segurnet PymeSeguraRioja

Guía Segurnet para PYMES

segurnet PYME SEGURA

Financia:
Gobierno de La Rioja
www.larioja.org
Agencia de Desarrollo Económico de La Rioja

Promueve:
fer Federación de empresarios de la Rioja

Incluido en:
Plan de Consolidación y Competitividad de la Pyme

SEGURNET: PYME SEGURA RIOJA

Proyecto incluido dentro del Plan de Consolidación y
Competitividad de la Pyme. PCCP.
Expediente 2006/P/INF/00005.
Guía elaborada por: Arsys Internet S.L.

Índice

Presentaciones

Estimado lector,

Nos encontramos ante uno de los mayores retos en el mundo de la empresa actual: Proteger la información, hoy en día uno de los principales activos de la empresa. La sociedad de la información ha introducido enormes ventajas para la estrategia global de las organizaciones, sea cual sea el sector, pero también ha propiciado algunos problemas que debemos afrontar y solucionar.

Esta publicación es el resultado de una de las acciones encaminadas a mejorar la seguridad de la información en las pymes riojanas. Se trata del proyecto Segurnet, que aporta soluciones reales a los principales riesgos para el desarrollo de la seguridad en la empresa.

Esta guía es un claro ejemplo del interés existente en La Rioja por implantar sistemas de seguridad dentro de la empresa. Como muestra de ello, 70 pymes riojanas han decidido establecer, a través de este proyecto, planes concretos para mejorar la seguridad de sus sistemas y lograr así el cumplimiento de la legislación vigente en esta materia.

La seguridad es una necesidad en todos los ámbitos del mundo empresarial, por eso, la Agencia de Desarrollo Económico de La Rioja (ADER) respalda este tipo de iniciativas que contribuyen a mejorar el tratamiento de la información en las pymes de nuestra Comunidad, contribuyendo así a su consolidación y mejorando su competitividad.

José Ángel García Mera
Director de la Agencia de Desarrollo Económico de La Rioja

Presentación guía proyecto Segurnet (PYME Segura Rioja)

Esta guía que ponemos en sus manos es el resultado del trabajo llevado a cabo a lo largo del año 2007 en el marco del proyecto SEGURNET: Pyme segura Rioja. Un proyecto promovido por la Federación de Empresarios de la Rioja y apoyado y financiado por el Gobierno regional a través de la Agencia de Desarrollo Económico de la Rioja que ha permitido diagnosticar y mejorar la situación de la seguridad informática en 70 pymes de la región.

La guía, de fácil lectura, intenta ser un instrumento útil que permita tomar conciencia de los riesgos y problemas que la no gestión de la seguridad informática implica. Si hablamos de que el conocimiento, las ideas, la información es actualmente nuestro principal activo, habrá que cuidarlo y protegerlo tomando una serie de medidas básicas que tiene mucho que ver con el sentido común.

Agradeciendo vuestra participación y el esfuerzo llevado a cabo por la pymes recibid un afectuoso saludo.

Emilio Abel de la Cruz Ugarte
Secretario general de la Federación de Empresarios de La Rioja.


User Login
User Name:
Password:
Login

Agradecimientos

Una atención especial merecen los agradecimientos a todas las personas, organizaciones, centros y empresas que han participado de forma desinteresada, ya que sin su participación no hubiera sido posible la realización de esta guía.

Destacamos con una mención especial al personal de la Agencia para el Desarrollo Económico de La Rioja, de la Federación de Empresarios de la Rioja y al Comité de Seguridad de La Rioja, que han colaborado en su elaboración.

Este proyecto ha sido apoyado por el Ministerio de Industria, Turismo y Comercio dentro del Plan de Consolidación y Competitividad de la Pyme (PCCP).

Introducción

Hoy en día la gran mayoría de las organizaciones dependen de su sistema informático, si éste se detiene, se detiene el negocio. Es vital para el día a día de las empresas y de la propia sociedad garantizar con referencia a su información y sistemas informáticos que son razonablemente seguros.

Hay que considerar que la seguridad basada en medidas tecnológicas se ha demostrado insuficiente; no hay más que comprobar el crecimiento sostenido de los incidentes y de las vulnerabilidades que afectan a los sistemas de información. Sin embargo, las organizaciones siguen sufriendo el síndrome de la Panacea, en virtud del cual buscan un producto barato, sencillo de instalar, que no tenga mantenimiento, que resuelva los problemas de seguridad y que nadie en la empresa tenga que cambiar sus hábitos de trabajo para que el problema se solvente y, todo eso, siempre después de que se haya producido un incidente (raramente se hace como medida preventiva).

Cuando la seguridad se rompe, y se rompe con frecuencia, lo hace por completo y de forma impredecible. Se pasa del aburrimiento al pánico en cuestión de minutos.

La seguridad es, por tanto, un requisito de negocio.

Por todo esto, la Federación de Empresarios de La Rioja (FER), con el apoyo de la Agencia para el Desarrollo Económico de La Rioja (ADER) ha elaborado un estudio sobre los problemas de seguridad que las empresas riojanas tienen con sus sistemas de información.

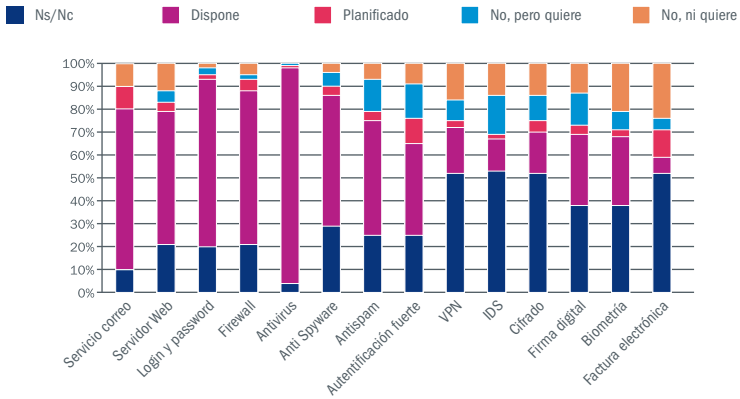
Con las conclusiones de este estudio se ha elaborado esta Guía Segurnet, basándose en los problemas que actualmente tienen las empresas de nuestra región, y no en datos generales que pueden coincidir o no con nuestra realidad empresarial.

Las recomendaciones de esta guía están especialmente orientadas hacia las PYMEs. Esperamos que las pautas y recomendaciones que encontrará en esta Guía Segurnet sean una ayuda para que su organización pueda mejorar la situación de la seguridad de sus sistemas de información.

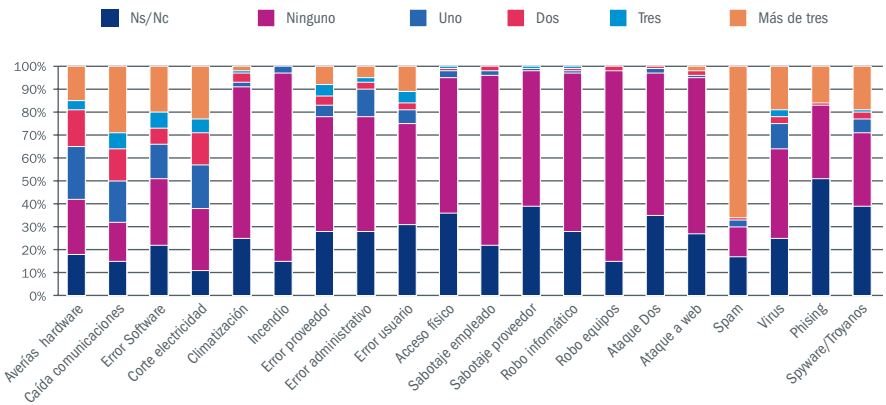
Resumen del estudio

Universo	3500 Empresas adscritas a la Federación de Empresarios de La Rioja
Tamaño de la muestra	252 cuestionarios válidos
Diseño muestral	Cuestionario remitido por correo postal, y entregado a los asistentes a cursos y jornadas relacionados con las tecnologías de la información
Periodo	No probabilístico accidental
Fiabilidad (alfa de Cronbach)	De marzo a septiembre de 2007
Margen de error	0,9063
Nivel de confianza	95%
Validez (proporción de variabilidad)	72,2%

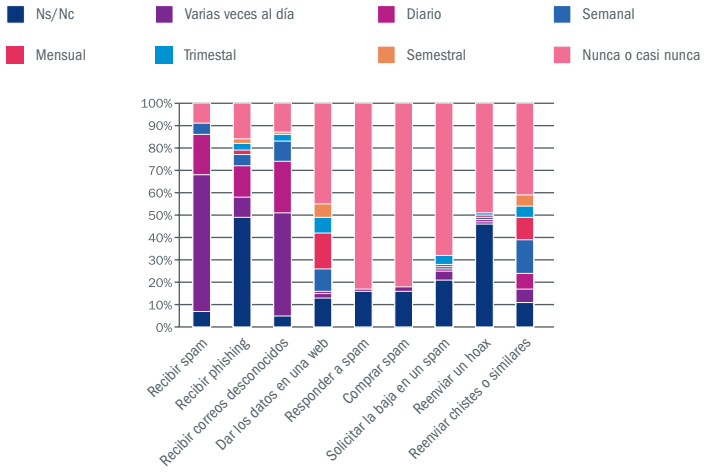
Elementos de seguridad o sistemas de que disponen las organizaciones



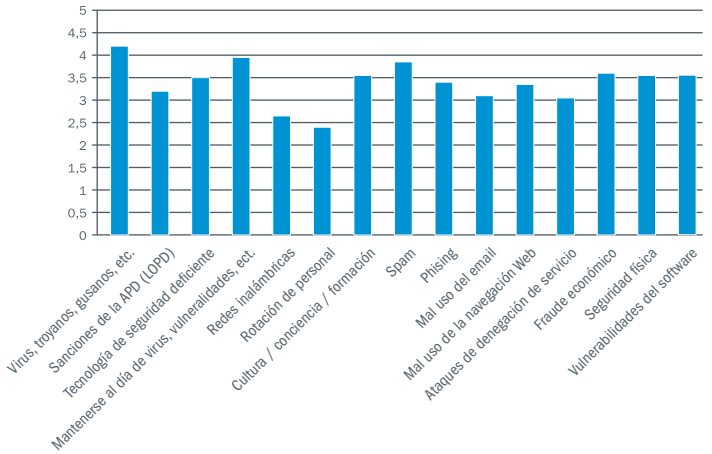
Tipos de incidentes y frecuencias en los últimos 12 meses



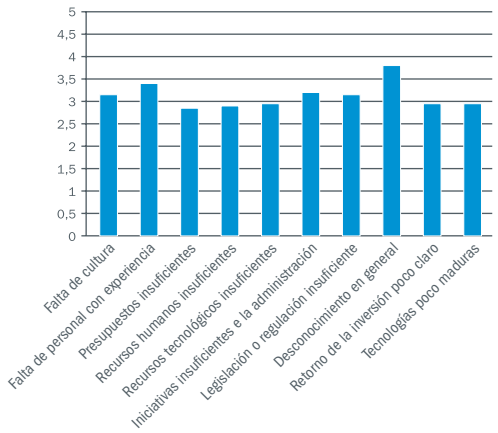
Frecuencias relacionadas con el correo electrónico en los últimos 12 meses



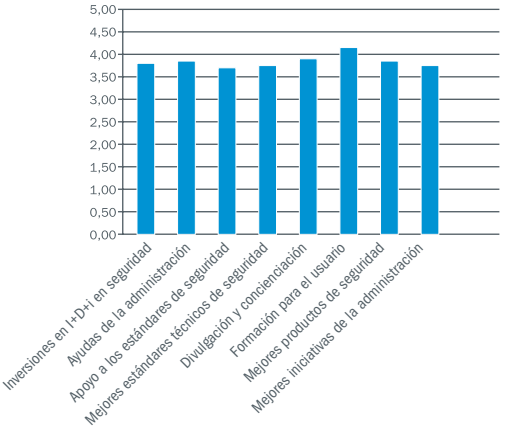
Mayores preocupaciones valoradas de 1 a 5



Principales obstáculos para la seguridad valorados de 1 a 5



Iniciativas que ayudarían a la seguridad valoradas de 1 a 5



El Conocimiento

Formación para los usuarios

El principal problema de la seguridad de la información es el desconocimiento por parte de los usuarios de las amenazas y las soluciones relacionadas con la seguridad de los sistemas de la información.

Es muy habitual que el personal de las empresas utilice sistemas informáticos para el desarrollo de las tareas relacionadas con su trabajo. En ocasiones, se les imparte formación sobre las herramientas informáticas que tienen que utilizar, pero los empleados que reciben formación, charlas o jornadas de concienciación son muy pocos.

Es importantísimo que las empresas faciliten a los empleados la posibilidad de asistir a charlas, conferencias, ponencias o formación (ya sea presencial o por Internet) para entender los riesgos que suponen el uso de los sistema informáticos que necesitan para hacer su trabajo.

El dinero que el empresario dedique a este mejor entendimiento de los riesgos por parte de sus empleados, será el que más contribuya a mejorar los niveles de seguridad de la empresa, por encima de cualquier tecnología que se quiera implantar.

Más información para encontrar acciones formativas y de concienciación en:

- www.fer.es
- www.ader.es
- www.isaca.org

Mantenerse al día

Los problemas relacionados con la seguridad de la información evolucionan cada día. Cada día surgen nuevas tecnologías, nuevos virus, nuevas vulnerabilidades, etc... que hacen recomendable mantenerse informados.

Los canales de noticias tipo RSS son una forma sencilla y ágil de mantenerse informado. Se pueden encontrar en la red varios programas que permiten leer y organizar las noticias buscando por el concepto “RSS Reader”. Existen bastantes fuentes de noticias diarias relacionadas con la seguridad que se actualizan automáticamente, manteniendo informado al usuario.

Más información para mantenerse al día en:

- www.inteco.es
- www.hispasec.com
- www.kriptopolis.org

Buenas prácticas

Al igual que en el resto de disciplinas (Financiero, Recursos Humanos, etc.), también en el ámbito de la seguridad de la información existen buenas prácticas comúnmente aceptadas.

Para las empresas que quieran ir avanzando más profundamente en el terreno de la seguridad de los sistemas informáticos, existen varios códigos de buenas prácticas que se pueden utilizar, algunos de ellos son gratuitos, mientras que otros son de pago. El más conocido es el que recoge la Norma ISO 27002 (la antigua ISO 17799), pero existen otros.

Más información sobre códigos de buenas prácticas en:

- www.iso.org
  Code of practice for information security management
- www.securityforum.org
  The standard of good practice for information security
- www.isecom.org/osstmm
  Open source security testing methodology manual

Las instalaciones

Comunicaciones adecuadas

Como ya hemos comentado, el desarrollo de la Sociedad de la Información está cambiando profundamente la forma de trabajo de las empresas. Una buena parte de este cambio viene del nuevo uso de las líneas de comunicaciones, haciendo que actualmente las organizaciones tengan una dependencia importante de estas líneas de comunicaciones.

En especial, se ha popularizado el uso de las líneas ADSL, pero en ocasiones se contratan para un uso profesional servicios que están diseñadas para un uso doméstico (con un precio pensado para este uso). Esto provoca que haya un número importante de caídas de las comunicaciones.

Para reducir este tipo de incidentes es necesario profesionalizar las líneas de comunicaciones que utilizan las organizaciones para el desarrollo de sus actividades de negocio.

Más información sobre líneas de comunicaciones profesionales en:

- www.telefonicaonline.com
- www.colt.net
- www.btglobalservices.com

Protección del suministro eléctrico

No es ningún secreto que el suministro eléctrico está dando muchos dolores de cabeza en nuestro país y en todo el mundo en los últimos años.

Esta situación no es fácil que mejore, por lo que las organizaciones deben comenzar a plantearse incorporar sistemas eléctricos de respaldo como Sistemas de Alimentación Ininterrumpida (SAI) o, dependiendo de la criticidad de los procesos, incluso Grupos Electrógenos de generación de electricidad.

Los cortes de suministro eléctrico no sólo suponen una pérdida de horas de trabajo, también pueden provocar pérdidas de datos y averías en el hardware.

Las empresas deben considerar seriamente la posibilidad de incorporar, al menos, SAIs para los servidores. Se comercializan SAIs pequeños especialmente indicados para utilizar incluso en los PCs.

Más información sobre SAIs en:

- www.apc.com
- www.gbo.es

Hardware coherente con el negocio

Las políticas de reducción de costes hacen que, en muchas ocasiones, se compre el hardware más barato, en lugar del que realmente se necesita y esto, al final, acaba saliendo caro.

A la hora de adquirir el equipamiento hardware que la empresa necesita, se debe analizar cual es el más adecuado, sin dar más importancia al coste que a las necesidades.

Más información sobre equipamiento hardware genérico en:

- www.ibm.es
- www.hp.es
- www.dell.es

La protección en la red

Cortafuegos o firewall

Contar con un cortafuegos o firewall (en el terreno de las tecnologías de la información) es equivalente a tener una puerta en la oficina para que los ciudadanos no puedan entrar y salir con facilidad. El firewall es la puerta, pero desde la perspectiva de Internet, que va a permitir o no entrar o salir de la empresa a través de la red. Es evidente que las organizaciones deben disponer, al menos, de un firewall que proteja sus sistemas frente a intentos de acceso no autorizado desde el exterior.

Saber si alguien está entrando en nuestros sistemas a través de Internet es muy difícil si no se dispone de cortafuegos o sistemas de detección de intrusiones, por lo que el hecho de que la empresa no tenga constancia de que hayan aparecido incidentes, no quiere decir que no estén ocurriendo.

La mayoría de las empresas de La Rioja disponen de cortafuegos, se debe mantener esta tendencia.

Más información sobre firewalls en:

- www.zonealarm.com
- www.cisco.com
- www.checkpoint.com
- www.watchguard.com
- www.personalfirewall.comodo.com

Red privada virtual o VPN

Las comunicaciones a través de redes públicas (fundamentalmente Internet) no tienen por si mismas ninguna característica de seguridad. Simplemente la información que viaja por las redes no tiene ninguna confidencialidad a menos que se la aportemos. Esto se puede hacer de muchas formas, pero la más difundida es la técnica de Redes Privadas Virtuales o VPN.

En los casos en que la empresa necesite establecer conexiones desde el exterior a los sistemas internos de la empresa (conexiones desde delegaciones, oficinas comerciales, ordenadores portátiles de directores, etc.), sin duda es recomendable que esta conexión se haga a través de una VPN o similar.

Más información sobre VPN en:

- www.cisco.com
- www.citrix.com
- www.watchguard.com
- www.checkpoint.com
- www.juniper.net
- www.aventail.com

Sistema de detección de Intrusos o IDS

Estos sistemas despertaron mucho interés a principios de la década de 2000, sin embargo, el elevado número de falsos positivos, así como la complejidad para optimizarlos y mantenerlos hizo que muchas organizaciones desistieran de utilizarlo.

En el estudio de realizado por la FER se ha detectado que hay un número de empresas en la región que están interesadas en disponer de esta tecnología.

Hay que tener presente que se trata de sistemas que no son sencillos de instalar y poner en producción. Algunas de las soluciones antivirus de última generación incorporan funcionalidades de detección y prevención frente a intrusiones, este tipo de soluciones es suficiente para proteger los puestos de trabajo o incluso algunos servidores.

Más información sobre sistemas de detección de intrusos en:

- www.tippingpoint.com
- www.symantec.com
- www.juniper.net
- www.mcafee.com

Redes inalámbricas

El uso de redes inalámbricas no tiene que representar un riesgo para la seguridad de los sistemas de información de la empresa, siempre que se configuren de forma adecuada. En este sentido hay dos aspectos especialmente importantes, por una parte que el acceso a la red inalámbrica esté protegido por un algoritmo seguro; y por otra que el segmento donde se encuentra la red inalámbrica esté debidamente aislado del resto de la red de la organización.

Más información sobre seguridad en redes inalámbricas en:

- www.cisco.com
- www.checkpoint.com
- www.airdefense.net
- www.nortel.com

La seguridad de los sistemas

Login y password

Uno de los elementos importantes para la seguridad de la información es la autenticación de los usuarios, es decir, verificar que quién pretende acceder a los sistemas es quien dice ser.

No se debe permitir a ningún usuario acceder sin verificar su identidad, y el método más frecuente para hacerlo es que el sistema al que pretende acceder le solicite un nombre de usuario y una contraseña, lo que se conoce como un login y un password.

Existen otros sistemas para verificar la identidad de la persona que está intentando acceder al sistema de información que se basan en que el usuario tiene algún dispositivo especial (por ejemplo una tarjeta, una llave USB, etc.), o donde se comprueba alguna característica del mismo (por ejemplo su huella digital). Cada vez iremos encontrando con más frecuencia el uso del nuevo DNI electrónico como un medio para que los usuarios se identifiquen ante los sistemas de información.

Todos los sistemas de la empresa deben tener implantada alguna de estas técnicas de autenticación, de forma que no se permita el acceso a ninguno de los sistemas sin que el usuario introduzca, al menos, un nombre de usuario y una contraseña válida.

Si escogemos las contraseñas como forma de identificar a nuestros usuarios, debemos tener claro que éstas deben ser razonablemente seguras, para lo cual se pueden dar algunas recomendaciones básicas:

- 1. Al menos ocho caracteres
- 2. Letras y números
- 3. No sean palabras que podamos encontrar en un diccionario
- 4. Fáciles de recordar, pero difíciles de adivinar
- 5. Cambiarlas periódicamente

Crearnos una regla pnemotécnica puede sernos de ayuda, por ejemplo:

- 1. Cambiar algunas letras por números o caracteres
  - a. JoseMaria => J0$eM@ri@
- 2. Combinar dos temas conocidos
  - a. Coche y piloto => McLarenAlonso
  - b. Equipo y jugador => RealMadridCasillas
  - c. Comida y lugar => Lech@z0Burg0s
- 3. Combinar un tema familiar con una fecha
  - a. Madre y cumpleaños => Carmen150462
  - b. Hermano y prima => MarcosJulia
  - c. Padre y matrícula del coche => Jose9261CTP
- 4. Meter la contraseña entre caracteres especiales
  - a. :)Carlos(:
  - b. <MariCarmen>
- 5. Escribir en castellano palabras inglesas tal como se pronuncian
  - a. Guindous
  - b. Pleiesteision
  - c. Velletabols

Contar con sistemas de autenticación basados en contraseñas supone que el usuario tiene que recordarlas. No es realista pensar que un usuario va a recordar todas las contraseñas que utiliza (acceso al sistema operativo, a las aplicaciones corporativas, al correo electrónico, a sistemas online como banca, reserva de billetes, etc.), por lo que, frecuentemente, se plantea el problema de cómo almacenar las contraseñas de forma segura. Se pueden utilizar soluciones intermedias como guardarlas en archivos protegidos con una contraseña especialmente fuerte (y que el usuario sí que tiene que recordar) como pueden ser archivos en Word, Excell, Access, o archivos de texto comprimidos con una contraseña. Otra solucion es utilizar aplicaciones especializadas para guardar contraseñas, aplicaciones que pueden ser gratuitas.

Más información sobre sistemas de autenticación en:

- www.rsa.com
- www.verisign.com
- www.activeidentity.com
- www.aladdin.com

Aviso de acceso a los sistemas

En los sistemas en los que sea posible se debe habilitar antes del acceso una ventana que informe de que se está intentando acceder a un sistema privado, de forma que ningún usuario pueda argumentar que no sabía que trataba de acceder a un sistema para el que no tenía autorización.

La información a mostrar puede ser parecida a la siguiente:

Acceso a los sistemas de información de PYME S.L.

Está usted intentando acceder a los sistemas de información de PYME S.L.. Se trata de un sistema privado y el acceso al mismo está permitido únicamente a usuarios autorizados expresamente por la empresa. Igualmente el uso que se haga de los sistemas de información debe respetar la política de seguridad aprobada por la misma.

Todos los accesos al sistema y los usos que se hacen del mismo están monitorizados y quedan registrados. Cualquier acceso de usuarios no autorizados, o uso inadecuado del sistema podrá ser investigado, reservándose PYME S.L. el derecho de emprender las acciones oportunas.

Copias de seguridad

Si en la introducción hemos afirmado que la información es el activo más importante de la empresa, parece indiscutible que debemos tener copias de la misma, por si sufriéramos algún incidente que la comprometa.

La empresa debe hacer copias de seguridad de toda la información que utiliza, tanto de los ficheros que generan (bases de datos, hojas de cálculo, documentos de Word, correos electrónicos, contactos, etc.), como de las configuraciones de los sistemas que utilizan. De esta forma, en caso de que, por ejemplo, un servidor se averíe, disponga de toda la información necesaria para restaurarlo con la misma configuración que tenía antes de averiarse, y por supuesto, con los mismos datos.

Debemos estudiar cada cuánto tiempo debemos hacer la copia de seguridad, teniendo presente que en caso de que se produzca un incidente perderemos toda la información que hayamos generado desde que se realizó la última copia. Cada empresa debe decidir esta periodicidad, pero parece razonable hacer copias de seguridad cada día.

Debemos tener presente que en la copia de seguridad estará guardada toda la información de nuestra empresa, por lo tanto, es conveniente proteger esa copia adecuadamente. Para ello debemos ponerle alguna contraseña a la copia (la mayoría de las aplicaciones lo permiten) de forma que si alguien se hace con el disco o la cinta donde está la copia, y quiere restaurarla, no pueda hacerlo o, al menos, no fácilmente.

Dicho esto, es evidente que los soportes donde hacemos las copias (cintas, discos, DVDs, memorias USB, etc.) no podemos dejarlos en cualquier sitio. Es recomendable que queden guardados bajo llave, y que no guardemos todas las copias siempre en el mismo lugar, sino que periódicamente (por ejemplo, una vez al mes) guardemos una copia en un lugar distinto, a ser posible externo a las oficinas de la empresa.

Otra solución que está cobrando cada vez más auge es hacer las copias de seguridad on line contratando este servicio con algún ISP. Este sistema tiene la ventaja de que las copias de seguridad quedan almacenadas en un lugar fuera de la empresa y que se gestionan de forma segura.

Por último, recordar que el hecho de que tengamos una copia de seguridad, no quiere decir que esté bien hecha. Para evitar sorpresas cuando vayamos a restaurar la copia, es conveniente hacer pruebas de vez en cuando para verificar que las copias funcionan y que se pueden restaurar los datos.

Más información sobre sistemas de copia de seguridad en:

- www.microsoft.com
- backup.comodo.com
- www.symantec.com
- www.nero.com

Virus, Troyanos, Spyware, Spam y demás

Protección contra código malicioso

Es importante resaltar que, aunque más del 90% de las organizaciones de la región disponen de soluciones antivirus, el número de incidentes relacionados con este tipo de amenazas es el más elevado. Esto sólo se puede entender como que las herramientas no están adecuadamente implantadas, mantenidas y actualizadas.

Puesto que la implantacion de este tipo de soluciones está ampliamente difundida, y prácticamente todas las empresas de La Rioja tienen lo que coloquialmente conocemos como antivirus, daremos aquí algunas recomendaciones importantes con respecto a la instalación y configuración de este tipo de soluciones:

1. El usuario no debe tener la posibilidad de desactivar el antivirus
2. Se debe actualizar automáticamente, a ser posible a diario
3. Los virus pueden entrar por muchas vías y hay que protegerlas todas. La herramienta debe estar configurada para protegerlas todas:
   a. Correo electrónico
   b. Navegar a través de páginas web
   c. Descargas por FTP
   d. Memorias USB, CDs, DVDs, etc.
4. Las amenazas no son sólo los virus, hay que proteger los sistemas frente a todas ellas:
   a. Virus
   b. Gusanos y troyanos
   c. Spyware y adware
   d. Phishing

El desconocimiento que existe sobre los temas de seguridad informática es uno de los factores que debemos tener presentes para poder entender el número tan elevado de incidentes que se producen, cuando las herramientas de protección están disponibles, prácticamente, en todas las empresas.

Fundamentalmente el uso adecuado del correo electrónico y la navegación web sería de gran ayuda para reducir el volumen de incidentes. Algunas recomendaciones que se deben tener en cuenta son:

1. No abrir correos electrónicos de desconocidos.
2. No abrir ficheros adjuntos en los correos que no estén relacionados con el trabajo. En ocasiones, las presentaciones, archivos de Word, o incluso archivos PDF tienen código malicioso inyectado.
3. No abrir nunca ningún fichero ejecutable (fundamentalmente los que tienen extensiones EXE, COM, PIF o BAT) que venga como adjunto a un correo.
4. No hacer caso a los correos que por ejemplo intentan explicarnos que hay un problema gravísimo con Windows y nos explican los cambios que tenemos que hacer para corregirlo (se les conoce como correos Hoax). Suelen ser falsos y sólo buscan que abras el sistema.

5. No hacer reenvíos de correos en pirámide (los que hablan por ejemplo de que se ha perdido un niño, o que se necesita un donante urgentemente). Pueden incluir código malicioso y lo estaríamos redistribuyendo a toda nuestra lista de contactos.
6. En la medida de lo posible no navegar por páginas web desconocidas, y evitar navegar por páginas de "dudosa reputación" desde equipos de la empresa.
7. No aportar nuestros datos personales en páginas web si no es necesario
8. No aportar nuestros datos bancarios o de tarjetas de crédito en ninguna web salvo que verifiquemos que se trata de una página de confianza
   a. Verificar que se trata de una conexión segura, comprobar que es una conexión https en la barra de direcciones
   b. Comprobar que aparece el candado en la barra inferior del navegador
   c. Verificar que si pinchamos en el candado, podemos comprobar que el certificado pertenece a la entidad en la que queremos introducir nuestros datos

El Phishing tiene unas implicaciones muy serias para los usuarios que caigan en la trampa, ya que afectará directamente a su bolsillo. Se están recibiendo muchos correos de Phishing, por lo que se debe incluir en las campañas de comunicación contenidos que permitan a los usuarios identificar este tipo de ataques.

Más información sobre protección frente a código malicioso en:

- www.mcafee.com
- www.trendmicro.com
- www.websense.com
- www.symantec.com
- www.pandasecurity.com
- www.karpersky.es
- es.clamwin.com

Antispam

El spam no es un ataque en sí mismo, pero es muy incómodo. Entre el 80% y el 90% de todos los correos que circulan por Internet son spam. Una solución antispam se basa fundamentalmente en dos técnicas: la primera es identificar de dónde llegan los correos y si se trata de una dirección desde la que se suele enviar spam, lo filtra; la segunda analiza el contenido del correo y en función de palabras, imágenes o enlaces (entre otros) decide si se trata de un spam o no.

Hay que decir que el spam es un problema que no tiene fácil solución, aunque tengamos instalada una solución antispam, y no demos nuestros datos en ningún sitio, aún así es más que posible que acabemos recibiendo spam.

Además de tener instalada una solución antispam, hay algunas recomendaciones básicas a tener en cuenta:

1. 1. Insistir nuevamente en que no se den datos personales en ninguna página web que no sea necesario
2. No responder en ningún sentido a los correos de spam, ni para solicitar la baja de la lista de distribución, ni por supuesto para comprar

Muchos usuarios confunden el correo que reciben desde estas páginas web, en las que han dado sus datos, con spam. En este caso, son los propios usuarios los que han dado los datos y generalmente solicitando que se les envíe información. Como siempre darse de alta en este tipo de servicios es muy sencillo, pero la baja no lo es tanto.

Aunque en España es ilegal enviar información comercial que no se ha solicitado expresamente, en la mayoría de los países no lo es, por lo que, en ocasiones, la información que se da en estas páginas es utilizada con fines publicitarios.

Lo mejor para evitar estos problemas es no dar datos personales en páginas web si no se tiene claro que el uso va a ser el que deseamos

Más información sobre protección frente a spam en:

- www.rediris.es/mail/abuso
- www.spamhaus.org
- spamlinks.net
- www.ironport.com
- www.trendmicro.com

Fraude económico

El fraude económico producido por medios electrónicos, como accesos a cuentas bancarias, números de tarjetas de crédito, repudio de contratos o transacciones, etc., puede tener un impacto económico importante en las empresas, por lo que se supuso que sería una preocupación.

Más información sobre fraudes económicos en la red en:

- www.antiphishing.org
- www.cert.org
- www.visa.com

Firma electrónica

La Ley de Firma Electrónica equipara (siempre que se den las condiciones previstas por esta ley) la validez jurídica de la firma digital a la de la firma manuscrita. Se trata de una de las tecnologías con mayor proyección en la región, que se puede apoyar en el despliegue del nuevo DNI electrónico.

Es muy frecuente aceptar pedidos, proyectos, envíos, etc. simplemente con la evidencia de un fax, email, o incluso llamada telefónica. Las acciones aceptadas mediante estos canales pueden ser rechazadas en un momento dado, hablando claro, alguien puede alegar a posteriori que ellos realmente no han aceptado ningún pedido, ni ordenado ningún envío. Para enviar este tipo de situaciones se tienen que emplear técnicas de no repudio, y la firma electrónica avanzada es una de ellas.

Más información sobre firma electrónica en:

- www.mityc.es/DGDSI/Servicios/FirmaElectronica/
- www.cert.fnmt.es
- www.camerfirma.com
- www.ipsca.com
- www.interactiva.com.es

Factura electrónica

La factura electrónica es un sistema de facturar que no utiliza el método tradicional de envío en papel, sino que genera un fichero informático que luego se remite por correo electrónico, incorporando una serie de características técnicas que garantizan que la factura es válida y exacta. Esta modalidad de facturación aporta una serie de beneficios a las empresas que lo utilizan, entre los que se pueden destacar las siguientes:

1. Ahorro en todo el proceso de emisión, recepción, almacenamiento, firma, devolución, etc. de factura
2. Más facilidad para organizar y almacenar las facturas, que redunda en:
   a. Rapidez a la hora de localizar la información
   b. Más seguridad, ya que se pueden hacer copias de respaldo
   c. Facilita las auditorias financieras
3. Reduce el espacio físico de archivo necesario que se utiliza actualmente para guardar las facturas en papel
4. Reduce la probabilidad de falsificación

Durante el estudio realizado por la FER se pudo observar que prácticamente un 25% de las empresas encuestadas (1 de cada 4) o tienen planificado o quieren implantar la factura electrónica. Esto es una apuesta clara del sector empresarial hacia los medios y canales electrónicos.

Más información sobre factura electrónica en:

- www.red.es/prensa/pdf/factura_electronica.pdf
- www.cert.fnmt.es
- www.ipsca.com
- www.interactiva.com.es

Autoevaluación

Comunicación	Modem conectado a la red telefónica	ADSL Doméstica	ADSL Profesional	Otras Profesionales
Qué tipo de conexión tiene contratada para sus comunicaciones por Internet				

Suministro Eléctrico	SI	NO
Tienen instalados estabilizadores de tensión		
Tienen Sistemas de Alimentación Ininterrumpida (SAI)		

Equipamiento Hardware	Menos de 1 año	Menos de 2 años	Menos de 3 años	Menos de 4 años	Menos de 5 años
Qué antigüedad tienen los equipos informáticos con los que trabaja su empresa					
	1	2	3	4	5
Cómo calificaría de 1 a 5 el criterio que se utiliza en su empresa a la hora de comprar sistemas informáticos, siendo 1 “Siempre el más barato” y 5 “Siempre el que mejor se adecúa a mis necesidades, independientemente del precio”					

Red	SI	NO
Han cambiado las contraseñas que vienen por defecto en el router		
Tienen cortafuegos de red instalado		
Tienen los puestos de trabajo activado algún cortafuegos de equipo		
Tienen conexiones con otras oficinas, delegaciones, etc		
Tienen WiFi protegida por contraseña que no sea WEP		

Sistemas	SI	NO
Hay algún sistema en la empresa que permita acceder sin tener que identificarse, introduciendo un nombre de usuario y una contraseña, o con técnicas mas avanzadas		
Se cambian las contraseñas periódicamente		
Se pide que las contraseñas tengan un mínimo de calidad		
Se hace copia de seguridad de todos los archivos relacionados con el trabajo		
Se hace copia de seguridad de las configuraciones de los equipos importantes		
Hay algún sistema del que no se haga copia de seguridad al menos una vez a la semana		
Se ha comprobado que las copias de seguridad se pueden restaurar		
Hay alguna copia de seguridad guardada en un lugar seguro, fuera de la oficina		

Código Malicioso	SI	NO
Están todos los equipos informáticos protegidos		
Se controlan los virus		
Y los gusanos		
Y los troyanos y programas espía en general		
Y el spam		
Y el Phishing		
Esta protegida la entrada de código malicioso por correo electrónico		
Y por CDRoms, DVD, memorias USB, etc		
Y por navegar en páginas web		
Y por descargar ficheros desde FTP		

Mantenerse al día	SI	NO
Se ha enviado al personal a alguna jornada, charlas, conferencias o cursos relacionados con la seguridad de los sistemas informáticos		
Se hace algo para mantenerse al día de las amenazas que van surgiendo y que amenazan a los sistemas informáticos de la empresa		

Glosario

1. ADSL: Asymmetric Digital Subscriber Line ("Línea de Abonado Digital Asimétrica"). Es una línea digital de alta velocidad que utiliza el mismo cableado de cobre que se usa para la telefonía de voz. Es la tecnología más utilizada actualmente para tener acceso a Internet de banda ancha y poder transmitir a mayor velocidad.
2. APD: Agencia de Protección de Datos (www.agpd.es).
3. Biometría: La "Biometría Informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos de un individuo, para "verificar" identidades o "identificarlo".
4. Firewall: O cortafuegos, es un elemento de hardware o software utilizado en una red para controlar las comunicaciones, permitiéndolas o prohibiéndolas, según las políticas de red que haya definido la organización responsable.
5. Denegación de servicio: O DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
6. Factura electrónica: Es una modalidad de factura en la que no se emplea el papel como soporte para demostrar su autenticidad. Por eso, la factura electrónica es un fichero que recoge la información relativa a una transacción comercial y sus obligaciones de pago y de liquidación de impuestos y cumple otros requisitos que dependen de la legislación del país en el que se emplea.
7. Firma electrónica: Es un método criptográfico que asegura la identidad del remitente. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.
8. Gusano: Código malicioso que se duplica a sí mismo intentando distribuirse al mayor número de equipos posible. Mientras que los virus intentan infectar los ordenadores que atacan, los gusanos generalmente sólo intentan reproducirse y redistribuirse.
9. Hoax: Es un intento de engañar a un grupo de personas haciéndoles creer que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos especialmente la Internet.
10. IDS: Un sistema de detección de intrusos (o IDS de sus siglas en inglés) es un programa usado para detectar accesos no autorizados a un ordenador o a una red.
11. LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
12. Phishing: Es un término usado en informática con el cual se denomina un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. La vía más frecuente por la que se intenta obtener esta información es mediante el envío de correos electrónicos que simulan

provenir de una entidad financiera y que solicitan esta información.

- 13. SAI: Sistema de alimentación ininterrumpida, es un dispositivo que incorpora baterías para seguir suministrando electricidad en el caso de un corte de suministro eléctrico.
- 14. Sociedad de la Información: Un estadio de desarrollo social caracterizado por la capacidad de sus miembros (ciudadanos, empresas y Administraciones Públicas) para obtener, compartir y procesar cualquier información por medios telemáticos instantáneamente, desde cualquier lugar y en la forma que se prefiera.
- 15. Spam: O correo basura, son mensajes no solicitados, normalmente publicitarios, enviados en cantidades masivas.
- 16. Spyware: O programas espía, son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento.
- 17. Troyano: Es un programa malicioso capaz de alojarse en ordenadores.
- 18. Virus: Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.
- 19. VPN: Es una tecnología de red que permite extender la red local sobre una red pública no controlada, p. e. Internet usando un canal cifrado.
- 20. WiFi: Es un conjunto de Normas para redes inalámbricas basados en las especificaciones IEEE 802.11 que nace con el objetivo de crear redes inalámbricas, que generalmente se utilizan como acceso a Internet, y como una forma de disponer de redes tipo LAN sin necesidad de cablear las oficinas.

SEGURNET: PYME SEGURA RIOJA

Proyecto incluido dentro del Plan de Consolidación y
Competitividad de la Pyme. PCCP.
Expediente 2006/P/INF/00005.
Guía elaborada por: Arsys Internet S.L.

Financia:

Gobierno de La Rioja
www.larioja.org
Agencia de Desarrollo Económico de La Rioja

Promueve:

fer
Federación de Empresarios de La Rioja

Incluido en:

Plan de Consolidación y Competitividad de la Pyme