Madrid, 14 de noviembre de 2024

Ref.: Solicitud de acceso a información pública. Expediente 001-097056

Con fecha 24 de octubre de 2024, tuvo entrada en este Ministerio una solicitud de acceso a la información pública al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, formulada por a través del Portal de la Transparencia, que quedó registrada con el número de expediente 001-097056, donde se solicitaba la siguiente información:

> *«En el marco de un estudio con la Universidad de Valencia, solicito se me haga extensible la documentación disponible relativa a ciberseguridad, medidas empleadas por el ministerio, políticas en activo, estudios o cualesquiera documentos que puedan ser de utilidad.»*

Una vez analizada la solicitud, esta Unidad de Información y Transparencia resuelve **conceder parcialmente** la información solicitada.

En este sentido, consultados los Centros Directivos de este Departamento, se aporta la siguiente información:

a. La Dirección General de Política Interior indica que:

La información solicitada no puede ser proporcionada y ello con fundamento en motivos de seguridad (artículo 14 de la LTGB).

Para el correcto funcionamiento del sistema, todas aquellas infraestructuras involucradas en el proceso electoral son tratadas con la misma criticidad que las contenidas en el Catálogo Nacional de Infraestructuras Estratégicas, con la categoría de “críticas”.

La seguridad en el proceso electoral alcanza un punto crítico en la integridad, confiabilidad y disponibilidad de la información durante la fase de difusión de Resultados Provisionales en Procesos Electorales, lo que es trascendental para poder garantizar el efectivo ejercicio del derecho fundamental a la participación política y, con ello, su imbricación con la propia legitimidad democrática de los resultados.

Como consecuencia de todo ello, se incluyó un capítulo específico respecto a la seguridad de la información en los procesos electorales en la Orden INT/424/2019, de 10 de abril, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior y las directrices generales en materia de seguridad de la información para la difusión de resultados provisionales en procesos electorales.

Asimismo, el pliego de prescripciones técnicas del acuerdo marco para la contratación de los servicios necesarios para la obtención y difusión provisional de los datos del escrutinio de resultados de los procesos electorales y consultas populares, prevé expresamente que la ejecución de este servicio está sometida al Esquema Nacional de Seguridad (nivel alto), con intervención a través de las correspondientes auditorias, del Centro Criptológico Nacional.

Obviamente, ofrecer información pública sobre cualquier aspecto de la seguridad del proceso, del sistema, o de las infraestructuras del mismo puede comprometer gravemente la seguridad del proceso electoral, lo que a toda costa debe evitarse. Es la Administración la que, a través de las herramientas mencionadas, lleva a cabo el control oportuno.

b. Desde la Dirección General de Tráfico se informa:

"Con respecto a la solicitud formulada por el interesado, se le informa de que la Política de Seguridad de la Información, de la DGT, es publica y puede acceder a ella a través de la siguiente URL:

https://www.dgt.es/export/sites/web-DGT/.galleries/downloads/muevete-con-seguridad/normas-de-trafico/NOR-normativa-general/POL-0001-Politica-de-Seguridad-DGT-v3.0-003.pdf

El resto de información solicitada por el ciudadano que ejerce su derecho de acceso, tal y como dispone la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*, puede suponer un perjuicio muy grave hacia la propia Seguridad Nacional, Seguridad Pública, Secreto Profesional y/o Garantía de la Confidencialidad, excepciones recogidas hacia el propio derecho de acceso, tal y como se regula en el Artículo 14 de la citada Ley. Por lo que no da lugar al envío de la documentación solicitada por el interesado.

CSV :
DIRECCIÓN DE VALIDACIÓN :
FIRMANTE(1) : JUAN ANTONIO PUIGSERVER MARTÍNEZ | FECHA : 15/11/2024 09:16 | Sin acción específica

No obstante a lo anterior, se comunica que el Ministerio del Interior está bajo la aplicación del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*, así como de la *Ley 9/1968, de 5 de abril, sobre secretos oficiales,* y se le otorga el debido cumplimiento a dicha legislación."

c. La Secretaría General de Instituciones Penitenciarias indica que:

Se informa que en la Secretaría General de Instituciones Penitenciarias, desde 2019, se siguen las instrucciones que en materia de política de Seguridad Informática impulsa y fija el Ministerio del Interior para todos sus organismos vinculados.

d. Por último, desde la Secretaría de Estado de Seguridad se indica que:

El Boletín Oficial del Estado ha publicado en su Biblioteca Jurídica Digital el Código de Derecho de la Ciberseguridad, que puede consultarse y descargarse en el enlace:

https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codig

La presente edición del código electrónico es de fecha 3 de mayo de 2024 y contiene toda la normativa actualizada sobre la materia.

En el ámbito concreto del Ministerio del Interior, cabe destacar que el Real Decreto 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, asigna a la persona titular de la Secretaría de Estado de Seguridad, bajo la inmediata autoridad de la persona titular del Ministerio, la dirección y coordinación de las políticas de ciberseguridad en el ámbito de las competencias del Ministerio. En la misma norma también se dispone que la Dirección General de Coordinación y Estudios es el órgano de apoyo y asesoramiento encargado de auxiliar al titular de la Secretaría de Estado en su función como coordinador de las políticas de ciberseguridad encomendadas al Ministerio; correspondiéndole, entre otras, las siguientes funciones a través de la Oficina de Coordinación de Ciberseguridad (OCC):

Ejercer de punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información; ejercer como canal específico de comunicación entre los Centros de Respuesta a Incidentes

CSV :
DIRECCIÓN DE VALIDACIÓN :
FIRMANTE(1) : JUAN ANTONIO PUIGSERVER MARTÍNEZ | FECHA : 15/11/2024 09:16 | Sin acción específica

Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, así como constituirse en Centro de Respuesta a Incidentes Cibernéticos del Ministerio del Interior de apoyo a la Policía Judicial (CSIRT-MIRPJ), con la finalidad dar soporte técnico y coordinar a las unidades de investigación de la ciberdelincuencia de las Fuerzas y Cuerpos de Seguridad del Estado en los supuestos que se determinen. Asimismo, la OCC desempeñará las funciones que, conforme a lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, tiene asignadas la Secretaría de Estado de Seguridad como autoridad competente en materia de seguridad de las redes y sistemas de información para los operadores de servicios esenciales que sean, además, designados operadores críticos.

Constituirse como Observatorio de la Cibercriminalidad del Ministerio del Interior con el objeto de monitorizar y detectar tendencias para hacer frente a nuevos retos y amenazas en dicho ámbito, recopilar, procesar y analizar información sobre ciberseguridad, cibercriminalidad y campañas de desinformación, con la finalidad de elaborar productos de inteligencia.

Asimismo, en el año 2021 se aprobó el Plan Estratégico Contra La Cibercriminalidad (PECC) mediante la Instrucción 1/2021 del Secretario de Estado de Seguridad, que tiene como objetivo principal potenciar las capacidades del propio Ministerio para detectar, prevenir, proteger, responder y perseguir la cibercriminalidad, de modo que permita la convergencia entre los ámbitos cibernético y físico, generando un impulso operativo y técnico eficaz que garantice la protección de los derecho y libertades y la seguridad ciudadana.

Para finalizar, en el Portal Estadístico de Criminalidad, cuya implementación y actualización constituye una de las tareas encomendadas al Sistema Estadístico de Criminalidad (SEC), incardinado dentro del Área del Sistema Estadístico y Atención a Víctimas de la Dirección General de Coordinación y Estudios (Secretaría de Estado de Seguridad), se pueden realizar consultas sobre cibercriminalidad:

https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/

Dicho lo cual, mediante el presente no se puede facilitar información más precisa sobre medidas empleadas o políticas en materia de ciberseguridad por el Ministerio del Interior, pues la misma estaría incluida entre las causas de denegación previstas en el artículo 14.1 d) y e) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

CSV :
DIRECCIÓN DE VALIDACIÓN :
FIRMANTE(1) : JUAN ANTONIO PUIGSERVER MARTÍNEZ | FECHA : 15/11/2024 09:16 | Sin acción específica

Contra la presente resolución, que pone fin a la vía administrativa, podrá interponerse previa y potestativamente, reclamación ante el Consejo de Transparencia y Buen Gobierno en el plazo de un mes, o bien directamente recurso contencioso-administrativo ante la sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, en el plazo de dos meses; en ambos casos el plazo se contará desde el día siguiente al de notificación de la presente resolución.

EL SECRETARIO GENERAL TÉCNICO

Firmado electrónicamente

Juan Antonio Puigserver Martínez

CSV :
DIRECCIÓN DE VALIDACIÓN :
FIRMANTE(1) : JUAN ANTONIO PUIGSERVER MARTÍNEZ | FECHA : 15/11/2024 09:16 | Sin acción específica