RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/16804 **07/09/2017** **46139**

AUTOR/A: GÓMEZ BALSERA, Marcial (GCS)

RESPUESTA:

El pasado 1 de septiembre de 2017 se produjeron diversos ciberataques de denegación del servicio desde servidores residenciados fuera de España contra la red de Telefónica, que es la prestataria de servicios de Internet. El objetivo del ataque era que el servicio de LexNET fuese inaccesible para los usuarios legítimos, intentando saturar el servicio para que los profesionales no pudiesen acceder al sistema.

Ya se encuentran implementadas todas las medidas de seguridad exigibles por la normativa vigente, el Esquema Nacional de Seguridad, así como las establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal, Ptales como:

- El cifrado de las comunicaciones.
- El proceso de copias de seguridad de la información. Ubicación de las mismas en dos Centros de Procesos de Datos diferentes.
- El control de acceso lógico a la aplicación y físico a las instalaciones del Centro de Proceso de Datos donde están ubicados los ficheros.
- El procedimiento de gestión de incidencias.

No obstante lo anterior, en el marco de mejora continua, el Ministerio de Justicia viene impulsando distintas medidas para reforzar el mantenimiento y la mejora de las medidas de seguridad.

Entre las actuaciones que se han llevado a cabo desde el año 2016 para reforzar la seguridad, cabe destacar la puesta en marcha de una oficina de seguridad informática y reforzar la seguridad de las comunicaciones ante posibles intrusiones.

Durante el año 2017, se continúan impulsando los servicios de consultoría especializada en seguridad y la adquisición de electrónica de red que supone un incremento de la seguridad, fundamentalmente en programas informáticos que controlan el acceso de los equipos conectados a la red.

Para garantizar que, aunque se produzcan incidencias, no se pierda información judicial, ni esta sea accedida ni alterada por quien no tenga ese derecho, se han implementado importantes mejoras en las infraestructuras tecnológicas, como:

- ✓ La coexistencia de dos centros de procesos de datos para dar soporte a la Administración de Justicia, entre los cuales se replica la información judicial y se mejora la respuesta ante posibles ataques o incidentes de seguridad.

- ✓ La integración de documentos judiciales en un Centro de Proceso de Datos. El procedimiento de almacenamiento de larga duración de la documentación judicial garantiza la conservación de la información, así como la disponibilidad inmediata de la misma en caso de pérdida.

- ✓ Solución Antivirus en Servidores y en ordenadores de los Órganos Judiciales, Fiscalías, Instituto Nacional de Toxicología y Ciencias Forenses, etc. de forma que se evite que se introduzcan en el sistema ficheros infectados por virus informáticos.

- ✓ Solución de Securización de la Infraestructura ("bastionado"), sistema que protege a los puestos de trabajo y sus accesos hacia el servidor.

- ✓ Se dispone de una Sonda de Alerta Temprana del Centro Criptológico Nacional (dependiente del Centro Nacional de Inteligencia-CNI) instalada en la conexión de Internet, que permite identificar incidentes de seguridad reportados por la herramienta y disparar las actuaciones de mitigación o remediación que sean necesarias. La mayoría de incidentes que se detectan mediante esta sonda son producidos por código dañino e intentos de intrusión.

Adicionalmente, existe una estrategia de coordinación a nivel interministerial para hacer frente a los posibles ataques a los servicios informáticos del Estado. Por ello, el Ministerio de Justicia tiene un protocolo de comunicación con el CCN-CNI (Centro Criptológico Nacional del Centro Nacional de Inteligencia), a través del cual éste informa al Ministerio de cualquier peligro y amenaza existente, con objeto de poder tomar las medidas preventivas pertinentes. Este protocolo de comunicación es bidireccional, de manera que en caso de que el Ministerio de Justicia detecte cualquier anomalía de seguridad que pueda suponer un riesgo o ataque, se avisa al CNI con el objetivo de obtener información adicional y pautas de seguridad recomendadas.

Para concluir, se indica que, aunque la seguridad absoluta no existe, desde el Ministerio de Justicia se han realizado esfuerzos en proteger convenientemente la información y los sistemas desde el punto de vista técnico, organizativo y normativo, y se han reforzado los

mecanismos de control existentes para la prevención, detección y respuesta ante cualquier incidente de seguridad.

El problema del 1 de septiembre no fue un fallo de LexNET, sino un ataque a la red que da servicio a esta aplicación, red gestionada por Telefónica. Tan pronto como se identificó el problema, se dio indicación a Telefónica para que lo mitigara.

Respecto a las notificaciones durante el mes de septiembre, cabe señalar que se ha habilitado un control programado para la práctica de los actos de comunicación, en los términos expresados en el artículo 16.4 del Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET. A este fin, se ha establecido una cuota para cada órgano judicial, tomando como referencia la media de notificaciones diaria de cada uno de los órganos, efectuadas entre el 1 de enero de 2017 y el 31 de julio (días naturales). Se han excluido de la cuota las notificaciones urgentes, las cuales se pueden practicar sin ningún tipo de limitación.

Madrid, 14 de noviembre de 2017