RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/16710, 184/16711 **04/09/2017, 04/09/2017** **45885, 45886**

AUTOR/A: CIURÓ I BULDÓ, Lourdes (GMX)

RESPUESTA:

El Gobierno no está valorando suspender la implementación de Lexnet.

LexNET comenzó a implantarse en los Juzgados y Tribunales en el año 2004. Desde entonces ha ido creciendo y desarrollándose de forma constante para adaptarse a las nuevas necesidades y entornos tecnológicos. En este sentido, se han realizado nuevos desarrollos en los sistemas y servicios de interoperabilidad para adaptarse a la normativa vigente, así como para facilitar la integración de los distintos profesionales, organismos y colectivos que se relacionen con la Justicia.

No se aprecian argumentos que justifiquen plantearse una suspensión de este sistema. LexNET es el sistema de gestión de comunicaciones electrónicas más extendido en la Administración de Justicia de España, ya que se usa en todo el territorio nacional, a excepción de las Comunidades Autónomas de Cantabria, Navarra y País Vasco. Es un sistema consolidado y seguro, de eficacia probada que se ha convertido en una herramienta de trabajo habitual como revelan los datos de uso. Proporciona cobertura a más de 230.000 usuarios y desde su puesta en funcionamiento ha intercambiado más de 330 millones de actos de comunicación.

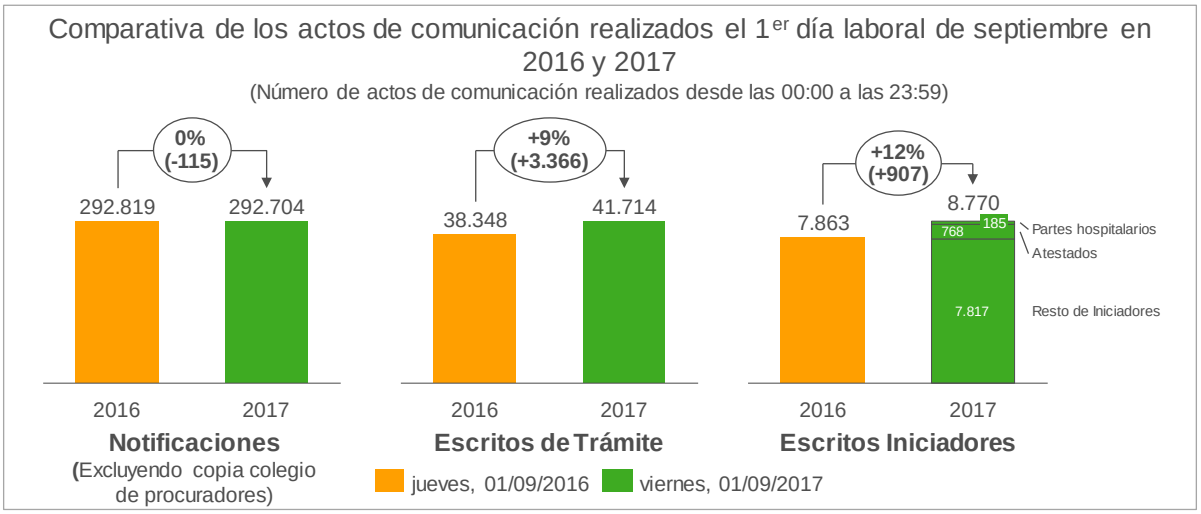
Entre el 1 de enero de 2016 y el 31 de julio de 2017 la disponibilidad del servicio de LexNET fue de un 98,2% (1% por paradas planificadas para la realización de trabajos de mantenimiento y el 0,8% por incidencias). En 2016, desde LexNET se realizaron 60.710.715 notificaciones, 1.378.652 escritos iniciadores (177 atestados, 104 partes hospitalarios y 1.378.371 resto de iniciadores) y 7.151.890 escritos de trámite.

Desde el pasado 1 de enero desde LexNET se han realizado 46.543.898 notificaciones, 1.278.921 escritos iniciadores (126.898 atestados, 28.488 partes hospitalarios y 1.123.535 resto de escritos iniciadores) y 6.509.711 escritos de trámite.

En cuanto a la incidencia del pasado 1 de septiembre a la que hace referencia Su Señoría, cabe señalar que, ésta no se produjo por un problema interno de la aplicación. Es decir, no falló LexNET, lo que se produjo fue una cadena de ciberataques dirigido a la red de

Telefónica que da acceso a LexNET. Estos ataques fueron del tipo "denegación del servicio" consistente en inundar la red a través de la cual cualquier usuario accede al sistema. Los atacantes tenían por objetivo impedir que los usuarios de LexNET pudieran acceder con normalidad al sistema. Fueron conscientes y deliberados y pretendían alterar el normal funcionamiento de la Administración de Justicia en un día tan señalado como el 1 de septiembre, con el único propósito de trasladar a la opinión pública que se trataba de un fallo en LexNET cuando realmente no era así. Se recibieron un total de 5 ataques de forma discontinua entre las 10:45 y las 14:40 horas.

A pesar de la degradación del servicio, en los gráficos puede verse que el uso en los órganos judiciales es igual al del año anterior, mientras que el uso de los profesionales ha sido algo superior que en la primera jornada de septiembre el año 2016.



Los ataques no afectaron a la seguridad del sistema. El sistema LexNET es seguro y fiable. El acceso a la información por parte de los usuarios legítimos de LexNET, dados de alta en el sistema, se realiza a través de un certificado digital cualificado y válido, de conformidad con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica y en el Reglamento UE Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. Esto redunda en que el acceso y la tentativa de acceder a la información de otro usuario mediante la utilización de herramientas o explotando las posibles vulnerabilidades del sistema constituya un delito.

Sólo los usuarios con acceso a aplicación, es decir, previamente registrados, validados y autenticados, pueden acceder a información de usuarios, mensajes y resguardos, en función de su perfil.

La aplicación genera información de auditoría donde se puede controlar la trazabilidad de un mensaje.

Asimismo, se han implementado las medidas de seguridad exigidas 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, tales como:

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

En el marco de mejora continua, el Ministerio de Justicia viene impulsando distintas actuaciones para reforzar el mantenimiento y la mejora de las medidas de seguridad.

Entre estas, destaca la puesta en marcha de una Oficina de Seguridad Informática y una mayor seguridad de las comunicaciones ante posibles intrusiones.

Durante 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, y que esta no sea accesible ni pueda ser alterada por quien no tenga ese derecho, se han implementado importantes mejoras en las infraestructuras tecnológicas como:

1. 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.
2. La centralización de las Bases de Datos de los servidores y la realización de copias de seguridad de manera centralizada.
3. El almacenamiento 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.
4. La implantación de la solución de Directorio Activo Centralizado de usuarios.
5. 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.
6. Solución de Securización de la Infraestructura (“bastionado”), sistema que protege a los puestos de trabajo y sus accesos hacia el servidor.
7. 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.

Por otra parte, cabe señalar que desde el punto de vista organizativo, para el supuesto de detectarse cualquier alerta o incidente de seguridad, se ha definido un Protocolo de Emergencia con las actuaciones de diagnóstico, preventivas, correctivas y de comunicación a realizar.

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.

Madrid, 10 de octubre de 2017