

UNIVERSIDAD DE CASTILLA-LA MANCHA
ESCUELA SUPERIOR DE INFORMÁTICA



**Auditoría y Seguridad de la
Información**

AUDITORÍA A DIGSOL

16 de noviembre de 2009

Juan Andrada Romero
Jose Domingo López López
Antonio Martín Menor de Santos
Francisco José Oteo Fernández

ÍNDICE

Índice	I
Índice de figuras	II
1. Carta al Director	1
2. Auditoría	2
2.1. Ausencia de un plan estratégico de Tecnologías de la Información	2
2.2. Gestión de la configuración y control de cambios	4
2.3. Integridad, disponibilidad y confidencialidad de los datos	5
2.4. Deficiencia en la seguridad de la información y en las instalaciones	7
2.5. Evaluación de riesgos, plan de contingencia y plan de continuidad	11
3. Papeles de Trabajo	12
ANEXO 1: Entrevista con el Director General de la empresa	12
ANEXO 2: Situación actual de las empresas competidoras	13
ANEXO 3: Organigrama de la empresa DIGSOL	14
ANEXO 4: Adquisiciones tecnológicas	14
ANEXO 5: Entrevista con uno de los desarrolladores informáticos de uno de los departamentos de la empresa	16
ANEXO 6: Instalación y configuración inicial del software en equipos informáticos	17
ANEXO 7: Vulnerabilidad a ataques informáticos	17
ANEXO 8: Adquisición de licencias por duplicado	20
ANEXO 9: Software con licencias caducadas	22
ANEXO 10: Software no corporativo	22
ANEXO 11: Cuentas de usuario	22
ANEXO 12: Ubicación y permisos de los archivos de datos	23
ANEXO 13: Seguridad de la red wifi	23
ANEXO 14: Vulnerabilidad del servidor	27
ANEXO 15: Copias de seguridad e información accesibles	27
ANEXO 16: Ficheros de log	28
ANEXO 17: Estanterías desprotegidas	28
ANEXO 18: Ordenadores abiertos	28
ANEXO 19: Ordenadores sin bloquear	29
ANEXO 20: Soportes de datos mal destruidos	29
ANEXO 21: Papeles con datos mal destruidos	29
ANEXO 22: Acta de evaluación y gestión de riesgos	33
ANEXO 22: Copias de seguridad	33

ÍNDICE DE FIGURAS

3.1.	Porcentaje de inversión en investigación de nuevas tecnologías	13
3.2.	Presencia en el mercado de las empresas	14
3.3.	Organigrama de la empresa DIGSOL	14
3.4.	Fragmento de la factura del 17-Junio-2008	15
3.5.	Factura del 27-Mayo-2009	15
3.6.	Lista de la configuración inicial de los equipos informáticos	18
3.7.	Número de ataques de Denegación del Servicio durante 12 meses	19
3.8.	Factura de adquisición de licencias de antivirus en Enero del 2009	20
3.9.	Factura de adquisición de licencias de antivirus en Junio del 2009	21
3.10.	Captura de pantalla del estado de un antivirus	22
3.11.	Software no alineado con la estrategia de negocio	23
3.12.	Ubicación y permisos de archivos inadecuados	24
3.13.	Usuarios del sistema	25
3.14.	Programa que desencripta la wifi	26
3.15.	Servidor vulnerable	27
3.16.	Cajones donde se guarda el disco de respaldo	28
3.17.	Ficheros de log	29
3.18.	Estanterías con documentos	30
3.19.	Ordenador sin tapas	30
3.20.	Disco duro destruido incorrectamente	31
3.21.	Papeles destruidos incorrectamente	31
3.22.	Ordenador sin bloquear	32
3.23.	Acta de evaluación y gestión de riesgos	33
3.24.	Copias de seguridad de los pedidos	34

1. CARTA AL DIRECTOR

16 de noviembre de 2009

Estimado Sr. Director General:

Tras realizar la auditoría a la sede de su empresa DIGSOL en Ciudad Real, tal y como nos solicitó, le resumimos los problemas más graves que se han encontrado:

- **Ausencia de un plan estratégico de Tecnologías de la Información:** no existe una integración total de las Tecnologías de la Información en la empresa, lo que conlleva que no se aprovechen correctamente las tecnologías, no se investigue en ellas para obtener mejores beneficios para la empresa, se realicen inversiones innecesarias y se prioricen incorrectamente los proyectos informáticos.
- **Problemas en la gestión de la configuración y control de cambios:** los documentos que definen la configuración inicial de los equipos no se han actualizado con el paso del tiempo, se ha encontrado instalado software no apropiado para el negocio de la empresa y no se han registrado las nuevas adquisiciones de aplicaciones y licencias. Esto conlleva que se realicen, en algunos casos, gastos totalmente innecesarios.
- **Ausencia de medidas de seguridad físicas:** no existen medidas que controlen o limiten el acceso a las instalaciones de la empresa y a sus diversos departamentos. Esto es un grave riesgo para la seguridad de las instalaciones y los dispositivos que hay en la empresa.
- **Mala elección y diseño del centro de datos:** la ubicación del servidor no cumple con las necesidades energéticas y de refrigeración necesarias. Además, ante un desastre ambiental o un incendio, el servidor estaría desprotegido y podría resultar dañado, llegando incluso a perder la información que contiene.
- **Ausencia de medidas de administración y protección de datos:** no se han definido procedimientos adecuados para el almacenamiento, copia y protección de los datos que posee la empresa: el acceso a la información no está controlado, las copias de respaldo no se tratan de forma correcta y, a la hora de eliminar datos, no se procede adecuadamente.
- **Ausencia de un plan de evaluación y gestión de riesgos formalizado:** aunque existe un plan de gestión y evaluación de riesgos, no es válido, ya que fue elaborado por algunos de los miembros del Consejo de Administración y no existe ningún informe en el cual se indique quiénes de estos miembros estaban presentes ni las personas a las que consultaron a la hora de realizarlo. Además, no se tratan mucho de los riesgos, lo que puede provocar grandes pérdidas a la empresa ante una posible catástrofe o contingencia.

Atentamente,

ExtAudi: Empresa especializada en Auditorías Externas.

2. AUDITORÍA

En los siguientes apartados se detallan los problemas que se han encontrado al realizar la auditoría a la sede localizada en Ciudad Real de la empresa DIGSOL. Dicha auditoría cubre los siguientes aspectos:

- Infraestructura hardware y software (seguridad, riesgos, planes, etc.).
- Integridad y confidencialidad de los datos.

2.1. Ausencia de un plan estratégico de Tecnologías de la Información

Consultando al Comité de Dirección de la empresa sobre la existencia de un plan estratégico de TI (Tecnologías de la Información), se ha observado que no existe dicho plan. Esto significa que, a la hora de intentar cumplir los objetivos de negocio que la empresa tiene fijados, las tecnologías no son algo importante para conseguirlos, si no una simple ayuda (**ver Anexo 1**).

Es decir, la empresa no está alineada con la tecnología, lo que puede suponer, a largo o medio plazo, que la empresa comience a perder presencia en el mercado, ya que para seguir siendo competitiva, es necesario investigar nuevas tecnologías, actualizar los recursos tecnológicos con los que ya cuenta la empresa y aprovechar las oportunidades que ofrecen las tecnologías de la información. En el **Anexo 2** se muestra la inversión que las empresas de la competencia realizan en I+D de nuevas tecnologías y la situación actual en el mercado. Como se puede observar, si la empresa no alinea las tecnologías con su objetivo de negocio, en poco tiempo perderá la posición en el mercado con respecto a su competidora más inmediata.

Derivado de la inexistencia de un plan estratégico de TI que alinee las tecnologías con el objetivo de negocio, aparece otro problema, que es la falta de un Departamento de Sistemas de Información en la organización de la empresa, tal y como se observa en el **Anexo 3**. Como consecuencia, los desarrolladores informáticos están asociados a los

diferentes departamentos de la empresa, desarrollando los proyectos que sean necesarios en cada momento (entre otras cosas), pero sin contar con un responsable experto en TI.

Al carecer de un Departamento de Sistemas de Información, no hay ningún responsable que se encargue de elaborar un plan para la adquisición y mantenimiento de recursos tecnológicos (**ver Anexo 1**). Por ello, como la empresa carece de dicho plan, cuando cada departamento solicita nuevos recursos tecnológicos, el departamento de contabilidad aprueba la inversión, bajo la orden del Comité de Dirección. Por esta razón, la inversión en tecnología que realiza la empresa es más elevada de lo necesario, lo que puede traducirse en pérdidas económicas importantes a largo plazo. Además, los recursos se adquieren de diversos proveedores, lo que pone en riesgo la compatibilidad, tanto de hardware como de software. Por otra parte, como el Comité de Dirección aprueba la inversión siempre que se solicitan nuevos recursos, existe el riesgo de que cualquier desarrollador cometa fraudes, pudiendo establecer como proveedor a uno con el que haya pactado alguna comisión o comprando recursos que él desee y que sean totalmente innecesarios. En el **Anexo 4** puede verse un ejemplo de estas situaciones.

Otro problema es que no existe un procedimiento por el que se sigan unas pautas a la hora de realizar pagos o devoluciones de los recursos adquiridos, así como tampoco los contratos firmados con los proveedores han sido revisados por un asesor legal, ni se indican cláusulas u obligaciones que deben cumplirse por parte de los proveedores (**ver Anexo 1**). Al no establecerse esas cláusulas contractuales, si un proveedor no satisface un pedido en el período acordado, puede repercutir en graves pérdidas económicas, lo que pone en riesgo la disponibilidad de algún recurso y, por tanto, el correcto funcionamiento de la empresa, con las correspondientes pérdidas económicas.

Al igual que no existe un plan para la adquisición de infraestructura tecnológica, tampoco existe un plan para su mantenimiento, como muestran los Anexos 1 y 5. Simplemente, los encargados de informática de cada departamento realizan las labores de mantenimiento necesarias cuando ocurre algún problema, al igual que se encargan de aplicar las actualizaciones necesarias al software instalado. Esto conlleva un descontrol, ya que no se relizan documentos acerca del mantenimiento realizado ni se sigue un control de cambios en el software que utiliza la empresa.

Para terminar, hay que señalar otro problema. Al no existir el plan estratégico que alinee la empresa con las TI, tampoco existen portafolios de proyectos (esto es, lista de proyectos a desarrollar en la empresa) que asigne correctamente las prioridades a los diferentes proyectos que maneja la empresa. Así, los desarrolladores informáticos se limitan a desarrollar las aplicaciones que dichos departamentos necesiten para llevar a cabo su tarea, en el orden en el que los empleados las van solicitando (**ver Anexo 5**).

Esto tiene el riesgo de que no se atiendan a tiempo los proyectos más prioritarios para mantener el objetivo de negocio de la empresa y que, por tanto, se produzcan pérdidas económicas, además de perder competitividad en el mercado.

2.2. Gestión de la configuración y control de cambios

La empresa dispone de una herramienta de soporte y un repositorio central para almacenar información relevante sobre los elementos de configuración hardware y software. El objetivo es garantizar la integridad de las configuraciones, pero este repositorio no se encuentra actualizado con las nuevas adquisiciones y necesidades de la empresa, ni con la evolución de las TI.

En el **Anexo 6** se observa un fragmento un documento, proporcionado por el Gerente de configuración, que especifica la configuración inicial de los equipos que utilizarán los empleados. Como se puede apreciar, el software que inicialmente se instalará en estos equipos está obsoleto y no existe una norma que estandarice la instalación de parches y actualizaciones de seguridad, así como la configuración de servicios y parámetros del sistema. Esto hace que los sistemas no sean seguros y sean cada vez más vulnerables a ataques informáticos (**ver Anexo 7**, proporcionado por el Jefe de Seguridad).

Otra de las consecuencias que acarrea no tener actualizado el repositorio afecta al uso y adquisición de licencias. En el **Anexo 8** se puede apreciar que en el último año se han adquirido licencias duplicadas para el antivirus y que aún así existen equipos con licencias caducadas (**ver Anexo 9**). Este problema, cuantificando únicamente el caso del antivirus, ha supuesto un total de 676 euros adicionales en 6 meses, un gasto totalmente innecesario.

Por otro lado, los cambios realizados no son registrados en ningún documento y no se mantiene una línea base de los elementos de la configuración para todos los sistemas y servicios como punto de comprobación al que volver tras el cambio. Además, no se garantizan los resultados de los cambios antes de realizarse, ya que éstos no están sujetos a ningún tipo de norma y cada usuario los hace libremente. Como prueba de ello, en el **Anexo 10** se observan capturas de pantalla de software personal, no licenciado o no alineado con el negocio de la empresa y que ha sido instalado en los equipos. Esto podría haberse corregido si los equipos se hubiesen sido revisados periódicamente por el Gerente de configuración.

2.3. Integridad, disponibilidad y confidencialidad de los datos

La empresa carece de servidor de respaldo donde se almacenen duplicados todos los datos de la empresa. Esto indica que existiría un problema serio de disponibilidad de los datos ante una posible avería en el servidor principal, o ante un desastre, provocando una interrupción en el servicio de venta online y por lo tanto la falta de continuidad del negocio.

Otro punto débil que se ha encontrado es la existencia de una única cuenta de usuario dentro del servidor que sirve de puerta de acceso a éste y a los datos que contiene, tanto para los empleados de la empresa relacionados con la parte informática de cada departamento, como para el administrador del servidor. Esta cuenta se llama igual que el nombre de la empresa y el servidor, por lo que sería fácil adivinar desde fuera cuál podría ser un usuario del sistema y lanzar un ataque contra él. (**ver anexo 11**).

Además, si un empleado con algún conocimiento de administración quisiese modificar datos de los archivos, no tendría grandes problemas, debido a que varios archivos tienen permisos de lectura y escritura para el grupo de usuarios al que pertenece el usuario *empleado* y el usuario *digsol*. (**ver anexos 11 y 12**).

Otro problema es el hecho de que se use el servidor tanto para almacenar los datos referidos a los productos que se venden en la web, como datos sensibles sobre la empresa, referidos a la información de carácter personal sobre empleados, clientes, nóminas,

etc. Ciertos archivos con información de carácter personal y/o confidencial tienen unos permisos inadecuados, lo que evidencia un gran riesgo ya que cualquiera (ya sea o no usuario del sistema) puede tener acceso a esta información y leerla, modificarla o borrarla. Incluso existen ficheros en texto plano y sin cifrar que contienen las claves de acceso al sistema. Esto repercute tanto en la confidencialidad de los datos como en la integridad y disponibilidad de los mismos. (**ver anexo 12**).

Al consultar al administrador del servidor sobre la administración y gestión de cuentas de usuario y sobre si existe una política definida a tal efecto, éste ha comunicado que no existe una política que obligue a los usuarios del sistema a cambiar su contraseña personal en un período definido de tiempo, no pudiendo ser ésta la misma que una contraseña anterior. Esto hace que si un usuario no autorizado consigue acceso mediante alguna cuenta, podrá hacerlo de por vida ya que la contraseña no será modificada en un futuro próximo.

Al igual que no existe un plan para la administración de los datos, tampoco existe un plan para su mantenimiento. Simplemente, el encargado del servidor se encarga de dar de alta a los usuarios del sistema y asignarles claves; pero a su vez también se encarga de actualizar los datos de la web de venta de artículos. Igualmente, los encargados de informática de cada departamento tienen acceso al servidor usando una única cuenta (como ya se ha comentado) y realizan las labores de mantenimiento necesarias con los datos y los archivos que los contienen, al igual que se encargan de aplicar las actualizaciones necesarias al software instalado.

Esto conlleva un serio riesgo de integridad y seguridad de los datos, ya que cualquier trabajador podría alterar archivos de datos sin ningún tipo de control sobre él.

No se han creado planes para poder monitorear el desempeño de las tecnologías de información ni para medir su capacidad. Puntualmente, los desarrolladores informáticos revisan los recursos para comprobar si pueden soportar la carga de trabajo de los distintos departamentos. Sin embargo, dichas revisiones no se documentan y las acciones tomadas se limitan a solicitar nuevos recursos tecnológicos si se observa que los actuales no soportan correctamente la carga de negocio.

Por tanto, no se monitorea la capacidad actual de los recursos, así como tampoco se tiene en cuenta el posible crecimiento futuro de la empresa, lo que supondrá un aumento

en la carga de trabajo, existiendo un riesgo que pone en peligro la disponibilidad de los recursos.

Respecto a los diccionarios de datos que utiliza la empresa, la empresa carece de un diccionario de datos empresarial que defina las reglas de sintaxis para los datos de la organización, lo que produce un peor entendimiento entre los usuarios del sistema y del negocio y la posibilidad de creación de elementos de datos incompatibles, por lo que existe un riesgo ante la integridad de los datos.

Otro punto débil que afecta a la integridad de los datos es el hecho de que las comunicaciones por la red no están cifradas por lo que, al no encriptar la información (que viaja en texto plano por la red local), es fácilmente interceptable por los demás usuarios de la empresa o incluso por usuarios externos, ya que además la protección de la wifi se realiza mediante clave WEP que es un tipo de clave fácil de obtener mediante aplicaciones como AirCrack, lo que compromete la integridad del sistema. (**ver anexo 13**).

Para terminar, existe un riesgo para la integridad de la información, ya que se carece de una base de datos centralizada que contenga la información completa de la empresa. Hay una base de datos que almacena una parte de los datos (productos, datos de clientes, etc.) y otra parte que se almacena en ficheros de texto (facturas, etc.) o en ficheros de bases de datos Access o Excel. Puesto que las facturas están relacionadas con productos, usuarios registrados y empleados entre otros, estas deberían estar integradas en una base de datos centralizada, y no repartidos por diferentes ubicaciones. (**ver anexo 12**).

2.4. Deficiencia en la seguridad de la información y en las instalaciones

Continuando con la auditoría, con respecto a las instalaciones de la empresa, se observa que:

- Las instalaciones son poco o nada seguras.
- Existen deficiencias en la ubicación del servidor.

Observando el entorno de trabajo y las instalaciones que posee la empresa se ve que carece de cualquier tipo de medida sobre la restricción del acceso a las instalaciones, tanto por parte del personal de la empresa, como por parte de personal ajeno a la empresa. Todas las salas en las que se ubican los departamentos carecen de cerraduras en las puertas o de sistemas de acceso controlado, así como tampoco se controla el acceso a la empresa de ninguna manera. Cualquiera puede entrar a las instalaciones y acceder a cada departamento pudiendo llevarse físicamente cualquier dispositivo que contenga información, lo que provoca un grave riesgo en la seguridad.

La ubicación del centro de datos y del servidor no ha sido bien planeada y estudiada ya que no se corresponde con el diseño óptimo que debe tener el espacio físico destinado a servidores, por lo que existe riesgo de que el servidor se caliente en exceso y se estropee dejando sin servicio de venta online a la empresa, lo que se traduciría en cuantiosas pérdidas económicas (**ver anexo 14**). Además, hay que destacar que no existe ningún sistema de alimentación ininterrumpida (SAI), ni tampoco una fuente de corriente alternativa, por lo que cualquier corte de luz llevaría forzosamente a una suspensión del servicio de venta por internet así como del acceso a datos de otra índole, por no hablar de posibles daños en el servidor y pérdida de datos.

Por otra parte, en caso de incendio, inundación o algún otro desastre, el servidor que contiene los datos podría estropearse, ya que, como se ha observado, el local en el que se ubica no es el apropiado ni está dotado de medidas de prevención y protección ante tales eventualidades.

Con respecto a medidas de seguridad físicas para limitar o impedir el acceso a dispositivos y a la información que estos contienen se puede observar que el servidor no se encuentra dentro de un armario de datos bajo llave, sino que se encuentra en una estantería junto con otros ordenadores.

Tanto las ranuras de expansión USB como la grabadora de DVD que contiene el servidor están visibles y accesibles, pero además, la parte posterior del servidor está también accesible y pueden observarse las tarjetas de red. Si algún empleado malintencionado quisiera llevarse datos podría hacerlo pinchando una memoria USB, grabando un DVD o conectando otro PC a una tarjeta de red del servidor, interrumpiendo además el servicio web o de acceso a los datos. (**ver anexo 14**).

La ausencia de un cortafuegos físico que limite el acceso al mismo desde fuera es otra deficiencia de la seguridad importante, ya que puede dar lugar a que datos de carácter personal sobre los empleados de la empresa, cuentas, claves, etc. pueden ser accedidos desde fuera de la empresa vía web.

Cuando se preguntó al personal responsable de informática sobre qué procedimientos se seguían para el correcto procesamiento y almacenamiento de los datos de la empresa se nos contestó que sí se había definido un responsable para administrar esos datos y su almacenamiento, pero que no se le había informado sobre la existencia de ningún procedimiento, por lo que se había optado por almacenar todos los datos en un mismo servidor, incluso en un mismo directorio dentro de éste. Indagando un poco más se descubrió que sí se realizaban copias de seguridad de los datos, tanto los referidos a la información sensible a la empresa, como la información de los productos que venden; lamentablemente el soporte en el que se almacena la copia de respaldo de esos datos es un disco duro externo que se guarda en un cajón, sin vigilancia ni medidas de seguridad, del mismo edificio en el que se encuentra el servidor. (**ver anexo 15**).

A parte del encargado de administrar los datos, nadie accede, en principio, a los datos, pero no se toman las medidas de seguridad apropiadas para asegurarse de que no accedan a los datos personas no autorizadas. Examinando los ficheros de *log*, se ha detectado que existen accesos al servidor por empleados que usan la cuenta *empleado* y no están relacionados con datos informáticos, incluso puede que alguno de esos accesos se hayan hecho por empleados que fueron despedidos, pero no se puede probar ya que todos los empleados usan la misma cuenta. Además, dichos logs corresponden únicamente a los últimos 3 meses de actividad, siendo de 2 años el período exigido por la ley para mantener dichos logs. (**ver anexo 16**).

Respecto a ficheros de datos, cuyo soporte no es el electrónico, se encuentra una estantería llena de papeles con información relevante para la empresa. Esta estantería no está protegida bajo llave u otros sistemas de seguridad, y además mezcla datos y cajas u otras cosas sin un orden aparente. Aquí existe también un serio problema de seguridad, ya que la información contenida en esos papeles puede ser fácilmente accedida. (**ver anexo 17**).

Estudiando los comportamientos de seguridad de los empleados se observa que:

- El estado de sus ordenadores no es el adecuado. Tienen los ordenadores abiertos físicamente, dejando al descubierto la electrónica y los dispositivos de almacenamiento de datos (como el disco duro), siendo relativamente fácil dañar un equipo o robar información del mismo. (**ver anexo 18**).
- Por otro lado, cuando un empleado abandona su puesto de trabajo, éste no bloquea el acceso al mismo, por lo que cualquier otro empleado podría usar este ordenador con fines malintencionados. (**ver anexo 19**).

A la hora de eliminar o destruir datos, existen dos vías para hacerlo: si los datos se encuentran en soporte electrónico, es el administrador de datos el que los borra. Si los datos están en papel, para eliminarlos se rompe el papel y se tira a la papelera. En cuanto al procedimiento a seguir cuando se estropea un soporte de almacenamiento, no está especificado, por lo que simplemente, o bien se tira a la basura o bien se lleva a reciclar, pero no se destruye la información que contiene, por lo que alguien podría recuperar esos datos de alguna manera usando un lector magnético, etc. (**ver anexos 20 y 21**).

Tampoco se han encontrado existencias de un libro de incidencias, tal y como dicta el artículo 10 del Real Decreto 994/99, en que hagan constar los siguientes puntos:

1. El tipo de incidencia
2. El momento en que se produce
3. La persona que realiza la notificación
4. A quién se le comunica
5. Los efectos que se deriven de la incidencia

2.5. Evaluación de riesgos, plan de contingencia y plan de continuidad

La evaluación y gestión de riesgos es un tema que no está abordado de una forma eficiente en la organización.

Aunque la empresa dispone de un plan de riesgos, éste ha sido elaborado por algunos de los miembros del Consejo de Administración y no existe ningún informe en el cual se indique quiénes de estos miembros estaban presentes en la elaboración del plan ni las personas a las que consultaron a la hora de realizarlo.

Además, tampoco existe ningún registro de la técnica de identificación de riesgos que emplearon para seleccionarlos, así como el cálculo de la probabilidad de ocurrencia y el impacto, lo cual puede significar que la elección de éstos parámetros fuese arbitraria o manipulada. En el **Anexo 22** se muestra el acta de los asistentes a dicha reunión, cedida por el Comité de Dirección.

La empresa por tanto, no tiene definido un plan de continuidad de TI por lo que en caso de interrupción de los sistemas el impacto será mayor y en consecuencia se verán afectados los procesos clave de negocio.

De lo anterior se extrae que la empresa tendría dificultades para volver a su actividad normal en caso de un desastre o contingencia lo que podría provocar perdidas muy grandes para la empresa.

Las copias de seguridad que posee la empresa no son suficientemente frecuentes. Además carece de copias de seguridad fuera de las instalaciones por lo que en caso de desastre en las instalaciones existe el riesgo de perder toda la información relevante de la empresa. En el **Anexo 23** se muestra cómo se almacenan algunas de las copias de seguridad.

3. PAPELES DE TRABAJO

ANEXO 1: Entrevista con el Director General de la empresa

- **Auditor:** En primer lugar, gracias por su colaboración y por haberme facilitado los documentos que le solicité.

De nada.

- **Auditor:** ¿Cuál es el cargo que desempeña usted en la empresa?

Soy el Director General de la empresa y pertenezco al Comité de Dirección.

- **Auditor:** ¿Cuál es el principal objetivo de negocio de su empresa?

Nuestro principal objetivo es mantenernos entre las 10 empresas más competitivas en la venta de componentes informáticos, tanto en tiendas como a través de la Web.

- **Auditor:** Para conseguir su objetivo de negocio, ¿cree que las tecnologías de información son algo fundamental que deben alinearse con los objetivos de la empresa?

En realidad, nosotros utilizamos los recursos tecnológicos como una herramienta para conseguir nuestro objetivo y para que los distintos departamentos puedan llevar a cabo su trabajo, pero no integramos las tecnologías de la información en los planes de negocio.

- **Auditor:** Por lo que me dice, ¿puede suponer que no cuentan con un plan estratégico de tecnologías de la información?

Así es.

- **Auditor:** Entonces, ¿quién es el responsable de las tecnologías de la información?

Cada uno de los departamentos de la empresa cuentan con unas personas expertas en informática que se encargan de todo lo relacionado con las tecnologías y los proyectos informáticos de la empresa: adquirir recursos, desarrollar proyectos, realizar mantenimiento, etc.

- **Auditor:** Por tanto, tampoco cuentan con un plan de mantenimiento y adquisición de recursos tecnológicos.

Así es. Cuando los informáticos nos dicen que necesitan comprar nuevos recursos, nosotros aprobamos la adquisición.

- **Auditor:** Si hay algún problema con los proveedores, ¿qué medidas toman?

No solemos tener problemas con los proveedores, porque llevamos varios años trabajando con ellos y tenemos buenas experiencias. Sin embargo, hubo un caso en el que el proveedor canceló un pedido que ya estaba pagado, por lo que tuvimos que tomar medidas legales y comprar urgentemente esos recursos a otro proveedor. Finalmente, conseguimos recuperar el dinero, pero una sección del Departamento de Almacenaje y Facturación estuvo paralizada durante unos días al no contar con esos recursos.

ANEXO 2: Situación actual de las empresas competidoras

Los gráficos de las Figuras 3.1 y 3.2 han sido obtenidos de una página Web que realiza análisis de mercado.

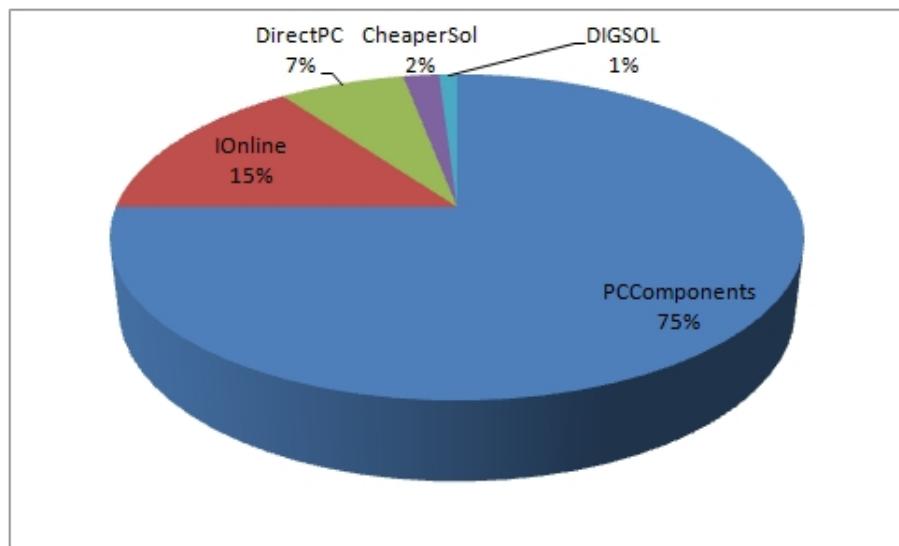


Figura 3.1: Porcentaje de inversión en investigación de nuevas tecnologías

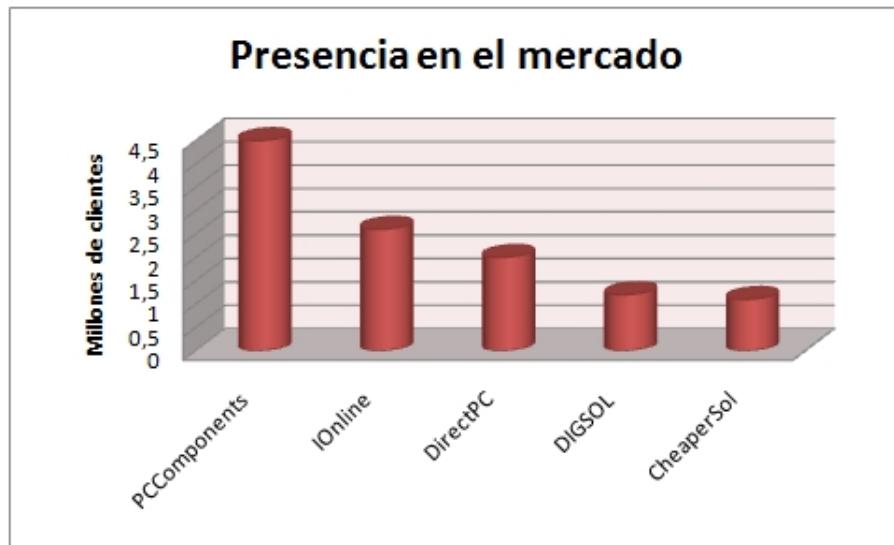


Figura 3.2: Presencia en el mercado de las empresas

ANEXO 3: Organigrama de la empresa DIGSOL

El organigrama mostrado en la Figura 3.3 ha sido cedido por el Comité de Dirección de la empresa DIGSOL.



Figura 3.3: Organigrama de la empresa DIGSOL

ANEXO 4: Adquisiciones tecnológicas

Los fragmentos de facturas mostradas en las Figuras 3.5 y 3.4 han sido cedidas por el Director de finanzas de la eomresa.

La Figura 3.4 muestra la adquisición que dicha empresa realizó a mediados del año

2008, cuando implantó el servicio de venta Web y actualizó los equipos de algunos de sus departamentos.

RECURSO	DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	PROVEEDOR
Base de datos Oracle Enterprise	Base de datos	1	259,85 €	259,85 €	Oracle
Equipo sobremesa	Equipos de trabajo para el departamento de almacenaje y para el de marketing	350	578,99 €	202.646,50 €	HP
Servidor	Servidor principal de la empresa	1	3.500,00 €	3.500,00 €	Dell
TOTAL					206.406,35 €

Figura 3.4: Fragmento de la factura del 17-Junio-2008

En la factura de la Figura 3.5 se muestra una de las últimas adquisiciones que ha realizado la empresa, remarcando gastos que podrían haberse evitado (en color amarillo) y gastos totalmente innecesarios que no aportan nada de beneficio al negocio (en color rojo).

RECURSO	DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	PROVEEDOR
Servidor	Servidor auxiliar para aumentar la capacidad del servidor principal	1	2.194,86 €	259,85 €	HP
Equipo sobremesa	Equipos de trabajo para el departamento de almacenaje	25	448,99 €	11.224,75 €	Acer
PDA	PDAs para el Comité de Dirección	7	539,00 €	3.773,00 €	Nokia
Bobina Cable UTP Cat. 6. (500m)	Cable UTP para cambiar cableado de red estropeado	10	389,56 €	3.895,60 €	CISCO
TOTAL					19.153,20 €

Figura 3.5: Factura del 27-Mayo-2009

ANEXO 5: Entrevista con uno de los desarrolladores informáticos de uno de los departamentos de la empresa

- **Auditor:** ¿Cuál es el cargo que desempeña usted en la empresa?

Soy uno de los desarrolladores que formamos el equipo de desarrollo del departamento de Almacenaje y Facturación.

- **Auditor:** ¿Puede indicarme las responsabilidades que tiene asignadas?

El equipo nos encargamos de desarrollar las aplicaciones que necesita este departamento para realizar su trabajo diario. También somos responsables de adquirir nuevos recursos (tanto hardware como software) y de mantenerlos.

- **Auditor:** ¿Quién aprueba las adquisiciones de tecnología?

Nosotros nos encargamos de elegir los recursos de entre diferentes proveedores y le pasamos el presupuesto a la Dirección.

- **Auditor:** ¿Cómo realizan la lista de proveedores?

Elegimos aquellos cuya relación calidad/precio es mejor, además de los proveedores con los que tenemos buenas impresiones personales.

- **Auditor:** Si el proveedor no entrega los recursos en fecha o hay algún problema, ¿cómo actúan?

Nos dirigimos a la Dirección e intentamos seguir haciendo el trabajo con los recursos disponibles. Nosotros sólo somos responsables de establecer los recursos que necesitamos y a qué proveedor los compramos. Es la Dirección quién debería tomar medidas a la hora de realizar los pedidos.

- **Auditor:** ¿Ha existido algún problema con algún pedido?

En una ocasión uno de los proveedores canceló un pedido sin dar explicaciones, por lo que tuvimos que realizar uno nuevo, pero una sección del departamento tuvo que estar paralizada unos días.

- **Auditor:** Volviendo al tema de los proyectos, ¿tienen definido un portafolio de proyectos?

En realidad, vamos desarrollando los proyectos según los empleados lo necesitan, pero no solemos asignar prioridades.

- **Auditor:** ¿Y qué sucede si hay un proyecto prioritario que la Dirección necesita para cumplir el objetivo de negocio de la empresa?

En ese caso, solemos dividir el equipo de desarrollo, para que una parte atienda ese proyecto prioritario y el resto atienda los proyectos normales y el resto de tareas de las que nos encargamos.

- **Auditor:** ¿Y tienen éxito siguiendo ese "método" de trabajo?

Muchas veces hemos tenido que echar bastantes horas extras, pero podemos entregar los proyectos en fecha. No podemos hacer otra cosa si la dirección no crea un Departamento especializado en estos temas y permite que nos limitemos únicamente a desarrollar.

ANEXO 6: Instalación y configuración inicial del software en equipos informáticos

En la Figura 3.6 se muestra la lista de software que será instalado en las computadoras. Como se puede apreciar, el documento es muy antiguo y no ha sido actualizado: las versiones del software están obsoletas, no se establece un criterio para aplicar parches y actualizaciones de seguridad, y no se establece una configuración de parámetros y servicios del sistema.

ANEXO 7: Vulnerabilidad a ataques informáticos

En la Figura 3.7 se muestra una gráfica que representa los crecientes ataques informáticos que se producen sobre la organización. Esto se puede deber a la falta de mantenimiento y seguimiento de la seguridad de los sistemas de información.

Instalación y configuración inicial del software en equipos informáticos.

A continuación se listan los programas y servicios que deberán ser instalados y configurados en los nuevos equipos adquiridos o formateados.

1. Windows XP Professional Service Pack 2
2. Microsoft Office 2000
3. Internet Explorer 7.
4. Avast 4 Professional Edition

Elaborado por	Felipe Juan García Antequera	Firma:		Fecha: 15 de Enero del 2008
Cargo	Gerente de configuración			
Revisado por	Antonio José Pérez Sánchez	Firma:		Fecha: 15 de Enero del 2008
Cargo	Jefe de desarrollo			
Aprobado por	Nohemy Antequera Sánchez	Firma:		Fecha: 17 de Enero del 2008
Cargo	Jefe de operaciones			

Figura 3.6: Lista de la configuración inicial de los equipos informáticos

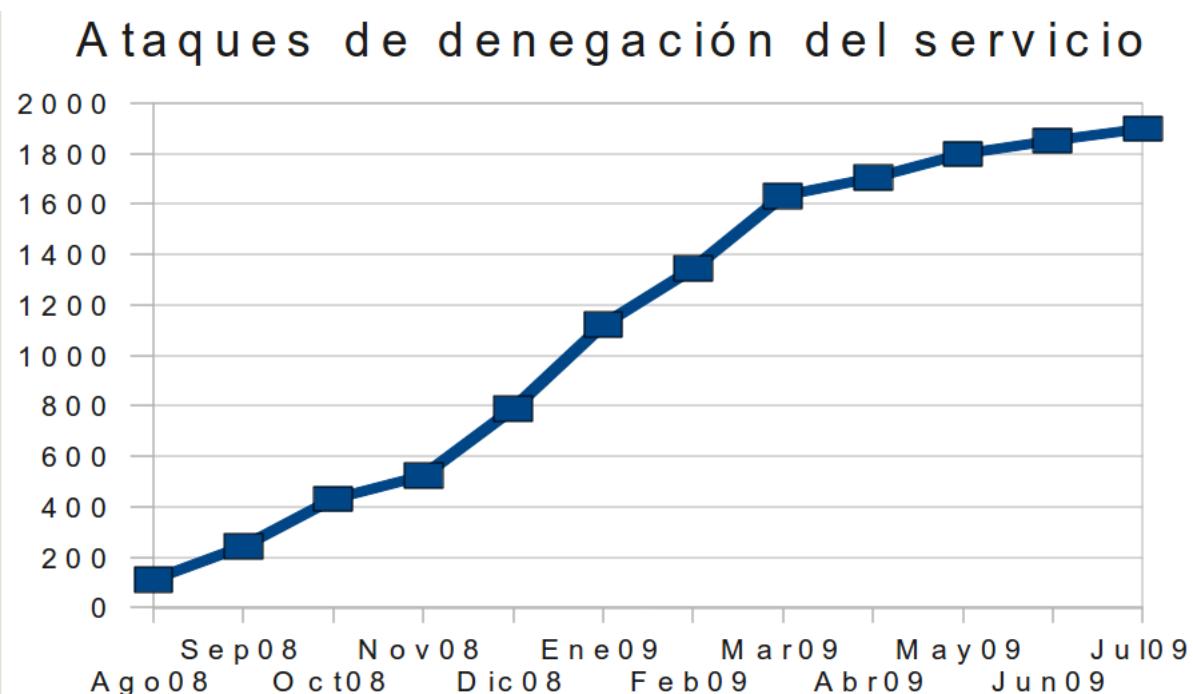


Figura 3.7: Número de ataques de Denegación del Servicio durante 12 meses

ANEXO 8: Adquisición de licencias por duplicado

En las Figuras 3.8 y 3.9 se muestran dos facturas, proporcionadas por el Director de finanzas, pertenecientes a los meses de Enero y Junio del 2009 respectivamente, en las cuales se adquieren 30 licencias de antivirus de 1 año de duración en cada una, haciendo un total de 60. Actualmente, la organización cuenta con 30 ordenadores por lo que el segundo pedido, que suma 676 euros, no estaba justificado. Esto se debe a que el repositorio central de licencias no fue actualizado cuando se hizo el primer pedido.

The screenshot shows a purchase invoice for avast! 4 Professional Edition, 1 year. The header includes the avast! logo, contact information for ALWIL Software a.s., and a date of 27 January 2009. The customer information section lists DIGSOL's address in Ciudad Real, Spain. The product details table shows one item: avast! 4 Professional Edition, 1 year, delivered electronically in quantities of 30 at a unit price of EUR 18.95. The subtotal is EUR 568.50, plus 19% sales tax/VAT: EUR 108.02, resulting in a total amount of EUR 676.52. A VISA payment method is indicated in the top right corner.

Product Name	Delivery	Qty.	Unit Price
avast! 4 Professional Edition, 1 year	electronic	30	EUR 18.95

Figura 3.8: Factura de adquisición de licencias de antivirus en Enero del 2009

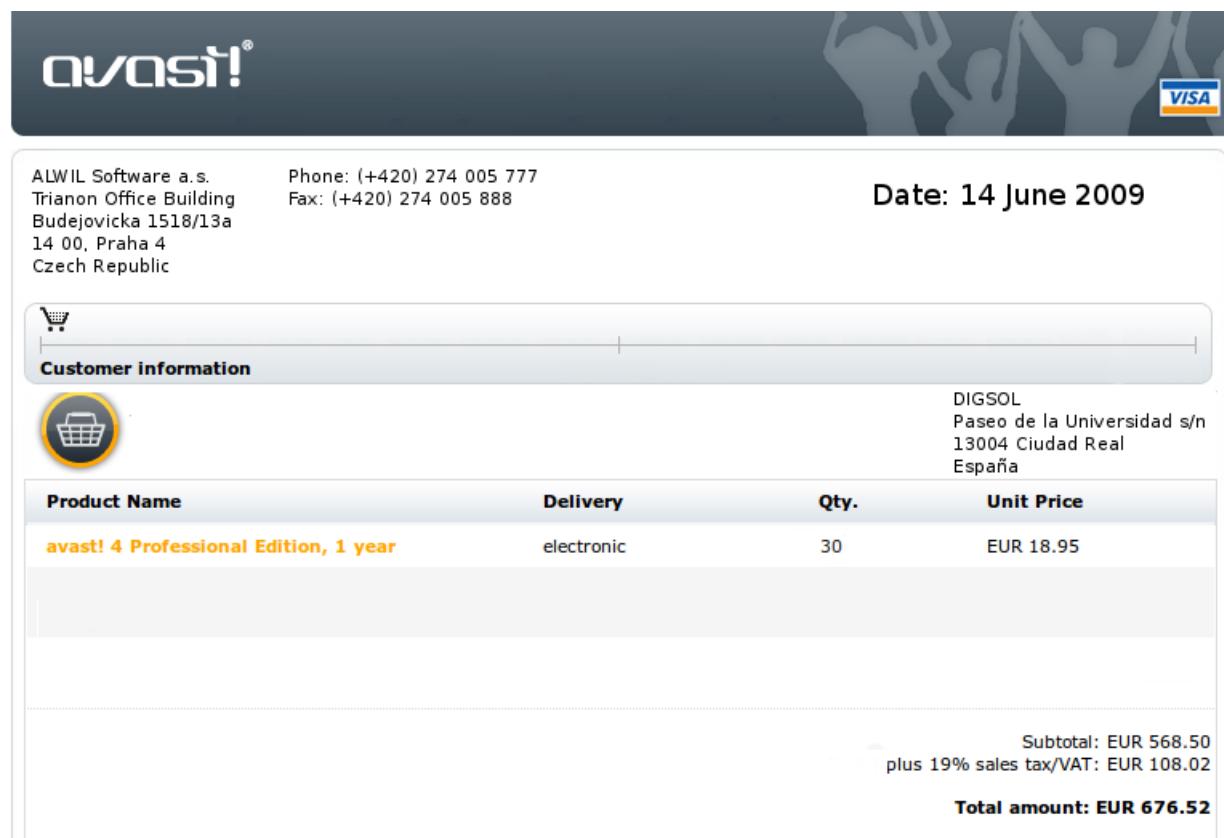


Figura 3.9: Factura de adquisición de licencias de antivirus en Junio del 2009

ANEXO 9: Software con licencias caducadas

En la Figura 3.10 se puede observar que, a pesar de haber adquirido licencias para el año 2009-2010 (ver Figura 3.8), aún se mantienen licencias caducadas en los equipos.

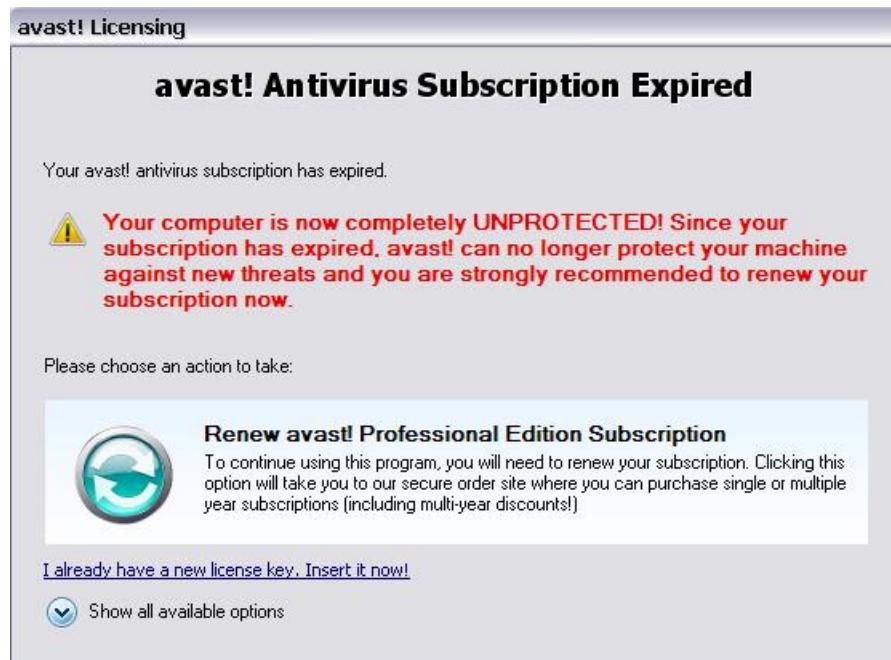


Figura 3.10: Captura de pantalla del estado de un antivirus

ANEXO 10: Software no corporativo

En la Figura 3.11 se muestra un caso en el que un empleado tiene instalado en su ordenador un juego de Poker Online. El software personal y no alineado con el negocio de la empresa puede introducir fallas de seguridad.

ANEXO 11: Cuentas de usuario

En la captura que se muestra en la Figura 3.13 se observan las cuentas de usuario que existen en el sistema. Existen riesgos debido a que sólo existen dos cuentas que son compartidas por todos los empleados de la empresa. También hay riesgo por pertenecer las dos cuentas al mismo grupo de usuarios.

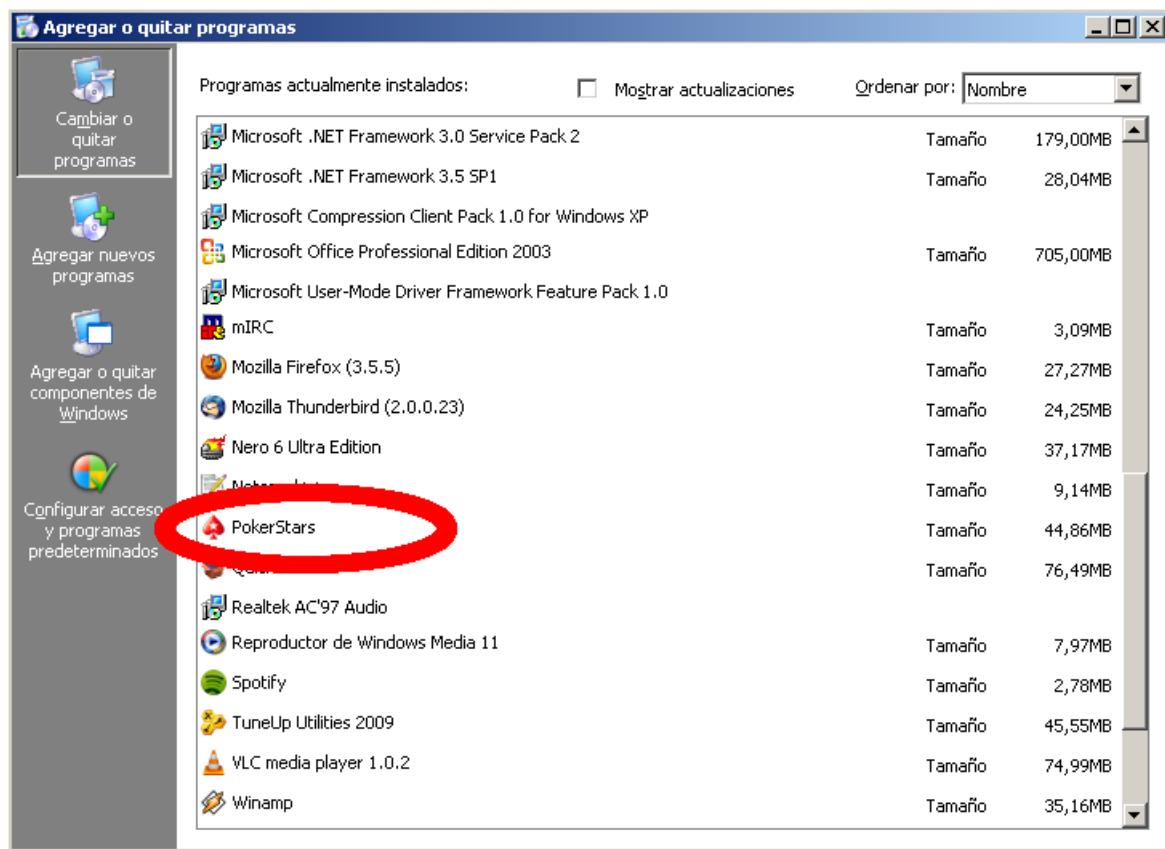


Figura 3.11: Software no alineado con la estrategia de negocio

ANEXO 12: Ubicación y permisos de los archivos de datos

En la captura que se muestra en la Figura 3.12 se observa que los archivos de datos con información sensible, relativa a la empresa, y los archivos de la web con datos de los productos que se venden, se almacenan en el mismo servidor y en la misma cuenta y carpeta. Además los permisos de los archivos son inadecuados para ficheros que contienen información delicada.

ANEXO 13: Seguridad de la red wifi

En la captura que se muestra en la Figura 3.14 se ve como con el programa Aircrack se puede desencriptar la red inalámbrica, por lo que la elección de un buen sistema de cifrado es muy importante para la seguridad en la red si no se puede prescindir de la conexión wifi.

```

digisol@DIGISOL:~>ls -lha
total 56K
drwxr-xr-x 7 digisol users 4,0K nov 13 11:19 .
drwxr-xr-x 7 root     root   4,0K nov 13 11:09 ..
-rw----- 1 digisol users  0 nov 13 11:09 .bash_history
-rw-r--r-- 1 digisol users 1,2K nov 13 11:09 .bashrc
drwxr-xr-x 2 digisol users 4,0K nov 13 11:09 bin
drwxr-xr-x 2 digisol users 4,0K nov 13 11:37 Documents
-rw-r--r-- 1 digisol users 1,6K nov 13 11:09 .emacs
drwxr-xr-x 2 digisol users 4,0K nov 13 11:09 .fonts
-rw-r--r-- 1 digisol users  861 nov 13 11:09 .inputrc
drwxr-xr-x 2 digisol users 4,0K nov 13 11:09 .mozilla
-rw-r--r-- 1 digisol users 1,1K nov 13 11:09 .profile
drwxrwxrwx 3 digisol users 4,0K nov 13 11:44 public_html
-rw----- 1 digisol users 1,3K nov 13 11:19 .viminfo
-rw-r--r-- 1 digisol users 1,9K nov 13 11:09 .xim.template
-rw xrwxrwxrwx 1 digisol users 1,5K nov 13 11:09 .xinitrc.template
digisol@DIGISOL:~>cd Documents/
digisol@DIGISOL:~/Documents> ls -lha
total 64K
drwxr-xr-x 2 digisol users 4,0K nov 13 11:37 .
drwxr-xr-x 7 digisol users 4,0K nov 13 11:19 ..
-rw-r--r-- 1 digisol users 10 nov 13 11:27 claves.dba
-rw-r--r-- 1 digisol users 10 nov 13 11:37 claves.mdb
-rw-r--r-- 1 digisol users 10 nov 13 11:27 claves.txt
-rw-r--r-- 1 digisol users 10 nov 13 11:37 claves.xls
-rw-r--r-- 1 digisol users 1,1K nov 13 11:09 .directory
drwxrwxrwx 1 digisol users 10 nov 13 11:19 empleados.dba
drwxrwxrwx 1 digisol users 10 nov 13 11:37 empleados.mdb
drwxrwxrwx 1 digisol users 10 nov 13 11:19 empleados.txt
drwxrwxrwx 1 digisol users 10 nov 13 11:37 empleados.xls
drwxrwxrwx 1 digisol users 25 nov 13 11:18 nominas.dba
drwxrwxrwx 1 digisol users 10 nov 13 11:37 nominas.mdb
drwxrwxrwx 1 digisol users 8 nov 13 11:17 nominas.txt
-rw-r--r-- 1 digisol users 10 nov 13 11:20 usuarios.dba
-rw-r--r-- 1 digisol users 10 nov 13 11:20 usuarios.txt
digisol@DIGISOL:~/Documents> cd ..
digisol@DIGISOL:~>cd public_html/
digisol@DIGISOL:~/public_html> ls -l
total 4
drwxrwxrwx 3 digisol users 4096 nov 13 12:11 venta_web
digisol@DIGISOL:~/public_html> cd venta_web/
digisol@DIGISOL:~/public_html/venta_web> ls -lha
total 48K
drwxrwxrwx 3 digisol users 4,0K nov 13 12:11 .
drwxrwxrwx 3 digisol users 4,0K nov 13 11:44 .
-rw xrwxrwxrwx 1 digisol users 0 nov 13 12:11 clientes.mdb
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:46 consumibles.html
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:46 cpus.html
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:45 discos.html
drwxrwxrwx 2 digisol users 4,0K nov 13 11:45 imagenes
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:45 impresoras.html
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:45 index.html
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:45 monitores.html
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:46 perifericos.html
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:46 peticiones.php
-rw xrwxrwxrwx 1 digisol users 5 nov 13 11:47 transacciones.php

```

Connected SSH2 - aes128-cbc - hmac-md5 - none 111x58

Figura 3.12: Ubicación y permisos de archivos inadecuados

```
digisol@DIGISOL:~>cat /etc/passwd
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
avahi:x:102:104:User for Avahi:/var/run/avahi-daemon:/bin/false
beagleindex:x:106:108:User for Beagle indexing:/var/cache/beagle:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
cyrus:x:96:12:User for cyrus-imapd:/usr/lib/cyrus:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
dhcpd:x:113:65534:DHCP server daemon:/var/lib/dhcp:/bin/false
fetchmail:x:114:2:mail retrieval daemon:/var/lib/fetchmail:/bin/false
flumotion:x:110:100::/var/lib/flumotion:/sbin/nologin
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
ftpsecure:x:108:65534:Secure FTP User:/var/lib/empty:/bin/false
games:x:12:100:Games account:/var/games:/bin/bash
gnump3d:x:63:65534:GNUMP3 daemon:/var/lib/nobody:/bin/false
haldaemon:x:104:106:User for haldaemon:/var/run/hal:/bin/false
icecast:x:109:113:Icecast streaming server:/var/lib/icecast:/bin/false
icecream:x:115:120:Icecream Daemon:/var/cache/icecream:/bin/false
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
mailman:x:72:67:GNU mailing list manager:/var/lib/mailman:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:101:103:User for D-Bus:/var/run/dbus:/bin/false
mysql:x:60:119:MySQL database admin:/var/lib/mysql:/bin/false
nagios:x:112:116:User for Nagios:/var/lib/nagios:/bin/false
named:x:44:44:Name server daemon:/var/lib/named:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:102:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:105:PolicyKit:/var/run/PolicyKit:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
pulse:x:107:110:PulseAudio daemon:/var/lib/pulseaudio:/sbin/nologin
quagga:x:111:115:Quagga routing daemon:/var/run/quagga:/usr/bin/false
root:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
suse-ncc:x:105:107:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
tomcat:x:116:121:Apache Tomcat:/usr/share/tomcat6:/bin/sh
upsd:x:117:2:UPS daemon:/sbin:/bin/false
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
uuidd:x:100:101:User for uuidd:/var/run/uuidd:/bin/false
vscan:x:65:118:Vscan account:/var/spool/amavis:/bin/false
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
digisol:x:1000:100:digisol:/home/digisol:/bin/bash
empleado:x:1001:100:empleado:/home/empleado:/bin/bash
```

Figura 3.13: Usuarios del sistema

```
aircrack 2.3
[00:00:05] 204 keys tested (34.53 k/s)
KEY FOUND! [ W0I1F2I3D4E5M60 ]
Master Key : 5D ED FC 40 4C 3B C2 04 9E 19 4C 18 BA 7D 52 39
              43 46 F9 73 C7 3A D9 BD B9 A4 58 C5 A5 F2 00 A5
Transient Key : FF 3C 9D C5 D7 76 6C 09 1D C4 6E 45 E8 DA 1E 1A
                  47 B3 C9 76 3F D6 CD 6D 30 1D 39 8D 1A 10 DA 7A
                  85 1E 0B 4B 4B 2C B8 0D 08 03 A1 E7 1D 9E 62 71
                  A8 32 0E 10 88 94 77 36 FE EA 6D 90 43 78 76 BC
EAPOL HMAC : BA 8A CA CA DC 66 B1 56 0B 88 FB 38 54 56 D2 D9
Press Ctrl-C to exit.
```

Figura 3.14: Programa que desencripta la wifi

ANEXO 14: Vulnerabilidad del servidor

En la captura que se muestra en la Figura 3.15 se ve como el servidor carece de las medidas de seguridad necesarias, además de tener una ubicación deficiente.



Figura 3.15: Servidor vulnerable

ANEXO 15: Copias de seguridad e información accesible

En la captura que se muestra en la Figura 3.16 se ven los cajones en los que se guarda el disco con los datos de respaldo, pero no se cierran con llave.



Figura 3.16: Cajones donde se guarda el disco de respaldo

ANEXO 16: Ficheros de log

En la captura que se muestra en la Figura 3.17 se ven los ficheeros de log, poco detallados y con poca información.

ANEXO 17: Estanterías desprotegidas

En la captura que se muestra en la Figura 3.18 se ven las estanterías donde se almacenan los documentos de la empresa, pero estas carecen de medidas de seguridad.

ANEXO 18: Ordenadores abiertos

En la captura que se muestra en la Figura 3.19 se ve que algunos empleados abren las tapas de sus ordenadores, lo que provoca que estos puedan ser vulnerados.

```

CELONA/O=systemadmin.es/CN= [REDACTED] @systemadmin.es
May 22 05:55:55 shuVak openvpn[20976]: [REDACTED] Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
May 22 05:55:55 shuVak openvpn[20976]: [REDACTED] Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
May 22 05:55:55 shuVak openvpn[20976]: [REDACTED] Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
May 22 05:55:55 shuVak openvpn[20976]: [REDACTED] Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
May 22 05:55:55 shuVak openvpn[20976]: [REDACTED] Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
[00] /var/log/messages 435283 - May 22 07:56:28 2009
May 22 07:53:01 shuVak sudo: nagios : TTY=unknown ; PWD=/usr/local/supervisord/nagios ; USER=root ; COMMAND=/usr/local//libexec/check_cuaqmail -w 25 -c 100
May 22 07:53:02 shuVak sudo: nagios : TTY=unknown ; PWD=/usr/local/supervisord/nagios ; USER=root ; COMMAND=/usr/bin/tail -n 500 /var/log/maillog
May 22 07:53:31 shuVak sudo: nagios : TTY=unknown ; PWD=/usr/local/supervisord/nagios ; USER=root ; COMMAND=/usr/local//libexec/check_procs -w 250 -c 400 -s RSZDT
May 22 07:53:33 shuVak sudo: nagios : TTY=unknown ; PWD=/usr/local/supervisord/nagios ; USER=root ; COMMAND=/usr/local//libexec/check_procs -c 1:1024 -C clamd
May 22 07:54:52 shuVak sudo: nagios : TTY=unknown ; PWD=/usr/local/supervisord/nagios ; USER=root ; COMMAND=/usr/local//libexec/check_procs -s Z -c 0}
[01] /var/log/secure 1408867 - May 22 07:56:28 2009
Mar 20 23:36:02 Installed: graphviz - 2.12-8.el5.x86_64
Mar 20 23:36:02 Installed: libXaw - 1.0.2-8.1.i386
Mar 20 23:36:02 Installed: libtool-ltdl - 1.5.22-6.1.i386
Mar 20 23:36:03 Installed: graphviz - 2.12-8.el5.i386
Mar 20 23:36:03 Installed: graphviz-devel - 2.12-8.el5.i386
Mar 20 23:36:04 Installed: graphviz-devel - 2.12-8.el5.x86_64
Mar 20 23:39:53 Installed: expat-devel - 1.95.8-8.2.1.i386
Mar 20 23:39:54 Installed: expat-devel - 1.95.8-8.2.1.x86_64
Apr 01 13:57:11 Installed: iperf - 2.0.4-1.el5.x86_64
Apr 23 09:17:35 Updated: sudo - 1.6.9p17-3.el5_3.1.x86_64
[02] /var/log/yum.log 27166 - May 22 07:56:28 2009

```

Figura 3.17: Ficheros de log

ANEXO 19: Ordenadores sin bloquear

En la captura que se muestra en la Figura 3.22 se ve un ordenador que no ha sido bloqueado cuando el empleado ha abandonado su puesto de trabajo.

ANEXO 20: Soportes de datos mal destruidos

En la captura que se muestra en la Figura 3.20 se ve en la papelera un disco duro. Contiene información en su interior y es accesible facilmente.

ANEXO 21: Papeles con datos mal destruidos

En la captura que se muestra en la Figura 3.21 se ve en la papelera un conjunto de documentos eliminados de forma incorrecta. Contienen información y es accesible facilmente.



Figura 3.18: Estanterías con documentos



Figura 3.19: Ordenador sin tapas



Figura 3.20: Disco duro destruido incorrectamente

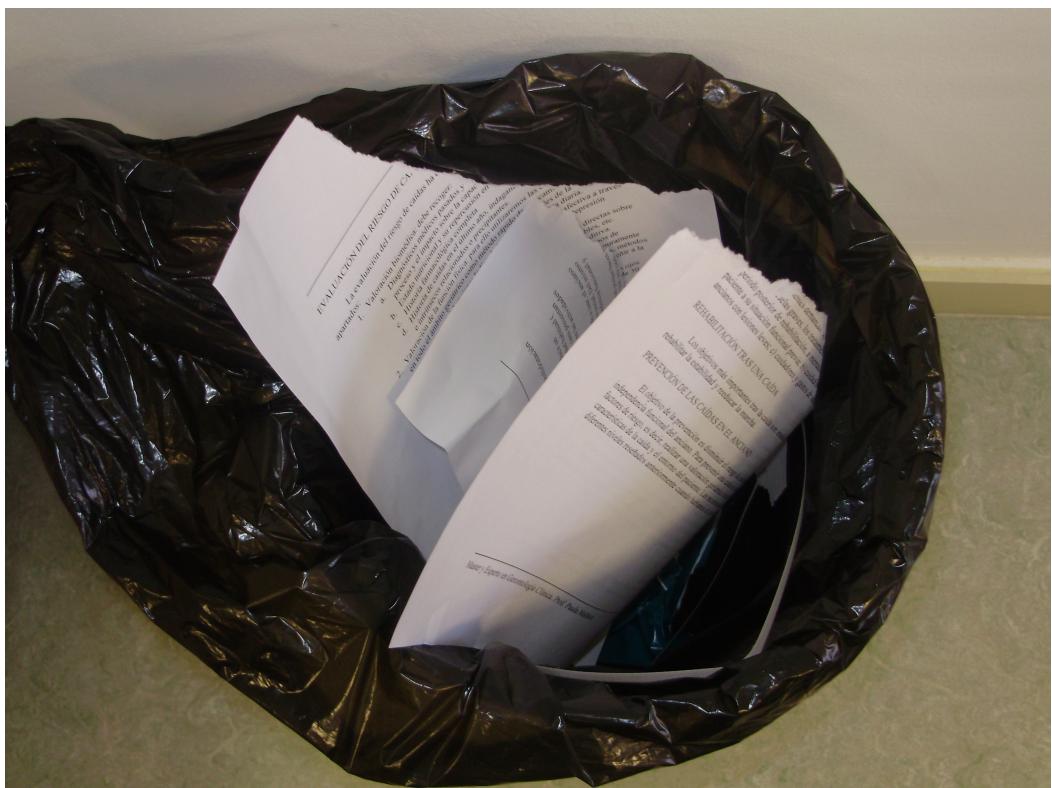


Figura 3.21: Papeles destruidos incorrectamente

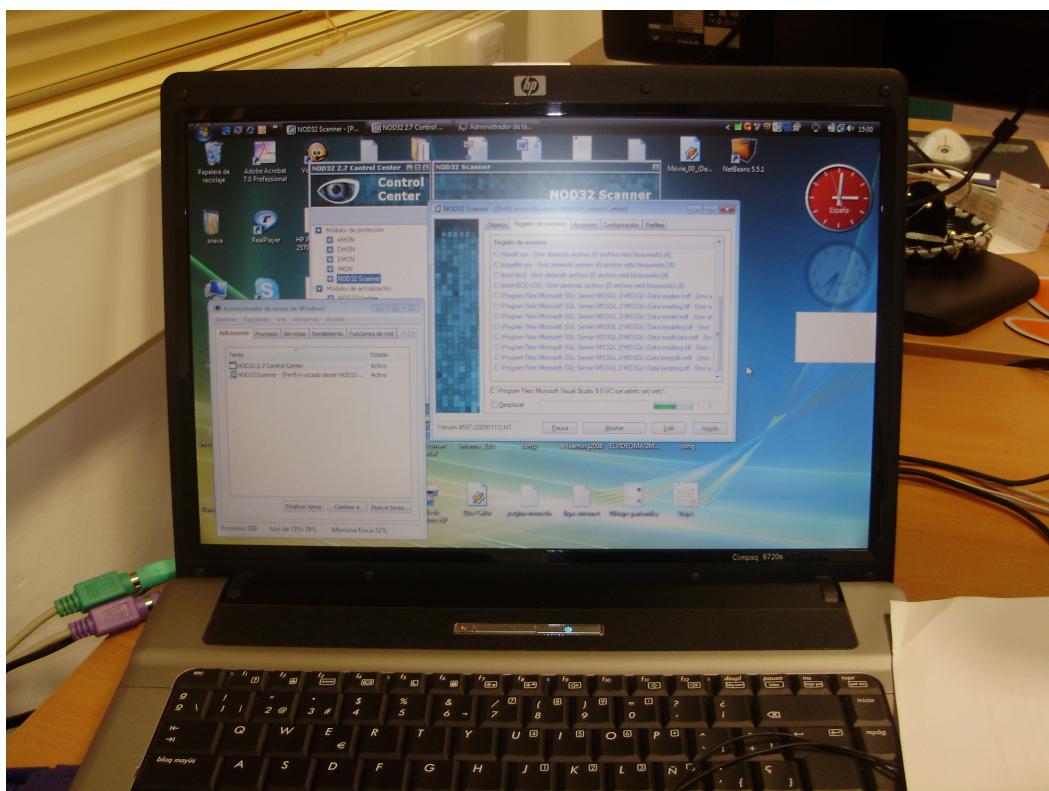


Figura 3.22: Ordenador sin bloquear

ANEXO 22: Acta de evaluación y gestión de riesgos

Un aspecto a destacar en los riesgos seleccionados y planificados es que se ciñen al ámbito software dejando de lado el ámbito hardware, no teniendo en cuenta, por ejemplo, factores externos sobre los cuales la organización puede no tener ningún control debido a su naturaleza (terremotos, colisiones de aviones, etc) o incluso el robo de material o incendios.

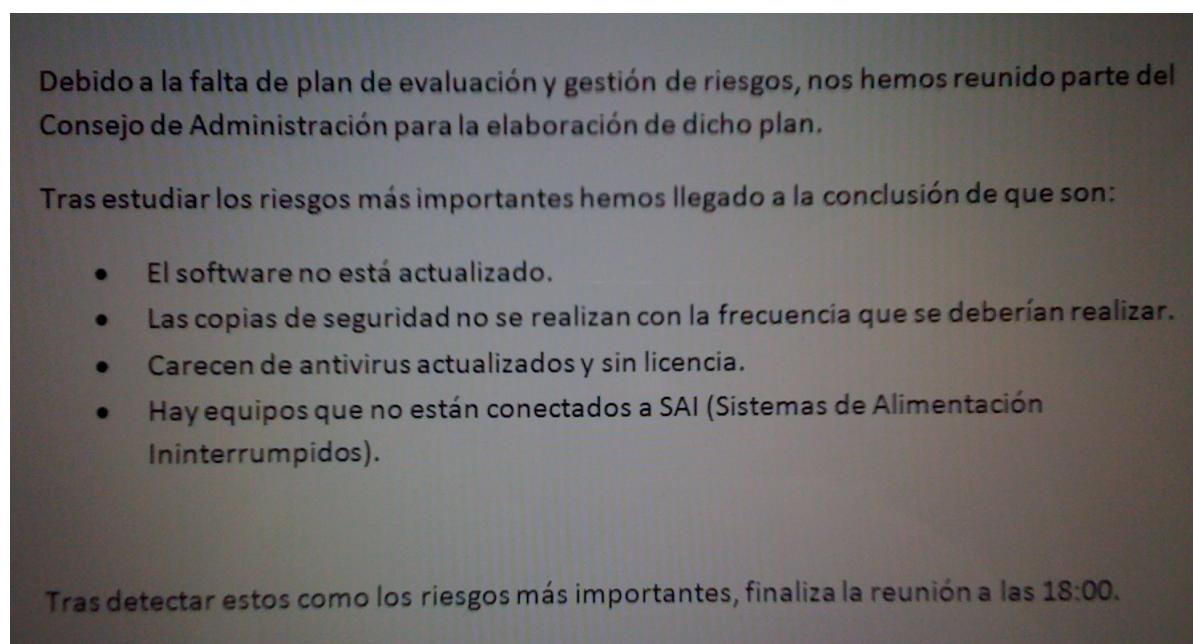


Figura 3.23: Acta de evaluación y gestión de riesgos

Como vemos se han identificado una serie de riesgos pero que no se han tomado medidas para solucionarlos, o no se ha dejado constancia de ello.

ANEXO 23: Copias de seguridad

Las copias de seguridad no son almacenadas correctamente.

Carecen de un sitio fijo donde almacenarlas y suelen estar en cajones o mesas como se muestra en la Figura.

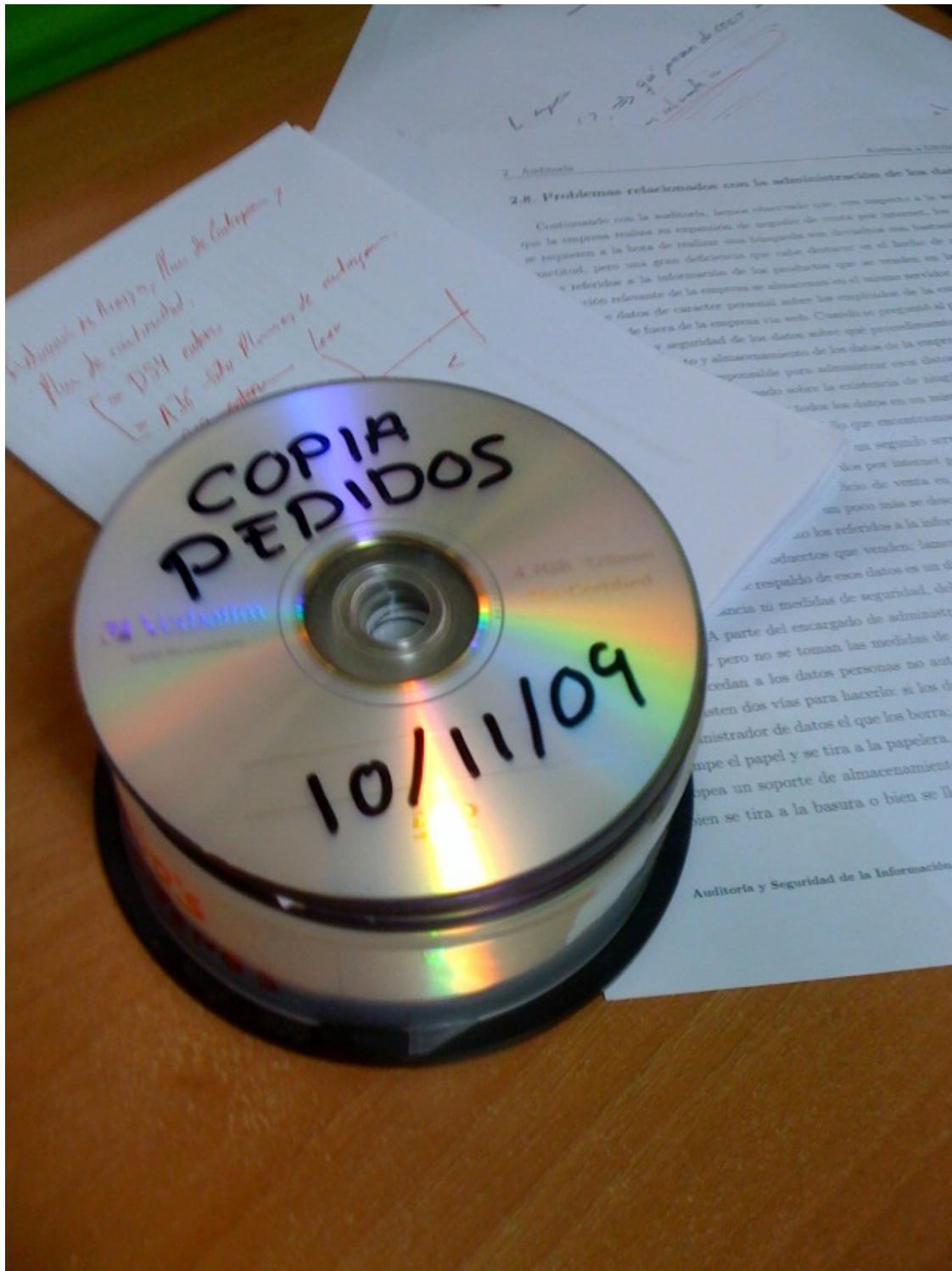


Figura 3.24: Copias de seguridad de los pedidos