Visto el expediente correspondiente a la solicitud de acceso a la información anotada al rubro, la cual fue turnada para su atención a la **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN** y a la **DIRECCIÓN GENERAL DE BIENES INMUEBLES Y RECURSOS MATERIALES**, y una vez analizado de forma exhaustiva el contenido del mismo, el Comité de Transparencia de la Secretaría de Relaciones Exteriores procede a confirmar la declaratoria de clasificación de parte de la información solicitada como **RESERVADA**, atendiendo a las siguientes consideraciones:

Solicitud 0000500062518:

"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: a. Numero de serie, de parte y de modelo. b. Marca. c. Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico. d. Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup). e. Si se encuentra activada la tecnología WIFI. f. Seguridad o cifrado implementado en la conexión WIFI (WEP - Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc). g. Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico.

..."

Derivado de las actuaciones de las Unidades Administrativas consultadas, se desprenden las siguientes consideraciones:

Para las preguntas: ***"1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: a. Numero de serie, de parte y de modelo. b. Marca. c. Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico."***

Antes de entrar al estudio de la solicitud, se precisa que esta Secretaría no tiene los conceptos Modem y Router en sus contratos de servicios de Telecomunicaciones.

Ahora bien, respecto a los módems de la pregunta 1 incisos a), b), c), d), e) y f), así como los incisos d), e) y f) de los routers, esta unidad administrativa señala que los servicios contratados a través de los proveedores de servicios de Telecomunicaciones a grandes rasgos son servicios múltiples de telefonía, red multiservicios nacional y servicio integral de voz y datos que incluyen la implementación, administración, operación, mantenimiento y suministro de servicios de red voz y datos, telefonía, acceso a internet y enlaces WAN en los diferentes inmuebles que ocupa "LA SECRETARÍA", y no el arrendamiento de Modems o routers, ya que dichos componentes son utilizados por los proveedores ya citados para poder proporcionar los servicios contratados, de ahí que esta Secretaría no cuente con la información solicitada o los dispositivos no cuentan con dicha funcionalidad/característica.

Para complementar lo anterior, los Modems y routers se encuentran en las instalaciones a nivel nacional de esta Secretaría.

De lo anterior se desprende que, la información requerida no se encuentra contenida en ningún documento previamente elaborado por el personal de esta unidad administrativa, en virtud de que los números de serie, partes y modelo no se encuentran integradas a la descripción, ni a las características del servicio al momento de lanzar una convocatoria para la contratación de los servicios, sino únicamente se establecen parámetros y características que deberán ser cubiertos por los proveedores al momento de brindar el mismo. Por lo anterior, cada proveedor se encuentra en total libertad de utilizar los bienes, insumos y productos que estimen necesarios al momento de presentar su propuesta, la cual únicamente se evalúa desde el punto de vista económico y de viabilidad técnica, no así en las marcas o modelos de los bienes que utilizará el proveedor al momento de prestar el servicio.

En este orden de ideas, una vez que finiquitado el proceso administrativo a través del cual se formalizó la contratación, el proveedor no tiene la obligación, ni la Secretaría de contar con un listado de características o descripciones adicionales a las necesarias para dar cuenta del cumplimiento a los requerimientos previamente señalados, por lo que al no estar contemplado el arrendamiento de Modems o Puntos de acceso inalámbricos, no existe obligación de contar con un listado conforme a lo requerido en la presente solicitud de acceso a la información, ni la de elaborar dicho documento, en términos del criterio intitulado **No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información**, que a la letra dispone:

> *"...Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información....".*

"Para los puntos de acceso inalámbrico, routers pregunta 1, incisos a), b) y c). Así como las preguntas: 1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: d. Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup). e. Si se encuentra activada la tecnología WIFI. f. Seguridad o cifrado implementado en la conexión WIFI (WEP - Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc)."

Ahora bien, por lo que hace a los incisos a) b) y c) de los puntos de acceso inalámbrico y routers e incisos d), e) y f), de los puntos de acceso inalámbrico, esta Dirección General manifiesta que no pueden ser proporcionada la información a que hace alusión el solicitante, ya que se pondría en riesgo la seguridad de la información perteneciente a la Secretaría que viaja por medio de estos dispositivos y misma que se encuentra contenida en los equipos conectados a éstos, ya que cualquier tercero, en conocimiento o posesión de estos datos, podría contar con los elementos suficientes para encontrar vulnerabilidades y utilizarlas en perjuicio de la Secretaría.

En ese sentido, al contar con los datos solicitados conllevaría a diversos riesgos, tales como:

1. Cualquier persona en posesión de la misma, podría buscar alguna vulnerabilidad de seguridad en la red de computadoras de la Secretaría y acceder a la información que viaja por dichos dispositivos y/o que está contenida en los sistemas de procesamiento y almacenamiento de información de la dependencia.
2. Lanzar ataques cibernéticos desde alguno o algunos de los equipos de la red de la Secretaría para obtener información de Seguridad Nacional.
3. Lanzar ataques cibernéticos en masa para inhabilitarlos y posiblemente también a los equipos conectados a éstos
4. Introducir algún tipo de malware a la red de la Secretaría.
5. Obtener acceso no autorizado a la red y/o segmentos críticos que pudieran comprometer servicios de TICs y/o sistemas críticos.
6. Paralizar las actividades o procesos que hacen uso de sistemas informáticos o la red de la Secretaría.

Para robustecer lo arriba citado, se informa que existen diversos tipos de intentos de hackeo:

- Los que corresponden a Antivirus son realizados por malware que se intenta infiltrar en el SO de los equipos personales y servidores.
- Los de Filtrado Web son troyanos que están dentro del código de páginas web y que el usuario no lo detecta al querer abrir y navegar por estos sitios. Estos ataques son contenidos por nuestra herramienta de filtrado de contenido.
- Los más severos son los de IPS y que si son lanzados directamente por hackers hacia las direcciones Ip de la SRE.

Antivirus SRE Nacional			Antivirus Exterior				Filtrado WEB	IPS Firewall Alameda	IPS Firewall Triangular
	amenazas detectadas y bloqueadas				amenazas detectadas y bloqueadas2		amenazas detectadas y mitigadas	ataques detectados y bloqueados	ataques detectados y bloqueados3
	235				26,618		91,500	99	2,556

Ahora bien, atendiendo a lo dispuesto en el artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, a continuación se establece la prueba de daño:

I. La divulgación de la información que se reserva representa un riesgo real, demostrable e identificable de perjuicio significativo a los intereses del gobierno mexicano. -La información reservada consistente en los números de serie, números de parte, números de modelo, marca, si se cuenta con contraseña para acceder a la configuración u administración, si se

encuentra activada la tecnología WPS, si se encuentra activada la tecnología WIFI, seguridad o cifrado implementado en la conexión WIFI los cuales se consideran sensibles en virtud de que dan cuenta de los equipos y tecnología empleadas por las Unidades Administrativas de esta Secretaría, resaltando que algunas de ellas realizan actividades en el marco de la Seguridad Nacional.

II. El riesgo de perjuicio supera el interés público general de que se difunda.- La divulgación de las características de los dispositivos solicitados permitiría conocer los mecanismos que sigue esta Secretaría para los servicios de red, a través de los cuales puede viajar información sensible y dan conectividad a equipos de cómputo. Adicionalmente, se protege el poder contar con una red y servicios de conectividad, que den continuidad operativa y permitan mejorar los sistemas y aplicativos con los que la Secretaría cuenta para funcionar internamente. En este sentido, es importante recalcar que los servicios brindados se realizan dentro del marco de seguridad nacional, por lo que el omitir la normatividad bajo la cual se rige, se traduciría en transgredir los sistemas en ambientes de desarrollo, calidad y producción que son utilizados para realizar la operación sustantiva; asimismo, se vulneraría los servicios los cuales requieren un alto nivel de disponibilidad, además del servicio de equipamiento para proporcionar servicios a la red interna de datos, entre otros.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.- La limitación del derecho del solicitante de información a conocer los números de serie, parte, modelo, marca, configuraciones, seguridad o cifrado implementado que se reservan es proporcional. El derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado siempre y cuando: i) el fin sea constitucionalmente válido (fin legítimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y, iv) la limitación sea proporcional en sentido estricto. (véanse tesis 1a. CCLXV/2016 (10a.),1a. CCLXVIII/2016 (10a.), 1a. CCLXX/2016 (10a.) y 1a. CCLXXII/2016 (10a.) de noviembre de 2016, derivadas del Amparo en Revisión 237/2014 Josefina Ricaño Bandala y otros, 4 de noviembre de 2015)."

Lo anterior, se refuerza tomando en cuenta que la información que viaja a través de los dispositivos, así como la que se aloja en los sistemas de procesamiento conectados a éstos, es la que de conformidad con sus atribuciones generan o pueden ser un medio de acceso a las unidades administrativas de la Cancillería que tienen el carácter de Instancias de Seguridad Nacional de conformidad con las Bases de Colaboración que en el marco de la Ley de Seguridad Nacional, celebran el Titular de la Secretaría de Gobernación, en su carácter de Secretario Ejecutivo del Consejo de Seguridad Nacional, y la Titular de la Secretaría de Relaciones Exteriores, publicadas en el DOF de fecha 27 de mayo de 2008.

Dado lo anterior, se actualiza la reserva de la información por un periodo de 5 años, de conformidad con lo previsto en el artículo 110, fracciones I y XIII de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el artículo 51, fracción I de la Ley de Seguridad Nacional que señala:

"Artículo 51.- Además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada por motivos de Seguridad Nacional:

I. Aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia

para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen, o

II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza."

Adicionalmente y en el ámbito de máxima transparencia, la Secretaría consultó al proveedor, el cual es dueño de los dispositivos, si encontraba algún inconveniente de que se otorgara la información requerida, argumentando lo siguiente:

"Consideramos que la información solicitada no debe de ser proporcionada ya que resulta un riesgo por lo sensible de la información para la Secretaria, el tener expuestos estos datos puede representar una posible amenaza . Considerando lo establecido en la Cláusula Décima del contrato acerca de la confidencialidad, el proveedor es responsable de salvaguardar la información que entregue o que produzca, para lo cual anexo un fragmento relevante del contrato "se compromete a tomar las medidas necesarias para salvaguardar la información confidencial y a evitar que tengan acceso personas ajenas al presente contrato sin consentimiento previo por escrito de "LA SECRETARÍA". Para brindar mayor claridad enlisto algunos riesgos de esta información:

- *Al tener versiones y modelos se podría buscar alguna vulnerabilidad de seguridad en la red de la Secretaría y acceder a la información contenida en los sistemas de procesamiento y almacenamiento de información de la dependencia.*

- *El acotar especificaciones de la seguridad establecida en la red Inalámbrica puede ser más susceptible a ser vulnerada.*
- *La entrega de información puede facilitar diversos ataques (Spoofing, Backdoor, Ataque DMA, Eavesdropping, phising, escalonamiento de privilegios, Trashing, DoS, etc.)*
- *Brinda factibilidad de una posible intrusión a la red y recursos de la Secretaría.*
- *Lanzar ataques desde el interior a otras dependencias comprometiendo el nombre de la Secretaria.*
- *Atacar los sitios Web de la Secretaría (DDoS, ataques de inyección, ataques de fuerza bruta, Cross-Site Scripting, etc.)*
- *Introducir algún tipo de malware, spyware, spam, o pharming, etc a la red de la Secretaría.*
- *Afectar algún servicio crítico a raíz de una intrusión*
- *Provocar alguna interrupción en la operación de la red de la Secretaría*
- *Se puede considerar el simple hecho de solicitar este tipo de información como un ataque de Ingeniería social*

En base a lo mencionado anteriormente nuestra recomendación es que la información no sea proporcionada."

En conclusión esta Secretaría considera NO viable proporcionar la información a que hace alusión el solicitante, en virtud de que proporcionarla pondría en riesgo la seguridad de la información que viaja por los dispositivos y/o contenida en los dispositivos conectados a éstos, ya que está considerado el hecho de que la persona, compañía, grupo o conjunto de personas con el conocimiento al respecto, podrían lanzar ataques cibernéticos a alguno o algunos de los equipos de la red, introducir algún tipo de malware a la red, utilizar alguna vulnerabilidad, pudiendo afectar la integridad, disponibilidad y confidencialidad de la red, entre otras.

Por lo que hace al inciso ***"g. Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico."***

Se informa que respecto a los dispositivos multicitados, éstos se encuentran instalados conforme al organigrama institucional en las siguientes áreas administrativas.

- Oficinas del C. Secretario
- Subsecretaría de Relaciones Exteriores
- Subsecretaría para América del Norte
- Subsecretaría para América Latina y el Caribe
- Subsecretaría para Asuntos Multilaterales y Derechos Humanos
- Oficialía Mayor
- Agencia Mexicana de Cooperación Internacional para el Desarrollo
- Consultoría Jurídica

Clasificación de la información solicitada: RESERVADA, los números de serie, números de parte, números de modelo, marca, si se cuenta con contraseña para acceder a la configuración u administración, si se encuentra activada la tecnología WPS, si se encuentra activada la tecnología WIFI, seguridad o cifrado implementado en la conexión WIFI, de conformidad con lo señalado por el solicitante.

Fundamentación Jurídica de la clasificación de información RESERVADA: Artículos 6, fracción I, de la Constitución Política de los Estados Unidos Mexicanos; 110, fracciones I y XIII de la Ley Federal de Transparencia y Acceso a la Información Pública; numerales Cuarto, Quinto, Séptimo, fracción I, Octavo, Décimo Séptimo, fracción IV, Trigésimo Segundo, Trigésimo Tercero y Trigésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, publicados en el Diario Oficial de la Federación el 15 de abril de 2016; 12, fracción VII, 50 y 51 de la Ley de Seguridad Nacional.

Periodo de reserva: 5 años.

Prueba de daño: La señalada en las consideraciones derivadas de las actuaciones de la Unidad Administrativa consultada.

Fundamentación jurídica de la resolución: Analizadas todas y cada una de las constancias que integran el expediente en comento, con fundamento en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 28, de la Ley Orgánica de la Administración Pública Federal; 34 y 36 del Reglamento Interior de la Secretaría de Relaciones Exteriores; Acuerdo por el que se adscriben orgánicamente las unidades administrativas a que se refiere el Reglamento Interior de la Secretaría de Relaciones Exteriores, publicado en el Diario Oficial de la Federación el 4 de octubre de 2011 última reforma publicada en el Diario Oficial de la Federación el 04 de mayo de 2016; Acuerdo por el que se crea la Unidad de Transparencia y se establece el Comité de Transparencia de la Secretaría de Relaciones Exteriores publicado en el Diario Oficial de la Federación el 30 de agosto de 2016; 1, 2, 3, fracción V, y 13, de la Ley Federal de Procedimiento Administrativo; 61, fracciones II y V, 64, 65, fracción II, 97, 98, fracción I, 100, 102, 103, 110, fracciones I y XIII, 111, 134, 135, 140, fracción I y Tercero Transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública; numerales Cuarto, Quinto, Séptimo, fracción I, Octavo, Décimo Séptimo, fracción IV, Trigésimo Segundo, Trigésimo Tercero y Trigésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información,

así como para la elaboración de versiones públicas, publicados en el Diario Oficial de la Federación el 15 de abril de 2016; artículo 24 de la Convención de Viena sobre Relaciones Diplomáticas, el Comité de Transparencia de la Secretaría de Relaciones Exteriores:

RESUELVE

PRIMERO. Que el Comité de Transparencia de la Secretaría de Relaciones Exteriores es competente para resolver respecto del presente asunto de conformidad con los artículos 102, 140, fracción I y tercero transitorio, de la Ley Federal de Transparencia y Acceso a la Información Pública.

SEGUNDO. Se confirma la clasificación de parte de la información requerida, como **RESERVADA** de conformidad con las consideraciones derivadas de las actuaciones de las Unidades Administrativas consultadas, respecto de la solicitud de acceso a la información identificada con el número de folio 0000500062518, por encontrarse apegada a derecho, atendiendo a los razonamientos expresados en la presente resolución.

TERCERO. Notifíquese la presente resolución al interesado para su conocimiento y efectos legales, hágase del conocimiento del solicitante que le asiste el derecho a interponer recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de conformidad con los artículos 61, fracción V y 147, de la Ley Federal de Transparencia y Acceso a la Información Pública, y 3°, fracción XV, de la Ley Federal de Procedimiento Administrativo.

ASÍ LO RESOLVIERON Y FIRMAN LOS INTEGRANTES DEL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE RELACIONES EXTERIORES, A DIECISIETE DE MAYO DE DOS MIL DIECIOCHO.

OSCAR SÁNCHEZ DELGADO

Titular de la Unidad de Transparencia de la
Secretaría de Relaciones Exteriores

DAVID ALEJANDRO OLVERA AYES

Director General del Acervo Histórico Diplomático y Coordinador de Archivos de la Secretaría de Relaciones Exteriores

ROSAURA GARCÍA PALMEROS

Suplente del Titular del Órgano Interno de Control en la Secretaría de Relaciones Exteriores

EEE/jmnm