SDIGITALES

- Sistemas
- Software a Medida
- Soporte Corporativo
- Consultoría Informática

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Requerimientos de equipamiento para garantizar el Soft de SDigitales

Introducción:

En los últimos años he visto como, en función de la masificación del uso de software, dispositivos, y otros elementos tecnológicos, se han difundido, y hecho común, una serie de malas prácticas, que ponen en riesgo al usuario y a su información.

Repetidas veces he publicado y enviado a mis usuarios información sobre el tema, pero muchas veces, la misma ha caído en balde. Y lo peor, es que muchas veces, luego, los usuarios no entienden que los problemas, pérdidas de tiempo, y costos, podrían haberse evitado.

Por lo tanto, y para evitar problemas, malos entendidos, y poder garantizar el funcionamiento de mis sistemas, emito este documento.

En el mismo, indico claramente que elementos, o formas de uso, pueden generar problemas en el equipamiento, o en los datos del sistema. Y si el usuario incurre en alguna irregularidad, con respecto a lo expresado en este documento, se hace responsable por los mismos.

En general:

- Se debe respetar el *Estándar de calidad de servicio técnico* de **SDigitales** (Apéndice II)
- Aplicar las prácticas recomendadas en el apéndice I - *Algunos conceptos importantes por seguridad*
- No debe tener instalado ningún software que no sea estrictamente necesario.
- Los sistemas operativos deben ser originales, o instalados de copias fieles de originales, y tener instaladas todas las actualizaciones publicadas por Microsoft.
- Los equipos deben estar protegidos por un antivirus reconocido.
- Los equipos deben estar conectados a la red por cable UTP de categoría 6 o superior.
- Se considera en 6 años la vida útil segura de un equipo.

Con respecto al Hardware y al sistema operativo

Servidores

- El servidor debe contar con un procesador y memoria adecuados a su función, al sistema operativo instalado, y a la cantidad de usuarios y sistemas que soporta.
- El servidor debe ser de dedicación exclusiva, o ser usado lo mínimo posible (para liberar recursos para atender a las terminales)
- Si se tiene acceso por RDP, el mismo debe realizarse a través de túnel SSH encriptado.

Terminales

- Las terminales deben contar con un procesador y memoria adecuados a su función, al sistema operativo instalado y a la forma de uso que de ella haga el usuario.
- Sus usuarios deben ser perfectamente identificados.

Con respecto al Software de Usuario

- El software instalado debe ser el mínimo necesario, y en todos los casos ser absolutamente seguros (Un software se considera peligroso cuando su distribución es viral, impuesta en forma forzada por alguna instalación, o consuma deliberadamente o no un exceso de recursos de la red o del equipo).

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Conclusiones

Entiendo que muchos van a cuestionar algunos de esto ítems, debido a conveniencias personales, a la influencia de publicidad o documentos que pueden encontrase en Internet, pero es importante comprender que toda esta información es el resultado de muchos años de análisis y servicio técnico, centrando mis objetivos en lograr que los equipos de mis usuarios tengan la menor cantidad de problemas, y el menor costo de servicio técnico, ya sea por inactividad, o por costo directo, posibles.

En la práctica, los usuarios que han seguido mis consejos, han tenido significativamente menos problemas. Por el contrario, los que no lo han hecho, tienen problemas casi de continuo.

En seguridad informática, muchas veces se habla del concepto de capas. El usuario, y su contexto, forman la capa superior de la infraestructura informática de su empresa. Si ellos fallan, o hacen mal uso del equipamiento, no hay nada que se pueda hacer. Los riesgos terminan siendo siempre altos.

Y algo más, muy importante: Las computadoras de todo tipo, procesan datos, en forma mecánica, sin entender razones, vencimientos, urgencias, etc. Todo depende del usuario. De los programas que instale. Del uso que le dé al sistema operativo. De los sitios por los que navegue. Del uso que haga de las redes sociales, y las aplicaciones en línea. Del mantenimiento que reciban los equipamientos. Sus acciones y decisiones son las que van a determinar, a la corta o a la larga, su costo en infraestructura. Capacite.

Por lo tanto, sugiero encarecidamente que aproveche toda la experiencia y el conocimiento (más de 28 años en el rubro), en su propio beneficio.

Muchas gracias.

Adrián E. Santarelli
Analista Universitario de Sistemas

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Apéndice I - Algunos conceptos importantes por seguridad

- **Almacenamiento de Documentos:** Todos los documentos generados deben almacenarse en la carpeta Mis Documentos, programada en el servidor. Esto se debe a que en el mismo se tienen todas las medidas de seguridad necesarias para su preservación, respaldo y eventual recuperación. Hoy en día, los documentos en equipos locales no son respaldados, y por lo tanto, en caso de pérdida (como ha ocurrido), es imposible prácticamente su recuperación.
- **Almacenamiento de Documentos (Locales):** Todos los documentos de uso local deben guardarse en Mis Documentos. Nunca, por ningún motivo, guardar archivos o documentos en la carpeta de Escritorio. Asimismo, las descargas deben redirigise a la carpeta Descargas, que todo Windows tiene configurada
- **Almacenamiento de Documentos (Personales):** Todos los documentos personales, fotos, videos, música, etc., deben almacenarse en carpetas personales, que no sean afectados por los respaldos programados en el servidor o en los equipos locales. Los respaldos de estos documentos y archivos debe hacerlo el usuario. El objetivo de esta medida es agilizar los respaldos y reducir su tamaño.
- **Uso correcto de Internet:** La conexión a Internet de la institución es limitada, debido a las propias limitaciones del servicio, y la cantidad de equipos y dispositivos conectados es muy grande. Por ello, se requiere un uso controlado y correcto de la misma. El streaming (video o audio a través de internet), uso de redes sociales, etc. causa un alto consumo que perjudica al uso realmente necesario. Por lo tanto, cada usuario debe ser consiente de este tema, y medirse en el uso de la red.
- **Uso seguro de Internet:** Muchos sitios de internet, incluso los que parecen seguros, no lo son. Scripts en redes sociales, uso de navegadores inseguros (como Google Chrome), ponen en alto riesgo la seguridad de la información que hay en cada equipo, ya sea por perdida por infección con virus o ransomware, o por habilitar el acceso a la misma por parte de usuarios externos (hacking). Evite, entonces, todo riesgo posible. No se debe navegar, en equipos de uso comercial, por cualquier lugar. Restringir únicamente a sitios seguros y necesarios. Evitar redes socales. Se sugiere el uso de Opera como navegador.
- **Uso de correos seguros:** Todos los correos que deben usarse en la institución deben ser provistos por la provincia, con dominio santafe.gov.ar. Estos son los únicos mails que se consideran seguros, tanto en confiabilidad como en cuanto a confidencialidad de la información que por ellos circula. Debe tenerse en cuenta que la información que circula por correos gratuitos (Gmail, Hotmail, Yahoo, etc.) se debe considerar pública. En la institución se trabaja con mucha información privada y confidencial, que debe ser preservada. Asimismo, los correos deben manejarse con un cliente local (Thunderbird, recomiendo), para evitar bloqueos y/o perdidas. Si no posee una dirección de la provincia, se debe gestionar e instalar de inmediato.
- **Uso de correos personales:** No deben usarse correos personales para intercambiar información relacionada con la institución, por cuestiones de seguridad y confidencialidad. Un correo personal puede ser vulnerado, accedido por virus o malware, y accedido desde dispositivos o equipos ajenos a la institución. Por otro lado, si alguien del personal deja de trabajar en la institución, se lleva con él toda la información (con el riesgo que esto puede traer).
- **Conexión de dispositivos:** La conexión de dispositivos a la red de la institución (Celulares, notebooks, tablets) debe estar auditada. Todos los dispositivos deben tener instalado un antivirus correcto y actualizado. No debe permitirse el uso de pendrives o discos externos sin autorización.
- **Acceso a sitios con información segura:** Cuando tenga que acceder a un sitio en el que se maneje información sensible (Home Banking, por ejemplo), tenga la precaución de verificar:

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

  - **Dirección segura:** La dirección tiene que estar sobre protocolo seguro: Debe comenzar con https
  - **Dominio correcto:** Toda la dirección del sitio (que se visualiza en la barra de direcciones, habitualmente en la parte superior del navegador), deber corresponder con el sitio al que desea ingresar.
  - **Acceso desde buscador:** Evite acceder a estos sitios buscándolos por Google. Una falla en el buscador permite posicionar como primer resultado sitios falsos. Esos sitios muchas veces copian exactamente la apariencia del sitio original, y solo pueden ser detectados por su dirección. Normalmente, tienen por objetivo captar y grabar datos de acceso (por ejemplo, los datos de acceso al home banking). Si no hay alternativa a ingresar por buscador, verifique a conciencia que sea dirección segura, y dominio correcto.
- **Instalación segura de Windows:** Su sistema operativo debe estar debidamente instalado, con todas las actualizaciones publicadas a la fecha, y tener la opción de actualización automática activa. Debe mantenerse activo el firewall, e inactivos y bloqueados todos aquellos servicios innecesarios. Fundamentalmente, el de escritorio remoto (Terminal Server)
- **Protección Antivirus:** Los equipos deben estar protegidos por antivirus reconocidos, y de licencia paga (se recomienda ESET o Kaspersky). En caso de servidores, es fundamental instalar alguna protección proactiva anti-ransom.
- **Conexión a Redes:** Para uso profesional y comercial, debe conectarse a la red de la organización, preferentemente, a través de cable UTP. Evitar el wifi, debido a su baja seguridad, estabilidad y confiabilidad. Si no hay otra alternativa, asegúrese de contar con routers correctamente configurados, y de la potencia y velocidad adecuadas para el ambiente físico en el que se ubica, y la cantidad de dispositivos que han de conectarse.
- **Correcto uso de programas (Administración de recursos):** Cada vez que se abre un programa, un sistema, etc., se abren archivos, se consume memoria del equipo, y en algunos casos, se consumen recursos de red. Estos recursos no son infinitos, y muchas veces, la apertura y conservación de programas y documentos innecesarios termina ralentizando al equipo, la red, e incluso, bloqueando archivos y registros en la red. Por este tema, y para maximizar tanto el rendimiento del equipo, de la red, y minimizar la posibilidad de pérdida de datos por programas o equipos que dejan de funcionar (cuelgues), cierre inmediatamente cualquier programa o documento cuando termine de usarlo. Más aún, al finalizar la jornada laboral, asegurese de cerrar todos los programas en su equipo, y apagarlo (Salvo expresa indicación).

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Apéndice II - Estándar de Calidad para Servicio Técnico

Con respecto a Hardware

- El hardware comprado debe ser siempre de 1º calidad, comprado en mayoristas reconocidos y confiables, y con al menos con 12 meses de garantía.
- Se debe comprar cualquier tipo de hardware en negocios especializados en informática, con servicio técnico propio, y que ellos mismos atiendan la garantía. NUNCA COMPRAR ELEMENTOS INFORMATICOS EN CASAS DE ARTICULOS DEL HOGAR, O EN LINEA.
- No se guie, para la compra, por publicidad. Hay marcas, como HP, Dell, y otras, que lo que venden en Argentina es de baja calidad. Las impresoras HP, por ejemplo, presentan un montón de incompatibilidades y problemas de funcionamiento. Sin embargo, tienen mucha publicidad, y eso hace parecer (únicamente parecer) que son de buena calidad.
- Se recomienda el uso de procesadores Intel, corriendo sobre motherboards con chipsets de la misma marca. Las marcas de motherboards probadas y recomendadas son Gigabyte, Asus y MSI.
- El hardware debe estar correctamente dimensionado para las aplicaciones que se han de correr (en cuanto a procesador, velocidad y memoria).
- Se debe contar con protección eléctrica por medio de UPS's, en todos los equipos y elementos activos de la red. Probar regularmente el funcionamiento de las baterías de las UPS's, y reemplazarlas en caso de cualquier tipo de falla. No se recomienda el uso de estabilizadores, sobre todo, si su capacidad es baja, debido a los graves problemas que pueden traer estabilizadores comunes, de baja calidad, ante picos de tensión, cuando su carga es cercana a su capacidad.
- Se recomienda conectar todo el equipamiento informático, ya sea equipos, impresoras, dispositivos activos de red, a una única línea eléctrica, debidamente dimensionada, con toma a tierra, y protegida con una térmica. Esta línea es exclusiva de informática, y no debe conectarse absolutamente nada más.
- Se debe optar por impresoras adecuadas al volumen de impresión y tipo de uso que han de sufrir, aunque su costo sea superior.
- Todos los equipos deben tener actualizados y correctamente instalados todos los drivers que recomiende el fabricante.
- El equipamiento debe mantenerse limpio y en condiciones óptimas de funcionamiento. Periódicamente, deben revisarse los ventiladores internos, y limpiarlos o reemplazarlos en caso necesario.
- Al comprar hardware, exigir cajas, manuales y CD's, para asegurarse su condición de nuevo, y verificar marca y modelo de cada componente comprado.
- No ahorre en hardware. Por cada peso ahorrado, gastará tres en servicio técnico.
- Considere que un componente puede fallar, normalmente, en los 6 primeros meses de uso. Si no falla en ese periodo (que es normal en mercadería de 1º calidad), durará varios años. Considere, además, que si compra mala calidad o mal dimensionado, por la rotación de modelos de componentes en el mercado, luego de 12 meses será muy complicado conseguir repuestos o ampliaciones para su equipamiento, y deberá directamente reemplazar equipos.
- Los elementos tales como fuentes, placas, discos y lectograbadoras de DVD no se deben reparar, sino directamente, reemplazar.
- Las impresoras, notebooks, y AIO solo deben ser reparadas (en caso de problemas de hardware) por servicios técnicos oficiales.
- Luego de cualquier reparación, se deben exigir los elementos reemplazados.

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

- La vida útil y efectiva de una PC es de 4 a 5 años. Luego, aunque funcione correctamente, se recomienda su reemplazo, dado que comienza a aumentar el riesgo de falla por fatiga o agotamiento de sus componentes. Además, por la misma evolución del software y del hardware, el equipo deja de soportar soft necesario, tales como suites ofimáticas o antivirus, dado que normalmente todo el soft se diseña para equipos actualizados.
- Investigar, antes de una compra, en foros de usuario, por el hardware. Hay marcas que actualmente tienen características de obsolencia programada (HP, por ejemplo), que limita mucho su vida útil. Optar por marcas alternativas, y con buenos comentarios de usuarios.

Con respecto al Software

- Se deben instalar siempre versiones legítimas de Windows, originales. Nunca instalar "distribuciones customizadas" o "dudosas".
- La versión de Windows que instale en el equipo debe ser adecuada al hardware. Siempre debe tener más equipo que el requerido por la versión de Windows.
- Se recomienda la instalación de Windows 7, en su edición Professional. o Windows 10. Evitar por todos los medios la instalación de Windows Vista, 8 u 8.1, dado no son lo suficientemente sólidos y estables para considerarlos seguros. Siempre asegurarse que el Sistema Operativo sea correcto para el hardware disponible.
- Instalar absolutamente todas las actualizaciones de Windows (publicadas por Microsoft). Esta actualización debería repetirse mensualmente (se recomienda el segundo miércoles de cada mes, dado que Microsoft publica las actualizaciones el segundo martes de cada mes).
- Se debe instalar en cada equipo el mínimo soft necesario. Optar por soft freeware a versiones "piratas".
- Se debe instalar un antivirus / firewall reconocido y liviano. Se recomienda la línea de productos ESET o Kaspersky. No usar nunca antivirus con licencias "piratas", dado que está comprobado que al ser detectada la anormalidad de la licencia, el antivirus se desactiva. Optar, si no se desea pagar, por versiones gratis, aunque debe tenerse en cuenta que muchos antivirus gratuitos no protegen realmente al equipo (por ejemplo, AVAST o AVG). Desconfié de cualquier servicio técnico que le ofrece soluciones antivirus "piratas". No funcionan.
- Si usa notebook, instalar siempre en ellas Suites completas de protección (necesarias por la movilidad de la misma).
- Desactivar del inicio de Windows todos los programas que no sean estrictamente necesarios. Asimismo, desactivar todos los servicios internos de Windows que no son necesarios. Su equipo ganará muchísimo en rendimiento y confiabilidad.
- Desactivar también, y evitar el uso, de temas visuales, protectores de pantalla, y fondos de pantalla. Ganará rendimiento y estabilidad.
- Nunca deje carpetas con documentos en el Escritorio de Windows. Todo debe estar en la carpeta "Mis Documentos". (Dejar documentos o archivos grandes en la carpeta de Escritorio causa problemas de velocidad y estabilidad).
- Se debe tener el máximo cuidado para evitar infecciones de virus o malware. Usar un navegador seguro (se recomienda Opera), con bloqueador de ventanas emergentes, ads (publicidades), y de rastreo. Evite navegar por sitios poco seguros (Facebook, juegos, pornografía, etc.). No abra mails con contenido dudoso, ni mensajes sospechosos de ningún tipo. Tenga mucho cuidado con el pishing (robo de identidad o de datos). Evite el envío de spam, y de participar en cadenas de cualquier tipo. Desconfíe de todo. Evite el uso de

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Internet Explorer, Mozilla Firefox o Google Chrome, debido a las vulnerabilidades que ofrecen a través de los complementos.
- Nunca utilice correos personales o de cuentas gratuitas para uso comercial. Debe tener dominio propio, hosting seguro, y descargar el correo en la maquina con un cliente de correos seguro (Thunderbird u Opera)
- Si es administrador, es conveniente que eduque correctamente a los usuarios que tiene a cargo. Es mucho mejor responsabilizar que restringir el acceso (dado que en este caso el usuario accede igual, normalmente, y sin ningún tipo de cuidados).

Con respecto a Redes

- El cableado de red debe estar correctamente planificado y realizado, por personal idóneo, capacitado en cableado estructurado. Se debe acreditar la capacitación recibida.
- Los materiales pasivos y activos de la red siempre deben ser de 1º calidad, y de origen reconocido.
- Las conexiones wi-fi siempre han de usarse (únicamente) para acceso a Internet, salvo que los sistemas corran con algún motor de base de datos SQL.
- En todo caso, las conexiones wi-fi deben estar aseguradas con contraseña de acceso de al menos 12 caracteres, mezclando letras y números.
- La configuración de los Routers y switchs debe estar asegurada por contraseñas.
- La configuración de la red debe estar bien planificada e implementada. Las IP's deben ser privadas y asignadas manualmente. Solo deben ser asignadas por DHCP aquellas correspondientes a notebooks. Se deben eliminar todos los servicios y protocolos innecesarios.
- Periódicamente, se debe auditar y medir el tráfico y performance de la red, detectando problemas y tomando acciones correctivas. Asimismo, se debe analizar si no hay accesos externos no permitidos (muy frecuentes al usarse wi-fi).
- Se deben compartir e instalar los recursos de red mínimos y estrictamente necesarios (Discos e impresoras).
- Se deben configurar contraseñas para aquellos recursos de red que deban estar compartidos, pero cuyo acceso deba ser restringido a los usuarios de mayor nivel.
- Impresoras y discos portables no deben moverse de un equipo a otro, salvo extrema necesidad. En estos casos, primero deben desinstalarse completamente del equipo de origen, y volver a instalar en el equipo de destino. También se deben reconstruir los mapeos y configuraciones.

Recomendaciones Generales

- Se debe instruir correctamente al personal, para evitar deterioro o problemas en el equipamiento o en el software.
- Se debe exigir siempre el detalle de trabajos de servicio técnico, con detalle de repuestos, tareas, horas utilizadas y costos. En caso de infección, detalle de virus y malware detectado.
- Los trabajos de servicio técnico, en su gran mayoría, no pueden ser realizados a domicilio. Tampoco pueden hacerse bajo presión de tiempo. No insista, es mejor que demore y el trabajo quede bien.
- Al detectar algún problema de funcionamiento, inmediatamente detenga el trabajo en el equipo, y comuníquese con el servicio técnico. Indíquele con exactitud que mensajes de error muestra el equipo, y respete las indicaciones que su service le dé.
- Nunca se debe "formatear" un equipo para solucionar un problema. Esto lo único que indica es la incapacidad del técnico para detectar el problema, y en estos casos, normalmente, se

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

termina con un altísimo costo en datos y tiempo. En mi experiencia personal, en más de 25 años solo he debido formatear 4 o 5 equipos. El proceso de Formateo para limpiar equipos es solo realizado por técnicos dudosos o mal capacitados.

- Antes de entregar el equipo al servicio técnico, si es posible, asegúrese de respaldar toda la información que el equipo contenga. Exigir al técnico que a su vez haga un respaldo antes de cualquier operación peligrosa.
- Responsabilizar al operador por virus o problemas que puedan ser generados por mal uso del equipo.
- Si en su equipo corre algún tipo de Sistema, informar al servicio técnico. Este deberá contactarse con los desarrolladores para evitar cualquier problema con el sistema y sus datos.
- Guarde absolutamente todos sus archivos y documentos en la carpeta “Mis Documentos”. En caso de usar otras carpetas, documéntelo e informe a su técnico, para evitar perdida de información