SEMAR
SECRETARÍA DE MARINA

SECRETARÍA DE MARINA
COMITÉ DE TRANSPARENCIA
RESOLUCIÓN DE CLASIFICACIÓN.
ACTA DE COMITE NÚM.-CT-C/ 029 /18

Ciudad de México, a 10 de agosto de 2018.

VISTO: PARA RESOLVER SOBRE LA CLASIFICACIÓN DE LA INFORMACIÓN RESERVADA QUE DA RESPUESTA RESPECTO DE LA SOLICITUD DE INFORMACIÓN CON EL NÚMERO DE FOLIO 0001300058818, PRESENTADA POR EL SOLICITANTE A TRAVES DE LA PLATAFORMA NACIONAL DE TRANSPARENCIA, EN VISTA DE LO ANTERIOR, SE FORMULA LA PRESENTE RESOLUCIÓN EN ATENCIÓN A LOS SIGUIENTES:

R E S U L T A N D O S.

PRIMERO: El particular presentó la solicitud de información con el número de folio **0001300058818**, mediante la Plataforma Nacional de Transparencia, requiriendo 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. 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].***

Continúa hoja dos…

SEGUNDO: En virtud de lo anterior, la Unidad de Transparencia de esta Dependencia, turnó la solicitud en referencia a la Dirección General Adjunta de Comunicaciones e Informática y a la Unidad de Ciberseguridad, por ser las áreas que pudiesen contar con la información requerida, de conformidad con las atribuciones que le confieren los artículos 1, 2 fracción I, 26 y 30 de la Ley Orgánica de la Administración Pública Federal.

TERCERO: Derivado de citada búsqueda, la Dirección General Adjunta de Comunicaciones e Informática hizo del conocimiento a este Comité de Transparencia que la información referente a:

"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..." ***[sic]***

Se encuentra clasificada como **RESERVADA**, **por un período de cinco años,** de acuerdo a lo establecido en el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, expresando como prueba de daño, de conformidad en lo establecido en los artículos 102, 105, 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, 103, 104, 114 de la Ley General de Transparencia y Acceso a la Información Pública y apartado Segundo, Sexto, Décimo Séptimo, Décimo Noveno y Trigésimo Segundo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, lo siguiente:

Continúa hoja tres...

DAÑO PRESENTE: *La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional; toda vez que ante la actual situación a nivel global, existen grupos denominados "hacktivistas", quienes han realizado penetraciones, robo de información, alteraciones, ataques y desfiguraciones a los sitios web, en perjuicio de las Instituciones y Ciberseguridad y Ciberdefensa, por lo que difundir los números de series, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión de esta de esta Dependencia, potencializa un riesgo real e inminente para que un "hacker" tenga acceso a información sensible, reservada y confidencial con la cual se puede vulnerar la seguridad de esta Institución y haga identificables las operaciones de seguridad nacional que realiza esta Dependencia, generando el riesgo de que se vulnere y atente en contra de las infraestructuras críticas de información, así como los sistemas, programas y desarrollos tecnológicos de la Secretaría de Marina.*

DAÑO PROBABLE: *El riesgo de perjuicio que supondría la divulgación de la información que solicita el particular, respecto los números de series, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión de esta de esta Dependencia, permitiría a los denominados grupos "hacktivistas" con altos conocimientos informáticos avanzados, conocer información sensible, reservada y confidencial, así como el estado de las infraestructuras críticas de información, sistemas, programas y desarrollos tecnológicos esta Dependencia, generando riesgos y desventajas en las estrategias y actividades operativas que se realizan en el aire, tierra y mar, lo que conllevaría a poner en riesgo las actividades que realizan las unidades operativas pertenecientes a esta Dependencia, así como la seguridad de la información y datos personales del personal militar y civil que se encuentren bajo custodia de esta Institución, por lo que en el presente caso el interés público, no se compara al riesgo de perjuicio en contra de la seguridad nacional.*

Continúa hoja cuatro…

DAÑO ESPECÍFICO: *De revelar la información, existe la posibilidad de que esta sea utilizada por grupos con conocimientos específicos en la rama de informática, pudiendo hacer un uso inadecuado de softwares y/o herramientas para vulnerar la seguridad de la información de la Secretaría de Marina, como los siguientes:*

- Suplantación de equipo.
- Ataque a tablas ARP.
- Denegación de servicios por sustracción de tablas.
- DNS Spoofing.
- Desbordamiento de tablas CAM (Memorias de Contenido Direccionable).
- Saturación de Switch's.
- MAC Spoofing.
- Man in the middle (Hombre en medio).

CUARTO: En el presente caso, es conveniente precisar que con fecha 06 de junio del 2018, **el Pleno del INAI**, resolvió el recurso de revisión **RRA 2536/18,** en contra de la respuesta proporcionada en la solicitud de información con número de folio **0001300022218**, referente a:

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

Continúa hoja cinco…

Teniendo el recurrente respecto de las pretensiones de los números 2, 3, 4, 5, 6 y 7, como **satisfechas** y **modificando** la respuesta primigenia respecto de la pretensión señalada con el número **1: referente al número de serie y de parte de cada uno de los equipos de cómputo de la Dependencia**, e instruyendo a esta Dependencia para que, en un término no mayor a diez días contados a partir del día hábil siguiente, el Comité de Transparencia emita una resolución fundada y motivada clasificando citada información como **RESERVADA**, únicamente a lo previsto en el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.

QUINTO: Así mismo con fecha 02 de agosto del 2018, **el Pleno del INAI**, resolvió el recurso de revisión **RRA 2547/18,** en contra de la respuesta proporcionada en la solicitud de información con número de folio **0001300024118**, referente a:

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

Continúa hoja seis...

que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de computo." **[Sic]**

Por lo que, para emitir la resolución del recurso de revisión **RRA 2547/18**, el Comisionado Joel Salas Suárez, formuló una consulta a la Dirección General de Tecnologías de la Información, explicando lo siguiente:

- *"Las amenazas informáticas pueden materializarse en cualquier momento y los ciberdelincuentes cada vez tienen mayor interés y herramientas para causar algún daño a organizaciones por medio de ataques dirigidos o aleatorios, a fin de obtener algún beneficio aprovechándose de alguna vulnerabilidad en las plataformas tecnológicas de las organizaciones, como puede ser la no aplicación de las actualizaciones de seguridad necesarias y dispuestas por los fabricantes de los diferentes dispositivos o aplicaciones de software, configuraciones defectuosas o con errores de algún componente tecnológico, selección, diseño o implantación incorrecto de las medidas de seguridad o fallas no previstas por los fabricantes de los dispositivos.*
- *Para integrar una red, los equipos de cómputo deben estar interconectados a través de una interfaz que les permite comunicarse, la cual se conoce como tarjeta de red o NIC (Network Interface Controller – Controlador de interfaz para red), misma que* ***tiene asignado un identificador único llamado MAC*** *(Media Access Control – control de acceso al medio), o dirección física, integrada por 48 bits y para mayor facilidad de su representación se utiliza el sistema hexadecimal, por lo que se utilizan 12 dígitos: los primeros seis dígitos son administrados por el IEEE (Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos) que, identifican al fabricante o proveedor y, de ese modo, abarcan el Identificador Exclusivo de Organización (OUI), mientras que los dígitos restantes abarcan el número de serie de interfaz, u otro valor administrado por el proveedor específico.*

Continúa hoja siete…

- *Uno de los principales riesgos es a través de la materialización de un ataque conocido como "MAC Spoofing" (falsificación de la dirección MAC), la cual es una técnica para cambiar la dirección MAC de un dispositivo de red. Si bien, la dirección MAC está codificada en una tarjeta de red y no se puede cambiar, existen herramientas que pueden hacer creer al sistema operativo el uso de otra dirección MAC. Entre los fines maliciosos que implica un ataque de MAC Spoofing están los siguientes:*
  - ✓ ***Asignación de IP estática:*** *Los enrutadores le permiten asignar direcciones IP estáticas a sus computadoras. Cuando un dispositivo se conecta, siempre recibe una dirección IP específica si tiene una dirección MAC coincidente. Des esta forma existe la posibilidad de que un posible atacante obtenga una IP que normalmente se asigna a un equipo a través del conocimiento de la dirección MAC.*
  - ✓ ***Filtrado de direcciones MAC:*** *Las redes pueden usar el filtrado de direcciones MAC, solo permitiendo que los dispositivos con direcciones MAC específicas se conecten a una red, Esta no es una gran herramienta de seguridad porque las personas pueden falsificar sus direcciones MAC.*
  - ✓ ***Autenticación MAC:*** *Algunos proveedores de servicios de Internet pueden requerir autenticación con una dirección MAC y sólo permiten que un dispositivo con esa dirección MAC se conecte a Internet. Es posible que deba cambiar el enrutador o la dirección MAC de su computadora para conectarse.*
  - ✓ ***Identificación del dispositivo:*** *Muchas redes Wi-Fi del aeropuerto y otras redes públicas con Wi-Fi usan la dirección MAC de un dispositivo para identificarlo. Por ejemplo, una red Wi-Fi del aeropuerto podría ofrecer 30 minutos gratis y luego prohibir que su dirección MAC reciba más Wi-Fi. Cambie su dirección MAC y podría obtener más Wi-Fi.*
  - ✓ ***Seguimiento del dispositivo:*** *Como son únicas, las direcciones MAC se pueden usar como medio de rastreo. Cuando camina, su teléfono inteligente busca redes Wi-Fi cercanas y transmite su dirección MAC.*

Continúa hoja ocho…

- *Una vez que el atacante ha obtenido algún accesos a través de la materialización de una vulnerabilidad convertida en un ataque (por ejemplo, MAC Spoofing) el atacante tiene como prioridad mantener el acceso en los dispositivos afectados e incluso migrar el ataque a otros elementos conectados a la red. Las actividades en este punto son variadas, con los recursos puede lanzar nuevos ataques a otros sistemas, obtener o colocar algún archivo, afectar las aplicaciones instaladas o modificar información o archivos.*

- *La materialización de un ataque y su alcance son su puerta de entrada a la consecuencia de otro tipo de ataques. Dichos ataques pueden ser tan extensos como las medidas y controles de seguridad de la Organización Víctima lo permitan, desde una pronta mitigación con afectaciones menores, hasta dejar inoperable por un periodo indeterminado las operaciones de la Organización que sufre el ataque. Con resultados que incluyen los aspectos consultados como elementos tangibles (intrusiones no autorizadas, vulneraciones a la infraestructura tecnológica, intromisión a las comunicaciones de red, divulgación de información sensible o personal) y aquellos elementos no tangibles como un posible daño a la reputación de la organización".*

Invocándose lo anterior como **"hecho notorio"**, con fundamento en el primer párrafo del artículo 92 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria en la materia en términos de los dispuesto en el artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública.

En virtud del análisis que efectuaron los Comisionados del Instituto Nacional de Transparencia, Acceso a la Información y protección de Datos Personales en el Recurso en comentó, se desprende que, **SE CONFIRMA** la respuesta emitida por la Secretaría de Marina, en términos del artículo 110 fracciones I y XIII de la Ley Federal de Transparencia y Acceso a la Información Pública, estableciendo un periodo de reserva de 5 años y cuya parte de análisis estribo en:

Continúa hoja nueve…

"se considera procedente la reserva de los números de serie o de partes de los equipos de cómputo con que cuenta el sujeto obligado, así como las direcciones MAC de cada tarjeta o adaptador de red con que disponga cada equipo, debido a que dan cuenta de las especificaciones técnicas a través de los cuales se obtiene acceso al almacenamiento de información relacionada con sus actividades de investigación e inteligencia, lo cual es procedente con fundamento en lo dispuesto en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, en la modalidad de seguridad nacional

Considerando que, los números de serie o de parte de los equipos de cómputo y las direcciones MAC de cada tarjeta o adaptador de red que dispone cada equipo, consisten en especificaciones técnicas, consistentes una serie de caracteres con los que pueden vincularse y acceder a la infraestructura tecnológica del sujeto obligado para realizar acciones tendientes a poner en peligro la seguridad nacional, ya que se conocería información de inteligencia y contrainteligencia en materia de seguridad nacional, permitiendo que terceros puedan acceder, modificar o destruir la misma, de tal manera que estaría potencializando una amenaza, tal y como lo prevé el artículo 51 de la Ley de Seguridad Nacional que le otorga el carácter de reservada."

SEXTO: Que el Director General Adjunto de Comunicaciones e Informática de esta Dependencia, manifestó con relación a la solicitud de información del particular:..."*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."...**[sic].***

Que como Área administrativa encargada de resguardar los nombres de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuarios "su", "root", etc) para el manejo, administración y control de la configuración de cada equipo, desea limitar el derecho de información del peticionario, respecto a la misma; tal y como

Continúa hoja diez...

se establece en el artículo 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el artículo 100 de la Ley General de Transparencia y Acceso a la Información Pública, en el que establece que la clasificación de la información es *"el proceso mediante el cual el sujeto obligado determina que la información en su poder, actualiza alguno de los supuestos de reserva o confidencialidad"*.

Obligación correspondiente a los titulares de las áreas que poseen la información, tal y como se establece en el artículo 100 de la Ley General de Transparencia y Acceso a la Información Pública, en tanto corresponde al Comité de Transparencia, confirmar, modificar o revocar dicha clasificación.

Toda vez que se actualiza el supuesto de reserva, establecida en la fracción V del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el artículo 113 fracción V de la Ley General de Transparencia y Acceso a la Información Pública.

SÉPTIMO: El titular del área administrativa en comento, expreso como prueba de daño, de conformidad con lo establecido en los artículos 102, 105, 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, 103, 104, 114 de la Ley General de Transparencia y Acceso a la Información Pública y apartado Segundo, Sexto, Décimo Séptimo, Décimo Octavo, Décimo Noveno, 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, lo siguiente:

DAÑO PRESENTE: *La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público y seguridad nacional; en razón de que dar a conocer los nombres de las personas físicas que cuentan con las contraseñas administrativas o su equivalente, para el manejo, administración y control de la configuración de cada equipo, los convertiría en un blanco fácil de grupos transgresores de la ley, denominados "hacktivistas", quienes en su desesperación por obtener información, penetración, alteración, ataques, desconfiguraciones de los sitios*

Continúa hoja once…

web en diversas Dependencias Gubernamentales, pondrían en un peligro latente al personal militar y civil que labora en la institución, pudiendo vulnerar su seguridad e integridad, con la finalidad de acceder a información sensible, reservada y confidencial, la que a su vez, vulneraría la seguridad de la Dependencia y haría identificable las operaciones que realiza la misma, así como las actividades en el internet, generando el riesgo de que se vulnere y atente contra las infraestructuras críticas de información, sistemas, programas y desarrollos tecnológicos.

DAÑO PROBABLE: *El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, de dar a conocer los nombres de las personas físicas que cuentan con las contraseñas administrativas o su equivalente, para el manejo, administración y control de la configuración de cada equipo, los pondría en eminente peligro, en su bienestar físico y su vida, pues se encontrarían en una constante vulnerabilidad de acoso por parte de grupos transgresores de la ley, denominados "hacktivistas", dándoles la posibilidad de acceder a información sensible, reservada y confidencial, así como el estado de las Infraestructuras críticas de información de esta Dependencia, generando riesgos y desventajas en las estrategias operativas que se realizan, lo que conllevaría a poner en riesgo las actividades que realizan las unidades operativas pertenecientes a esta Dependencia, así como la seguridad de la información y datos personales del personal militar y civil que se encuentra bajo custodia de la Dependencia, pudiendo llevar a cabo incluso ataques en contra de instalaciones navales, con la finalidad de destrucción o inhabilitación de infraestructuras de carácter estratégico, poniendo en peligro la vida, seguridad y salud del personal naval.*

DAÑO ESPECÍFICO*: La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio de que en la especie se actualice algún menoscabo a la vida, integridad y seguridad física al personal naval que cumple con sus actividades de resguardo de contraseñas administrativas o su equivalente, para el manejo, administración y control de la configuración de cada equipo de la dependencia, con el fin de cumplir algún tipo de amenaza a la seguridad nacional por parte de grupos transgresores de la ley, denominados "hacktivistas", con altos*

Continúa hoja doce…

conocimientos informáticos avanzados, en perjuicio del interés colectivo y de la vida, seguridad y salud del personal naval.

OCTAVO: Este órgano colegiado revisó las constancias del expediente en el que se actúa con el objeto de contar con los medios de convicción necesarios para el pronunciamiento de la presente resolución, con base en los siguientes:

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

PRIMERO: Este Comité es competente para conocer y resolver el presente procedimiento de acceso a la información, de conformidad con los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos; 43, 44 fracción II, 137 de la Ley General de Transparencia y Acceso a la Información Pública, 64, 65 fracción II y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública.

SEGUNDO: Durante la sesión extraordinaria del Pleno de este Comité, analizó las constancias del expediente, por actualizarse alguno de los supuestos de clasificación, a fin de **CONFIRMAR, MODIFICAR O REVOCAR** la decisión del Área Administrativa, de conformidad a lo establecido en el artículo 102 de la Ley Federal de Transparencia.

TERCERO: Con el objeto de ilustrar la controversia planteada y lograr claridad en el tratamiento del tema de estudio, resulta conveniente precisar la solicitud de información, que el particular en la modalidad de: **"Entrega por Internet en la PNT"**.

Por lo anterior este Comité determinó entrar al estudio del presente caso.

CUARTO: De la interpretación lógica jurídica, del artículo 30 fracción XX de la Ley Orgánica de la Administración Pública Federal, 1 de la Ley Orgánica de la Armada de México, 5, 12 fracción IV, 50, 51 de Ley de Seguridad Nacional, que a la letra señalan:

Continúa hoja trece…

30 FRACCIÓN XX DE LA LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL: *Ejercer acciones para llevar a cabo la defensa y seguridad nacionales en el ámbito de su responsabilidad, así como coordinar con las autoridades competentes nacionales el control del tráfico marítimo cuando las circunstancias así lo lleguen a requerir, de acuerdo con los instrumentos jurídicos internacionales y la legislación nacional.*

ARTÍCULO 1 DE LA LEY ORGÁNICA DE LA ARMADA DE MÉXICO: *La Armada de México es una institución militar nacional, de carácter permanente, cuya misión es emplear el poder naval de la Federación para la defensa exterior y coadyuvar en la seguridad interior del país; en los términos que establece la Constitución Política de los Estados Unidos Mexicanos, las leyes que de ella derivan y los tratados internacionales.*

ARTÍCULO 5 DE LA LEY DE SEGURIDAD NACIONAL. - *Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:*

I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;

II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;

IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

VI. Actos en contra de la seguridad de la aviación;

VII. Actos que atenten en contra del personal diplomático;

VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;

IX. Actos ilícitos en contra de la navegación marítima;

X. Todo acto de financiamiento de acciones y organizaciones terroristas;

Continúa hoja catorce...

XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y

XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

IX. Actos ilícitos en contra de la navegación marítima;

XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia.

***ARTÍCULO 12 DE LA LEY DE SEGURIDAD NACIONAL**. - Para la coordinación de acciones orientadas a preservar la Seguridad Nacional se establece el Consejo de Seguridad Nacional, que estará integrado por:*

...IV. El Secretario de Marina;...

***ARTÍCULO 50 DE LA LEY DE SEGURIDAD NACIONAL**. - Cada instancia representada en el Consejo es responsable de la administración, protección, clasificación, desclasificación y acceso de la información que genere o custodie, en los términos de la presente Ley y de la Ley Federal de Transparencia y Acceso a la Información Pública gubernamental.*

***ARTÍCULO 51 DE LA LEY DE SEGURIDAD NACIONAL**.- 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.

Se desprende que, esta Secretaría, al ser parte integrante del Consejo de Seguridad Nacional, tiene la responsabilidad de **administrar, proteger, clasificar, desclasificar y**

Continúa hoja quince...

acceder a la información que genere o custodie, en los términos de Ley de Seguridad Nacional y la facultad de **EJERCER ACCIONES PARA LLEVAR A CABO LA DEFENSA Y SEGURIDAD NACIONALES EN EL ÁMBITO DE SU RESPONSABILIDAD,** siendo nuestro Titular parte del Consejo de Seguridad Nacional, para ello, esta Dependencia emplea para el cumplimiento de citada misión **tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, así como recurso humano que resguardar las contraseñas para su manejo, administración y control de configuración de equipos de cómputo.**

Bajo ese contexto se advierte, la importancia de reservar, la información referente en primer lugar, a:

"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..." ***[sic]***

Aún se trate **de una serie de caracteres citada información, una vez pública** puede ser empleada por los Gobiernos Estados, Terroristas, Delincuencia Organizada, Hacktivistas, Hackers u otros grupos criminales, para desarrollar software malicioso por sí mismos o través de terceros (hackers y/o empresas), ya que vinculando la misma a **otras especificaciones técnicas de los equipos de cómputo o de software que utiliza esta Secretaría para el desempeño de sus funciones, se puede obtener datos relevantes, como: la localización, lotes, fabricantes, actualizaciones y controladores de los equipos, entre otras especiaciones técnicas**, como en la especie ha acontecido, pues como se advierte con los siguientes número de solicitudes de información, han solicitado a esta Secretaría, especificaciones técnicas de los equipos de cómputo de esta SEMAR:

Continúa hoja dieciséis...

ASUNTO: Hoja dieciséis del acta de Clasificación.

NÚMERO DE SOLICITUD.	**NÚMERO DE RECURSO.**	**ESTATUS**
0001300041917: "Copia de todas las licencias de software para el Centro de Control de Ciberseguridad y Ciberdefensa (C4)"	*Sin recurso.*	INFORMACIÓN CLASIFICADA COMO RESERVADA.
0001300070017: "Copia de todas las licencias de software para el Centro de Control de Ciberseguridad y Ciberdefensa (C4)"	***RRA 5026/18 (finalizado)***	INFORMACIÓN CLASIFICADA COMO RESERVADA.
0001300022218: *"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.*	***RRA 2536/18 (finalizado)***	INFORMACIÓN CLASIFICADA COMO RESERVADA
1. De cada uno de los equipos de computo utilizados en el Secretaria de Marina: a. Numero de serie y de parte. *b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Maraca. d. Si se cuenta con contraseña apara acceder a la configuración de la BIOS (siglas en ingles de Basic Input/Output System). e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad administrativa que hace uso del equipo de computo". **[Sic].***		.

Continúa hoja diecisiete...

1. Desglosado por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, *nombre de los navegadores de Internet que se encuentran instalados en dichos equipos de cómputo. 2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación al punto anterior. 3. Número de serie o número de parte de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet*	***RRA 2547/18***	INFORMACIÓN CLASIFICADA COMO RESERVADA.
denominado YANDEX BROWSER. 4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET. 6. Cuáles son las redes sociales oficiales utilizadas como medios de comunicación. 7. Motivos por los cuales son utilizados únicamente las redes sociales a las que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de computo." ***[Sic]***		

Continúa hoja dieciocho...

0001300042318: ***"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***	***RRA 3662/18***	INFORMACIÓN CLASIFICADA COMO RESERVADA.
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."* ***[Sic]***		

Inclusive, de la misma dirección de correo: **focalizada@mail.ru**

Continúa hoja diecinueve…

Lo que permitiría perpetrar ciberataques de manera puntual y remota, burlando los controles de ciberseguridad establecidos, comprometiendo en el caso específico de SEMAR los procesos de planeación, ejecución, supervisión y rendición de cuentas de las operaciones que realiza la institución en materia de Seguridad Nacional, Seguridad Pública y actualmente como autoridad marítima nacional, de la navegación marítima y control de los puertos del país; paralizar los sistemas informáticos institucionales e inferir la vulnerabilidad intrínseca de cada sistema, teniendo además acceso a los datos personales y datos personales sensibles del personal civil y militar que trabaja en esta Institución, poniendo en riesgo de perjuicio su vida y seguridad, así como la de sus familiares.

Este Comité no pasa por alto, que un principio básico para llevar un ciberataque, es conocer como se está protegiendo el blanco objetivo al cual va dirigido el ataque, y a partir de esta información determinar sus vulnerabilidades, con la información obtenida del blanco objetivo, para comprometer las actividades y operaciones navales, así como la protección de los Puertos del país, constituyendo citados actos, una amenaza a la seguridad nacional, a la navegación de cabotaje y altura, por consiguiente, al comercio nacional e internacional que ahí se realiza, lo que permitiría a los actores criminales ejecutar acciones tendientes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional; a obstaculizar o bloquear operaciones navales, de inteligencia y contrainteligencia contra la delincuencia organizada; a realizar actos ilícitos en contra de la navegación marítima y/o a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

Las acciones descritas anteriormente, son consideradas amenazas a la Seguridad Nacional, mismas que encuentran su sustento legal, en el artículo 5 de la Ley de Seguridad Nacional, que a la letra establece:

> *I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;*

Continúa hoja veinte...

II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;

IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

VI. Actos en contra de la seguridad de la aviación;

VII. Actos que atenten en contra del personal diplomático;

VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;

IX. Actos ilícitos en contra de la navegación marítima;

X. Todo acto de financiamiento de acciones y organizaciones terroristas;

XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y

XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

Aunado a lo anterior, al encontrarse establecido en una **LEY** (**LEY DE SEGURIDAD NACIONAL**), que las **especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional,** solo por esa razón es motivo suficiente para reservar la difusión de cualquier **especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional,** constituyendo además su difusión una prohibición legal.

Continúa hoja veintiuno…

Lo anterior, encuentra su fundamento legal en los artículos 51, 54 y 59 de la Ley de Seguridad Nacional, mismos que prevén:

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.***

ARTÍCULO 54.- *La persona que por algún motivo participe o tenga conocimiento de productos, fuentes, métodos, medidas u operaciones de inteligencia, registros o información derivados de las acciones previstas en la presente Ley,* ***debe abstenerse de difundirlo por cualquier medio y adoptar las medidas necesarias para evitar que lleguen a tener publicidad.***

ARTÍCULO 59.- *Los informes y documentos distintos a los que se entreguen periódicamente, sólo podrán revelar datos en casos específicos, una vez que los mismos se encuentren concluidos. En todo caso, omitirán cualquier información cuya revelación indebida afecte la Seguridad Nacional, el desempeño de las funciones del Centro o la privacidad de los particulares. Para tal efecto, ningún informe o documento deberá revelar información* ***RESERVADA.***

Por lo que en ese orden de ideas, es de advertirse que en la especie sí se actualizan la causal prevista en la fracción I del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, que a la letra establece:

Continúa hoja veintidos…

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

*I. Comprometa la **SEGURIDAD NACIONAL**, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;*

Como lo señalado en los apartados de los LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN, ASÍ COMO PARA LA ELABORACIÓN DE VERSIONES PÚBLICAS:

***Décimo séptimo.** De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando:*

*I. **Se obstaculicen o bloqueen las actividades de inteligencia o contrainteligencia y cuando se revelen normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional**;*

*II. **Se puedan menoscabar, obstaculizar o dificultar las estrategias o acciones para combatir la delincuencia organizada, la comisión de los delitos contra la seguridad de la nación, entendiéndose estos últimos como traición a la patria, espionaje, sedición, motín, rebelión, terrorismo, sabotaje, conspiración, el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva**.*

Se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, así como la

Continúa hoja veintitrés...

indispensable para la provisión de bienes o servicios públicos de agua potable, de emergencia, vías generales de comunicación o de cualquier tipo de infraestructura que represente tal importancia para el Estado que su destrucción o incapacidad tenga un impacto debilitador en la seguridad nacional.

DÉCIMO SÉPTIMO. LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN, ASÍ COMO PARA LA ELABORACIÓN DE VERSIONES PÚBLICAS. *(Último párrafo) Asimismo, podrá considerarse como* ***RESERVADA aquella que revele datos que pudieran ser aprovechados para conocer*** *la capacidad de reacción de las instituciones encargadas de la seguridad nacional; sus 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.***

Así mismo este Comité concluye que, **la aplicación de la prueba de daño** realizada por el Área Administrativa, fue realizada de acuerdo a lo establecido en los artículo 102, 105, 111 de la Ley Federal en la Materia, 103, 104, 114 de la Ley General de Transparencia y Acceso a la Información Pública y en los apartados Segundo y Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Pública, atendiendo a los apartados Diecisiete, Diecinueve y Treinta y dos de dichos Lineamientos, bajo el siguiente contexto.

Con relación a la fracción I), el Área Administrativa citó la fracción y causales aplicables al artículo 110 de la Ley Federal en la materia, supuesto normativo que otorga el carácter de información reservada.

Bajo esa premisa, se desprende que el Área Administrativa, en la motivación de la clasificación acreditó las circunstancias de modo, tiempo y lugar del daño, así también, limitó adecuadamente al principio de proporcionalidad, el cual representa el medio menos restrictivo disponible para evitar el perjuicio de que en la especie se actualice, protegiendo el interés público.

Continúa hoja veinticuatro…

QUINTO: Aunado a lo anterior, este Comité de Transparencia no pasa por alto, el razonamiento lógico – jurídico realizado por el Pleno de INAI, en el cual resolvió el recurso de revisión **RRA 2536/18,** respecto de la respuesta proporcionada en la solicitud de información con número de folio **0001300022218**, referente a:

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

En la cual **INSTRUYÓ** a esta Dependencia para que en un término mayor a diez días contados a partir del día hábil siguiente, el Comité de Transparencia emita una resolución fundada y motivada clasificando citada información como **RESERVADA**, de acuerdo a lo previsto en el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, respecto de los números de serie y de parte de los equipos de cómputo de esta Dependencia.

Bajo ese contexto, es procedente hacer notar que, las resoluciones del Instituto son **VINCULATORIAS**, de conformidad a lo previsto en el artículo 163 de la Ley Federal de Trasparencia y Acceso a la Información Pública.

Por lo que, en ese orden de ideas y conforme a lo previsto en el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, la información solicitada, debe de ser **CONFIRMADA** como **RESERVADA.**

Continúa hoja veinticinco…

Por lo anteriormente expuesto, este Comité de Transparencia concluye, de acuerdo a las facultades y atribuciones, establecidas en el artículo 65 de la Ley Federal de Transparencia y Acceso a la Información Pública, que revelar la información solicitada, posibilita que esta pueda ser utilizada, por parte de los delincuentes cibernéticos o grupos de la delincuencia organizada, para accesar y apoderarse de la información sensible de esta Dependencia, con la finalidad de obstaculizar, bloquear menoscabar, o dificultar las estrategias, actividades o acciones de inteligencia o contrainteligencia que esta Dependencia realiza; así como realizar la comisión de los delitos contra la seguridad de la nación, constituyendo por lo tanto el riesgo de perjuicio una amenaza de **SEGURIDAD NACIONAL**, por tal motivo **CONFIRMA Y DECLARA FORMALMENTE COMO INFORMACIÓN RESERVADA por un período de cinco años**, con fundamento en lo establecido en el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, la información referente a:

"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..." ***[sic]***

Así mismo con fecha 02 de agosto del 2018, **el Pleno del INAI**, resolvió el recurso de revisión **RRA 2547/18,** en contra de la respuesta proporcionada en la solicitud de información con número de folio **0001300024118**, referente a:

Continúa hoja veintiséis...

ASUNTO: Hoja veintiséis del acta de Clasificación.

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

Por lo que, para emitir la resolución del recurso de revisión **RRA 2547/18**, el Comisionado Joel Salas Suárez, formuló una consulta a la Dirección General de Tecnologías de la Información, explicando lo siguiente:

Continúa hoja veintisiete...

- *"Las amenazas informáticas pueden materializarse en cualquier momento y los ciberdelincuentes cada vez tienen mayor interés y herramientas para causar algún daño a organizaciones por medio de ataques dirigidos o aleatorios, a fin de obtener algún beneficio aprovechándose de alguna vulnerabilidad en las plataformas*

  tecnológicas de las organizaciones, como puede ser la no aplicación de las actualizaciones de seguridad necesarias y dispuestas por los fabricantes de los diferentes dispositivos o aplicaciones de software, configuraciones defectuosas o con errores de algún componente tecnológico, selección, diseño o implantación incorrecto de las medidas de seguridad o fallas no previstas por los fabricantes de los dispositivos.
- *Para integrar una red, los equipos de cómputo deben estar interconectados a través de una interfaz que les permite comunicarse, la cual se conoce como tarjeta de red o NIC (Network Interface Controller – Controlador de interfaz para red), misma que* ***tiene asignado un identificador único llamado MAC*** *(Media Access Control – control de acceso al medio), o dirección física, integrada por 48 bits y para mayor facilidad de su representación se utiliza el sistema hexadecimal, por lo que se utilizan 12 dígitos: los primeros seis dígitos son administrados por el IEEE (Institute of Electrical and Electronics Engineers – Instituto de Ingenieros Eléctricos y Electrónicos) que, identifican al fabricante o proveedor y, de ese modo, abarcan el Identificador Exclusivo de Organización (OUI), mientras que los dígitos restantes abarcan el número de serie de interfaz, u otro valor administrado por el proveedor específico.*
- *Uno de los principales riesgos es a través de la materialización de un ataque conocido como "MAC Spoofing" (falsificación de la dirección MAC), la cual es una técnica para cambiar la dirección MAC de un dispositivo de red. Si bien, la dirección MAC está codificada en una tarjeta de red y no se puede cambiar, existen herramientas que pueden hacer creer al sistema operativo el uso de otra dirección MAC. Entre los fines maliciosos que implica un ataque de MAC Spoofing están los siguientes:*

Continúa hoja veintiocho…

- ✓ ***Asignación de IP estática:*** *Los enrutadores le permiten asignar direcciones IP estáticas a sus computadoras. Cuando un dispositivo se conecta, siempre recibe una dirección IP específica si tiene una dirección MAC coincidente. Des esta forma existe la posibilidad de que un posible atacante obtenga una IP que normalmente se asigna a un equipo a través del conocimiento de la dirección MAC.*
- ✓ ***Filtrado de direcciones MAC:*** *Las redes pueden usar el filtrado de direcciones MAC, solo permitiendo que los dispositivos con direcciones MAC específicas se conecten a una red, Esta no es una gran herramienta de seguridad porque las personas pueden falsificar sus direcciones MAC.*
- ✓ ***Autenticación MAC:*** *Algunos proveedores de servicios de Internet pueden requerir autenticación con una dirección MAC y sólo permiten que un dispositivo con esa dirección MAC se conecte a Internet. Es posible que deba cambiar el enrutador o la dirección MAC de su computadora para conectarse.*
- ✓ ***Identificación del dispositivo:*** *Muchas redes Wi-Fi del aeropuerto y otras redes públicas con Wi-Fi usan la dirección MAC de un dispositivo para identificarlo. Por ejemplo, una red Wi-Fi del aeropuerto podría ofrecer 30 minutos gratis y luego prohibir que su dirección MAC reciba más Wi-Fi. Cambie su dirección MAC y podría obtener más Wi-Fi.*
- ✓ ***Seguimiento del dispositivo:*** *Como son únicas, las direcciones MAC se pueden usar como medio de rastreo. Cuando camina, su teléfono inteligente busca redes Wi-Fi cercanas y transmite su dirección MAC.*

- *Una vez que el atacante ha obtenido algún accesos a través de la materialización de una vulnerabilidad convertida en un ataque (por ejemplo, MAC Spoofing) el atacante tiene como prioridad mantener el acceso en los dispositivos afectados e incluso migrar el ataque a otros elementos conectados a la red. Las actividades en este punto son variadas, con los recursos puede lanzar nuevos ataques a otros sistemas, obtener o colocar algún archivo, afectar las aplicaciones instaladas o modificar información o archivos.*

Continúa hoja veintinueve...

- *La materialización de un ataque y su alcance son su puerta de entrada a la consecuencia de otro tipo de ataques. Dichos ataques pueden ser tan extensos como las medidas y controles de seguridad de la Organización Víctima lo permitan, desde una pronta mitigación con afectaciones menores, hasta dejar inoperable por un periodo indeterminado las operaciones de la Organización que sufre el ataque. Con resultados que incluyen los aspectos consultados como elementos tangibles (intrusiones no autorizadas, vulneraciones a la infraestructura tecnológica, intromisión a las comunicaciones de red, divulgación de información sensible o personal) y aquellos elementos no tangibles como un posible daño a la reputación de la organización".*

Invocándose lo anterior como **hecho notorio**, con fundamento en el primer párrafo del artículo 92 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria en la materia en términos de los dispuesto en el artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública.

En virtud del análisis que efectuaron los Comisionados del Instituto Nacional de Transparencia, Acceso a la Información y protección de Datos Personales en el Recurso en comentó, se desprende que, **SE CONFIRMA** la respuesta emitida por la Secretaría de Marina, en términos del artículo 110 fracciones I y XIII de la Ley Federal de Transparencia y Acceso a la Información Pública, estableciendo un periodo de reserva de 5 años y cuya parte de análisis estribo en:

"se considera procedente la reserva de los números de serie o de partes de los equipos de cómputo con que cuenta el sujeto obligado, así como las direcciones MAC de cada tarjeta o adaptador de red con que disponga cada equipo, debido a que dan cuenta de las especificaciones técnicas a través de los cuales se obtiene acceso al almacenamiento de información relacionada con sus actividades de investigación e inteligencia, lo cual es procedente con fundamento en lo dispuesto en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, en la modalidad de seguridad nacional.

Continúa hoja treinta…

Considerando que, los números de serie o de parte de los equipos de cómputo y las direcciones MAC de cada tarjeta o adaptador de red que dispone cada equipo, consisten en especificaciones técnicas, consistentes una serie de caracteres con los que pueden vincularse y acceder a la infraestructura tecnológica del sujeto obligado para realizar acciones tendientes a poner en peligro la seguridad nacional, ya que se conocería información de inteligencia y contrainteligencia en materia de seguridad nacional, permitiendo que terceros puedan acceder, modificar o destruir la misma, de tal manera que estaría potencializando una amenaza, tal y como lo prevé el artículo 51 de la Ley de Seguridad Nacional que le otorga el carácter de reservada."

Ahora bien, de la lectura íntegra de la solicitud en mérito, se desprende que el particular al solicita el acceso a la siguiente información:

:..."*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."...**[sic].***

Por lo que dar a conocer la información solicitada por el particular, se pondría en eminente peligro, a los servidores públicos que desempeñan su trabajo en la Dependencia, amenazando su bienestar físico y su vida, pues se encontrarían en una constante vulnerabilidad de acoso por parte de grupos transgresores de la ley, denominados "hacktivistas", dándoles la posibilidad de acceder a información sensible, reservada y confidencial, así como el estado de las Infraestructuras críticas de información de esta Dependencia, generando riesgos y desventajas en las estrategias operativas que se realizan, lo que conllevaría a poner en riesgo las actividades que realizan las unidades operativas pertenecientes a esta Dependencia, así como la seguridad de la información y datos personales del personal militar y civil que se encuentra bajo custodia de la Dependencia, pudiendo llevar a cabo incluso ataques en contra de instalaciones navales, con la finalidad de destrucción o inhabilitación o sabotaje de cualquier infraestructuras de

Continúa hoja treinta y uno...

carácter estratégico o prioritario, teniendo como efecto poner en riesgo la vida, seguridad y salud del personal naval, resultando dichos actos un impacto debilitador en la seguridad nacional, por lo que el riesgo de perjuicio, supera el interés general.

Bajo ese contexto, el artículo 110 fracción V de la Ley Federal de Transparencia y Acceso a la Información Pública y en los apartados Décimo Séptimo, Décimo Octavo, Décimo Noveno, 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, establecen lo siguiente:

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

V. Pueda poner en riesgo la vida, seguridad o salud de una persona física;

LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN, ASÍ COMO PARA LA ELABORACIÓN DE VERSIONES PÚBLICAS.

Décimo octavo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público.

Se pone en peligro el orden público cuando la difusión de la información pueda entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública, menoscabar o dificultar las estrategias contra la evasión de reos; o menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales.

Continúa hoja treinta y dos…

Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.

Vigésimo tercero. Para clasificar la información como reservada, de conformidad con el artículo 113, fracción V de la Ley General, será necesario acreditar un vínculo, entre la persona física y la información que pueda poner en riesgo su vida, seguridad o salud.

Aunado a lo anterior, no pasa por alto este Comité que, de acuerdo a la fracción II del artículo 51 de la Ley de Seguridad Nacional, otorga el carácter de **INFORMACIÓN RESERVADA**, a aquella información cuya revelación pueda ser utilizada o potenciar una amenaza, por lo que de conformidad con el artículo 110 fracción V de la Ley Federal de Transparencia y Acceso a la Información Pública y en el apartado Trigésimo Tercero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, que a la letra establecen:

Trigésimo tercero. 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;

Continúa hoja treinta y tres...

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.

En virtud de lo anterior, este Comité de Transparencia concluye que difundir la información solicitada respecto a los nombres de las personas físicas que cuentan con las contraseñas para el manejo, administración y control de la configuración de cada equipo informático de la Institución pone en grave peligro la seguridad y la vida del personal naval que labora para la Institución toda vez que se convierten en blancos fáciles de grupos de transgresores de la ley, denominados "hacktivistas", quienes podrían amenazarlos para obtener dicha información y lograr sus objetivos de *cumplir algún tipo de amenaza a la seguridad nacional por parte de estos grupos, con altos conocimientos informáticos avanzados, en perjuicio del interés colectivo y de la vida, seguridad y salud del personal naval.*

En mérito de lo expuesto, este Comité de Transparencia:

Continúa hoja treinta y cuatro…

ASUNTO: Hoja treinta y cuatro del acta de Clasificación.

R E S U E L V E.

PRIMERO: Este Comité de Transparencia **CONFIRMA Y DECLARA FORMALMENTE COMO INFORMACIÓN RESERVADA, por un período de cinco años,** de conformidad a lo previsto en el artículo 110 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública la información referente a:

"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..." ***[sic]***

SEGUNDO: El Pleno de este Comité **CONFIRMA Y DECLARA FORMALMENTE COMO INFORMACIÓN RESERVADA, por un periodo de cinco años,** de acuerdo a lo establecido en el **artículo 110 fracción V de la Ley Federal de Transparencia y Acceso a la Información Pública**, la información relativa a:

..."*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."...****[sic].***

TERCERO: Se emite la presente resolución, misma que se registra en el libro correspondiente con el número de acta que al rubro se indica, conforme a lo dispuesto en el artículo 110 fracciones I y V de la Ley Federal de Transparencia y Acceso a la Información Pública.

Continúa hoja treinta y cinco...

ASUNTO: Hoja treinta y cinco del acta de Clasificación.

CUARTO: Se instruye a la Unidad de Transparencia para que remita la presente resolución al interesado.

Así, por unanimidad de votos lo resolvieron los integrantes del Comité de Transparencia de la Secretaría de Marina, quienes firman la presente resolución para su debida constancia legal.

COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE MARINA.

SECRETARIA DE MARINA
COMITE DE TRANSPARENCIA

ALMIRANTE
OFICIAL MAYOR DE LA SECRETARÍA DE MARINA.
PRESIDENTE
JOSÉ LUIS VERGARA IBARRA

ALMIRANTE
INSPECTOR Y CONTRALOR GENERAL DE MARINA.
PRIMER VOCAL
JOSÉ RAFAEL OJEDA DURÁN.

VICEALMIRANTE
JEFE DE LA UNIDAD DE TRANSPARENCIA
SEGUNDO VOCAL-SECRETARIO
CARLOS HUMBERTO LANZ GUTIÉRREZ