Utilización de portátiles

Introducción.

Los equipos portátiles de la Universitat Jaume I de Castellón (UJI, en adelante) son utilizados por el personal de la universidad con objeto de facilitar el correcto desempeño de sus tareas. Tales sistemas, a pesar de ser imprescindibles para facilitar el desempeño de labores académicas, investigadoras y de gestión de la UJI en cualquier lugar, introducen importantes riesgos que deben ser gestionados para garantizar la seguridad de los sistemas de información corporativos.

Desarrollo

1. Uso de ordenadores portátiles

No se permite la manipulación de los ordenadores portátiles administrados por el SI de la UJI ni la instalación de componentes software o modificación de las configuraciones ya realizadas por parte de personas ajenas al Servicio de Informática; estas modificaciones pueden comprometer la integridad del propio equipo y, por extensión, la de todos los sistemas de la organización.

Los portátiles ofrecidos por la biblioteca en régimen de préstamo poseen una normativa específica disponible en http://www.uji.es/cd/cas/portatiles/.

2. Gestión de la información

Toda la información almacenada en un equipo portátil es responsabilidad del usuario que deberá realizar las pertinentes copias de seguridad.

En los equipos portátiles de la UJI no debe almacenarse más información perteneciente a la institución que la estrictamente necesaria para el desarrollo correcto de las tareas del usuario dentro de la organización; toda información corporativa que no se utilice con este fin debe ser borrada del sistema.

3. Conexión a redes

Debe minimizarse la conexión a redes ajenas a la UJI a aquellos casos estrictamente necesarios para ejecutar las tareas propias del usuario del equipo en la organización; la conexión a redes no confiables, incluida Internet, pone en peligro la seguridad del equipo y por extensión la de la organización al completo. Ante una conexión no fiable, en la medida de lo posible, el usuario deberá asociarse a la VPN de la UJI estableciendo así un canal cifrado.

Son necesarias todas las precauciones en especial frente a virus y otro software malicioso al utilizar un equipo portátil de la organización; aunque todos ellos llevan

instalado un sistema antivirus capaz de detectar y bloquear la mayor parte del software dañino, es imposible garantizar este extremo en su totalidad. La conexión a redes no confiables puede favorecer la infección del equipo portátil, ya que se deja su protección casi exclusivamente a merced del antivirus instalado en el propio equipo; si durante la utilización de un portátil de la UJI se sospecha de la infección por virus u otro software malicioso, es necesario dejar de procesar la información, apagar el equipo y comunicarlo al CAU o a la entidad que lo ha proporcionado a la mayor brevedad posible.

4. Transporte de los equipos

No se debe someter al equipo a condiciones climáticas extremas que puedan dañar sus componentes o impedir el acceso a la información almacenada.

Si se transporta el equipo en un automóvil, este no debe estar a la vista ni ser fácilmente accesible; es importante no dejar el equipo sólo en el automóvil en ninguna situación.

En caso de robo o pérdida del equipo, este hecho debe notificarse al CAU a la mayor brevedad posible, indicando cualquier dato que pueda ser relevante para la recuperación del mismo (lugar, fecha, hora, etc.).

Si en el equipo se almacenan datos confidenciales o especialmente protegidos por el Real Decreto 1720/2007, éstos deberán ser debidamente protegidos mediante el uso de herramientas de cifrado de archivos o particiones.

5. Responsabilidades

Es responsabilidad única del usuario del equipo portátil el garantizar la seguridad tanto del equipo en sí como de la información que contiene, cumpliendo la presente normativa y todas las relativas a la seguridad de los sistemas de información de la UJI, y en especial, es obligación del usuario la notificación de cualquier incidente relacionado con la seguridad del equipo o de la información a través del SPI “Notificació d’incidències de seguretat”.