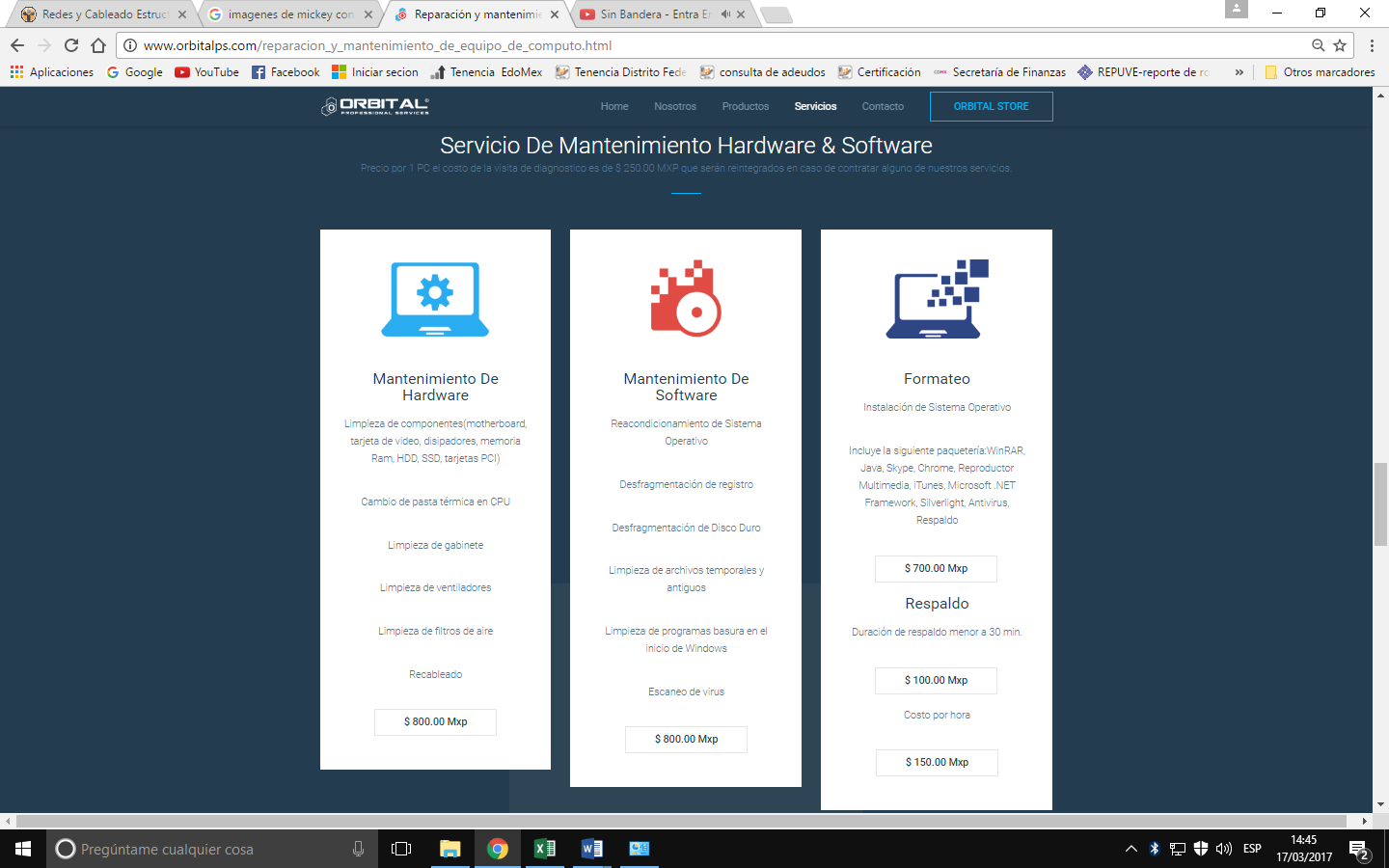
Redes

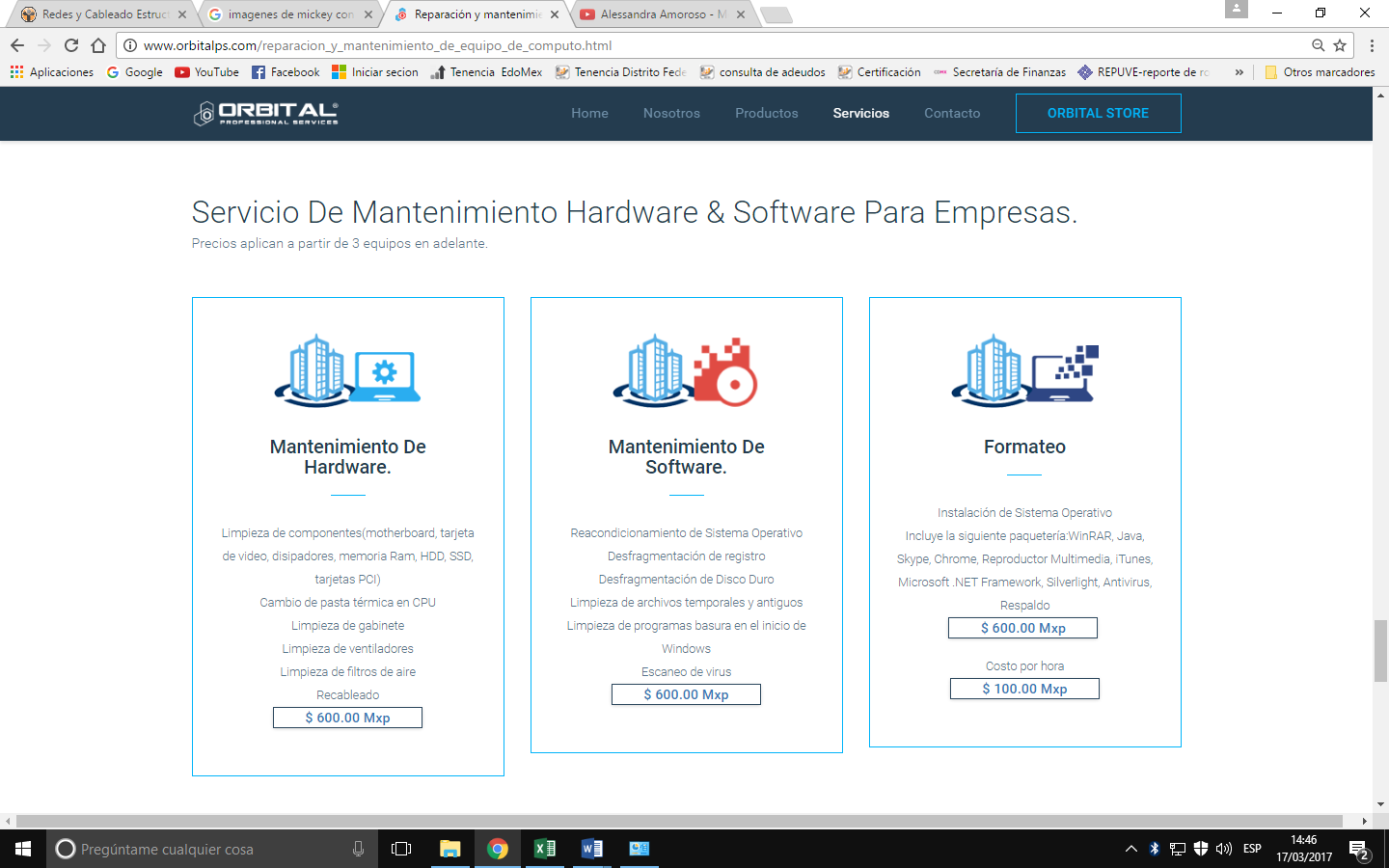
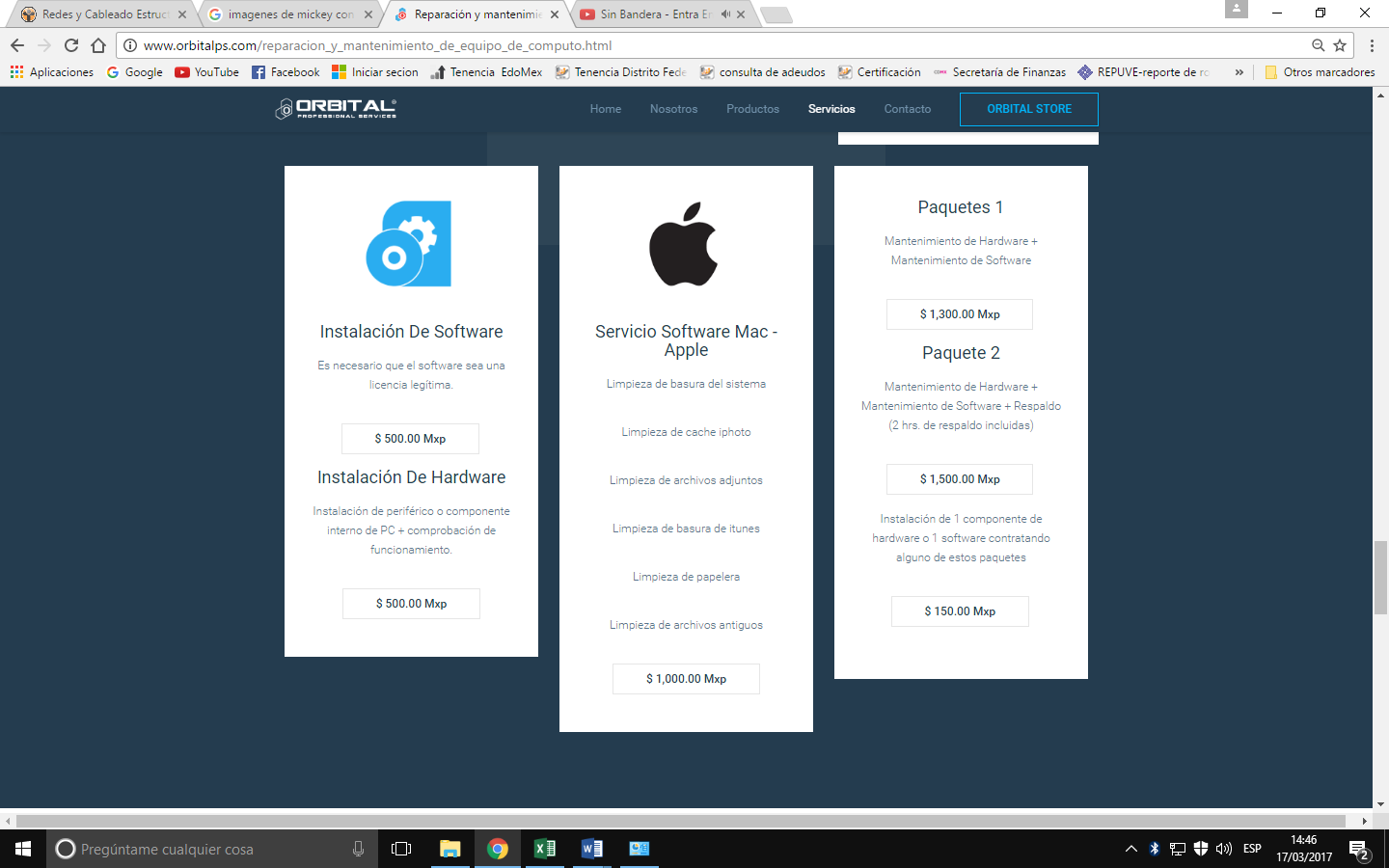
<http://www.centralderedes.com/?utm_source=central-de-redes&utm_medium=cpc&utm_content=redes-pregunta&utm_campaign=redes&gclid=CIKslK3y3dICFYIBaQodAuIDQA>

<http://www.orbitalps.com/reparacion_y_mantenimiento_de_equipo_de_computo.html>

Reparación y mantenimiento de Hardware & Software

Preventivo / Correctivo





<http://www.homedesk.co/Soporte-en-Informatica/soporte-en-informatica-computadores-redes-e-impresoras.html>

<http://www.enbex.es/sistemas-y-redes>

<http://www.intercomm.com.mx/index.php?option=com_content&view=article&id=55&Itemid=69>

Pólizas de soporte y aviso de privacidad.

<http://www.telecoandaluzas.com/politica-de-calidad/>

Políticas de calidad

<http://karlastar93.blogspot.mx/2010/09/planeacion-y-cotizacion-de-una-red-lan.html>

PLANEACIÓN

<https://daviddiazdelacruz.wordpress.com/2009/05/12/politicas-informaticas-para-tu-empresa/>

Políticas informáticas para tu empresa

Publicado el mayo 12, 2009 de daviddiaz

Aquí dejo un pequeño conjunto de políticas de seguridad informática básicas diseñadas por el área de sistemas de una PYME y que el personal está pendiente a cumplir en todo momento.

Las políticas de seguridad de la información son lineamientos a nivel general a seguir por la empresa para asegurar su información valiosa, así como los programas, hardware y áreas físicas relacionadas.

Que tu empresa cuente con estos lineamientos aportará una serie de ventajas a considerar:

– La infraestructura de sistemas representa una inversión considerable en los activos de la organización, los lineamientos sobre el uso adecuado del equipo de cómputo sugieren un tiempo de vida útil más extendido, minimizando reparaciones e inversión por actualización.

– Tener reglas sobre el uso adecuado del equipo de cómputo incrementa la productividad de los empleados. Muchas empresas incluyen dentro de sus políticas las restricciones sobre programas de ocio y el uso de internet en actividades ajenas al entorno laboral.

– Como tercer punto y no menos importante, es imprescindible contar con políticas informáticas encaminadas al aseguramiento de la información.Como bien se sabe, la información es el activo intangible más valioso de una empresa y generalmente el más descuidado. En muchos casos, la pérdida de información puede ser considerada inaceptable y peor aún la fuga o mal uso de la misma.

(Update, Junio 2016). Las políticas descritas aquí se denominaron políticas informáticas y no políticas de la información, la diferencia la puedes encontrar en 5 puntos para entender la seguridad de la información

Dato técnico:

Una política de seguridad define el 'QUE': qué necesita ser protegido, qué es más

importante, cuales son las prioridades y cual debería ser el enfoque general al manejar

los problemas de seguridad informática que se presenten.

La política de seguridad por si misma no dice COMO se deben proteger las cosas.

Este es el rol de los procedimientos de seguridad. La política de seguridad es un

documento de alto nivel que provee una estrategia general. Los procedimientos de

seguridad deben ser establecidos, a detalle, con los pasos precisos de seguridad.

El documento RFC1244 contiene las definiciones e información técnica más avanzada

sobre políticas de seguridad.

Dicho de otra forma, el conjunto de políticas de seguridad es una “declaración de principios” sobre la que se cimentará la Seguridad de la Información de nuestras organizaciones. A partir estas políticas, es necesario desarrollar los procedimientos específicos que detallen lo establecido en nuestra política.

Tus políticas informáticas deben ser concisas y claras. El rigor debe estar en función de poderlas cumplir sin perder de vista la actividad de nuestro negocio.

Lo más importante es que no pierdan sentido y que en todos los casos la actuación del personal esté guiada hacia el cumplimiento de dichas políticas.

Políticas informáticas

Alcance

El presente documento es aplicable a todos los empleados, consultores, contratistas, colaboradores, practicantes o residentes, incluyendo a todo el personal externo que en algún momento cuente con acceso a los recursos informáticos o información de la empresa.

Sobre la asignación y el uso de los recursos

1. Cada empleado tiene asignado un equipo de cómputo al cual debe ingresar con un usuario y contraseña.

2. El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe asegurar que se cumpla esta política. Además, todo el personal deberá informar a sistemas sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.

3. Todo el personal tendrán una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades. Estas cuentas de correo, sólo son para uso interno, no tienen la capacidad de enviar correos públicos.

4. El uso de internet queda reservado solo para las actividades de trabajo que así lo requieran. En general se restringe el acceso mediante el uso de contraseña en el administrador de contenidos de Internet Explorer.

Sobre la seguridad de la información

5. Diariamente se realizan backups automáticos a la base de datos según los mecanismos establecidos y se realizan a cada hora.

6. Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados.

7. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.

8. Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.

9. Coordinación o sistemas designarán periódicamente nuevas contraseñas tanto para el acceso a las sesiones Windows como para el acceso a los programas.

10. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.

11. Todos los equipos asignados a los conectores/gestores tendrán deshabilitados los accesos a puertos USB, CD o Diskettes. Esta medida tiene 3 objetivos:

Evitar ataques de virus en los equipos y el servidor.

Evitar extracciones no autorizadas.

Evitar la carga de archivos ajenos a la labor de gestión.

12. Los equipos autorizados para el uso de dispositivos de almacenamiento externos están supervisados por coordinación y por el área de sistemas, para la entrada y salida de información.

13. A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

Actualizar su base de firmas de virus (actualización de la lista de amenazas)

Búsqueda de virus (análisis del equipo)

Eliminación de virus si fue detectado.

14. En caso autorizado de memorias USB y discos, es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Además los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

Sobre el mantenimiento y buen uso de la infraestructura

15. Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.

16. Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.

17. Si se presentara una suspensión de servicio eléctrico y el servidor solo se sostuviera con el no-break, se tendrán que apagar primero todos los equipos de la agencia y posteriormente el servidor.

18. El servidor y la máquina principal del área administrativa deberán conectarse a un equipo no-break para evitar la pérdida de información en los equipos por variaciones o fallas de energías.

19. Una vez al año se realizara una revisión en la red para detectar desperfectos y dar así mantenimiento a la agencia.

20. Periódicamente, por espacio de 4 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas.

21. Toda actividad elaborada por el equipo de sistemas deberá de estar debidamente documentada para darle seguimiento y que sirva como evidencia en los procesos de auditoria interna.