SOLICITUD DE HABILITACIÓN PUERTOS USB.

Una vez leída la notificación rellene y firme el formulario de la página 5, enviándola por FAX al CSU-CEIURIS.

NOTIFICACIÓN SOBRE AUTORIZACIÓN DE HABILITACIÓN DE PUERTOS USB

Atendiendo a esta solicitud debe saber que se autorizará, en virtud del 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, del que puede encontrar versión electrónica en http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf, la habilitación para el/la/los/las usuario/a/s indicado/a/s de los puertos USB en cuanto a la conexión de dispositivos de almacenamiento masivo (PENDRIVES).

La autorización será otorgada tomando como base el artículo 92.2 del R.D. 1720/2007, ya que usted, **como responsable del fichero de datos de carácter personal** declarado mediante pleno del Consejo General del Poder Judicial, de creación de ficheros de carácter personal dependientes de los órganos judiciales y publicado en Boletín Oficial del Estado 244/2006, de 12 de octubre (http://www.boe.es/boe/dias/2006/10/12/pdfs/A35360-35362.pdf), autorizará expresamente la salida de los soportes digitales que constituyen los pen-drives USB. La redacción de dicho artículo es la que sigue:

> *"2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad."*

Pero además, al ser los datos objeto de tratamiento una vez han abandonado el local del responsable del fichero, es necesario hacer hincapié en el artículo 86.1:

> *"Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*
> *1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.*
> *2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas."*

Los términos en los que se autoriza dicha habilitación son los siguientes:

Debido a la obligación de garantizar que el nivel de seguridad correspondiente al fichero tratado

una vez abandonen los datos el local del responsable del fichero es el mismo que el existente en dicho local, es necesario que el/la usuario/a autorizado acepte expresamente dicha responsabilidad, aceptación que se entiende realizada al haber realizado la solicitud. Además, deberá comprometerse a notificar a este Servicio de Informática Judicial cualquier incidente relacionado con dicho soporte: pérdida, robo, cualquier sospecha de que haya sido utilizado y/o consultado sin su consentimiento, infecciones detectadas notificadas por el software antivirus corporativo, etc.

Así mismo, se recuerda que según RESOLUCIÓN de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía, que establece lo siguiente en su artículo 4.4:

> *"4.4. Los usuarios no tienen permitido conectar a los equipos informáticos que se les provea, otros equipos distintos de los que tengan instalados."*

Además, en el ámbito de la Administración de Justicia, tenemos la *INSTRUCCIÓN 2/2003, de 26 de febrero, del Pleno del Consejo General del Poder Judicial, sobre Código de Conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia*, que en el artículo 5.2 nos dice lo siguiente:

> *"5.2 No está permitido alterar cualquier parte de los equipos informáticos ni conectar otros (asistentes personales, impresoras, reconocedores de voz, etc.) a iniciativa del usuario, sin contar con la autorización expresa del Servicio de Soporte competente."*

Debido a estos dos artículos citados, **las personas usuarias no están autorizadas a conectar a los equipos** proporcionados por la Junta de Andalucía **otros equipos** como discos duros, pen-drives, cámaras, etc. a través de puertos USB, **mientras no sean proporcionados por esta Administración**.

En la citada instrucción del C.G.P.J. se define sobre quiénes resulta de aplicación dicha normativa, en su artículo 4.1:

> *"4.1 Las pautas de comportamiento incluidas en el presente Código serán de aplicación a todos los usuarios, sin perjuicio de las normas reguladoras de su respectivo Estatuto jurídico; resultando igualmente aplicables a todas las comunicaciones realizadas a través de la red interna o Intranet, o de la red externa o Internet que en su caso se hubiera puesto a disposición de los usuarios."*

Considerando las definiciones siguientes:

> *"Definiciones.—A los efectos del presente Código de Conducta se considerará:*
> *Usuario: A todos los profesionales que prestan sus servicios en los órganos judiciales. A efectos de las presentes normas, los Jueces, Magistrados, Secretarios Judiciales, funcionarios, personal laboral, Médicos Forenses, Contratados, etc., son usuarios de equipos informáticos, por lo que en el presente Código de Conducta la denominación se hace en el sentido más amplio posible siempre que desarrollen tareas, permanentes u*

ocasionales, en los órganos judiciales.
Administración/es Pública/s: A las distintas Administraciones con competencia sobre medios materiales y humanos al servicio de la Administración de Justicia; esto es, el Ministerio de Justicia y, en su caso, las Comunidades Autónomas. La Administración Pública competente constituye el Servicio de Soporte."

No obstante, el citado Real Decreto y la citada Ley Orgánica nos obligan a informar sobre las circunstancias y los riesgos a los que se expone la información contenida en el fichero de datos de carácter personal del que es usted responsable, siendo el primero la obligación de controlar qué soportes son los que abandonan en cada momento las instalaciones donde se encuentra el fichero de datos de carácter personal; adoptar las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte, etc. Medidas que están reguladas en los art. 92, 97 y 101 del R.D; llegando a exigir, para los ficheros de datos de carácter personal de Nivel Alto las medidas, en el art. 101:

"Artículo 101. Gestión y distribución de soportes.
1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.
3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos."

Hemos de informarle, además sobre el peligro existente, debido a que que una vez el soporte (pen-drive USB, disco duro USB, etc) abandone el local del responsable del fichero, se pierde el control sobre el uso de éste:

- Cuántas veces se copia o retransmite la información.
- La vigencia de dicha información transmitida o copiada, es decir, durante cuánto tiempo estará dicha información almacenada en los lugares de destino.
- Los destinatarios de dicha copia o retransmisión de la información.
- La protección de los datos frente a accesos no autorizados ante pérdidas o robo del dispositivo físico.
- Si se conecta el dispositivo USB a un equipo infectado por virus, gusanos, troyanos, etc. -que denominaremos a partir de ahora "malware"- y resulta, por lo tanto infectado a su vez.

A todo el desarrollo normativo hay que incluir consideraciones de seguridad. El uso de los puertos USB, así como los DVD ROM y/o CD ROM supone, además de una puerta de salida de

información, una puerta de entrada de ésta a la Red Judicial.

Uno de los principales problemas que dicha entrada de información supone es la infección por virus informático. Es de conocimiento de todos que la infección por "malware" es noticia frecuente en los diversos medios de comunicación. Sin ir más lejos, en la Red Judicial ya se ha sufrido alguna que otra infección, con diversos efectos negativos, tanto en propagación como en daños a los equipos y/o la información contenida en éstos. Hay que decir que en la mayoría de las ocasiones la puerta de entrada de dichas infecciones han sido los dispositivos USB de los equipos que los tenían habilitados.

Las casas antivirus reconocen que es prácticamente imposible estar protegido de las últimas amenazas en todo momento, y que los antivirus no son capaces de reconocer las amenazas a medida que se van creando los malware. Esto se traduce en que las infecciones ocurren incluso antes de que se detecten los malware; en los conocidos 0-day, que son vulnerabilidades en los sistemas que han sido explotadas por los atacantes (fabricantes de malware) mucho tiempo antes de ser descubiertas por las casas antivirus ni por los desarrolladores de software como Microsoft, y que no es posible saber a ciencia cierta desde cuándo pueden haber estado funcionando. Por lo tanto, aunque se fuerce un escaneo exhaustivo de cada dispositivo que se conecte justo en el momento de conectarlo, es posible que se produzcan infecciones víricas, ya que una vez que se permita la salida de los dispositivos USB, escapa a nuestro control el uso exacto que se haga de ellos, así como la seguridad de equipos a los que se conecte.

SOLICITUD DE HABILITACIÓN PUERTOS USB.

Datos del secretario judicial.

Apellidos:

Nombre:

Órgano Judicial:

Teléfono contacto:

correo-@ contacto:

Datos de la petición.

Petición Nº

Habilitación puertos USB para el/los usuario/s:

Observación /Motivo:

FIRMA DEL SR /A. SECRETARIO JUDICIAL	SELLO DEL ÓRGANO
Fdo. D./Dª.:	

Nota:

La firma de esta sulicitud implica el conocimiento de la notificación descrita en las páginas iniciales.

La solicitud siempre debe ser firmada por el secretario judicial y enviada al FAX 955625412.

No se aceptarán aquellas solicitudes que no estén debidamente cumplimentadas.

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, se le informa que los datos personales obtenidos mediante la cumplimentación de este formulario van a ser incorporados para su tratamiento en un fichero automatizado. Asimismo, se le informa que la recogida y tratamiento de dichos datos tienen como finalidad proporcionar los servicios de acceso a aplicaciones y sistemas informáticos de la Red Judicial de Andalucía. Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición, previstos por la Ley, dirigiendo un escrito al Servicio de Informática de la Secretaría General para la Justicia.