Universitat d'Alacant
Universidad de Alicante

Servicio de Informática

PROTECCIÓN DEL PUESTO DE TRABAJO INFORMÁTICO

Versión 1

1.- Objeto

El objeto del presente documento es enumerar una serie de recomendaciones que permitirán utilizar los equipos informáticos personales con mayor seguridad.

Los ordenadores personales utilizados como puestos de trabajo son administrados directamente por los usuarios responsables de los mismos. Dichos equipos pueden contener información corporativa y acceder, en algunos casos, a los Sistemas de Información corporativos: deberán, por tanto, estar sujetos a estrictos controles de seguridad y contar con las medidas de protección descritas en este documento.

La Universidad de Alicante facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la Universidad de Alicante pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales.

En general, el ordenador personal será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos de la Universidad de Alicante, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

2.- Ámbito de aplicación

Estas recomendaciones son de aplicación a todo el ámbito de actuación de la Universidad de Alicante, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad de la misma.

3.- Revisión y evaluación

La gestión de estas recomendaciones corresponde al Comisión TI, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.

-Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comisión TI revisará las presentes recomendaciones.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento

4.- Protección del puesto de trabajo informático

4.1- Responsabilidades

- El usuario es responsable de mantener los elementos de seguridad operativos, las aplicaciones instaladas en el equipo y el estado y uso del mismo.
- La salvaguarda y confidencialidad de los datos del ordenador corporativo son responsabilidad del usuario.
- Los ordenadores personales deben utilizarse únicamente para fines institucionales.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CD/DVD, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
- El usuario será responsable de toda la información que extraiga fuera de la organización a través de dispositivos tales como memorias USB, CD, DVD... Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.

4.2- Almacenamiento de información

- Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.
- La Universidad puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso limitado y

compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos.

4.3- Buenas prácticas

- Establezca una contraseña de inicio de sesión. La contraseña debe ser robusta. No guarde las contraseñas en un lugar accesible.
- Evite que el equipo contenga claves de acceso almacenadas capaces de habilitar el acceso a las aplicaciones corporativas.
- Si el ordenador contiene información de los sistemas corporativos, datos personales o información confidencial, cifre los ficheros que la contienen. No olvide realizar procedimientos de borrado seguro para eliminar la información sin cifrar.
- Valore la conveniencia de utilizar sistemas de archivos cifrados.
- Instale y mantenga actualizado el antivirus corporativo.
- No instale software descargado de repositorios no oficiales.
- No utilice software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.
- Configure bloqueo del sistema operativo de forma automática, para que se active cuando transcurra un periodo de inactividad en el ordenador (15 minutos).
- Active de forma manual el bloqueo del sistema operativo si se ausenta de su puesto de trabajo.

4.4- Buenas prácticas adicionales para equipos portátiles.

- Para evitar substracciones considere las siguientes medidas no técnicas:
    - Elija un maletín de transporte discreto.
    - Mantenga el portátil al alcance de la mano.
    - Etiquete el portátil y todos los accesorios.
    - Utilice cables de seguridad Kesington cuando mantenga el equipo en una ubicación durante un periodo largo de tiempo.
- Active o instale un sistema de protección perimetral (cortafuegos/firewall) en el equipo que minimice la visibilidad exterior.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la Universidad para la adopción de las medidas que correspondan y a efectos de baja en el inventario.

4.5- Uso eficiente de equipos y recursos informáticos.

- Apague el PC (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
- Imprima únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color.
- Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.