Soluciones Digitales

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

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

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 deben 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 sociales. Se sugiere el uso de Opera como navegador.
- **Uso de correos seguros:** Todos los correos que deben usarse deben ser de dominio propio. 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. Asimismo, los correos deben manejarse con un cliente local (Thunderbird, recomiendo), para evitar bloqueos y/o perdidas.
- **Uso de correos personales:** No deben usarse correos personales para intercambiar información relacionada con la organización, 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:
    - **Dirección segura:** La dirección tiene que estar sobre protocolo seguro: Debe comenzar con https

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

  - **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, asegúrese de cerrar todos los programas en su equipo, y apagarlo (Salvo expresa indicación).