Nº DE EXPEDIENTE	**001-066740**
Solicitante	
NIF:	
E-mail	
Fecha entrada	**13 marzo de 2021**
Datos solicitados	**Ciberataques**

Vista la solicitud de acceso a la información pública detallada anteriormente, formulada al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, se informa lo siguiente:

Atendiendo al contenido de la consulta planteada, la normativa aplicable al caso se circunscribe principalmente a los siguientes ámbitos:

- **Protección de las infraestructuras críticas (PIC):**
  - Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
  - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
  - Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
  - Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

- **Seguridad de la Información Clasificada**:
  - Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

- Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.
- Normas de la Autoridad Nacional para la Protección de la Información Clasificada.

- **Transparencia de la información pública**
  - Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

La Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas y el Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas tienen como finalidad, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas clasificadas como tal. La Ley 8/2011, designa al CNPIC como órgano responsable del impulso, coordinación y supervisión la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad (Ministerio del Interior), en relación con la protección de las Infraestructuras Críticas en el territorio nacional.

Atendiendo a su ámbito competencial, el CNPIC considera cómo estratégicos a aquellos sectores que se encuentran definidos y dentro del ámbito de aplicación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Asimismo, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales, comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

La citada Ley 8/2011, de 28 de abril, determina que es Infraestructura crítica, las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los

servicios esenciales. Dichas infraestructuras críticas, así como las esenciales se encuentran recogidas en el Catálogo Nacional de Infraestructuras Estratégicas.

El Catálogo Nacional de Infraestructuras Estratégicas es el registro de carácter administrativo, que tiene como finalidad el poder disponer de una información completa, actualizada y contrastada sobre la totalidad de las infraestructuras estratégicas en el territorio nacional, incluidas las infraestructuras críticas, así como aquéllas clasificadas como críticas europeas, que afecten a España.

Con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo mediante el que se estableció el marco estructural que permitirá dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha de España contra el terrorismo, donde se determinó que la documentación contenida en el Catálogo Nacional de Infraestructuras Estratégicas, de acuerdo con la vigente normativa de materias clasificadas, tenía la calificación de SECRETA, dada la alta sensibilidad para la seguridad nacional de la información contenida en dicho Catálogo.

El Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales, en su artículo tercero, estipula que la clasificación de secreto se aplicará a todas las materias que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello, pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado, o pudiera comprometer los Intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional.

Las Normas de la Autoridad Nacional para la Protección de la Información Clasificada constituyen el desarrollo normativo con el que se regula el manejo de la información clasificada en España y se da respuesta a las obligaciones contraídas en el ámbito internacional por nuestro país con otros estados u organizaciones internacionales.

Para acceder a la información clasificada es imprescindible tener “necesidad de conocer” y haber sido instruido previamente en el manejo de materia de protección de información clasificada. Además, para aquella información clasificada como CONFIDENCIAL o superior es necesario estar en posesión de una Habilitación Personal de Seguridad (HPS), que es la determinación positiva por la que la Autoridad Nacional, en nombre del Gobierno reconoce formalmente la capacidad e idoneidad de una persona para tener acceso a

Información al haber superado el oportuno proceso de acreditación de seguridad y haber sido adecuadamente concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento.

La "necesidad de Conocer" se define como la determinación positiva por la que se confirma que un posible destinatario requiere el acceso a, el conocimiento de, o la posesión de información para desempeñar servicios, tareas o cometidos oficiales. Ninguna persona podrá tener acceso a Información Clasificada exclusivamente por razón de su cargo o posición, o por estar en posesión de una HPS, sin la preceptiva necesidad de conocer.

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en su artículo 12, regula el derecho de todas las personas a acceder a la información pública, entendida, según el artículo 13 de la 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".* Sin embargo, el derecho de acceso está sujeto a ciertos límites, recogidos en el artículo 14 de la Ley 19/2013, de 9 de diciembre, entre ellos cuando dicho acceso suponga un perjuicio para la **SEGURIDAD NACIONAL.**

La Sentencia núm. 60/2016, de 18 de mayo de 2016, del Juzgado Central de lo Contencioso Administrativo núm. 6 de Madrid, dictada en el PO 57/20156, dictamina que: *"(…) Este derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información –derivado de lo dispuesto en la Constitución Española– o por su entrada en conflicto con otros intereses protegidos. En todo caso, los límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad". "La ley consagra la prevalencia del derecho subjetivo a obtener la información y correlativamente el deber de entregarla, salvo que concurran causas justificadas que limiten tal derecho, a las que se refiere el art. 14. Tales causas constituyen conceptos jurídicos indeterminados cuya relevancia y trascendencia deben ser concretadas en cada caso, ponderando los intereses en conflicto, como la norma indica, de tal modo que, frente a los actos típicamente discrecionales, (…).*

De acuerdo con el Criterio Interpretativo CI/002/20155, de 24 de junio, del Consejo de Transparencia, los límites a que se refiere el artículo 14 de la LTAIBG, y así 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, como resulta ser la SEGURIDAD NACIONAL, derivada de la protección de las infraestructuras críticas.

Por todo lo expuesto anteriormente, se deniega la solicitud de acceso a información requerida (instrucciones dadas por el Ministerio del Interior frente a posibles ciberataques a instituciones esenciales tras la invasión de Rusia a Ucrania, así como la relación de ciberataques detectados y neutralizados relativos a este ámbito), constituyéndose como causa de limitación del acceso a la información la SEGURIDAD NACIONAL, contemplada en el artículo 14.1.a) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Contra la presente Resolución, podrá interponerse con carácter potestativo, reclamación ante el Consejo de Transparencia y Buen Gobierno en el plazo de **UN MES**, desde el día siguiente al de la fecha de notificación de la misma, de conformidad con lo dispuesto en los artículos 23 y 24 de la Ley 19/2013, en concordancia con lo establecido en el artículo 112.2 de la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Una vez resuelta dicha reclamación, o de no hacer uso de la misma, podrá interponer, ante la Jurisdicción Contencioso-administrativa, **recurso contencioso-administrativo**, en el plazo de **DOS MESES**, desde el día siguiente a aquel en que se notifique la resolución expresa de la reclamación o en que éste deba entenderse presuntamente desestimada, y en el caso de no hacer uso de la misma, desde el día siguiente al de la notificación de esta resolución, con arreglo a lo dispuesto en los artículos 20.5 de la Ley 19/2013, y 25, 26, 45 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

Madrid, 18 de marzo de 2022.
El DIRECTOR GENERAL

José Antonio Rodríguez González

MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD