Resolución reclamación art. 24 LTAIBG

Número y fecha de resolución: indicados al margen.

Número de expediente: 2218/2025

Reclamante: [redacted]

Organismo: AEAT / MINISTERIO DE HACIENDA.

Sentido de la resolución: Desestimatoria.

Palabras clave: conexiones, alertas, arts. 14.1. a) y 14.1. d) LTAIBG.

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el 25 de marzo de 2025 el reclamante solicitó a la AEAT / MINISTERIO DE HACIENDA, al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[1] (en adelante, LTAIBG), la siguiente información:

   «Solicito información sobre tres cuestiones:

   1º. De las sesiones de conexiones en movilidad, esto es desde fuera de los edificios de la AEAT, que he realizado a lo largo de los años a las aplicaciones de la AEAT 2

   1-De los días del año o de la semana y horas considerados de riesgo y en los que, de producirse la conexión o inicio de sesión, se producen las alertas, según los protocolos de seguridad de la AEAT.

[1] https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887

2-De las alertas que se produjeron con motivo de mis accesos en movilidad en días u horas poco corrientes y considerados de riesgo y que servían de advertencia a los responsables del control de seguridad informática.

3-De las alertas sobre las que se me envió mensaje de advertencia al respecto.

3º. Del número de alertas que se han producido con motivo de los accesos en movilidad en días u horas poco corrientes acontecidos en relación al total de funcionarios de la AEAT y que servían de advertencia a los responsables del control de seguridad informática (Ver documentación original)».

2. Mediante resolución de 24 de septiembre de 2025, la AEAT responde lo siguiente:

«La LTAIBG en su artículo 14.1 a) señala como límite al derecho de acceso la seguridad nacional y en el artículo 14.1 d) señala que está limitada por razones de seguridad pública.

La concesión de la información solicitada puede afectar a las medidas de ciberseguridad de la Agencia Tributaria, cuyos sistemas de información son infraestructura crítica de acuerdo con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Así, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 identifica como riesgo para la seguridad nacional los ciberataques «contra la Administración General del Estado y sus organismos públicos, así como contra las administraciones autonómicas y locales».

En el mismo sentido, la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional contempla como objetivo prioritario la «Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.»

De hecho, la misma Ley 8/2011, de 28 de abril, contiene un motivo de denegación específico pues su artículo 15 dispone que:

2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.

3. Los sistemas, las comunicaciones y la información referida a la protección de las

infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

Por su parte, el art. 15 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información declara que:

Artículo 15. Confidencialidad de la información sensible.

Sin perjuicio de lo dispuesto en el artículo 5, las autoridades competentes, los CSIRT de referencia y el punto de contacto único preservarán, como corresponda en Derecho, la seguridad y los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, así como la confidencialidad de la información que recaben de éstos en el ejercicio de las funciones que les encomienda el presente real decreto-ley.

Cuando ello sea necesario, el intercambio de información sensible se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio.

En suma, de acuerdo con lo anteriormente expuesto, se DENIEGA el acceso a la información solicitada por resultar de aplicación los apartados a) y d) del artículo 14.1 de la LTAIBG».

3. Mediante escrito registrado el 9 de octubre de 2025, el solicitante interpuso una reclamación ante el Consejo de Transparencia y Buen Gobierno (en adelante, el Consejo) en aplicación del artículo 24[2] LTAIBG en la que pone de manifiesto lo siguiente:

   «(...) Se me contestó por la normativa de protección de datos, si bien, en vez del responsable del tratamiento, lo hizo un Jefe de Seguridad Regional.

   Por consiguiente, siendo incompetente por razón de materia (...), la resolución es nula de pleno Derecho [art 47.1.b) de la Ley 39/2015] y no puede desplegar ningún efecto (...)

   No obstante, incluso así, y pese a que la nula resolución manifiesta..//...

   " PRIMERO..... ....se procede a estimar su solicitud.....",

[2] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a24

…//… no se procedió a cumplirla puesto que:

Lo cierto es que esa declaración es una falsa estimación de mi solicitud por dos razones:

1ª.- La resolución me remite (…) a un expediente electrónico en mi espacio personal dentro de la sede electrónica de la AEAT, sin posibilidad de poderla presentar yo ante nadie en tanto que si la obtengo, lo descargado no tiene sello, hash, CSV o garantía alguna erga omnes (…)

2ª.- La información que se me proporciona no es completa (…) y con aquella resolución nada se dice ni se me proporciona al respecto los accesos a horas intempestivas a nivel global.

Resulta que ahora (…) recibo resolución fechada el 24.09.25 y firmada por el Director del Servicio de Planificación y Relaciones Institucionales en virtud de la Delegación permanente y general que hace el Director General de la AEAT por Resolución de 27.01.25 (BOE 09.02.15).

Resolución investida, ésta sí, de formalidades propias de un expediente de Transparencia (…)

No dice que la concesión de la información solicitada "afecta" a las medidas de ciberseguridad de la Agencia tributaria sino que "puede afectar", es decir, en términos de presunción.

El art 14 de la Ley 19/2013

En su apartado 1 no habla en términos hipotéticos o potenciales. Es tajante. Dice " El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para…..". -Además, su apartado 2 preceptúa que "La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés …… privado superior que justifique el acceso."

Por su parte, tampoco señala la AEAT de qué manera y con motivo de qué se puede ver afectada la seguridad cibernética o la seguridad nacional y la seguridad pública si me facilitan la información de accesos laborales en movilidad que he solicitado. Por ello, las alegaciones de la AEAT no constituyen motivación, tal como exige el art 20.2 de la Ley de Transparencia.

He de denunciar que al igual que la recibida bajo la normativa de protección de datos, la resolución de 24.09.25 también es nula de pleno derecho.

La nulidad de pleno derecho de esta otra resolución proviene de la nulidad que tiene la del Director General de fecha 27.01.15 y por la que decide la delegación de competencias que originariamente no tiene, pues se había arrogado antes facultades que ninguna ley le otorgó.

(...) Es el titular del órgano administrativo o entidad el que tiene que contestar. Esto es, resolver. Pero no resolvió el titular del Departamento de Informática a quien me dirigí y tiene la información nacional al respecto de lo solicitado sino que lo hizo el Director del Servicio de Planificación y Relaciones Institucionales por delegación del Director General.

(...)

En caso de una pretendida avocación previa que hubiera transferido la competencia del órgano (Departamento de Informática) al Director General, éste no podría a continuación delegarla(...)».

4. Con fecha 20 de octubre de 2025, el reclamante presenta nuevo escrito al Consejo, expresando lo siguiente:

«(...) La información que solicito yo a la AEAT ya existe, y está disponible para ella por diversas razones de control y no hay que aplicar fórmulas, cálculos, interpretaciones de planes o prácticas contables de costes, ni cosa parecida (...).

(...) Existen solicitudes de ciudadanos acogidas a la Ley 19/2013 para obtener información pública que, por su objeto, pueden solicitar también en virtud del Reglamento UE 2016/679.

Cuando esos ciudadanos no vemos satisfecha nuestra solicitud por la Administración a la que se ha requerido acogiéndose a la Ley de Transparencia, podemos reclamar ante el Consejo según el art 24 de la Ley 19/2013, con independencia de que lo hayamos hecho o no también ante la AEPD si alegamos en la solicitud igualmente la normativa que controla ésta.

Es criterio del Consejo en estos casos, o al menos lo ha sido conmigo ante las reclamaciones afectas a los expedientes ya resueltos números 1097/2025 y 1200/2025, que si la información objeto de reclamación está constituida o concierne a datos cuyo tratamiento está protegido por el Reglamento de la Unión procede a inhibirse a favor de la Agencia Española de Protección de Datos y así resuelve, notificando al reclamante que el expediente lo deriva a esa otra Autoridad Administrativa Independiente.

R CTBG Número: 2026-0622 Fecha: 10/06/2026

Al menos yo me siento desamparado por el Consejo y considero que ha dejado de cumplir su función con independencia de que dé conocimiento a otra Autoridad que, no me cabe duda, también es competente para conocer del caso si reclamo yo ante ella (...)».

5. Con fecha 10 de octubre de 2025 el Consejo trasladó la reclamación al Ministerio requerido solicitando la remisión de la copia completa del expediente derivado de la solicitud de acceso a la información y el informe con las alegaciones que considere pertinentes. El 7 de enero de 2026 tuvo entrada en este Consejo, junto al expediente, escrito en el que se señala lo siguiente:

   «En primer término, cabe precisar que los datos a los que pide acceso referidos a su persona suponen el ejercicio del derecho de acceso a los datos personales que asiste al interesado, regulado en el artículo 15 del Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), de ahí que haya recibido información por esta vía.

   En lo que atañe al ámbito de competencia de la LTAIBG, y en particular, en lo relativo a «Los días del año o de la semana y horas considerados de riesgo y en los que, de producirse la conexión o inicio de sesión laboral, se producen las alertas, según los protocolos de la AEAT» y «El número de alertas que se han producido con motivo de los accesos en movilidad en días u horas poco corrientes para estar trabajando un funcionario de la AEAT y acontecidos en relación al total de funcionarios de este Organismo y que servían de advertencia a los responsables.» tal y como se puso de manifiesto en la Resolución de esta Agencia de 24 de septiembre de 2025, la LTAIBG en su artículo 14.1 a) señala como límite al derecho de acceso la seguridad nacional y en el artículo 14.1 d) señala que está limitada por razones de seguridad pública.

   La concesión de la información solicitada puede afectar a las medidas de ciberseguridad de la Agencia Tributaria, cuyos sistemas de información son infraestructura crítica de acuerdo con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

   Así, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 identifica como riesgo para la seguridad nacional los ciberataques «contra la Administración General del Estado y sus organismos públicos, así como contra las administraciones autonómicas y locales».

En el mismo sentido, la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional contempla como objetivo prioritario la «Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.»

De hecho, la misma Ley 8/2011, de 28 de abril, contiene un motivo de denegación específico pues su artículo 15 dispone que:

2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.

3. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

Por su parte, el art. 15 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información declara que:

Artículo 15. Confidencialidad de la información sensible.

Sin perjuicio de lo dispuesto en el artículo 5, las autoridades competentes, los CSIRT de referencia y el punto de contacto único preservarán, como corresponda en

Derecho, la seguridad y los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, así como la confidencialidad de la información que recaben de éstos en el ejercicio de las funciones que les encomienda el presente real decreto-ley.

Cuando ello sea necesario, el intercambio de información sensible se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio.

Si por parte de esta Agencia se indican los días y horas considerados de riesgo a los efectos de activar alertas, se está informando a los potenciales ciberdelincuentes de los días y horas en los que no deben intentar ataques o de los días y horas en los que se puede ser más vulnerable a un ciberataque.

Lo mismo ocurre con el número de alertas, porque con ese dato un ciberdelincuente que haya intentado ataques a los sistemas de la Agencia puede determinar el porcentaje de estos que han generado una alarma y tantear qué sistemas de

ataque generan mayor o menor número de alertas y por tanto cuáles son más eficaces.

En otro orden de asuntos, por lo que respecta a la afirmación del reclamante sobre la nulidad de la resolución de esta Agencia de 24 de septiembre de 2025 por falta de competencia, ha de indicarse en primer término que la falta de competencia únicamente es motivo de nulidad cuando es manifiesta por razón de la materia o del territorio de acuerdo con lo dispuesto en el artículo 47.1.b Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Hecha esta precisión, cabe señalar asimismo que la LTAIBG no atribuye expresamente la competencia para resolver las peticiones de acceso a la información sólo al «titular del órgano administrativo» sino también al titular de la «entidad» que en este caso es la Dirección General de la Agencia Estatal de Administración Tributaria, habiéndose estructurado en el ámbito de la Agencia Estatal de Administración Tributaria la tramitación de estos procedimientos a través de su centralización en la Dirección General que ha delegado la competencia en el Director del Servicio de Planificación y Relaciones Internacionales por Resolución de 8 de noviembre de 2012, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueba la política de seguridad de la información de la Agencia Estatal de Administración Tributaria, en base a la competencia que le atribuye el artículo 21 de establecer «sistemas para integrar la gestión de solicitudes de información de los ciudadanos en el funcionamiento de su organización interna».

6. El 7 de enero de 2026, se concedió audiencia al reclamante para que presentase las alegaciones que estimara pertinentes; recibiéndose escrito el 12 de enero de 2026 en el que señala:

   «(...) En su párrafo 13ª dice la AEAT que si se me comunicasen los días y horas en que el acceso a se considera de riesgo ello supone estar informando a los potenciales ciberdelincuentes de los momentos en que no deben intentar atacar o de cuándo la AEAT es más vulnerable.

   Parece asimilar:

   El hecho de proporcionarme a mí esa información, un funcionario público, policía judicial por demás, empleado de la propia AEAT y que por ley tengo la obligación de no divulgar.

   Con el hecho de pregonar la propia AEAT, urbi et orbi, o con acuse de recibo de los propios delincuentes esa información.

(…)

En su párrafo 14º dice que con la información sobre el número de alertas un ciberdelincuente puede determinar el porcentaje de ataques que de los que pudiera haber hecho han generado alertas y qué sistema de los que haya empleado es más eficiente.

(…)

Pero lo más importante que tiene que tener en cuenta el Consejo es que la AEAT, para confundir, habla de alertas como si de avisos de ataques externos se tratara. Yo no he pedido que me digan cuántas alertas han existido, entre las que podrían estar esas de ciberdelincuentes, o espías de diversos países. He pedido alertas de acceso de trabajadores de la propia AEAT en teletrabajo, incluyendo las mías.

(…)

Yo he pedido sólo y exclusivamente las alertas (…) que los (aparentes) funcionarios que teletrabajaban hicieron saltar por acceder en horarios intempestivos.

(…)

La denominada por la AEAT Unidad gestora del derecho de acceso a la información pública de la AEAT no es quien tiene que resolver la solicitud de información. Ni por ley, ni por resolución (la de 27.01.15). La resolución sobre la solicitud del ciudadano ha de emitirla y la información ha de proporcionarla el titular del órgano o entidad al que se dirige la solicitud y tiene la información.

(…)

Termina su hoja 12 sin ni siquiera firmar.

Un organismo que no admite un escrito de los ciudadanos sin las más altas garantías de identificación, se permite dar por bueno un escrito sin identificación personal de quién firma el acto con el que se pretende justificar el cierre de la vía a un derecho constitución de un ciudadano.

Niego por tanto validez alguna a ese papel de 07.01.26 (…)».

II. FUNDAMENTOS JURÍDICOS

1. De conformidad con lo dispuesto en el artículo 38.2.c) de la LTAIBG[3] y en el artículo 13.2.d) del Real Decreto 615/2024, de 2 de julio, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno, A.A.I.[4], la Presidenta de esta Autoridad Administrativa Independiente es competente para conocer de las reclamaciones que, en aplicación del artículo 24 de la LTAIBG[5], se presenten frente a las resoluciones expresas o presuntas recaídas en materia de acceso a la información.

2. La LTAIBG reconoce en su artículo 12[6] el derecho de todas las personas a acceder a la información pública, entendiendo por tal, según dispone en el artículo 13, «*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*».

   De este modo, la LTAIBG delimita el ámbito material del derecho a partir de un concepto amplio de información, que abarca tanto documentos como contenidos específicos y se extiende a todo tipo de "*formato o soporte*". Al mismo tiempo, acota su alcance, exigiendo la concurrencia de dos requisitos que determinan la naturaleza "*pública*" de las informaciones: (a) que se encuentren "*en poder*" de alguno de los sujetos obligados, y (b) que hayan sido elaboradas u obtenidas "*en el ejercicio de sus funciones*".

   Cuando se dan estos presupuestos, el órgano competente debe conceder el acceso a la información solicitada, salvo que justifique de manera clara y suficiente la concurrencia de una causa de inadmisión o la aplicación de un límite legal.

3. La presente reclamación trae causa de una solicitud, formulada en los términos que figuran en los antecedentes, en la que se pide el acceso a información relacionada con las conexiones en remoto realizadas por el solicitante a las aplicaciones de la AEAT y a los criterios de activación de alertas y el número de las producidas respecto al total de funcionarios del organismo.

   La AEAT denegó el acceso a lo solicitado con fundamento en los artículos 14.1.a) y 14.1.d) LTAIBG, por considerar que facilitar esta información podría afectar a las

[3] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a38
[4] https://www.boe.es/eli/es/rd/2024/07/02/615
[5] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[6] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a12

medidas de ciberseguridad del organismo. A la vista de la reclamación interpuesta, en la que el solicitante cuestiona la falta de motivación del perjuicio a los bienes invocados, la AEAT amplía sus argumentos y reitera los límites alegados en su resolución inicial, confirmando asimismo la competencia del órgano que ha dictado la resolución

4. Antes de entrar a examinar el fondo de asunto, procede recordar que el artículo 20.1 LTAIBG dispone que *«[l]a resolución en la que se conceda o deniegue el acceso deberá notificarse al solicitante y a los terceros afectados que así lo hayan solicitado en el plazo máximo de un mes desde la recepción de la solicitud por el órgano competente para resolver. Este plazo podrá ampliarse por otro mes en el caso de que el volumen o la complejidad de la información que se solicita así lo hagan necesario y previa notificación al solicitante*».

   En este caso, el órgano competente no respondió al solicitante en el plazo máximo legalmente establecido, sin que conste causa o razón que lo justifique. A la vista de ello, es obligado recordar a la Administración que la observancia del plazo máximo de contestación es un elemento esencial del contenido del derecho constitucional de acceso a la información pública, tal y como el propio Legislador se encargó de subrayar en el preámbulo de la LTAIBG al manifestar que «*con el objeto de facilitar el ejercicio del derecho de acceso a la información pública la Ley establece un procedimiento ágil, con un breve plazo de respuesta*».

5. Sentado lo anterior, resulta necesario delimitar el objeto de la solicitud de acceso. Así, de su lectura, se infiere que, por un lado, se solicitó información relativa a los accesos realizados por el propio reclamante. Y, por otro, se pretendió el acceso a información relacionada con los criterios de la AEAT para la activación de alertas y a datos agregados sobre el conjunto de funcionarios del organismo.

   Tal distinción ha tenido su reflejo en la tramitación de la solicitud. En ese sentido, la AEAT ha alegado que *«los datos a los que pide acceso referidos a su persona suponen el ejercicio del derecho de acceso a los datos personales que asiste al interesado, regulado en el artículo 15 del Reglamento (UE) 2016/679, de 27 de abril de 2016»*. Y el propio reclamante ha expresado que recibió resolución por esta vía, discrepando de la suficiencia de la información proporcionada.

   No obstante, el procedimiento del derecho de acceso no constituye el cauce para resolver las controversias que se susciten sobre el ejercicio del derecho de acceso a los datos personales regulado en el Reglamento (UE) 2016/679, de 27 de abril.

R CTBG Número: 2026-0622 Fecha: 10/06/2026

Así, el objeto de este procedimiento se circunscribe a las siguientes pretensiones enunciadas por el reclamante: *«1-De los días del año o de la semana y horas considerados de riesgo y en los que, de producirse la conexión o inicio de sesión, se producen las alertas, según los protocolos de seguridad de la AEAT»*; y al punto *«3º. Del número de alertas que se han producido con motivo de los accesos en movilidad en días u horas poco corrientes acontecidos en relación al total de funcionarios de la AEAT y que servían de advertencia a los responsables del control de seguridad informática».*

6. Realizada esa precisión, procede a continuación verificar la concurrencia de los límites previstos en los apartados a) y d) del artículo 14.1 LTAIBG, invocados por la AEAT para denegar el acceso a los puntos 1 y 3º de la solicitud de acceso.

   Esta comprobación debe partir de la necesaria interpretación estricta, cuando no restrictiva, tanto de las causas de inadmisión enumeradas en el artículo 18.1 LTAIBG como de los límites que se contemplan en el artículo 14.1 LTAIBG, «*sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información»* [por todas, Sentencia del Tribunal Supremo (STS) de 16 de octubre de 2017 (ECLI:ES:TS:2017:3530); lo que exige una *«justificación expresa y detallada que permita controlar la veracidad y proporcionalidad de la restricción establecida»* [STS de 11 de junio de 2020 (ECLI:ES:TS:2020:1558)].

   En este sentido, conviene recordar que *«(...) solo son aceptables las limitaciones que resulten justificadas y proporcionadas, así lo dispone el artículo 14.2 de la Ley 19/2013: "[...] 2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso". Por tanto, la posibilidad de limitar el derecho de acceso a la información no constituye una potestad discrecional de la Administración y solo resulta posible cuando concurra uno de los supuestos legalmente establecido, que aparezca debidamente acreditado por quien lo invoca y resulte proporcionado y limitado por su objeto y finalidad»*.

7. En este caso, como consta en los antecedentes, la AEAT expone que los sistemas de información de la AEAT están catalogados como infraestructura crítica de conformidad con la Ley 8/2011, de 28 de abril, disponiendo su artículo 15 que las Administraciones deben garantizar la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso. Por ello, considera que

divulgar la información solicitada puede afectar a las medidas de ciberseguridad de la AEAT.

Con posterioridad, en fase de alegaciones explica que facilitar los días y horas que se consideran de riesgo a los efectos de activar alertas (1) permitiría a los potenciales ciberdelincuentes tener acceso a los días y horas que deben evitar ataques, así como a aquellos que son más vulnerables a un ciberataque. Y en relación al número de alertas producidas por accesos en días u horas poco corrientes con respecto al total de funcionarios del organismo (3º), añade que proporcionar este dato puede facilitar que los ciberdelincuentes determinen el porcentaje de ataques que han generado una alarma e inferir qué sistemas de ataque ocasionan mayor o menor número de alertas, lo que permitiría conocer cuáles son más eficaces.

En este punto, es necesario precisar que la argumentación de la AEAT tanto en su resolución como en el escrito de alegaciones se articula esencialmente en torno al límite relativo a la seguridad nacional previsto en el artículo 14.1.a) LTAIBG.

Por el contrario, nada se ha alegado acerca de la eventual afectación al límite de la seguridad pública previsto en el artículo 14.1.d) LTAIBG. En este sentido, no se ha hecho referencia a riesgos para la protección de personas y bienes, para la seguridad ciudadana o el orden público, ámbitos tradicionalmente asociados al concepto de seguridad pública, sino a la protección de sistemas de información estratégicos de la Administración General del Estado frente a amenazas de naturaleza cibernética, que guarda en cambio relación con el concepto de seguridad nacional contemplado en el artículo 14.1.a) LTAIBG.

En consecuencia, las alegaciones de la AEAT deben examinarse exclusivamente desde la perspectiva del límite relativo a la seguridad nacional, sin que resulte posible apreciar una justificación autónoma y diferenciada de la eventual afectación a la seguridad pública en los términos exigidos por el artículo 14.2 LTAIBG.

Desde esta perspectiva, en lo que respecta al punto 1 de la solicitud, este Consejo considera que la justificación ofrecida por la AEAT resulta suficiente para apreciar la concurrencia del límite previsto en el artículo 14.1.a) LTAIBG. En efecto, la información solicitada se refiere a parámetros internos utilizados por la AEAT para la detección de comportamientos potencialmente anómalos en los accesos a sus sistemas de información. Su divulgación permitiría conocer aspectos relevantes de los mecanismos de control implantados, permitiendo a los ciberdelincuentes evitar la activación de tales alertas o reducir su eficacia. Existe, por tanto, una relación suficientemente directa entre el acceso a la información y el perjuicio alegado para la seguridad de los sistemas de información.

R CTBG
Número: 2026-0622 Fecha: 10/06/2026

[redacted]

La misma conclusión debe alcanzarse respecto del punto 3.º de la solicitud, relativo al número de alertas producidas por accesos en movilidad en días u horas poco corrientes respecto del total de funcionarios del organismo. La AEAT ha puesto de manifiesto que la divulgación de este dato permitiría obtener información acerca de la frecuencia con la que determinados ataques generan alertas de seguridad y valorar la eficacia de los sistemas de ataque desplegados. Ello posibilitaría extraer conclusiones acerca de la capacidad de respuesta de los sistemas de control establecidos, aportando referencias útiles para adaptar comportamientos o planificar actuaciones orientadas o eludir o dificultar su detección.

Tal circunstancia podría, en efecto, comprometer la efectividad de los sistemas de control establecidos para la protección de sus sistemas de información, por lo que este Consejo considera que se ha acreditado el perjuicio a la seguridad nacional y, en consecuencia, resulta de aplicación el límite previsto en el artículo 14.1.a) de la LTAIBG.

Asimismo, no concurren en el presente caso las circunstancias que permitan apreciar un interés público o privado superior que deba prevalecer sobre la protección del bien jurídico invocado, toda vez que la información solicitada no está conectada con las finalidades de transparencia que persigue la LTAIBG.

8. En consecuencia, por las razones expuestas, procede desestimar la reclamación presentada.

III. RESOLUCIÓN

En atención a los antecedentes y fundamentos jurídicos descritos, procede **DESESTIMAR** la reclamación presentada frente a la resolución de la AEAT / MINISTERIO DE HACIENDA.

De acuerdo con el artículo 23.1[7], de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la reclamación 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, de 1 de octubre[8], de Procedimiento Administrativo Común de las Administraciones Públicas.

[7] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a23
[8] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a112

R CTBG Número: 2026-0622 Fecha: 10/06/2026

Contra la presente resolución, que pone fin a la vía administrativa, se podrá interponer recurso contencioso-administrativo, en el plazo de dos meses, directamente ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, de conformidad con lo previsto en el apartado quinto de la Disposición adicional cuarta de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-administrativa[9].

LA PRESIDENTA DEL CTBG

Fdo.: María de la Concepción Campos Acuña

[redacted]

[9] https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718&p=20230301&tn=1#dacuarta