESERVA** de la siguiente información:*

Área: Dirección General de Tecnologías de la información y Comunicaciones.

Nombre del expediente o documento:

Número de serie de cada uno de los equipos de cómputo en posesión de la Secretaría de Educación Pública.

Tema: Seguridad Informática y seguridad de la información

*Momento de la clasificación de la información como reservada: Momento de recibir la solicitud de información pública con número de folio **0001100194719***

Plazo de reserva: Cinco años.

Fecha de inicio de la clasificación: 14 de mayo de 2019.

Fecha de término de la clasificación: 14 de mayo de 2024.

*Fundamento legal de la clasificación: **Artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública en relación con el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública** y Lineamientos Generales en materia de Clasificación y Desclasificación en su artículo Vigésimo Sexto.*

Justificación:

Entregar los datos concernientes al número de serie de equipos de cómputo en posesión de la Secretaría de Educación Pública, representa un riesgo de ataque informático, ya que incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado.

En este sentido, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la Secretaría de Educación Públicas, es



que se colige que dar a conocer la misma facilitaría que personas expertas en informática perturben el sistema de la infraestructura tecnológica de la Secretaría de Educación Pública, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, por lo tanto, en términos de lo dispuesto por los artículos 106 de la Ley General de Transparencia y Acceso a la Información Pública fracción I, 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, su análogo en el 110, fracciones VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en los Lineamientos Generales en materia de Clasificación y Desclasificación en su artículo Vigésimo Sexto, puede tener la calidad de Información reservada.

Razones y motivos de la clasificación:

En caso de proporcionar dichos números de serie, se pone en riesgo la seguridad informática y la seguridad de la información de conformidad con el siguiente detalle que consta de la solicitud y las razones para reservar la información requerida:

Proporcionar el número de serie de equipos de cómputo del sujeto obligado, puede ocasionar intrusiones, robo de identidad, afectación en las comunicaciones y por ende un ataque masivo a los equipos de cómputo que se encuentren conectados en la red interna de la Secretaría de Educación Pública y con ello, una afectación en los equipos informáticos y la información contenida en estos.

De esta forma, con la publicidad de los números de serie se generaría un riesgo potencial para la infraestructura tecnológica de la Secretaría de Educación Pública, ya que pueden ser utilizados para la realización de ataques informáticos de diversa índole.

Por lo anterior, y con fundamento en los artículos 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 en los "Lineamientos Generales en Materia de Clasificación y desclasificación de la Información, así como para la Elaboración de las Versiones Públicas", en su apartado, Décimo séptimo, último párrafo, Décimo octavo, Décimo noveno y Vigésimo

segundo, fracción I, se procede al correspondiente análisis de la PRUEBA DE DAÑO, en los siguientes términos:

Difundir o hacer del conocimiento público la información solicitada supondría una enorme ventaja para cualquier atacante de sistemas y redes de telecomunicaciones al proporcionarle herramientas para facilitar un ataque a los sistemas de telecomunicaciones con que cuenta la Secretaría poniendo en riesgo la información contenida tanto en los equipos de cómputo como la contenida en los equipos de servidores que procesan información que dependiendo el área de la Secretaría que sea atacado supondría, por ejemplo, un ataque equipos del Órgano Interno de Control o a la Unidad de Asuntos Jurídicos que podría obstruir el seguimiento de procesos administrativos en forma de juicio o



entorpecer investigaciones, conocer la ubicación física de una persona identificada o identificable, realizar una suplantación de identidad.

La divulgación de la información relativa a los números de serie de los equipos de cómputo de la Secretaría de Educación Pública representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que se colocaría en estado de vulnerabilidad que permitiría el acceso ilícito de los equipos de cómputo e información contenida en estos.

RIESGO REAL

La divulgación de la información representa un riesgo real ya que de entregarse, se proporcionaría información para llevar a cabo ataques informáticos a los equipos de cómputo y equipos de procesamiento de aplicativos que cuentan con bases de datos con datos personales de ciudadanos usuarios de sistemas y portales web de la Secretaría, en concordancia con lo mencionado, cabe señalar que la SEP realiza esfuerzos para mantener la seguridad de sus equipos y sistemas, por lo cual actualmente 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 y redes de telecomunicaciones de esta Secretaría.

El riesgo de perjuicio que supondría la divulgación de información supera el interés público general de que se difunda, toda vez que la misma 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 atacar y obtener información de los equipos, redes y conocer información crítica.

RIESGO DEMOSTRABLE

En razón de que es altamente probable y de inminente peligro que dar a conocer la información solicitada, materializaría el riesgo que se busca evitar al contar con un servicio de seguridad informática, con lo cual se busca minimizar efectos negativos en la infraestructura tecnológica de la Secretaría, ejemplo de ello es que actualmente se cuenta con un servicio administrado de seguridad informática y que el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y comunicaciones así como de la Seguridad en la Información privilegia la seguridad en los sistemas y redes de telecomunicaciones de la Administración Pública Federal.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar un perjuicio ya que únicamente se están solicitando reservar los conceptos de información que puede poner en riesgo a la infraestructura tecnológica de la Secretaría.

RIESGO IDENTIFICABLE



En el caso que nos ocupa, el riesgo identificable es el uso que se le dé a la información solicitada puesto que el mal uso de ella causaría una vulnerabilidad específica en los sistemas, equipos y redes de telecomunicaciones de la Secretaría pudiendo inhabilitar segmentos red, identificando ubicación física de los usuarios, intentos de ataque de tipo de intrusión y robo de datos, una posible intervención en la comunicación, la suplantación de equipos de la información que se almacena en el servidor, el detrimento de las instalaciones tecnológicas, el hackeo de los sistemas informáticos.

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectaría severamente el funcionamiento de la infraestructura tecnológica.

Lo anterior resulta relevante, ya que, de la negativa de acceso a la información se motiva en razón de prevenir la comisión de un delito de carácter cibernético que afectaría los equipos informáticos y la información contenida en estos.

Lo anterior en relación con el Código Penal Federal sobre el acceso ilícito a sistemas y equipos de informática dispuesto en los siguientes:

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se



impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

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

En este sentido divulgar la información solicitada, permitiría que terceros contaran con los elementos para intentar algún tipo de ataque cibernético para ingresar sin autorización, a todos y cada uno de los equipos de cómputo de esta Secretaría, lo que permitiría la comisión de delitos, como podrían ser los relacionados con el acceso ilícito a sistemas y equipos informáticos, entre otros.

Ahora bien, la divulgación de esta información reservada representa un riesgo real, demostrable e identificable y de perjuicio significativo al interés público, toda vez que al hacerla pública se proveen elementos técnicos que podrían obstruir la prevención de delitos demostrables e identificables, como los de suplantación de identidad y de acceso ilícito a sistemas y equipos informáticos.

*Con base en lo anterior, en este caso particular, **concorre tanto el derecho de acceso a la información como la obligación de los sujetos obligados de clasificar como información reservada aquella que obstruya la prevención o persecución de los delitos**, ambos constituyen fines legítimos, los cuales están consagrados en el artículo 6 de nuestra Constitución Política de los Estados Unidos Mexicanos y normatividad aludidos. De esta forma, al ponderar entre tales derechos **se considera que en este caso concreto debe prevalecer la reserva de la información para no obstaculizar la prevención de delitos**, lo cual tiene sustento en el marco jurídico mencionado.*

De acuerdo con el principio de proporcionalidad, se concluye que la afectación que podría traer la divulgación de la información solicitada es mayor que el interés público de que se difunda, por lo que se considera que en este caso debe prevalecer la reserva, pues ello representa el medio menos restrictivo disponible para evitar un perjuicio a la prevención de delitos demostrables e identificables." (SIC)

Por tanto, la **Dirección General de Presupuesto y Recursos Financieros (DGPYRF)**, solicitan a este H. Comité, la confirmación de la clasificación de la información como reservada parcialmente por un periodo de 05 (cinco) años, en los términos descritos con anterioridad.

ACUERDO DE COMITÉ: ACT/CT/SO/16/07/2019-R.3.- CON FUNDAMENTO EN EL ARTÍCULO 65, FRACCIÓN II DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, EL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, CONFIRMA POR UNANIMIDAD LA



SEP
SECRETARÍA DE
EDUCACIÓN PÚBLICA

SESIÓN ORDINARIA

ACT/CT/SO/16/07/2019-R

CLASIFICACIÓN DE LA INFORMACIÓN COMO RESERVADA PARCIALMENTE POR UN PERIODO DE 05 (CINCO) AÑOS, ATENDIENDO LOS ARGUMENTOS VERTIDOS CON ANTERIORIDAD, Y CON FUNDAMENTO EN LOS ARTÍCULOS 113, FRACCIONES V y VII DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA; ASÍ COMO 110, FRACCIONES V y VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, Y LOS NUMERALES VIGÉSIMO TERCERO, VIGÉSIMO SEXTO TRIGÉSIMO TERCERO Y TRIGÉSIMO CUARTO DE LOS LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN.

No habiendo más asuntos que tratar, se da por terminada la sesión, firmando al inicio los que en ella intervinieron.