

Claves para controlar y gestionar los equipos informáticos en los establecimientos sanitarios de óptica

Mantener un buen control de los dispositivos informáticos de la óptica resulta esencial para la optimización y eficacia del trabajo diario, pero también garantiza la seguridad de todos los datos, tanto de clientes y proveedores como los datos contables y económicos de la compañía. Deberemos instar al personal de la óptica para que organice bien el sistema de forma que se pueda trabajar sobre servidores de ficheros y servidores de aplicaciones, manteniendo así los datos a salvo de errores o manipulaciones.

En la actualidad, la mayoría de establecimientos sanitarios de óptica, ya sean grandes o pequeños, necesitan utilizar equipos informáticos para poder llevar a cabo su actividad diaria y su control económico, así como para realizar las tareas básicas de gestión empresarial, como la facturación, la contabilidad, las campañas de marketing digital o una adecuada atención al cliente, así como una completa base de datos. Cuanto mayor es el número de trabajadores de la empresa, mayor es la inversión que hay que realizar en ordenadores, *tablets*, impresoras y *software* de todo tipo, y más importante es alargar la vida útil de los equipos informáticos para poder amortizar la inversión realizada. Hasta hace poco tiempo, un ordenador se quedaba obsoleto en unos dos o tres años, pues las mejoras tecnológicas en los equipos se sucedían a un ritmo vertiginoso, y los re-

querimientos de las nuevas versiones de programas informáticos hacían imposible extender la vida de los equipos. Sin embargo, esta tendencia ha cambiado bastante en los últimos años, y excepto en el caso de los ordenadores que se utilizan para aplicaciones de máxima exigencia, ya es posible disfrutar de parques informáticos con cinco o más años de antigüedad que permiten trabajar a pleno rendimiento, con el consiguiente ahorro de costes que ello implica.

Consejos prácticos para sacar el máximo partido

Para alargar al máximo la vida de los ordenadores de una óptica es importante asegurarnos de que tanto las acciones de los empleados en el día a día como las decisiones estratégicas de gestión deben estar alineadas con una serie de buenas prácticas que contribuyan a conseguir este objetivo.



MANTENIMIENTO INFORMÁTICO CORRECTO

Dentro de las tareas de mantenimiento informático preventivo se pueden destacar las siguientes:

- Utilizar *software* que se encargue de eliminar archivos innecesarios, temporales y duplicados.
- Desinstalar aplicaciones que ya no son útiles.
- Borrar historiales de navegación y *cookies*.
- Instalar actualizaciones del sistema operativo y de otras aplicaciones clave para la óptica.
- Realizar copias de seguridad de todos los datos, archivos, historial de cada cliente y base de datos en la nube.

- Instalar antivirus, cortafuegos, *software* anti-espía y otras medidas de ciberseguridad para evitar ataques de *hackers* (que cada día hay más).
- Llevar a cabo la limpieza y realizar revisiones periódicas de los componentes de los equipos informáticos.
- Algunas de estas tareas son muy sencillas de llevar a cabo, y las pueden realizar los miembros del equipo de trabajo. Otras son acciones más avanzadas, para las que es recomendable contratar apoyo técnico de forma puntual, con el fin de evitar que se pierdan datos importantes o que se produzcan daños en los equipos informáticos durante su manipulación.



Para ello, resulta imprescindible utilizar los equipos con los cuidados básicos que merecen, ya que eso alargará su vida útil. Eso se traduce en que sean utilizados con cuidado, siguiendo recomendaciones como, por ejemplo:

- Evitar altas temperaturas, proporcionando buena ventilación a los ordenadores. Nunca hay que dejarlos expuestos al sol y siempre hay que apagarlos cuando no estén en uso.
- Mantener un entorno de trabajo limpio para evitar el exceso de polvo y suciedad en el interior de los equipos informáticos.
- Evitar los golpes y movimientos bruscos de los ordenadores, especialmente si se trata de portátiles, pues son más delicados que los ordenadores de escritorio.
- Procurar que el cableado de la oficina esté ordenado para evitar que se desenchufen los equipos por error.
- Evitar dejar los ordenadores encendidos 24h/día, ya que esto puede desgastar el ventilador, la fuente de alimentación o el propio disco duro de los equipos.
- No dejar líquidos, bebidas o café cerca de los ordenadores portátiles, pues existe una alta probabilidad de que acaben derramándose y estropeando los circuitos eléctricos internos.
- Realizar tareas preventivas de mantenimiento informático. Un buen mantenimiento preventivo es fundamental para la correcta gestión de los equipos informáticos, pues permite prevenir la ocurrencia de fallos informáticos y problemas de todo tipo.

Claves para agilizar los equipos informáticos

Es posible que algunos equipos informáticos no funcionen correctamente por culpa de un mal manteni-

miento informático. Por eso, resulta imprescindible asegurarse de ciertas cuestiones sencillas que son muy importantes:

- **Revisar si el disco duro está lleno.** Si el disco duro del ordenador de la óptica está completo, lo habitual es que todo el equipo funcione de forma **más lenta**. Para resolverlo hay que hacer una limpieza. Es importante desinstalar todos los programas que no se utilizan o traspasar la información a un disco duro externo.
- **La memoria RAM es antigua.** En ocasiones, puede ocurrir que la memoria RAM sea antigua y no sea capaz de soportar sistemas nuevos. Si existen aplicaciones instaladas en el ordenador esto puede dar problemas, de ahí que lo más recomendable sea optar por servicios informáticos en la nube.
- **Fallos de seguridad.** La lentitud de un ordenador también puede deberse a que haya entrado algún virus que ralentice su funcionamiento. Para resolverlo, hay que asegurarse de contar con un buen programa antivirus actualizado y no desactivarlo nunca.

Seguridad con éxito

En ocasiones, mantener a buen recaudo la seguridad informática de la óptica se convierte en un problema de primer orden por falta de conocimiento de los riesgos a los que se está expuesto. Por un lado, se pueden recibir ataques de seguridad, pero también pueden darse casos de pérdida de datos motivadas por falta de previsión o fallos estratégicos. En cualquier caso, ser precavidos y contar con las herramientas necesarias se convierte en el mejor camino a seguir.

Así, para cuidar la seguridad informática de la óptica es posible delegar estas funciones a una empresa de informática especializada para que, al menos en un par de ocasiones al año, revise todos los

PARA CUIDAR LA SEGURIDAD INFORMÁTICA DE LA ÓPTICA ES POSIBLE DELEGAR ESTAS FUNCIONES A UNA EMPRESA DE INFORMÁTICA ESPECIALIZADA QUE REVISE TODOS LOS SISTEMAS



sistemas y garantice que los protocolos de seguridad estén funcionando correctamente. En cualquier caso, también existen algunos consejos muy sencillos y que deben realizarse de forma rutinaria para evitar riesgos añadidos:

- **Usar contraseñas en todos los ordenadores.** Un aspecto fundamental es el de evitar los accesos no autorizados desde dentro de la óptica. De este modo, cada empleado debe tener permisos para acceder a determinadas áreas, pero no tienen por qué tener acceso a todo, lo que garantiza mayor seguridad. En este sentido, proteger cada ordenador con contraseñas personales evitará que cualquiera pueda conectarse a los equipos sin permiso.

- **Mantener los equipos actualizados.** Los sistemas operativos antiguos son altamente vulnerables a los virus informáticos. Por eso resulta imprescindible mantener los ordenadores actualizados periódicamente. En este caso, lo más aconsejable es dejar esta parte a técnicos especializados en informática y concienciar a los profesionales de la óptica de la necesidad de cumplir con las alertas de actualización que indica cada dispositivo.

- **Realizar copias de seguridad periódicas.** Aunque nunca se haya sufrido una pérdida de datos importante o ningún dispositivo haya perdido su información, lo cierto es que estas cosas ocurren y, casi siempre, en el momento más inoportuno. Por ello, merece la pena realizar copias de seguridad periódicas para que sea posible restaurar los datos en caso de pérdida de información. En este sentido, lo mejor es optar por la nube o servidores encriptados.

- **Instalar un buen sistema de antivirus.** Aunque ningún antivirus resulta infalible, pueden proteger el sistema de algunos virus informáticos. Lo ideal es disponer de un sistema antivirus y un *firewall*, además de una herramienta *anti-spyware* que ayude a la óptica a mantener la privacidad de la información.

- **Mantener los datos en red.** Cuando disponemos de una red informática en la óptica, todos los ordenadores pueden compartir datos. Pero a su vez estos equipos pueden estar conectados a un servidor, para

el que se conectan a la hora de usar determinados programas o para guardar archivos. De esta manera, no hay por qué guardar los archivos en cada ordenador de cada empleado, sino que puede guardarlos en una unidad de servidor.

- **Formar a los empleados.** Los profesionales de la óptica que utilizan los equipos informáticos deben estar preparados para prevenir problemas de seguridad *online*. Por ello, es recomendable formar a los empleados para actuar ante determinadas situaciones como ataques de *phishing* o *malware*. La primera de ellas se trata de suplantaciones de identidad para el robo de datos. Ciberdelincuentes que crean una web que simula ser de un banco, una empresa, un proveedor, una institución pública, etcétera. En segundo lugar, el *malware* hace referencia a personas que te envían enlaces a través de las redes sociales o adjuntos por correo electrónico, pero que en realidad son algún tipo de *malware*.

- **Crear un protocolo de seguridad sencillo.** Las empresas deben contar con un protocolo de seguridad para saber cómo actuar en cada situación. Así los empleados podrán saber dónde deben guardar sus datos o qué deben hacer en caso de cualquier incidencia.

- **Proteger los datos externos.** La movilidad es una realidad en la óptica, ya que se pueden utilizar ordenadores de sobremesa, pero cada vez más se emplean portátiles, *tablets* y teléfonos móviles de la empresa compañía para mantenerse en contacto con los clientes. Estos dispositivos deben seguir también un protocolo de seguridad. Los usuarios que los utilicen deberían poder conectarse a una intranet para poder acceder a cualquier información.

Además, existen formas de seguridad muy exigentes que permiten, por ejemplo, el uso de móviles por reconocimiento facial, lo que permite que ninguna persona ajena a la empresa pueda ser autorizada a usarlo, aunque también hay otras alternativas más factibles como la vinculación de los dispositivos a un teléfono móvil al que se le envía una clave de seguridad, garantizando así su protección.

