

¿Cómo puedo proteger los datos de mi empresa?

Conozca los peligros informáticos que amenazan
a su negocio y la mejor forma de prevenirlos

¿Están seguros los datos de su empresa?

Seguramente, NO.

Aunque siete de cada diez empresas españolas ha sufrido problemas de seguridad informática¹, apenas la mitad cuenta con alguien a cargo de este asunto. En más del 60% de los casos, el único sistema de seguridad es un antivirus y pocas PYMES están protegidas contra nuevas amenazas como el software espía (10%) o el correo electrónico no deseado (5,5%)². Incluso a nivel legal, apenas una de cada diez cumple con las medidas de seguridad que determinan normativas como la Ley Orgánica de Protección de Datos³. ¿Es su empresa una excepción?

A nivel mundial, los fallos de seguridad cuestan entre el 5 y el 7% de los ingresos anuales de las empresas⁴. El 8% de las PYMES españolas ha tenido que interrumpir o incluso cesar su actividad tras ser infectada por un virus informático⁵. Sólo la inofensiva tarea de borrar los mensajes comerciales no deseados (spam) cuesta una media de 15 minutos al día por empleado, una jornada entera de trabajo cada mes, 25.000 millones de euros al año en pérdidas de productividad para el conjunto de las empresas europeas⁶. ¿Cuánto le está costando a usted?

Podría ser peor. El Banco Central de Rusia sufrió el robo de sus listados de operaciones de los dos últimos años, que ahora se pueden comprar en Internet por 85€; CitiBank perdió los datos de un millón de clientes a causa de un fallo en las copias de seguridad; Bank of America descubrió recientemente que algunos empleados habían estado vendiendo al mejor postor información sobre 670.000 clientes⁷. Sin ir tan lejos, tras el incendio de la Torre Windsor, las empresas Deloitte y Garrigues tuvieron que aplazar más de 10.000 procesos judiciales por no tener copias de seguridad, sufriendo un gran deterioro de imagen frente a sus clientes⁸.

Si está totalmente convencido de que su empresa es segura, pase este documento a algún colega menos precavido; si tiene dudas, siga leyendo y descubrirá que mejorar la protección de su negocio depende más del sentido común que de gastar mucho dinero.

Internet o la puerta del infierno

La mayoría de problemas de seguridad informática proviene de Internet y el correo electrónico. En una comunidad de casi 1.000 millones de usuarios⁹ que se desarrolla vertiginosamente, aparecen nuevas amenazas a diario.

Virus y troyanos: los **virus** son el peligro informático más conocido. Estos pequeños programas nacieron como bromas entre estudiantes, pero han acabado convirtiéndose en una pesadilla. En los seis primeros meses de 2005 se registraron en España más de 2.500 alertas de virus¹⁰, cuyos efectos van desde abrir y cerrar la bandeja del CD-ROM (con el consiguiente susto para el usuario) a borrar todo el contenido del disco duro, o cifrarlo y exigir dinero para liberarlo. Sólo el virus Slammer colapsó en 2003 más de 200.000 servidores en 48 horas, afectando especialmente a las universidades españolas¹¹.

Los **troyanos** o "caballos de Troya" son una variante de los virus que se oculta para actuar sin que el usuario se dé cuenta, destruyendo información o abriendo las puertas del sistema a ataques externos.

¹Estudio sobre el estado actual de la seguridad de los sistemas de información en las empresas ASIMELEC 2003.

²Estudio Niveles de Protección en la PYME Española 2005 de Red.es, Panda Software y Asociación de Internautas

³Declaraciones del director de la Agencia Española de Protección de Datos a Diario Atlántico Abril 2005

⁴Estudio de Omni Consulting Group 2005

⁵Estudio Niveles de Protección en la PYME Española 2005 de Red.es, Panda Software y Asociación de Internautas

⁶Comparecencia en el Senado del Director de la Agencia Española de Protección de Datos Mayo 2005

⁷Pocas organizaciones inscriben sus ficheros en la Agencia de Protección de Datos artículo El País Junio 2005

⁸Artículo en web de Belt Ibérica Febrero 2005

⁹Unión Internacional de las Telecomunicaciones (ITU) Internet World Stats, Marzo 2005

¹⁰Servicio de Análisis, Notificación y Alertas (SANA) de Hispasec

¹¹Los equipos españoles de seguridad cumplen un década de lucha artículo de El País Julio 2005

¿Qué puedo hacer?

- Nunca abra o ejecute un archivo desconocido
- Instale las actualizaciones del sistema operativo y los programas
- Compre un software antivirus y manténgalo actualizado
- Escanee con un antivirus cualquier soporte sospechoso
- Haga revisar los equipos ante comportamientos extraños
- Contrate un servicio de correo electrónico con antivirus
- Instale un firewall
- Limite el acceso a sitios web y servicios inseguros
- Disponga de una copia de seguridad o imagen del registro del sistema

Spam y phishing: hasta seis de cada diez mensajes recibidos por un usuario contienen información comercial no deseada¹². Aunque muchas ofertas son fraudes, uno de cada diez usuarios de correo electrónico acaba comprando productos promocionados mediante **spam**¹³. Además de las estafas y de saturar el correo, el spam genera pérdidas de tiempo y productividad al tener que eliminar manualmente los mensajes. También puede ser una amenaza a la inversa: si su empresa envía comunicaciones comerciales sin tener en cuenta la ley, se arriesga a multas de hasta 600.000€¹⁴.

El **phishing** (o pesca de contraseñas) es una variante del spam que consiste en mandar mensajes en nombre de una empresa o institución para que el receptor visite un sitio web falso y facilite sus contraseñas bancarias y números de tarjetas de crédito. En los seis primeros meses de 2005, más de 34.500 empresas y usuarios españoles sufrieron estos intentos de fraude electrónico¹⁵, que afectan a sectores como banca, administración pública o recarga de tarjetas telefónicas. En la modalidad llamada **pharming** se manipula el navegador del usuario, para mostrarle una página falsa aunque escriba la dirección correcta.

¿Qué puedo hacer?

- Nunca haga caso ni responda mensajes de desconocidos
- Desconfíe de ofertas y chollos
- No facilite su dirección de e-mail a cualquiera
- Disponga de un segundo e-mail para envíos publicitarios
- Compruebe cualquier mensaje en nombre de su empresa
- Mantenga confidenciales sus contraseñas
- Revise periódicamente sus cuentas bancarias
- Consulte con su banco cualquier petición extraña
- Registre su dominio en un proveedor autorizado
- Contrate un servicio de correo electrónico con antispam
- Instale un firewall
- Limite el intercambio de mensajes con chistes, videos, fotos, etc. en la empresa
- Forme a sus empleados
- Instale sistemas de autenticación en sus contratos y pedidos online
- Legalice sus bases de datos

¹²Estudio de Symantec 2005

¹³Estudio de Radicati Group 2005

¹⁴Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico

¹⁵Global Business Security Index Report IBM 2005

¹⁶Estudio de las empresas Webroot y Earthlink 2005

Software malicioso e ingeniería social: el 90% de los PCs conectados a Internet oculta una media de 25 programas **malware**¹⁶, software malicioso de legalidad dudosa que intenta obtener beneficios a costa del usuario. Existen programas espía (**spyware**) que anotan las webs visitadas para vender información sobre sus aficiones a empresas dedicadas al spam. Otros programas desvían la página de inicio para que siempre empiece a navegar en una web determinada; o cambian su conexión a un sistema de

pago por marcaje telefónico (**dialer**). El malware suele ocultarse en programas y documentos aparentemente inofensivos como juegos, chistes, fotos curiosas, etc.

La **ingeniería social** aprovecha la falta de conocimientos y la buena fe de los usuarios para inducirles a provocar daños. La técnica más conocida es el **bulo** (hoax), una falsa alerta de seguridad que provoca que el usuario realice alguna acción supuestamente preventiva que acaba siendo destructiva (como borrar archivos del registro de Windows). Otros bulos siembran la confusión, anunciando por ejemplo el cierre inminente del popular servicio de correo Hotmail. También hay mensajes curiosos (como el que ofrecía gatitos vivos dentro de botellas de cristal) para que el usuario los reenvíe a sus contactos; así el creador del bulo va recolectando direcciones de e-mail activas que luego venderá a empresas que envían spam.

¿Qué puedo hacer?

- Forme a sus empleados
- Actualice su sistema operativo y navegador de Internet
- Descargue programas solamente de sitios de confianza
- No instale ningún software si no está seguro de qué es
- Instale y mantenga actualizado un programa contra el malware o un antivirus con esta prestación.
- Limite el intercambio de mensajes con chistes, videos, fotos, etc. en la empresa.
- Limite la posibilidad de instalar programas y modificar la configuración a los usuarios que lo necesiten

Ataques e intrusiones: los piratas informáticos aprovechan los fallos de seguridad y los descuidos de los usuarios para apuntarse un tanto "tumbando" una web conocida o cotilleando en las entrañas de una empresa. No siempre se trata de desconocidos: los ataques más dañinos suelen ser obra de empleados descontentos o despedidos (70%)¹⁷. En cualquier caso, las consecuencias de un ataque informático pueden ser devastadoras: interrupción del servicio, robo de datos sensibles, borrado de información, deterioro de la imagen de la empresa...

¿Qué puedo hacer?

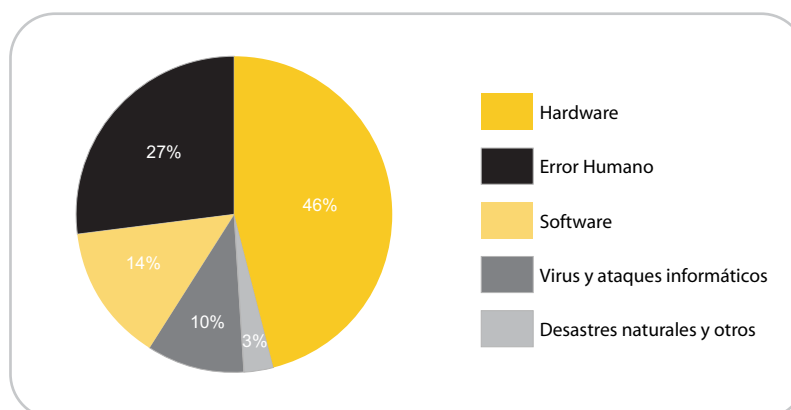
- Revise frecuentemente el funcionamiento de su web y aplicaciones
- Encargue el diseño y programación de su web y aplicaciones a profesionales de confianza
- En caso de despido conflictivo, haga revisar el sistema
- Utilice equipos distintos para trabajar y para Internet
- Cifre los datos importantes que vaya a transmitir
- Instale un firewall y revise los informes que genera
- Contrate una red privada virtual (VPN) para interconectar sus equipos informáticos
- Contrate un servicio de detección de intrusiones (IDS)
- Aloje su web o su servidor en un centro de datos de alta seguridad

¹⁷ *Consejos de Seguridad para las PYMES* en la web de la Unidad de Delitos Telemáticos de la Guardia Civil

¿Qué pasó con mis datos?

Pese a la amenazadora fauna de virus, troyanos, spam, hoaxes, spyware, etc. que puebla Internet, la mayoría de pérdidas de datos en las empresas son provocadas por otras causas: fallos de hardware y software y errores humanos.

Causas de pérdidas de datos



*Gráfico elaborado con datos de las empresas Recovery Labs, Ontrack, Stellar, VaultLogix y Graziadio Consulting

Fallos de hardware y software

El disco duro es el componente de hardware más crítico. Un problema en este dispositivo suele comportar que se pierdan datos, ya que es donde se almacena la información. Un pequeño porcentaje de los discos duros sufre defectos de fabricación (en 2004 Fujitsu tuvo que sustituir más de 200.000 unidades¹⁸) y todos son especialmente sensibles a los golpes, altas temperaturas y oscilaciones eléctricas. La ola de calor del verano de 2003 aumentó un 33% el número de empresas españolas que perdieron datos al fallar los discos duros por sobrecalentamiento¹⁹.

También los fallos de software provocan pérdidas de información. Normalmente el fabricante corrige el problema mediante un parche del programa, aunque sirve de poco si ya hemos sufrido el error. Sólo el sistema operativo Windows XP tiene más de 200 correcciones de seguridad. Y no parece que este problema vaya a reducirse: el 48% de los responsables tecnológicos de las empresas opina que los fallos de software tienden a aumentar²⁰.

A veces, la pérdida de datos está provocada por la incompatibilidad entre las distintas aplicaciones que utiliza una empresa; o por una migración mal planificada a aplicaciones superiores o a sistemas integrados de gestión empresarial (ERP/CRM).

¹⁸Noticia en PC World Online
18/09/02

¹⁹Entrevista a Galo Mateos,
Recovery Labs en LiderDigital.com
Septiembre 2003

²⁰Informe *The Chaos Report* de
Standish Group 1994

¿Qué puedo hacer?

- Compre productos de marcas y tiendas de confianza
- Nunca instale productos pirata
- Utilice productos del mismo fabricante o 100% compatibles

- Contrate un informático profesional o un servicio de mantenimiento
- Registre los programas y manténgalos actualizados
- Compre equipos con discos duros redundados para las tareas más críticas
- Realice copias de seguridad de los datos importantes y guárdelas fuera de la oficina
- Integre las diversas aplicaciones y bases de datos de su negocio en un único programa de gestión
- Externalice su servidor a un centro de datos

Errores humanos y robos

Algunas empresas especializadas llegan a relacionar con la intervención humana hasta el 83% de las pérdidas de datos²¹. En la mayoría de casos el incidente es debido al desconocimiento de las herramientas utilizadas y de las normas elementales de seguridad informática. Las anécdotas de los servicios técnicos son muy reveladoras: desde usuarios que cepillan el teclado con agua y jabón a los que consiguen introducir más de un disquete o CD-ROM a la vez por la misma ranura²². Muchos incidentes son provocados, aunque parezca sorprendente, por ataques de ira: uno de cada cinco usuarios ha golpeado alguna vez su ordenador y el 75% lo insulta habitualmente²³.

Otra gran fuente de pérdidas de datos por intervención humana son los robos: cada año desaparece en Europa medio millón de ordenadores portátiles²⁴, la mayoría en aeropuertos, hoteles y ferias.

¿Qué puedo hacer?

- Forme a su personal en ofimática
- Procure que la información clave no dependa de una sola persona
- Conciencie a los empleados de que son responsables de los daños en los equipos informáticos
- Establezca niveles de acceso a la información según el puesto
- Realice un inventario de equipos informáticos y asegúrelos
- Controle quién tiene llaves y tarjetas de acceso
- Instale alarmas, puertas y ventanas de seguridad
- Nunca pierda de vista su portátil, PDA, móvil, etc.
- Procure no llevar encima más información de la necesaria
- Cree contraseñas seguras en los equipos y aplicaciones
- Cambie las contraseñas frecuentemente
- Impida que los documentos importantes queden a la vista.
- Limpie el disco duro antes de deshacerse de un ordenador
- Limite el uso de soportes tipo CD, DVD, llaveros USB y similares a razones de trabajo
- Instale hardware y software de protección para portátiles (candados, bloqueo, encriptación, rastreo, etc.)
- Realice copias de seguridad de los datos importantes y guárdelas fuera de la oficina
- Facilite un acceso seguro al servidor corporativo para los empleados móviles
- Realice copias de seguridad en línea de los equipos portátiles
- Haga firmar un contrato de confidencialidad a los empleados clave
- Establezca sistemas de cifrado en las comunicaciones inalámbricas
- Encargue una auditoría de seguridad informática
- Instale un sistema de video-vigilancia en la oficina
- Instale un sistema de control de acceso basado en biometría

²¹ *Data Disaster Recovery for SMBs*
LiveVault 2005

²² Casos reales de los servicios técnicos de IBM y Dell publicados por el Wall Street Journal en 2001

²³ *Costly computer rage* BBC 1999

²⁴ *Not all the PCs are the same*
IBM Personal Systems Group 2004

Catástrofes y desastres naturales

Es imposible hasta que sucede: mientras se construye un edificio, una viga aplasta el portátil que contiene el único plano de la obra; cae un rayo y se borran 1.200 expedientes de una empresa médica; se inunda una fábrica y desaparecen cuatro años de documentos contables; arden las oficinas de una red de concesionarios de coches y se esfuman todos los documentos y archivos²⁵. Las pérdidas de datos asociadas a catástrofes son poco frecuentes, pero cuando suceden ponen en peligro la propia continuidad del negocio. Tras el primer ataque contra el World Trade Center de Nueva York en 1993, 147 de las 450 empresas del complejo cerraron durante un año por no disponer de un plan frente a este tipo de desastres. Algunas no volvieron a abrir nunca.

¿Qué puedo hacer?

- Adopte medidas de protección contra incendios e inundaciones
- Realice un inventario de los equipos y la información que contienen
- Instale un Sistema de Alimentación Ininterrumpida en el servidor y los equipos más importantes
- Identifique junto a sus empleados los procesos y datos clave
- Guarde copias de seguridad de los datos importantes en otra ubicación o al menos en armarios de seguridad
- Externalice su servidor a un centro de datos
- Contrate un plan continuidad de negocio

²⁵Casos reales de las webs de las empresas OnTrack Recovery, Recovery Labs y Data Recovery Unlimited.

La ley que nadie cumple

Proteger adecuadamente los datos de su empresa también puede evitarle serios problemas legales. La Ley Orgánica de Protección de Datos (LOPD), por ejemplo, obliga a limitar el acceso a los ficheros con datos de carácter personal, garantizar su confidencialidad y realizar una copia de seguridad semanal a otra ubicación encriptando los datos durante la transmisión. Aunque las sanciones pueden llegar a los 600.000€, apenas el 10% de las PYMES cumple estas estipulaciones²⁶.

Otro 42% de las empresas incumple la Ley de Servicios de la Sociedad de la Información (LSSI), sobretudoo al enviar e-mails publicitarios sin contar con la autorización del receptor²⁷. Se arriesgan a sanciones contundentes: la Agencia de Protección de Datos ha llegado a multar con 30.000 euros a un comercial por enviar un mensaje a 13 personas sin su consentimiento²⁸.

El desconocimiento y la falta de medidas de seguridad informática puede comportar además complicaciones en ámbitos como la propiedad intelectual, el secreto de las comunicaciones o el derecho a la intimidad, con multas, inhabilitaciones y penas de hasta cuatro años de cárcel²⁹.

²⁶Declaraciones del director de la Agencia Española de Protección de Datos a Diario Atlántico Abril 2005

²⁷Estudio sobre el cumplimiento de la LOPD y de la LSSI de Grupo Penteo y Landwell-PwC Mayo 2004

²⁸La Letra de la LOPD se aprende a base de multas artículo El Mundo Julio 2005

²⁹Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

¿Qué puedo hacer?

- Establezca controles en el acceso a datos sensibles como currículums, expedientes médicos, etc.
- Controle el envío de comunicaciones comerciales de su empresa
- Consulte con su asesor cualquier duda sobre gestión de datos
- Encripte la información confidencial antes de transmitirla
- Realice copias de seguridad de la información confidencial
- Encargue una auditoría legal sobre su empresa

Externalizar, una opción a tener en cuenta

Si no dispone de personal especializado o no desea afrontar grandes inversiones, la externalización puede ser una buena solución para mejorar la seguridad y la gestión de la informática en su negocio. Actualmente el 33% de las empresas españolas externaliza sus sistemas de tecnologías de la información o parte de ellos³⁰ y más del 80% considera posible delegar completamente la gestión de la informática. Las ventajas principales son la reducción de costes, la liberación de personal y recursos, la mejora del servicio y la posibilidad de afrontar proyectos que estaban fuera del alcance de la empresa³¹.

Sin embargo, no es una decisión que tomar a la ligera: los temores más habituales al afrontar un proceso de outsourcing son elegir un proveedor inadecuado y perder el control de los servicios externalizados. Para evitarlo, al plantear una externalización es necesario tener en cuenta tres aspectos básicos: asegurarse de que la compañía que prestará el servicio dispone de un centro de datos con la tecnología, el personal y las garantías necesarias; establecer un acuerdo detallado de calidad y disponibilidad; e implantar un sistema de seguimiento para que el servicio externalizado se adapte en todo momento a las necesidades cambiantes de la empresa.

¿Qué puedo hacer?

- Analice qué aspectos de la informática de su empresa son susceptibles de ser externalizados.
- Compare ofertas de varios proveedores exigiendo información que avale la propuesta: infraestructura tecnológica, certificaciones de calidad, casos de otros clientes, etc.
- Exija acuerdos de nivel de servicio (SLA's) y compromisos firmes del proveedor respecto a la calidad y disponibilidad de los servicios externalizados.

³⁰Informe Grupo Penteo 2004

³¹Estudio *Informática Distribuida* de IBM, 2004

Resumen de amenazas y consejos

Amenaza	Efectos	Protección Básica	Protección Avanzada
Virus y troyanos	Pérdida de datos Interrupción de la actividad Daños a otros	Nunca abra o ejecute un archivo desconocido. Instale las actualizaciones del sistema operativo y los programas. Compre un software antivirus y manténgalo actualizado. Escanee con un antivirus cualquier soporte sospechoso. Haga revisar los equipos ante comportamientos extraños.	Contrate un servicio de correo electrónico con antivirus. Instale un firewall. Limite el acceso a sitios web y servicios inseguros. Disponga de una copia de seguridad o imagen del sistema.
Spam y phishing	Pérdidas económicas, de datos y de productividad. Saturación del correo electrónico. Mala imagen de la empresa.	Nunca haga caso ni responda mensajes de desconocidos. Desconfíe de ofertas y chollos. No facilite su dirección de e-mail a cualquiera. Disponga de un segundo e-mail para envíos publicitarios. Compruebe cualquier mensaje en nombre de su empresa. Mantenga confidenciales sus contraseñas. Revise periódicamente sus cuentas bancarias. Consulte con su banco cualquier petición extraña.	Registre su dominio en un proveedor autorizado. Contrate un servicio de correo electrónico con antispam. Instale un firewall. Limite el intercambio de mensajes con chistes, videos, fotos, etc. en la empresa. Forme a sus empleados. Instale sistemas de autenticación en sus contratos y pedidos online. Legalice sus bases de datos.
Software malicioso e ingeniería social	Pérdidas de datos y de productividad. Robo de información.	Forme a sus empleados. Actualice su sistema operativo y navegador de Internet. Descargue programas solamente de sitios de confianza. No instale ningún software si no está seguro de qué es.	Instale y mantenga actualizado un programa contra el malware o un antivirus con esta prestación. Limite el intercambio de mensajes con chistes, videos, fotos, etc. en la empresa. Limite la posibilidad de instalar programas y modificar la configuración a los usuarios que lo necesiten.
Ataques e intrusiones	Pérdidas de datos y de productividad. Robo de información. Interrupción de la actividad. Mala imagen de la empresa.	Revise frecuentemente el funcionamiento de su web y aplicaciones. Encargue el diseño y programación de su web y aplicaciones a profesionales de confianza. En caso de despido conflictivo, haga revisar el sistema. Utilice equipos distintos para trabajar y para Internet.	Cifre los datos importantes que vaya a transmitir. Instale un firewall y revise los informes que genera. Contrate una red privada virtual (VPN) para interconectar sus equipos informáticos. Contrate un servicio de detección de intrusiones (IDS). Aloje su web o su servidor en un centro de datos de alta seguridad.
Fallos de hardware o software	Pérdida de datos. Interrupción de la actividad.	Compre productos de marcas y tiendas de confianza. Nunca instale productos pirata. Utilice productos del mismo fabricante o 100% compatibles. Contrate un informático profesional o un servicio de mantenimiento. Registre los programas y manténgalos actualizados.	Compre equipos con discos duros redundados para las tareas más críticas. Realice copias de seguridad de los datos importantes y guárdelas fuera de la oficina. Integre las diversas aplicaciones y bases de datos de su negocio en un único programa de gestión. Externalice su servidor a un centro de datos.
Errores humanos y robos	Pérdida materiales y de datos. Robo de información.	Forme a su personal en ofimática. Procure que la información clave no dependa de una persona. Conciencie a los empleados de que son responsables de los daños producidos en los equipos informáticos. Establezca niveles de acceso a la información según el puesto. Realice un inventario de equipos informáticos y asegúrelos. Controle quién tiene llaves y tarjetas de acceso. Instale alarmas, puertas y ventanillas de seguridad. Nunca pierda de vista su portátil, PDA, móvil, etc. Procure no llevar encima más información de la necesaria. Cree contraseñas seguras en los equipos y aplicaciones. Cambie las contraseñas frecuentemente. Impida que los documentos importantes queden a la vista. Limpie el disco duro antes de deshacerse de un ordenador. Limite el uso de soportes tipo CD, DVD, llaverosUSB y similares a razones de trabajo.	Instale hardware y software de protección para portátiles (candados, bloqueo, encriptación, rastreo, etc.). Realice copias de seguridad de los datos importantes y guárdelas fuera de la oficina. Facilite un acceso seguro al servidor corporativo para los empleados móviles. Realice copias de seguridad en línea de los equipos portátiles. Haga firmar un contrato de confidencialidad a los empleados clave. Establezca sistemas de cifrado en las comunicaciones inalámbricas. Encargue una auditoría de seguridad informática. Instale un sistema de video-vigilancia en la oficina. Instale un sistema de control de acceso basado en biometría.
Catástrofes y desastres naturales	Pérdida de datos. Interrupción de actividad.	Adopte medidas de protección contra incendios e inundaciones. Realice un inventario de los equipos y la información que contienen. Instale un Sistema de Alimentación Ininterrumpida en el servidor y los equipos más importantes. Identifique junto a sus empleados los procesos y datos clave.	Guarde copias de seguridad de los datos importantes en otra ubicación o al menos en armarios de seguridad. Externalice su servidor a un centro de datos. Contrate un plan continuidad de negocio.
Incumplimiento LOPD, LSSI y otras leyes	Sanciones económicas. Inhabilitación de la empresa. Procesos judiciales.	Establezca controles en el acceso a datos sensibles como currículums, expedientes médicos, etc. Controle el envío de comunicaciones comerciales de su empresa. Consulte con su asesor cualquier duda sobre gestión de datos.	Encripte la información confidencial antes de transmitirla. Realice copias de seguridad de la información confidencial. Encargue una auditoría legal sobre su empresa.

¿Cuánto cuesta estar protegido?

Servicio	Protección frente a...	Desde...
Registro de dominios	Suplantación de la marca en Internet	2 €/mes
Correo electrónico con filtro antivirus / antispam	Virus y saturación del correo electrónico	8 €/mes
Correo electrónico con sistema de salvaguarda (relay)	Pérdida de mensajes por fallos del servidor de correo	11 €/mes
Alojamiento web en servidor compartido	Ataques contra la web, lentitud, falta de disponibilidad	12 €/mes
Firewall	Virus, spam, ataques informáticos, navegación por sitios inseguros	14 €/mes
Copia de seguridad online	Pérdida de datos o robo de ordenadores de sobremesa y portátiles Incumplimiento de la LOPD	18 €/mes
Pack de diseño web todo incluido	Errores de diseño, usabilidad y programación Costes adicionales inesperados Multiplicidad de proveedores Mala imagen frente a clientes	35 €/mes
Instalación de su servidor en centro de datos de alta seguridad	Incendios, inundaciones, cortes de suministro eléctrico, etc. Gasto excesivo en equipos y personal TI	65 €/mes
VPN (Red Privada Virtual)	Robo de información Falta de seguridad en la conexión de equipos informáticos	73 €/mes
Copia de seguridad en cinta	Pérdidas de datos o recuperaciones lentas Gasto excesivo en equipos y personal TI	125 €/mes
Alquiler de un servidor dedicado en exclusiva a su empresa	Ataques contra la web, lentitud, falta de disponibilidad Incendios, inundaciones, cortes de suministro eléctrico, etc. Gasto excesivo en equipos y personal TI	189 €/mes
Sistema de gestión empresarial ERP/CRM externalizado	Incompatibilidad entre las distintas aplicaciones de facturación, nóminas, etc. Gasto excesivo en equipos y personal Dispersión de la información Limitaciones de crecimiento	198 €/mes
Consultoría de Seguridad	Pérdidas de datos Ataques informáticos Incumplimiento de LOPD, LSSI	Presupuesto a medida
Plan de Continuidad de Negocio	Interrupción de la actividad por catástrofe Pérdidas de datos	Presupuesto a medida

* Precios orientativos basados en las tarifas de Digital Parks



Llámenos al 902 505 005

Industria, 56 - 08908 - L'Hospitalet de Llobregat - Barcelona - España
info@digitalparks.com - Fax: (+34) 93 335 09 29

www.digitalparks.com