# RESOLUCIÓN

S/REF: 001-015688

N/REF: R/0377/2017

FECHA: 30 de octubre de 2017

[redacted]

**ASUNTO: Resolución de Reclamación presentada al amparo del artículo 24 de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno**

En respuesta a la Reclamación presentada por [redacted] mediante escrito con entrada el 9 de agosto de 2017, el Consejo de Transparencia y Buen Gobierno, considerando los Antecedentes y Fundamentos Jurídicos que se especifican a continuación, adopta la siguiente **RESOLUCIÓN:**

## 1. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, [redacted] presentó solicitud de acceso a la información, con fecha 13 de junio de 2017 y al amparo de la Ley 19/2013, de 9 de diciembre de Transparencia, acceso a la información pública y buen gobierno (en adelante, LTAIBG), dirigida al MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, en la que solicitaba lo siguiente:

   - *Al hilo de repetidas noticias en la prensa sobre determinadas "censuras" o "filtros" en los accesos a Internet en instituciones públicas, y preocupado por haber sufrido personalmente alguna vez el no poder acceder a algún contenido en Internet desde una conexión pública, solicito los siguientes documentos:*

     *1 - Una copia del protocolo/reglamento/reglas por las que se determinan el bloqueo a determinados tipos de contenidos, dominios o IPs en las conexiones de su Ministerio que incluya tanto los criterios aplicados para decidir si una web se bloquea o no desde su conexión, como los cargos de las personas que lo deciden.*

     *2 - Un listado de los dominios y/o direcciones IP a los que bloquean el acceso desde las conexiones a Internet de su Ministerio. (En caso de ser una lista*



[redacted]

*dinámica en la que varíen las webs/IPs a las que se bloquea el acceso, se solicita copia de la última lista con fecha anterior a un mes de la recepción de esta petición)*

*3 - En caso de tener distintos accesos a Internet con distintos privilegios en su Ministerio, un listado con la categorización de las distintas conexiones a Internet que tienen, así como un listado de los dominios y/o direcciones IP a los que bloquean el acceso desde cada una de sus conexiones. (En caso de ser listas dinámicas en la que varíen las webs/IPs a las que se bloquea el acceso, se solicitan copias de las últimas listas con fecha anterior a un mes de la recepción de esta petición)*

- *Les ruego que la información solicitada me sea facilitada de la forma más desglosada y detallada posible, que los datos estén en formatos estructurados para que puedan ser procesados de forma automática por un ordenador, y que preferiblemente estén en un formato de archivo no propietario.*

*2.* Mediante Resolución de fecha 27 de julio de 2017, el MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL informó a [redacted] de lo siguiente:

- *Primeramente, y sobre la cuestión relativa a "los criterios aplicados para decidir si una web se bloquea o no desde su conexión, como los cargos de las personas que lo deciden" indicar que el Ministerio de Energía, Turismo y Agenda Digital dispone de distintas herramientas y productos de seguridad (firewalls, antivirus de puesto, etc.), que, entre otras acciones, permiten bloquear el acceso de los empleados del Ministerio a contenidos que puedan entrañar riesgos de seguridad (tanto a nivel de nombre lógico, como de dirección física). Son los propios productos de protección los que de forma autónoma y en base a distintas categorías, bloquean el acceso a contenidos que pueden comprometer la seguridad, que vulneran leyes de propiedad intelectual, etc.*
- *Tal y como ya se ha indicado previamente, mediante la Orden IET/1934/2014, de 14 de octubre, se establece la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Energía y Turismo (actual Ministerio de Energía, Turismo y Agenda Digital) y se constituye el Comité Director de la Seguridad de la Información en el departamento, cuyas funciones y miembros se detallan en el artículo 4 de la citada orden.*
- *Asimismo, existe una instrucción interna sobre seguridad de la Información del Ministerio, documento éste último que sólo es público para los empleados del Ministerio, a quienes aplica, y que, por motivos de seguridad no puede ser objeto de publicidad, conforme a lo previstos en el citado artículo 14.1 d) de la LTAIBG, a diferencia de las dos normas de rango superior previamente mencionadas.*
- *El listado de dominios y/o direcciones IP bloqueados por los citados productos y herramientas no está disponible para su consulta por motivos de seguridad*



[redacted]

*informática, por ello se limita esta información conforme al artículo 14. Apartado d) de la LTAIBG, previamente mencionado. El revelar y dar conocimiento general de las estrategias de seguridad de la información en el ámbito del departamento, haría que las mismas perdieran su eficacia, como ya se ha puesto de manifiesto.*

- *Por último y en respuesta a la última de sus cuestiones, se le informa de que las normas de seguridad y herramientas de bloqueo de acceso a Internet se aplican por igual a todos los empleados del Ministerio y sin importar el canal de acceso utilizado.*

3. El 9 de agosto de 2017, tuvo entrada en este Consejo de Transparencia Reclamación de [redacted], de acuerdo con lo previsto en el artículo 24 de la LTAIBG, contra la Resolución del MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, en la que alegaba lo siguiente:

   - *No se me ha provisto de la información solicitada. Tampoco han justificado el procedimiento que siguen para el bloqueo de direcciones web ni las personas encargadas, lo que también era objeto de la presente petición.*
   - *No entiendo como el conocer a qué webs no puedo acceder desde una conexión a Internet pública, lo que puede afectar a mis derechos a la libertad de expresión o derecho a recibir o emitir una información veraz como ciudadano puede en alguna afectar a la estrategia de seguridad, como alegan en la contestación acogiéndose al párrafo 14.1 d).*
   - *No se han solicitado conocer procedimientos de seguridad o protección de las conexiones del Ministerio ni ningún otro dato que pudiera comprometer la seguridad de este servicio. Sólo un listado de webs censuradas en la conexión y los criterios aplicados para ello, así como las personas encargadas.*
   - *Les ruego que atiendan la presente reclamación, entendiendo que el derecho de acceso a información pública en este tema, que afecta a la libertad de expresión y al derecho a recibir o emitir una información veraz prevalece sobre los argumentos expuestos por el Ministerio.*

4. El 11 de agosto de 2017, este Consejo de Transparencia trasladó a la Unidad de Información del MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL la documentación obrante en el expediente para alegaciones. El escrito de alegaciones tuvo entrada el día 30 de agosto de 2017 y en el mismo se indicaba lo siguiente:

   - *La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. En consecuencia, el acceso público a las medidas específicas que se adopten en el ámbito del departamento para garantizar la seguridad de la información, está limitado de forma general,*



[redacted]

*puesto que un acceso sin control supondría un perjuicio para la seguridad pública (en el sentido previsto en el citado artículo 14.1 d) de la LTAIBG).*

- *El acceso a contenidos web desde las infraestructuras técnicas de los Ministerios es una cuestión de política de seguridad de la información interna de cada Departamento ministerial, que se fija en función de diferentes parámetros, y con mayores o menores restricciones en cada caso. En los "routers" de acceso a internet hay dos tipos de filtros:*

  *1. Unos que impiden mostrar determinados elementos de una página por seguridad. Son elementos ejecutables (controles ActiveX …) de una página web que pueden enmascarar software maligno (malware) pero no impiden ver el resto de la información.*

  *2. Otros que impiden la visita a páginas concretas: pornográficas, descargas (las ilegales), televisiones (por el consumo de banda ancha), algunas deportivas, Redes sociales, etc.*

  *Por ello, las limitaciones de acceso a páginas web en el Ministerio de Energía, Turismo y Agenda Digital se establecen en base a diferentes razones de servicio público: evitar ataques e infecciones por virus, uso adecuado de recursos públicos administrativos para los fines marcados por el ordenamiento jurídico, eficacia, eficiencia, calidad, etc., pero no existe un listado cerrado de páginas web bloqueadas.*

- *La resolución sí da respuesta a dos cuestiones de las planteadas: por un parte, se le han indicado los cargos de las personas con competencias en el Departamento en materia de seguridad de la información y por otra, se le ha indicado que no existen en el departamento distintos accesos a Internet con distintos privilegios. En la Resolución del Subsecretario, de 27 de julio de 2017, se le exponía que, mediante la Orden IET/1934/2014, de 14 de octubre, se establecía la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Energía y Turismo (actual Ministerio de Energía, Turismo y Agenda Digital) y se constituía el Comité Director de la Seguridad de la Información en el departamento, cuyas funciones y miembros se detallan en el artículo 4 de la citada orden.*
- *El listado de dominios y/o direcciones IP bloqueados por los citados productos y herramientas no está disponible para su consulta por motivos obvios de seguridad informática, como tampoco el acceso público a las medidas específicas que se adopten en el ámbito del departamento para garantizar la seguridad de la información, limitado de forma general, puesto que este acceso supondría un perjuicio para la seguridad pública, en el sentido previsto en el citado artículo 14.1 d) de la LTAIBG, teniendo en cuenta, asimismo, que dar publicidad de las medidas adoptadas, haría que las mismas perdieran su eficacia como medidas de protección.*
- *El revelar y dar conocimiento general de las estrategias de seguridad de la información en el ámbito del departamento, haría que las mismas perdieran su eficacia, como ya se ha puesto de manifiesto. Se hace necesario en este*



[redacted]

*apartado, por tanto, ponderar qué prima en este supuesto, el acceso a la información pública o la seguridad de la información en el ámbito del Departamento. Como ya se ha indicado, el listado de webs bloqueadas, o cuyo acceso se limita por los sistemas de seguridad de los sistemas informáticos del departamento, forma parte de las medidas de seguridad. Por otra parte, no existe una lista cerrada de páginas web bloqueadas, sino que en función de los grados de seguridad que garantice el acceso a determinadas páginas, su acceso se puede limitar o bloquear. Si por parte del departamento se indicara qué estrategia concreta se sigue en este sentido, se desvelaría información que podría ser utilizada para desbloquear las medidas de seguridad adoptadas, con lo que dejarían de cumplir su finalidad. En consecuencia, este Departamento no ha rechazado de forma caprichosa el acceso a la información, sino que ha valorado que, en este supuesto concreto, la seguridad pública y de las comunicaciones de las Administraciones publicaciones, justifica plenamente la denegación objeto de este recurso.*

- *Por ello, y reiterando la argumentación del punto primero de estas alegaciones, las limitaciones de acceso a páginas web en el Ministerio de Energía, Turismo y Agenda Digital se establecen en base a diferentes razones de servicio público: evitar ataques e infecciones por virus, uso adecuado de recursos públicos administrativos para los fines marcados por el ordenamiento jurídico, eficacia, eficiencia, calidad, etc…, garantizar la seguridad de la información que se gestiona en el departamento, así como garantizar la seguridad de los datos carácter personal que se custodian por la administración.*
- *A la vista de lo expuesto, se solicita que se admita a trámite este escrito y a la vista de las alegaciones contenidas en el mismo se desestime la reclamación formulada contra la resolución de este Ministerio del día 27 de julio de 2017, por haberse dictado conforme a derecho, sin que se haya vulnerado el derecho de acceso a la información pública en los términos regulados en los artículos 17 y siguientes de la Ley 19/2013, de 9 de diciembre, y que el denegar la información conforme al artículo 14.1 d) prevalece sobre el derecho a recibir o remitir dicha información solicitada, y no afecta al derecho del solicitante a su libertad de expresión.*

## II. FUNDAMENTOS JURÍDICOS

1. De conformidad con lo dispuesto en el artículo 24 de la LTAIBG, en relación con el artículo 8 del Real Decreto 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno, la Presidenta de este Organismo es competente para resolver las reclamaciones que, con carácter potestativo y previo a un eventual Recurso Contencioso-Administrativo, se presenten en el marco de un procedimiento de acceso a la información.

2. La Ley 19/2013, de 19 de diciembre, de Transparencia, acceso a la información pública y buen gobierno reconoce en su artículo 12 el derecho de todas las personas a acceder a la información pública, entendida, según el artículo 13 de la



[redacted]

misma norma, como "*los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*".

Por lo tanto, la Ley define el objeto de una solicitud de acceso a la información en relación a información que ya existe, por cuanto está en posesión del Organismo que recibe la solicitud, bien porque él mismo la ha elaborado o bien porque la ha obtenido en ejercicio de las funciones y competencias que tiene encomendadas.

3. En cuanto al fondo del asunto y en atención a los argumentos indicados, debe analizarse, en primer lugar, si resulta de aplicación el límite del articulo 14.1 d), invocado por la Administración, según el cual *el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para la seguridad pública*.

   Sobre la aplicación de los límites al acceso a la información, es conocido el Criterio Interpretativo nº 2 de 2015, aprobado por este Consejo de Transparencia y Buen Gobierno en cumplimiento de las funciones legalmente encomendadas por el art. 38.2 a) y que se pronuncia en los siguientes términos:

   *Los límites a que se refiere el artículo 14 de la LTAIBG, a diferencia de los relativos a la protección de los datos de carácter personal, no se aplican directamente, sino que de acuerdo con la literalidad del texto del número 1 del mismo, "podrán" ser aplicados.*

   *De esta manera, los límites no operan ni automáticamente a favor de la denegación ni absolutamente en relación a los contenidos.*

   *La invocación de motivos de interés público para limitar el acceso a la información deberá estar ligada con la protección concreta de un interés racional y legítimo.*

   *En este sentido su aplicación no será en ningún caso automática: antes al contrario deberá analizarse si la estimación de la petición de información supone un perjuicio (test del daño) concreto, definido y evaluable. Este, además no podrá afectar o ser relevante para un determinado ámbito material, porque de lo contrario se estaría excluyendo un bloque completo de información.*

   *Del mismo modo, es necesaria una aplicación justificada y proporcional atendiendo a la circunstancia del caso concreto y siempre que no exista un interés que justifique la publicidad o el acceso (test del interés público).*

   Por lo tanto, al acceso a la información o documentación le son de aplicación los límites contenidos en el artículo 14 de la LTAIBG y el relativo a la protección de datos de carácter personal, regulado en su artículo 15. En todo caso, la aplicación de los límites deberá ser motivada, restringida, justificada y proporcionada así como atender a las circunstancias del caso concreto, de acuerdo con los criterios contenidos en el indicado Criterio Interpretativo y en las sentencias de los Tribunales Contencioso-Administrativos.



[redacted]

En este sentido, debe tenerse presente que facilitar la información es la regla general y la aplicación de los limites es la excepción y hemos de tener presente que la LTAIBG, en su *Preámbulo*, afirma expresamente que el derecho de acceso a la información pública se configura de forma amplia y dicho derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información o por su entrada en conflicto con otros intereses protegidos. *"Así, la finalidad, principio y filosofía que impregna la reseñada Ley, es un acceso amplio a la información pública; y los límites a tal acceso han de motivarse, interpretarse y aplicarse de modo razonado, restrictivo y aquilatado a tenor del llamado, test de daño; a la luz de la determinación del perjuicio que el acceso a determinada información puede producir sobre el interés que se pretende salvaguardar con la limitación"* (Sentencia 85/2016, de 14 de junio de 2016, del Juzgado Central de lo Contencioso Administrativo nº 5 de Madrid. PO 43/2015).

Por otro lado, la Sentencia 46/2017, de 22 de junio de 2016, del Juzgado Central de lo Contencioso Administrativo nº 2 de Madrid, dictada en el PO 38/2016, se pronuncia en los siguientes términos:

"*El derecho de acceso a la información es un derecho fundamental reconocido a nivel internacional como tal, debido a la naturaleza representativa de los gobiernos democráticos; es un derecho esencial para promover la transparencia de las instituciones públicas y para fomentar la participación ciudadana en la toma de decisiones. Además las Administraciones Públicas se financian con fondos procedentes de los contribuyentes y su misión principal consiste en servir a los ciudadanos por lo que toda la información que generan y poseen pertenece a la ciudadanía.* (…)

Finalmente, la reciente sentencia del Tribunal Supremo de 16 de octubre de 2017 dictada en el Recurso de Casación nº 75/2017 indica lo siguiente:

*(...) "Esa formulación amplia en el reconocimiento y en la regulación legal del derecho de acceso a la información obliga a interpretar de forma estricta, cuando no restrictiva, tanto las limitaciones a ese derecho que se contemplan en el artículo 14.1 de la Ley 19/2013 como las causas de inadmisión de solicitudes de información que aparecen enumeradas en el artículo 18.1".(...) sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información.*

*(…) Asimismo, la posibilidad de limitar el derecho de acceso a la información no constituye una potestad discrecional de la Administración o entidad a la que se solicita información, pues aquél es un derecho reconocido de forma amplia y que sólo puede ser limitado en los casos y en los términos previstos en la Ley; (…)*

4. A juicio de este Consejo de Transparencia, más que afectar a la Seguridad pública, proporcionar cierta información como la que se solicita podría afectar a la Seguridad Nacional, contemplada como límite en el articulo 14.1 a) de la LTAIBG: "*el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para la seguridad nacional*."

   Por su parte, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional dispone que esta se entiende como *la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos (*artículo 2*)*

   Su artículo 4 establece lo siguiente:

   *1. La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional.*

   *2. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración.*

   *3. La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley.*

   Finalmente, su artículo 11 establece que:

   *1. En el marco del Sistema de Seguridad Nacional, las Administraciones Públicas con competencias en los ámbitos de especial interés de la Seguridad Nacional, estarán obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.*

   *2. Asimismo, sin perjuicio de lo establecido en la normativa reguladora de protección de infraestructuras críticas, las Administraciones Públicas citadas anteriormente asegurarán la disponibilidad de los servicios esenciales y la garantía del suministro de recursos energéticos, agua y alimentación,*



[redacted]

*medicamentos y productos sanitarios, o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico.*

Igualmente, al Sistema de Seguridad Nacional le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en la Ley de Seguridad Nacional, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema.

5. En el campo de la Ciberseguridad, el Consejo Nacional de Ciberseguridad, órgano colegiado de apoyo al Consejo de Seguridad Nacional y en concreto de asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional en el ámbito de la ciberseguridad, adoptó el Plan Nacional de Ciberseguridad, al que el Consejo de Seguridad Nacional dio su conformidad.

   Se trata del primer nivel en la planificación resultante de la Estrategia de Ciberseguridad Nacional y desarrolla, a través de planes de acción derivados, las líneas de acción previstas en la Estrategia. Estos planes derivados abordan distintos aspectos de la ciberseguridad, como incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en la Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y otros sistemas de interés nacional, la investigación y persecución del ciberterrorismo, el ciberspionaje y la ciberdelincuencia, así como la ciberseguridad en el sector privado o la cultura de ciberseguridad.

   Asimismo, la Estrategia de Ciberseguridad Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2013 en el ámbito de la ciberseguridad, fijando como objetivo global lograr que España haga un uso seguro de los sistemas de información y las telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. Seguidamente, la Estrategia fija seis objetivos específicos:

   - Para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia (o capacidad para afrontar situaciones adversas);
   - Para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular;
   - En el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio;



[redacted]

- En materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio;
- En capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad;
- En lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.

6. Por tanto, el concepto de ciberseguridad nacional emana de los dos documentos estratégicos referidos, entendiendo la misma como la acción del Estado dirigida a proteger los intereses nacionales, vitales y estratégicos, referentes a:

    - Los sistemas de información y telecomunicaciones e infraestructuras comunes a todas las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés para la Seguridad Nacional.;
    - La libertad y seguridad de los ciudadanos;
    - La industria;
    - El patrimonio tecnológico.

    Todo ello cumpliendo la legislación nacional y el derecho internacional, así como el respeto de las normas internacionales en cumplimiento de los compromisos adquiridos por España.

    La Estrategia de Ciberseguridad Nacional establece igualmente unas *Líneas de Acción* orientadas a alcanzar los objetivos propuestos y un total de 45 medidas concretas.

    Para el desarrollo efectivo de estas *Líneas de Acción*, el Consejo Nacional de Ciberseguridad propuso la elaboración del *Plan de Acción* que enmarca su desarrollo, de manera específica, para los dos próximos años.

    El Plan Nacional de Ciberseguridad (PNCS), aprobado por el Consejo de Seguridad Nacional (CSN), constituye el primer nivel en la planificación de la Estrategia de Ciberseguridad Nacional que, siguiendo las directrices generales de la misma, identifica de manera más exhaustiva los riesgos y amenazas. El estado de estos riesgos y amenazas de la Ciberseguridad Nacional se concreta en el Informe Anual de Seguridad Nacional que aprueba el CSN antes de su presentación en Sede Parlamentaria, reflejo del compromiso con la necesaria transparencia e implicación de la sociedad. De este informe se desprende cómo el Sistema de Seguridad Nacional se configura para hacer frente y dar respuesta a estos desafíos.



[redacted]

7. La Estrategia de Seguridad Nacional, elaborada por Presidencia del Gobierno en el año 2013, dispone lo siguiente en materia de ciberseguridad:

   ***1.*** *Incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas con apoyo en un marco jurídico operativo y eficaz. Se mejorarán los procedimientos y se impulsarán los recursos necesarios con especial énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés nacional.*

   ***2.*** *Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Se finalizar á la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio, mediante el refuerzo de las capacidades de detección y la mejora de la defensa de los sistemas clasificados. Se fortalecerá la seguridad de los sistemas de información y las redes de comunicaciones que soportan las infraestructuras críticas. Se impulsará la normativa sobre protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.*

   ***3.*** *Mejora de la seguridad y resiliencia de las Tecnologías de la Información y la Comunicación (TIC) en el sector privado a través del uso de las capacidades de los poderes públicos. Se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.*

   ***4.*** *Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un Plan de I+D+i.*

   ***5.*** *Implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.*

   ***6.*** *Intensificación de la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable. En todo momento se salvaguardarán los intereses nacionales.*

8. De los documentos y preceptos legales citados pueden extraerse las siguientes conclusiones:

   - La Seguridad Nacional afecta a la libertad y el bienestar de los ciudadanos, la defensa de España y sus principios y valores constitucionales.
   - La Ciberseguridad debe entenderse como la garantía del uso seguro de las redes y los sistemas de información a través del fortalecimiento de la prevención, detección y respuesta a los ciberataques.
   - La Ciberseguridad forma parte de la Estrategia de Seguridad Nacional, haciendo especial énfasis en la Administraciones Públicas. Para estas, se



[redacted]

trata de garantizar que sus sistemas de información y telecomunicaciones, redes de comunicaciones e infraestructuras comunes poseen el adecuado nivel de seguridad y resiliencia.

- El bloqueo a determinados tipos de contenidos, dominios o IPs en las conexiones del Ministerio, que es por lo que se interesa el Reclamante, puede incardinarse, con carácter general, dentro de la estrategia de ciberseguridad que han de adoptar las Administraciones Publicas para evitar ciberataques, puesto que permitiendo esos accesos se corre el riesgo cierto, no hipotético, de sufrir ataques externos que incidan en la seguridad de la información que maneja el Ministerio, así como en los datos personales almacenados en sus ficheros y sistemas, con el consiguiente perjuicio para los ciudadanos que tienen o han tenido relaciones con el mismo, mermando, sin duda, sus derechos y su bienestar, que es lo que se pretende proteger bajo el paraguas de la Seguridad Nacional. Todo ello, como resultado de un incidente de ciberseguridad o de un aviso previo por parte del Centro Criptológico Nacional en el que indican que se trata de dominios maliciosos.

9. Sin embargo, no obstante lo anterior, a juicio de este Consejo de Transparencia y Buen Gobierno, no toda la información que se solicite relativa a bloqueo de accesos a Internet debe quedar subsumida en el límite de la Seguridad Nacional, como así lo entiende también el Ministerio, que ha dado parte de la información.

   Este Consejo de Transparencia entiende que la parte de la solicitud no atendida no está afectada por el límite citado, por las siguientes razones:

   - Respecto a la solicitud de *copia del protocolo/reglamento/reglas por las que se determina el bloqueo a determinados tipos de contenidos, dominios o IPs*, el Ministerio de ENERGÍA, TURISMO Y AGENDA DIGITAL ya ha contestado, informando que *dispone de distintas herramientas y productos de seguridad (firewalls, antivirus de puesto, etc.), que, entre otras acciones, permiten bloquear el acceso de los empleados del Ministerio a contenidos que puedan entrañar riesgos de seguridad (tanto a nivel de nombre lógico, como de dirección física). Son los propios productos de protección los que de forma autónoma y en base a distintas categorías, bloquean el acceso a contenidos que pueden comprometer la seguridad, que vulneran leyes de propiedad intelectual, etc.*
   - En cuanto a *los cargos de las personas que deciden si una web se bloquea o no desde su conexión,* este Consejo de Transparencia entiende que debe darse la información, ya que es objetivo de la LTAIBG conocer cómo se toman las decisiones que afectan a los ciudadanos o bajo qué criterios actúan nuestras instituciones, lo que incluye conocer qué cargo toma esas decisiones con trascendencia pública, por lo que no debe aplicarse el límite invocado en este punto. La Seguridad Nacional no depende de la identificación del cargo que toma decisiones sobre ciberseguridad favorables también para la ciudadanía.

En este sentido, el Ministerio también ha ofrecido información remitiendo al solicitante al artículo 4 de la Orden IET/1934/2014, de 14 de octubre, que establece la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Energía y Turismo (actual Ministerio de Energía, Turismo y Agenda Digital) y constituye el Comité Director de la Seguridad de la Información en el Departamento, de la siguiente manera:

*1. Se crea el Comité Director de la Seguridad de la Información (en adelante, el Comité), que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información y ejercerá las siguientes funciones:*

*a) Elaborar las propuestas de modificación y actualización permanente de la PSI.*

*b) Aprobar la normativa de seguridad derivada de segundo nivel que sea de obligado cumplimiento (procedimientos STIC, normas STIC e instrucciones técnicas STIC).*

*c) Aprobar el procedimiento de control de accesos a la red y a las bases de datos de la administración electrónica del Ministerio de Industria, Energía y Turismo, así como los demás procedimientos de actuación en lo relativo al uso de los sistemas de información.*

*d) Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.*

*e) Informar sobre el estado de las principales variables de seguridad en los sistemas de información al Comité Sectorial de Administración Electrónica (CSAE) para la elaboración de un perfil general del estado de seguridad de las mismas.*

*f) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.*

*2. El Comité estará compuesto por los siguientes miembros:*

*a) Presidente: El Subsecretario de Industria, Energía y Turismo.*

*b) Vocales: Con categoría mínima de Subdirector General o asimilado, pudiendo delegar en un suplente por cada uno de los siguientes órganos u organismos autónomos del Departamento:*

*1. Secretaría General Técnica.*

*2. Secretaría de Estado de Energía.*

*3. Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.*

*4. Secretaría de Estado de Turismo.*



[redacted]

*5. Secretaría General de Industria y de la Pequeña y Mediana Empresa.*

*6. Oficina Española de Patentes y Marcas.*

*7. Instituto para la Reestructuración de la Minería del Carbón y Desarrollo Alternativo de las Comarcas Mineras.*

*8. Centro Español de Metrología.*

*9. Instituto de Turismo de España.*

*c) Secretario: Con voz y voto, el Subdirector General de Tecnologías de la Información y de las Comunicaciones, que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar.*

*d) Con carácter facultativo, el Presidente del Consejo de Administración del Instituto Nacional de Tecnologías de la Comunicación (INTECO) podrá formar parte del Comité como vocal, con voz, o bien delegar en un suplente con categoría mínima de Subdirector General o asimilado.*

*3. El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones.*

Una simple lectura de este articulo hubiera informado al solicitante de lo que pretendía conocer, esto es, que las decisiones sobre bloqueos Web la decide el Comité Director de la Seguridad de la Información del Ministerio, que es un órgano colegiado que toma las decisiones por votación de sus miembros, los cuales pueden participar en los debates de las sesiones, ejercer su derecho al voto y formular su voto particular, así como expresar el sentido de su voto y los motivos que lo justifican, aunque *los miembros de un órgano colegiado no pueden atribuirse las funciones de representación reconocidas a éste, salvo que expresamente se les hayan otorgado por una norma o por acuerdo válidamente adoptado, para cada caso concreto, por el propio órgano* (ex artículo 19.3 de la Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público).

- Sin embargo, respecto del *listado de los dominios y/o direcciones IP a los que bloquean el acceso desde las conexiones a Internet del Ministerio,* éste no ha proporcionado la información, aduciendo problemas de seguridad pública. A juicio de este Consejo de Transparencia, facilitar esos datos no sólo no pone en peligro las estructuras básicas del Ministerio, sino que ayuda a proteger la libertad y el bienestar de los ciudadanos, informándoles de sitios Web maliciosos a los que no es recomendable acceder, que es la finalidad de la Ley de Seguridad Nacional, por lo que tampoco debe aplicarse el límite invocado en este punto.

  Asimismo, debe tenerse en cuenta que, normalmente, el bloqueo viene derivado del hecho de que el acceso a los dominios y/o direcciones IP bloqueadas puede provocar un perjuicio a las redes y sistemas, por lo que, es

precisamente con el bloqueo de dichos dominios y/o direcciones IP con el que se está evitando un daño a la seguridad. Cuestión distinta sería si se pidiera y conociera información sobre los dominios y/o direcciones IP respecto de los que se haya constatado su carácter malicioso y también sobre los efectivamente bloqueados, lo que podría permitir una comparación y la identificación de los dominios y/o direcciones IP maliciosos frente a los que no se hubiera puesto ninguna medida. Esta última información si podría eventualmente, a nuestro juicio, producir un perjuicio a la seguridad del sistema, caso de ser conocida por terceros ajenos al mismo, ya que permitiría conocer fallos y quiebras del sistema de seguridad.

Por ello, debe estimarse la Reclamación en este apartado concreto.

- Finalmente, el Ministerio también ha informado que dispone de un único perfil de acceso a Internet, no existiendo, por tanto, un *listado de los distintos accesos a internet* con la categorización de las distintas conexiones, que es lo que quería saber el Reclamante.

10. Por todo lo anteriormente expuesto, debe estimarse en parte la Reclamación presentada, debiendo el Ministerio facilitar al Reclamante la siguiente información:

    - *El listado de los dominios y/o direcciones IP a los que bloquean el acceso desde las conexiones a Internet del Ministerio.*

## III. RESOLUCIÓN

En atención a los Antecedentes y Fundamentos Jurídicos descritos, procede

**PRIMERO**: **ESTIMAR parcialmente** la Reclamación presentada por [redacted] con entrada el 9 de agosto de 2017, contra la Resolución del MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, de fecha 27 de julio de 2017.

**SEGUNDO: INSTAR** al MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL a que, en el plazo máximo de 7 días hábiles, remita a [redacted] la información referida en el Fundamento Jurídico 10 de la presente Resolución.

**TERCERO: INSTAR** al MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL a que, en el mismo plazo máximo de 7 días hábiles, remita a este Consejo de Transparencia y Buen Gobierno copia de la información remitida al Reclamante.

De acuerdo con el artículo 23, número 1, de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, la Reclamación



[redacted]

prevista en el artículo 24 de la misma tiene la consideración de sustitutiva de los recursos administrativos, de conformidad con lo dispuesto en el artículo 112.2, de la Ley 39/2015, 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En consecuencia, contra la presente Resolución, que pone fin a la vía administrativa, únicamente cabe, en caso de disconformidad, la interposición de Recurso Contencioso-Administrativo ante los Juzgados Centrales de lo Contencioso-Administrativo de Madrid en plazo de dos meses a contar desde el día siguiente al de su notificación, de conformidad con lo previsto en el artículo 9.1, c), de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

LA PRESIDENTA DEL
CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO

Fdo: Esther Arizmendi Gutiérrez.



[redacted]