

A LA MESA DEL CONGRESO DE LOS DIPUTADOS

Marcial Gómez Balsera y José Ignacio Prendes Prendes, Diputados del Grupo Parlamentario Ciudadanos, al amparo de lo dispuesto en los artículos 185 y siguientes del vigente Reglamento de la Cámara, presentan la siguiente pregunta, para la que se solicita al Ministro de Justicia **respuesta por escrito, sobre el Procedimiento de Declaración de Infracción de la Agencia Española de Protección de Datos contra la Subdirección General de Nuevas Tecnologías de la Justicia.**

En el Congreso de los Diputados, a 12 de abril de 2018.

EXPOSICIÓN DE MOTIVOS

Según el artículo 236 nonies de la Ley Orgánica del Poder Judicial, la Agencia Española de Protección de Datos conoce de los tratamientos de datos llevados a cabo con fines no jurisdiccionales. De acuerdo con dicha competencia, la Agencia Española de Protección de Datos ha determinado en su Procedimiento de Declaración de Infracción nº AP/00066/2017, a través de su Resolución R/00433/2018, que la Subdirección General de Nuevas Tecnologías de la Justicia, dependiente del Ministerio de Justicia, infringió lo dispuesto en el artículo 9.1 de la Ley Orgánica 15/1999, de Protección de Datos, en su labor de administración de la plataforma informática LexNET. Dicha infracción, además, está tipificada como grave en el artículo 44.3.h) de la misma ley orgánica.

Es preciso recordar que el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la administración de justicia, establece que LexNET es una plataforma de intercambio de información entre los órganos judiciales y operadores jurídicos que, en su trabajo diario, necesitan intercambiar documentos judiciales.

Pese a la función que dicha plataforma está llamada a desempeñar, el pasado 27 de julio se puso en evidencia un fallo de seguridad que permitía a usuarios visualizar documentos de terceras personas, accediendo a su bandeja de entrada privada y a los documentos de cada uno de los procesos judiciales que tenían en marcha.

En efecto, la versión LexNET 4.10.1.0, que tenía una brecha de seguridad, se había puesto en marcha el 20 de julio, se detuvo el 27 de julio al mediodía y fue sustituida por una nueva versión a las 16:25 horas. Por si fuera poco, este parche de seguridad no fue completamente efectivo y hasta la nueva versión del día siguiente no se detuvieron los accesos indebidos. Así, de conformidad con las noticias publicadas en diversos medios de tirada nacional, durante aquel periodo, la plataforma dejó al descubierto 11.000 documentos de la Justicia.

De ese modo, la Agencia Española de Protección de Datos considera que la Subdirección General de Nuevas Tecnologías de la Justicia incurrió en una infracción grave, al vulnerar los artículos 9 y 10 de la Ley Orgánica 15/1999 de Protección de Datos. Aunque esta resolución no conlleva ninguna sanción efectiva más allá de la publicación de este expediente, ello no conlleva a una exención de las responsabilidades políticas que este episodio han generado.

C.DIP 85139 17/04/2018 17:13

A estos efectos, la Subdirección General de Nuevas Tecnologías de la Justicia enunció en sus alegaciones hasta 58 medidas preventivas planificadas para garantizar la no repetición del incidente de seguridad.

Por lo anteriormente expuesto, se formulan al Ministro de Justicia las siguientes preguntas:

1. ¿Piensa su Ministerio recurrir esta resolución, o considera afortunada la tipificación como "grave" de la infracción, y que el gravísimo fallo de seguridad no pasara a mayores?
2. ¿Qué responsabilidades políticas van a asumirse por la conducta de la Subdirección General de Nuevas Tecnologías de la Justicia que la Agencia Española de Protección de Datos incardina en las letras d) y h) del artículo 44.3 de la Ley Orgánica de Protección de Datos?
3. ¿Se ha puesto ya en funcionamiento el Command Center, una de esas acciones planificadas para el futuro para centralizar el análisis de logs, la vigilancia de las aplicaciones en tiempo real y prevenir incidentes?
4. ¿Se ha suscrito ya el Convenio para desarrollar un SOC (Centro de Operaciones de Seguridad)?
5. ¿Se ha creado ya la Oficina de Gestión del Servicio?
6. ¿Qué medidas concretas se han adoptado para mejorar la calidad del código?
7. ¿Qué medidas concretas se han adoptado para la revisión de ejecución de comandos, la revisión de la gestión de la autenticación, el filtrado adecuado de datos, la revisión de los esquemas de autorización, la prevención de suplantación al usuario, la eliminación de la posibilidad de filtrado de datos sensibles, la actualización de los componentes de software, la mejora de la configuración de seguridad de los sistemas de información, la mejora de estrategias en detección de ataques y otros aspectos organizativos y legales?
8. ¿Contempla el Gobierno la posibilidad de aumentar la capacidad de 15GB a los usuarios del sistema, toda vez que resultan insuficientes a los usos actuales?


Marcial Gómez Balsera

Diputado del Grupo Parlamentario Ciudadanos


José Ignacio Prendes Prendes

Diputado Grupo Parlamentario Ciudadanos

Grupo Parlamentario Ciudadanos

Congreso de los Diputados

Carrera de San Jerónimo, s/n

28071 · Madrid · España