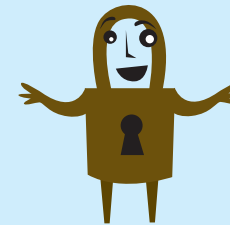


LA SEGURIDAD DE LA INFORMACIÓN EN SU EMPRESA

GUÍA PARA ...

Autónomos,
profesionales liberales,
PYMES...



LA SEGURIDAD DE LA INFORMACIÓN EN SU EMPRESA



Las medidas de seguridad

La información es uno de los principales activos de las empresas y por ello las nuevas tecnologías de la información y la comunicación se han convertido en una herramienta imprescindible para desarrollar cualquier actividad económica, así como en un factor clave para mejorar la productividad. Aragón no permanece ajena a este fenómeno y el grado de utilización de las nuevas tecnologías en sus empresas está en niveles equiparables a los de los países más avanzados de la Unión Europea ya que, según indican los estudios del Observatorio Aragonés de la Sociedad de la Información, en 2006 casi el 95% de las empresas tienen ordenador y cerca del 90% acceso a Internet.

LAS MEDIDAS DE SEGURIDAD SE DIVIDEN EN TRES NIVELES,

- **Físico:** VELA POR LA INTEGRIDAD DE LOS EQUIPOS Y POR LA CONTINUIDAD DE LOS SUMINISTROS QUE NECESITAN.
- **Lógico:** SE ENCARGA DE LA SEGURIDAD DE LOS PROGRAMAS.
- **ORGANIZACIONAL:** ASIGNA LAS FUNCIONES Y RESPONSABILIDADES EN MATERIA DE SEGURIDAD DENTRO DE LA EMPRESA.



Aunque las tecnologías informáticas han demostrado sobradamente su fiabilidad, al utilizarlas hay que observar unas reglas básicas de seguridad como ocurre con cualquier otra herramienta. Por ello, en este folleto le damos unos consejos de seguridad básicos, pensados para una pequeña o mediana empresa, y que le permitirán estar más protegido contra las interrupciones del trabajo por fallos en los sistemas informáticos, los accesos inadecuados a la información, la pérdida de datos y otros problemas similares.

La seguridad absoluta no existe en ningún ámbito de la actividad humana. Por ello las medidas de seguridad se diseñan buscando el equilibrio entre su coste, las probabilidades de los distintos riesgos y los daños que estos producirían en caso de materializarse. Cabe decir que, pese a su sencillez, las medidas de este folleto le permitirán evitar la gran mayoría de los percances que puedan ocurrir en sus sistemas.

La seguridad física

Haga copias de seguridad (backup)

Es la primera y la más importante de las medidas de seguridad. No deje ningún día de hacer una copia de seguridad de la información de su empresa. Hay distintas formas de organizar las copias, pero una bastante sencilla y eficiente es tener una cinta o disco por cada día laborable de la semana, de este modo, si la copia más reciente fallara, puede utilizar otra hecha sólo 24 horas antes. Guarde la cinta o disco del último día de la semana en un lugar distinto a la sede de su empresa, porque sino en caso de robo o incendio puede perder toda la información.

Aunque pueda parecer increíble, el incidente grave que se produce con más frecuencia es la pérdida de información por no haber seguido una política correcta de copias de seguridad.



HAY PROGRAMAS QUE PERMITEN PROGRAMAR LAS COPIAS DE SEGURIDAD PARA QUE SE HAGAN DE FORMA AUTOMÁTICA, POR EJEMPLO, AL MEDIODÍA O POR LA NOCHE. ENTRE ELLOS ALGUNOS SON GRATUITOS COMO COBIAN BACKUP, MCOPIAS O SYNCBACK.



Utilice sistemas de alimentación ininterrumpida (SAI)

Para evitar que los procesos en curso se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los “microcortes” y picos de intensidad, que resultan imperceptibles pero que pueden provocar averías en los equipos, es muy aconsejable disponer de sistemas de alimentación ininterrumpida, al menos para los servidores y equipos más importantes.

EL TIEMPO DE AUTONOMÍA DEPENDE DE LA POTENCIA DE LA UNIDAD Y DE LOS EQUIPOS CONECTADOS. EN GENERAL ES SUFICIENTE CON UNOS 10-15 MINUTOS, PLAZO QUE PERMITE TERMINAR DE FORMA ORDENADA LOS TRABAJOS EN CURSO.

➤ La autenticación

Asigne nombres de usuario y contraseñas a los empleados

Para identificar a las personas que acceden a sus sistemas es posible configurar los ordenadores de forma que al arrancar soliciten al usuario su nombre y contraseña, y otro tanto ocurre con muchos programas. Utilice estas opciones y no deje libre el acceso a los ordenadores de su empresa, sino que proporcione a cada empleado un nombre de usuario y una contraseña, y cuide de que mantengan esta en secreto.

Las contraseñas no han de ser nombres propios ni palabras del diccionario, deben tener una longitud de al menos ocho caracteres y, preferiblemente, algunos de éstos deben ser números o signos de puntuación. También aumenta la seguridad el combinar mayúsculas y minúsculas. Por último, no olvide cambiar las contraseñas periódicamente.

NO DÉ NUNCA SUS CONTRASEÑAS O PIN POR CORREO ELECTRÓNICO O POR TELÉFONO, NI LOS INTRODUZCA EN PÁGINAS WEB A LAS QUE HAYA LLEGADO SIGUIENDO UN LINK RECIBIDO EN UN CORREO. SU BANCO JAMÁS SE LAS PEDIRÁ DE ESTA FORMA.

DESDE 2002 LAS FACTURAS CON FIRMA ELECTRÓNICA TIENEN PLENA VALIDEZ LEGAL. PIENSE EN LOS ÁRBOLES Y EL DINERO QUE SE AHORRARÍAN ENVIANDO POR CORREO ELECTRÓNICO AL MENOS PARTE DE LAS FACTURAS QUE HOY SE ENVÍAN EN PAPEL.



Comience a utilizar la firma electrónica

Los certificados electrónicos permiten realizar numerosos trámites con las Administraciones a través de Internet así como firmar los documentos electrónicos de forma que estos pueden sustituir al papel en documentos auténticos. Hay certificados para personas físicas, como el DNI electrónico, y para empresas, como los emitidos por las Cámaras de Comercio (Camerfirma), los Registradores (SCR) o los Notarios (ANCERT).

Otra clase de certificados son los de servidor. Estos no se utilizan para firmar, sino que identifican a los sitios web y cifran la conexión para que no pueda ser leída por terceros. No introduzca ni solicite datos en Internet sin que la conexión esté cifrada.

➤ Los virus

Instale antivirus en los ordenadores

Tener un antivirus actualizado es una medida básica de seguridad, instale uno en todos los equipos y manténgalo actualizado. Tenga en cuenta, además, que algunos virus aprovechan vulnerabilidades del sistema operativo y para protegerse de ellos hay que instalar las actualizaciones que publica el fabricante (en el caso de *Windows* es aconsejable activar la opción de *Actualizaciones Automáticas*). También pueden llegar virus en un correo electrónico, así que nunca abra mensajes de origen desconocido y elimínelos lo antes posible de su ordenador. Tenga en cuenta que se suelen elegir asuntos que despiertan la curiosidad del destinatario. Otro medio de infección es la instalación de *plugins*, conteste NO cuando el sistema le diga que se va a instalar un programa si no conoce la procedencia del mismo.



ALGUNOS ANTIVIRUS GRATUITOS:
BITDEFENDER
WWW.BITDEFENDER-ES.COM
ANTIVIR
WWW.FREE-AV.COM
FREE AVAST!
WWW.ASW.CZ



ALGUNOS ANTISPYWARE GRATUITOS:
WINDOWSDEFENDER
WWW.MICROSOFT.COM/SPAIN/ATHOME/SECURITY/SPYWARE/SOFTWARE/DEFAULT.MSPX
ADWARE
WWW.LAVASOFTUSA.COM

Defiéndase de los programas espía (*spyware*)

Hay programas que se instalan de forma oculta en un ordenador y pueden enviar a quien los controla la información contenida en el mismo e incluso las contraseñas que se tecleen en él, y también le permiten convertirlo en un *zombie* y utilizarlo para sus propios fines.

Los programas anti-espías nos protegen de este *software*, pero desconfíe de aquellos que se le ofrezcan sin haberlos buscado expresamente, porque algunos programas desinstalan los espías que encuentran en su equipo sólo para instalar uno propio.



➤ La información dañina o no deseada

Utilice un cortafuegos (firewall)

Los cortafuegos son programas que analizan la información que entra y sale de un ordenador o de la red de la empresa. Evitan los ataques desde el exterior y, además, permiten detectar los programas espía, ya que nos avisan de que hay procesos desconocidos intentando enviar información a Internet. Junto con el antivirus es una de las medidas básicas de seguridad para los ordenadores conectados a Internet.

Evite el correo electrónico no deseado (spam)

No dé la dirección de correo a cualquiera, le ayudará a evitar el *spam*. Si recibe correo de origen desconocido no lo abra, porque puede introducirle un virus, ni lo conteste, porque si contesta confirma al que lo envió que la dirección es correcta y está activa. Tampoco publique direcciones personales en el web de la empresa, utilice mejor direcciones corporativas.

Los programas de correo tienen utilidades para filtrar el *spam* y también hay programas específicos y empresas especializadas que ofrecen el servicio de filtrar, con un elevado grado de eficacia, el correo que llega a su empresa.

Y, por supuesto, no envíe propaganda por correo electrónico a quien no le haya autorizado previamente para ello, ya que podrá ser sancionado como *spamer* por la Agencia de Protección de Datos.



ALGUNOS CORTAFUEGOS GRATUITOS:

ZONEALARM

DOWNLOAD.ZONELABS.COM

COMODO

WWW.PERSONALFIREWALL.COMODO.COM

EN EL SITIO ALERTA-ANTIVIRUS.RED.ES PUEDE ENCONTRAR MÁS ANTIVIRUS Y CORTAFUEGOS GRATUITOS.

ALGUNOS FILTROS ANTISPAM GRATUITOS:

G-LOCK SPAMCOMBAT

WWW.GLOCKSOFT.COM/SC

K9

WWW.KEIR.NET/K9.HTML

OUTLOOK SECURITY AGENT

WWW.OUTLOOKSECURITYAGENT.COM

SPAMFIGHTER

WWW.SPAMFIGHTER.COM

SPAMHILATOR

WWW.SPAMHILATOR.COM

SPAMPAL

WWW.SPAMPAL.ORG



SI RECIBE CORREO DE ORIGEN DESCONOCIDO NO LO ABRA.



➤ La protección de datos de carácter personal

Registre los ficheros

Es muy probable que su empresa maneje ficheros con datos de carácter personal. Recuerde que debe inscribirlos en el Registro de la Agencia Española de Protección de Datos. Para ello dispone de un formulario en el web de la Agencia (www.agpd.es). Normalmente en una empresa los ficheros a inscribir son los de personal, clientes y proveedores. Dedique un poco de tiempo a ello o, si lo prefiere, consulte a un profesional especializado.

Tenga cuidado si da los datos a un tercero

Si la información de los ficheros de datos de carácter personal se cede, de forma total o parcial, a otra persona o empresa, estamos ante una comunicación de datos y es obligatorio contar con el consentimiento de los titulares de los datos.

Si la cesión se hace sólo para que un tercero le preste un servicio como, por ejemplo, enviar un *mailing*, se trata de un tratamiento de datos por cuenta de tercero. En este caso es preciso firmar un contrato específico con la persona o entidad destinataria estableciendo expresamente que los datos se tratarán únicamente conforme a sus instrucciones y que no serán utilizados con un fin distinto ni cedidos, bajo ningún concepto, a otras personas.

Elabore el Documento de Seguridad de su empresa


El Reglamento de Medidas de Seguridad de la LOPD establece tres niveles de seguridad en función del tipo de datos personales que se manejan. El básico se aplica a todos, el medio a los datos de carácter financiero y el alto a los relativos a la salud, ideología, religión y creencias. Es obligatorio disponer de un Documento de Seguridad conforme al nivel de seguridad que corresponda a sus ficheros.

Una buena idea es aprovechar la obligación que la Ley impone para los datos personales y extender las medidas de seguridad de éstos a toda la información de la empresa.

➤ La seguridad de la información como objetivo de toda la empresa

Defina unos objetivos


Una idea clave es que la seguridad no es una cuestión que pueda dejarse a escalones inferiores de la organización, sino que debe ser asumida por la dirección al más alto nivel. Ésta deberá marcar la estrategia, definiendo las medidas que se van a implantar, así como las funciones y las responsabilidades de los miembros de la empresa en relación con la seguridad. En las grandes organizaciones estos extremos se plasman en un documento llamado Plan de Seguridad, que se actualiza periódicamente.




EL DOCUMENTO DE SEGURIDAD DE LA **LOPD** PUEDE SER SU PLAN DE SEGURIDAD. MARQUE EN ÉL UNOS OBJETIVOS REALISTAS E IMPLIQUE A TODA LA EMPRESA PARA CONSEGUIRLOS.

Conciencie a sus empleados

Los expertos en seguridad saben que el factor humano es siempre el eslabón más débil. Ninguna medida de seguridad funciona si las personas que han de aplicarla no están debidamente informadas, formadas y, sobre todo, concienciadas. Además, es preciso mantener esta concienciación a lo largo del tiempo ya que siempre hay una tendencia a relajarse en el cumplimiento de las medidas de seguridad.



REDACTE DE FORMA CLARA Y CONCISA LAS OBLIGACIONES QUE LOS DISTINTOS TIPOS DE EMPLEADOS TENGAN EN RELACIÓN CON LA SEGURIDAD. CUANDO ALGUIEN SE INCORPORA A LA EMPRESA, Y A TODOS LOS EMPLEADOS DE FORMA PERIÓDICA, PÍDALES QUE LEAN ESTÁS INSTRUCCIONES Y FIRMAN LA HOJA QUE LAS CONTIENE.



DE LA TOTAL CONCIENCIACIÓN DE LOS MIEMBROS DE LOS DISTINTOS NIVELES DE LA EMPRESA DEPENDE EL ÉXITO DE ESTAS ACCIONES.



PUEDE UTILIZAR EL MODELO DE DOCUMENTO DE SEGURIDAD QUE PROPONE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EN SU WEB (WWW.AGPD.ES)



Copia de seguridad (backup): Volcado de los datos a otro soporte para disponer de varias copias de los mismos. No se incluyen los programas, por lo que el volumen de información no suele ser muy grande. En grandes sistemas el medio más utilizado son las cintas, pero en pequeñas empresas se utilizan disquetes, CDs o DVDs regrabables o memorias USB (*pendrives*).

Cortafuegos (firewall): Dispositivo que analiza la información que entra y sale de un ordenador o de una red. Si la empresa tiene red local se coloca en la conexión de esta con Internet. El cortafuegos se configura para que sólo determinados programas puedan intercambiar información con Internet.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD): Establece que, salvo contadas excepciones, el tratamiento de los datos personales exige el consentimiento de su titular y que los datos que se tratan deben ser adecuados, pertinentes y no excesivos de acuerdo con la finalidad a la que se destina el fichero.

Vínculo (link): Enlace con una página web, dirección de correo u otro recurso de Internet. Es un elemento característico del hipertexto con el que se construyen las páginas web, ya que permite navegar por las mismas. Los vínculos entre sitios web se basan en un sistema unificado de direcciones que se llama *Uniform Resource Locator (URL)*.

Phishing: Es la estafa con más éxito en Internet y consiste en obtener el PIN o las contraseñas mediante engaño, normalmente pidiéndolas en un correo electrónico que simula provenir de un banco o una entidad oficial como, por ejemplo, la Agencia Tributaria. Estos correos son siempre falsos, ya que las contraseñas no se piden nunca por correo.

Personal Identification Number (PIN): Número de cuatro cifras que se utiliza en los sistemas de tarjetas y en la banca electrónica. Al introducirlo sólo se permiten tres intentos para evitar los ataques de “fuerza bruta”, que consisten en ir probando todas las opciones posibles.

Plugins: Pequeños programas que se descargan de Internet, normalmente para poder ejecutar funciones especiales de alguna página web.

Sistema de alimentación ininterrumpida (SAI): En inglés *Uninterrupted Power Supply (UPS)*. Equipo con baterías que garantizan la continuidad del suministro eléctrico. Algunos disponen de programas que avisan de los cortes de suministro a todas las estaciones de trabajo y finalizan de forma ordenada las tareas en curso, evitando las pérdidas de información.

Spam: Correo electrónico no deseado. Se ha convertido en uno de los principales problemas de Internet, ya que se calcula que supone más del 80% del correo que circula por la red. Se denomina *spammers* a quienes lo envían, valiéndose de programas al efecto (robots). En España el organismo encargado de combatir el *spam* es la Agencia Española de Protección de Datos.

Spyware: Programas que envían información sobre las acciones del usuario. Algunos son legítimos como, por ejemplo, la barra de Google si la autorizamos para que envíe información sobre nuestras búsquedas. Otros se instalan subrepticamente y envían la información sin nuestro consentimiento.

Titular de los datos: Es la persona física a la que se refieren los datos de carácter personal.

Virus: Habitualmente se denomina virus a todo el *software* maligno o *malware*, pero propiamente sólo son virus los programas que necesitan del usuario para propagarse, mientras que los gusanos se propagan sin intervención humana. Otro tipo de *malware*, los *troyanos*, se disfrazan de programas útiles.

Zombie: Es un ordenador que, sin que su propietario lo sepa, está controlado por un usuario malicioso. Éstos suelen tener un gran número de *zombies* que emplean para fines como enviar *spam*, distribuir *malware* o para fraudes como el *phishing*.

