segurnet PymeSeguraRioja

Informe del Estudio de Seguridad Segurnet

segurnet PYME SEGURA

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

Promueve:
fer federación de empresarios de la rioja

Incluido en:
pyE+ 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.
Estudio elaborado por Arsys Internet S.L.

Índice

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 este informe.

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

Debido a la actual necesidad en el campo de la seguridad de la información, de obtener datos sobre la situación actual en las organizaciones de la región, la Federación de Empresarios de La Rioja (en adelante la FER) ha elaborado un cuestionario para recoger datos sobre la misma. Este cuestionario ha pasado las fases de validación estadística, recogido en un documento que incluye los análisis desde esta perspectiva.

La FER tiene, aproximadamente, 3500 empresas inscritas, lo que supone una muestra significativa de las empresas de La Rioja. Con el fin de conocer la situación de la seguridad dentro de las mismas, y debido a la imposibilidad de acceder a todas ellas para obtener unos datos reales, se ha realizado este estudio que ofrece unas garantías científicas para que los datos obtenidos puedan ser generalizados a todas las empresas que componen la FER.

La finalidad de este informe es exponer las conclusiones a las que llega el estudio con respecto a la situación de la seguridad de la información en las empresas de la región.

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.

Ficha Técnica

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%

Resumen Ejecutivo

Tras un análisis de todos los datos obtenidos en el cuestionario se pueden extraer las siguientes conclusiones de tipo general:

- En términos generales las empresas desconocen tanto los riesgos de seguridad relacionados con los sistemas de información, como las soluciones disponibles para reducirlos.
- Las tecnologías clásicas de seguridad (firewalls y antivirus fundamentalmente) están ampliamente implantadas, mientras que otras más avanzadas tienen un nivel de implantación muy bajo.
- Más de un 7,5% de las empresas no usa ni siquiera login y password para autenticar a sus usuarios.
- Un 12% de las organizaciones no disponen de firewall, sin embargo el uso de Internet está ampliamente difundido, por lo que todas estas empresas no cuentan con herramientas que les protejan adecuadamente frente a intentos de acceso desde el exterior a través de Internet.
- Cabe destacar en este punto que aunque las tecnologías de protección contra código malicioso tienen un elevado nivel de implantación, las

empresas continúan sufriendo con frecuencia incidentes relacionados con virus, spyware, etc., que son la mayor preocupación de las organizaciones. Todo esto hace pensar que las soluciones no se están convenientemente implantadas, o al menos que tal como están implantadas no son eficaces.

- La incidencia del spam en la región es muy elevada, sin embargo sólo algo más del 50% de las empresas cuentan con soluciones antispam.
- Se reciben muchos correos de phishing.
- Un porcentaje significativo de empresas ha manifestado que tienen planificado o quisieran implantar soluciones de factura electrónica y la firma digital.
- Los sistemas de detección y prevención de intrusiones también son del interés de las empresas encuestadas, y les gustaría contar con este tipo de soluciones.
- En otro orden de cosas, los incidentes relacionados con las interrupciones de suministro eléctrico, caídas de las comunicaciones y averías de hardware son elevados.
- Los incidentes provocados por errores de empleados, administradores y proveedores también son frecuentes aunque menos.
- Tras los aspectos relacionados con el código malicioso y el spam, la mayor preocupación en materia de seguridad de las empresas es mantenerse al día en lo que respecta a amenazas y vulnerabilidades, y mejorar la cultura, concienciación y formación en seguridad.
- En línea con lo anterior, las empresas consideran que el mayor obstáculo para el desarrollo de la seguridad es el desconocimiento que existe sobre estos temas, seguido de la carencia de profesionales con experiencia en este campo.
- Es significativo que las empresas consideran que las iniciativas que más ayudarían a mejorar la seguridad son la formación para los usuarios, seguido de acciones de divulgación y concienciación.

Más información para mantenerse al día en:

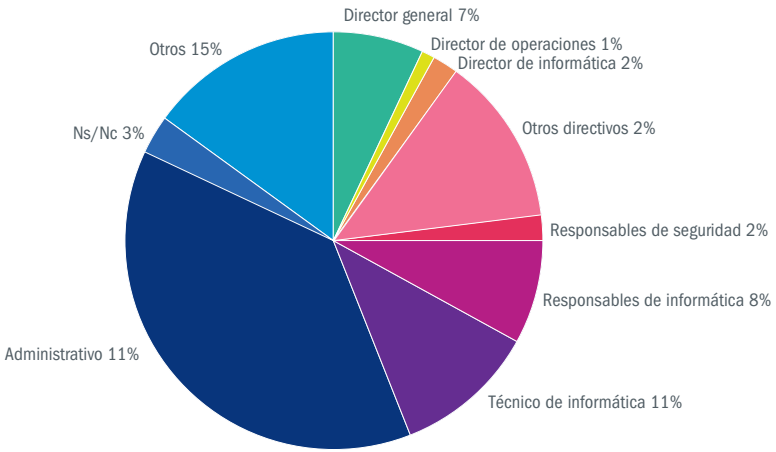
- www.inteco.es
- www.hispasec.com
- www.kriptopolis.org

Análisis de los resultados

A continuación se detallan los valores obtenidos tras el análisis de las respuestas, lo que da una visión de la situación de la seguridad de la información en las empresas riojanas.

Cargo de la persona que responde el test

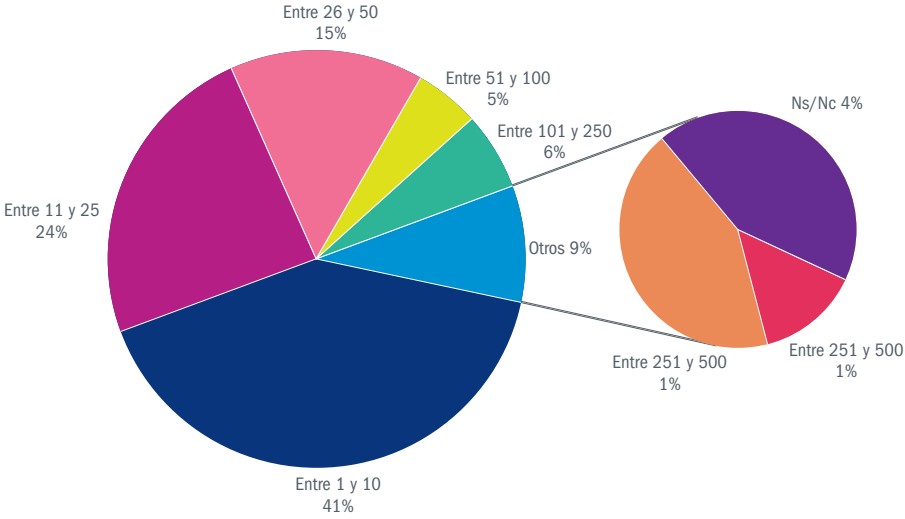
Casi la totalidad de los cuestionarios han sido contestados por algún miembro del equipo directivo o por personal administrativo, así como por personas que tienen una estrecha relación con el mundo de la seguridad como pueden ser el director, el responsable o un técnico de informática, o por la persona encargada de la seguridad.



Número de empleados

Casi dos terceras partes de los cuestionarios recibidos pertenecen a empresas con menos de 25 empleados, y casi un 40% tienen menos de 10. Esto es un indicador del tamaño de las organizaciones que componen el tejido empresarial de la región, y que por otra parte es coherente con la situación a nivel nacional.

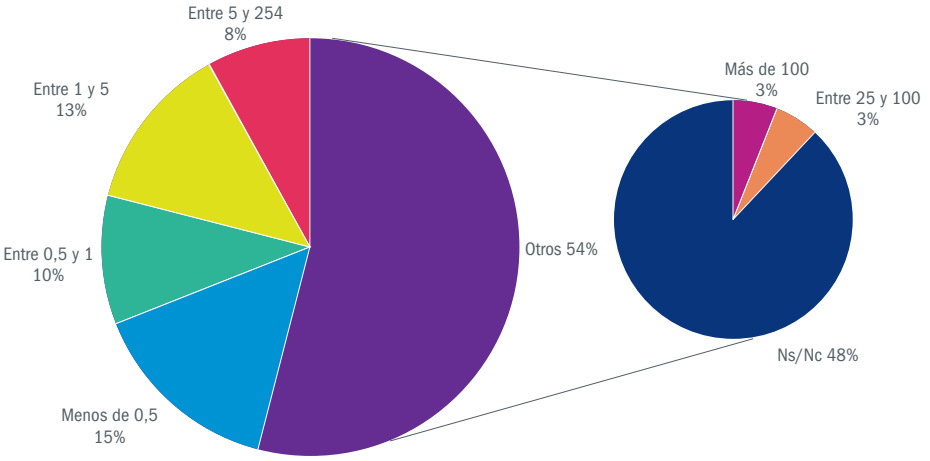
Para empresas de este tamaño no es sencillo contar con personal especializado en sistemas de información, y menos en seguridad, por lo que se deben plantear soluciones que ayuden a mejorar la situación de estas organizaciones con respecto a la seguridad de sus sistemas de información, teniendo en cuenta esta realidad. Sin duda alguna, las tareas de formación y concienciación del personal no técnico de la empresa pueden significar una mejora sustancial.



Facturación en millones de euros al año

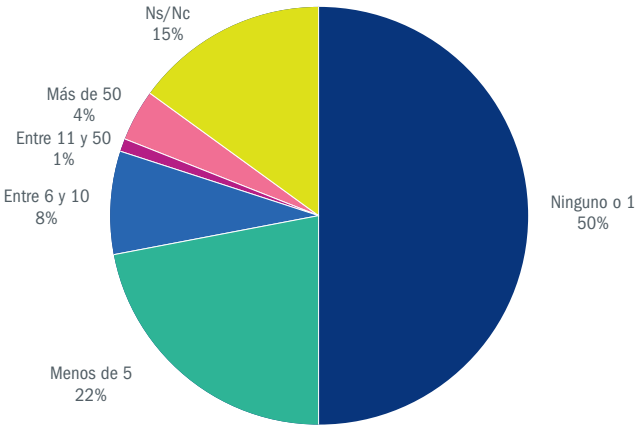
Teniendo en cuenta que un 48% de las empresas no han contestado a esta cuestión, y que sólo un 6% de los encuestados han manifestado tener una facturación superior a 25 millones de € anuales, volvemos a estar ante un escenario donde la PYME es el actor principal, por lo que las soluciones que se planteen para mejorar la situación de la seguridad en las empresas deben ir orientadas hacia este tipo de empresas.

Facturación en millones de euros al año



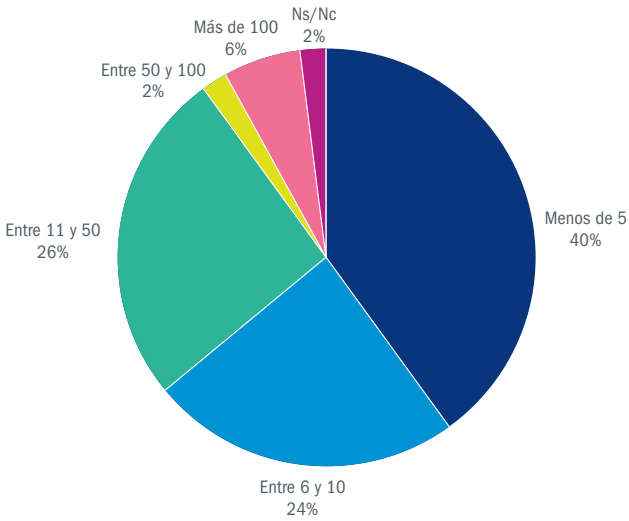
Número de servidores operados por la organización

Al menos un 35,7% de las organizaciones disponen de más de un servidor en producción, lo cual muestra un escenario con un uso significativo de los sistemas de información.



Número de puestos de trabajo con ordenadores tipo PC

Más de la mitad de las empresas tienen en sus instalaciones más de 5 ordenadores tipo PC para el desarrollo de su trabajo. Por lo tanto la necesidad de contemplar las medidas concretas en temas relacionados con la seguridad es evidente.



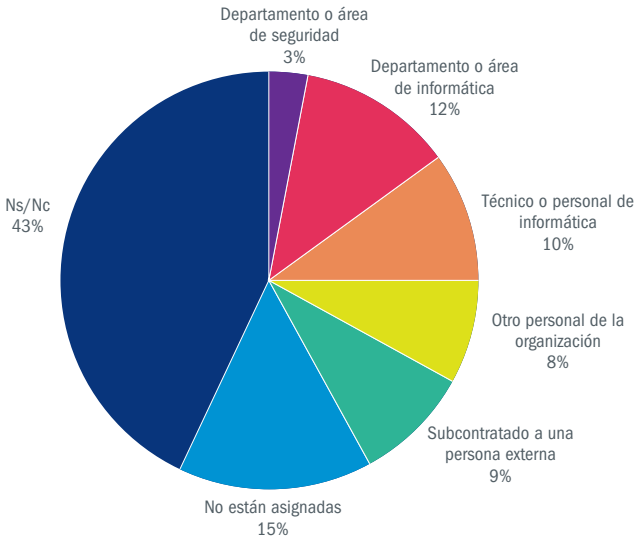
La gestión de la seguridad

En lo referente a la seguridad de la información, es importante que su gestión esté asignada a alguien. No es una condición indispensable que quién tenga asignada esta tarea lo haga en dedicación exclusiva a la seguridad.

Teniendo en cuenta que la mayoría de las empresas que han contestado al cuestionario son empresas pequeñas, es normal que la función de seguridad esté tan dispersa. Esta característica hace especialmente importante el que el personal de las empresas conozca los riesgos y las buenas prácticas de seguridad.

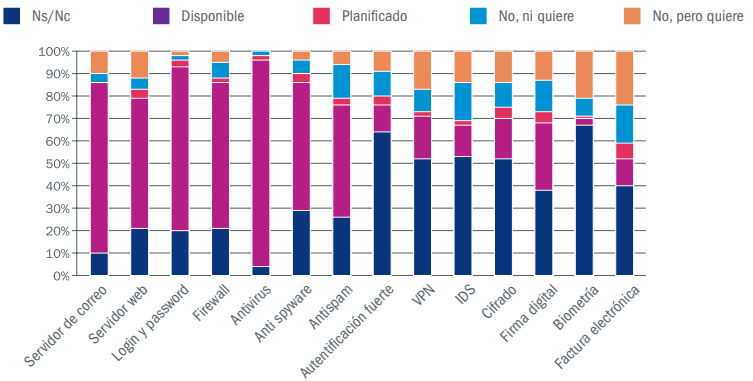
El que un 43,3% de las empresas no sepa o no conteste si la función de seguridad está asignada a alguien, presumiblemente signifique que no están asignadas.

Asignación de la función de seguridad



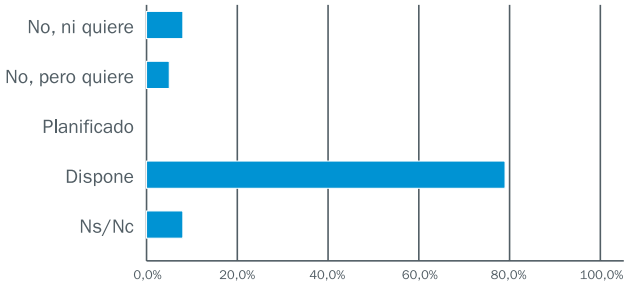
Elementos de que dispone

El primero de los grandes bloques de preguntas sobre el que se recoge información, hace referencia a los elementos de los cuales dispone la organización. En concreto, se solicita información sobre la disposición o no de 14 elementos. La gráfica siguiente resume los resultados obtenidos.



› Servidor de correo

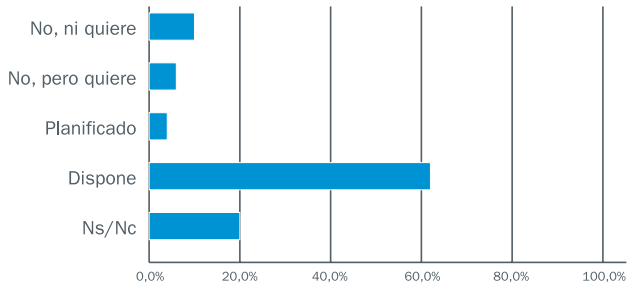
Desde la perspectiva de la seguridad de la información se trata de un dato especialmente relevante en su análisis global. Implica que se hace un uso generalizado del correo electrónico, y junto con las conclusiones a las que se llega en el estudio sobre los incidentes relacionados con código malicioso y spam, y carencias de cultura y formación, hace que el correo electrónico sea un potencial problema desde la perspectiva de la seguridad para un número elevado de organizaciones en la región.



› Servidor web

De forma similar a lo que ocurre con los servidores de correo, el uso de servidores web está ampliamente implantado. Los problemas de cultura y formación continúan estando presentes, sin embargo en este caso las organizaciones no han manifestado que estén sufriendo un número relevante de incidentes relacionados con este servicio. Lo que nos hace suponer que o bien las tecnologías de seguridad que los protegen (fundamentalmente los cortafuegos o firewalls) son más efectivas, o bien que su gestión está externalizada a personal experto.

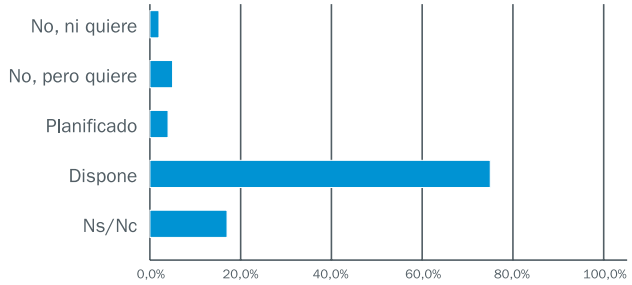
También es oportuno volver a resaltar el interés que ha manifestado un número relevante de organizaciones de disponer de sistemas de detección y prevención de intrusiones.



› Login y password

La autenticación de los usuarios es uno de los problemas complejos de resolver desde el punto de vista de los sistemas de información. Se trata de verificar que quién pretende acceder a los sistemas es quien dice ser para luego determinar a qué tiene acceso y dejarle entrar o no. El método de autenticación más difundido es el uso de un nombre de usuario y una contraseña, lo que se conoce como login y password.

El que con todo lo que se ha andado en materia de seguridad, continúen habiendo un 7,6% de empresas que aun no dispongan de algo tan básico como autenticación por login y password, da una idea de la dimensión del problema cultural y de concienciación existente.

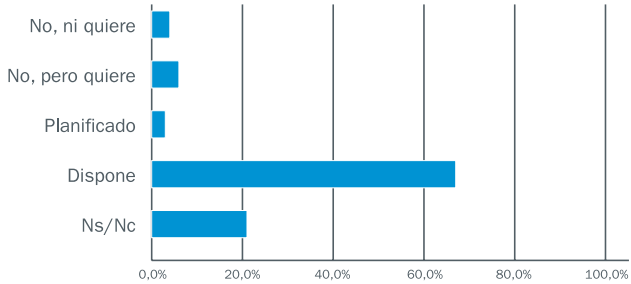


› Cortafuegos o firewall

La lectura de que actualmente al menos un 12% de las organizaciones no disponga de firewall, junto con el dato de uso de correo electrónico y web, indican que al menos ese porcentaje de empresas en la región no cuentan con vías de protección elementales de sus sistemas frente a intentos de acceso no autorizado desde el exterior.

Los incidentes relacionados con el acceso desde el exterior a los sistemas de la empresa a través de Internet son difíciles de detectar si no se dispone de cortafuegos o sistemas de detección de intrusiones, por lo que el hecho de no hayan aparecido datos relevantes en las cuestiones sobre incidentes, no quiere decir que no estén ocurriendo.

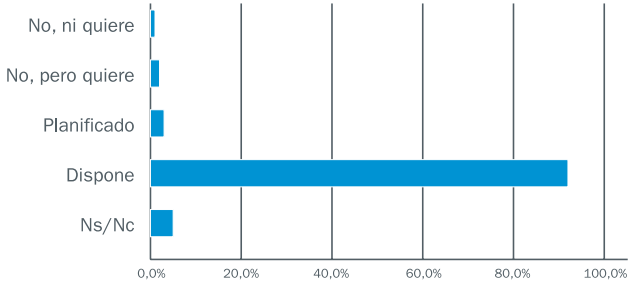
Esto, en el terreno de las tecnologías de la información, es equivalente a decir que más de un 13% de las empresas de la región no tienen una puerta en sus oficinas, por lo que los ciudadanos pueden entrar y salir con facilidad.



› Antivirus

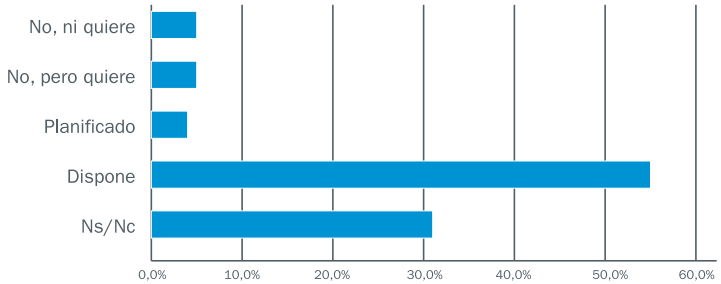
Es importante resaltar que, aunque más del 90% de las organizaciones disponen de soluciones antivirus, el número de incidentes relacionados con este tipo de amenazas es el más elevado. Esto sólo se puede entender como que las herramientas no están adecuadamente implantadas, mantenidas y/o actualizadas.

También el desconocimiento y la falta de cultura de seguridad ayudan de forma importante a que se continúen produciendo incidentes relacionados con el código malicioso, aunque las herramientas tecnológicas estén presentes en la inmensa mayoría de las organizaciones.



› Anti Spyware

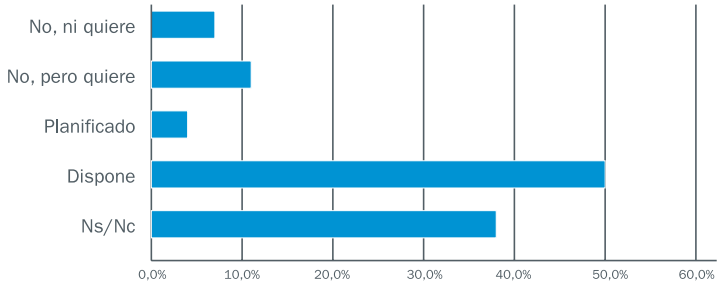
El spyware o código espía es una de las amenazas que con más frecuencia se materializa desde hace unos años. El impacto que tiene sobre la organización es bastante elevado, sin embargo pasan prácticamente desapercibidos, de hecho se han diseñado para que no levanten sospechas en el usuario infectado. De esta forma el atacante continuará recibiendo información de ese equipo, o utilizándolo para sus fines.



› 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. Resulta casi necesaria la utilización de un antispam que evite los problemas relacionados con este tipo de correos.

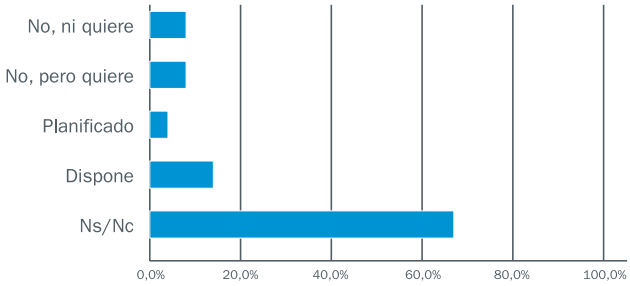
Es sorprendente que apenas llegue a la mitad el porcentaje de organizaciones que disponen de soluciones antispam, y que sin embargo el porcentaje de empresas que afirma recibir spam a diario esté por encima del 70%.



› Autenticación fuerte

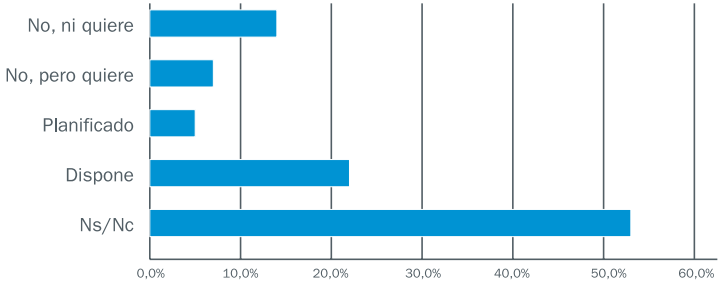
Como se ha comentado anteriormente en el apartado de login y password, la autenticación de los usuarios es uno de los puntos fundamentales en seguridad de la información. Existen técnicas de autenticación fuerte más robustas que el login y password, que se basan en que además de saber algo (la contraseña) el usuario debe tener algo (una tarjeta, un dispositivo USB especial, etc).

Estas técnicas no están muy difundidas, pero el abaratamiento de los tokens USB y de las tarjetas inteligentes, junto con el despliegue del DNIe, están convirtiéndolo en una tecnología que cuenta cada vez con más partidarios, especialmente para la autenticación ante sistemas que tienen unos requerimientos de seguridad especiales.



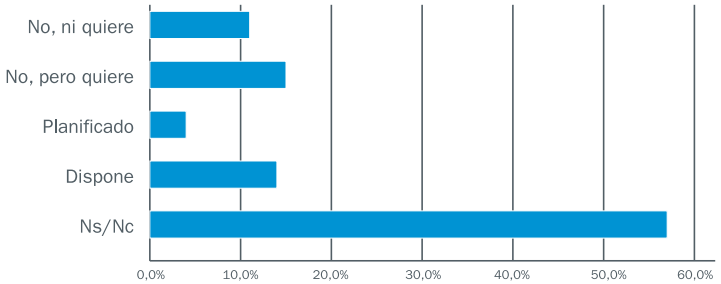
› Red privada virtual o VPN

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. Es reconfortante que más de un 20% de las organizaciones ya esté utilizando esta tecnología, y un 11,1% más tengan planificado ya, o quieran implantarla.



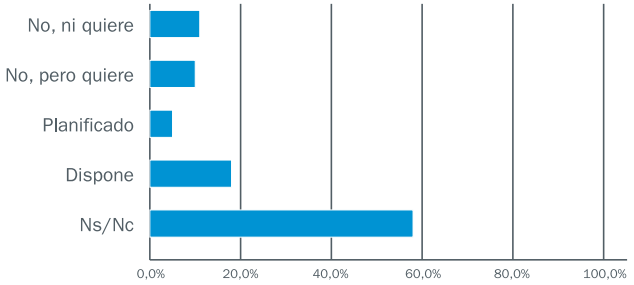
› Sistema de detección de intrusos o IDS

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. Resulta sorprendente el número de organizaciones que le gustaría disponer de esta tecnología.



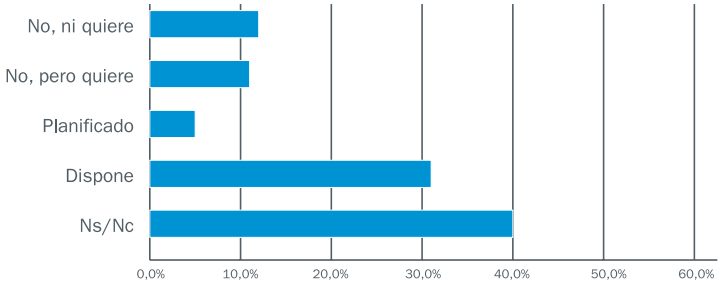
› Cifrado

Las empresas de la región hacen un uso importante del correo electrónico, intercambiando información a través de este medio que, lo menos que se puede afirmar, es que no le gustaría que se divulgara. Sin embargo la gran mayoría no utiliza herramientas de cifrado para proteger esta información, cuando se trata de una tecnología madura y barata.



› Firma Digital

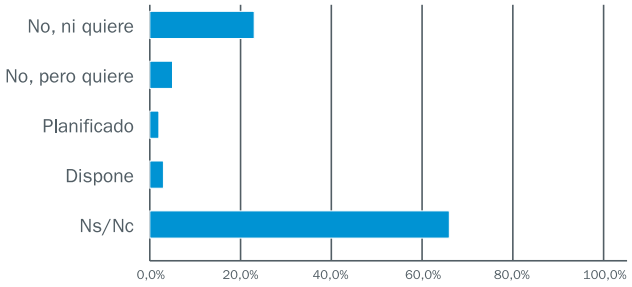
Se trata de una de las tecnologías con mayor proyección, que apoya el despliegue del nuevo DNIe. Más de un 17% de las organizaciones encuestadas tienen planificado o quieren implantar este tipo de soluciones en sus sistemas.



› Biometría

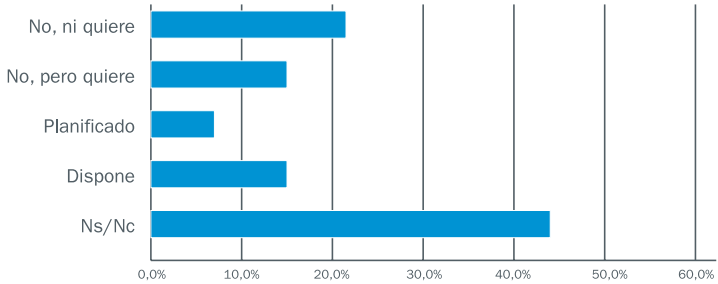
Es importante reseñar que a la biometría se le ha colocado un halo de ciencia ficción, de tecnología muy avanzada, indicada para aplicaciones militares o de alto secreto. Nada más lejos de la realidad, la biometría nace como una forma de facilitar a los usuarios la autenticación frente a los sistemas, de forma que no tengan que recordar contraseñas, ni llevar encima dispositivos de autenticación, sino que sea suficiente con su huella dactilar, voz o reconocimiento de cara.

En su uso civil no se pretende que sea infalible, como de hecho no lo son las alternativas actuales más difundidas como el sistema tradicional de login y password. El uso de la biometría facilita mucho la vida a los usuarios y hoy en día ya no es una tecnología cara.



› Factura electrónica

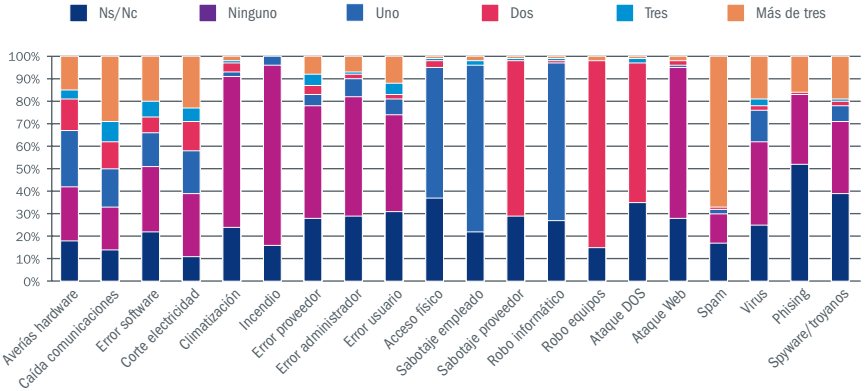
Un 20,7% de las empresas encuestadas (más de 1 de cada 5) o tienen planificado o quieren implantar la factura electrónica. Esto supone una apuesta clara del sector empresarial hacia los medios y canales electrónicos.



Los incidentes

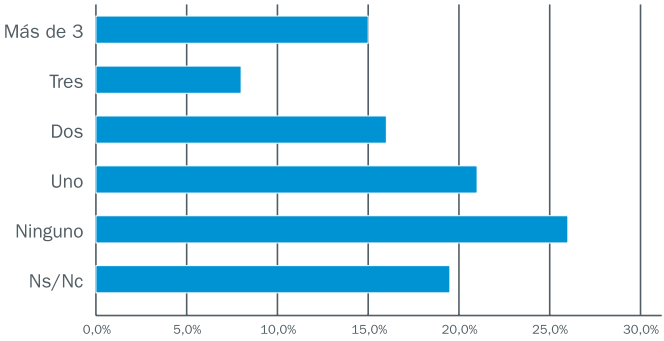
Tras la recogida de datos acerca de los elementos de seguridad de los que disponen las distintas empresas, se solicitó información acerca del número de incidentes, dentro de una lista dada, que habían sufrido en los últimos 12 meses.

La grafica que se muestra a continuación resume los resultados.



› Averías en el hardware

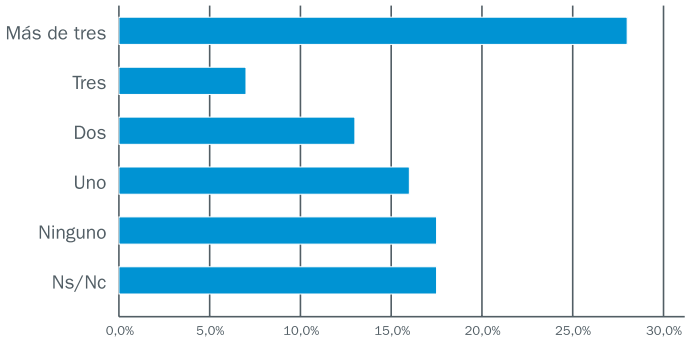
El número de incidentes por averías de hardware es significativo. Las políticas de reducción de costes, hacen que en muchas ocasiones se compre el hardware más barato en lugar del más adecuado, lo que al final acaba saliendo caro.



› Caídas en las Comunicaciones

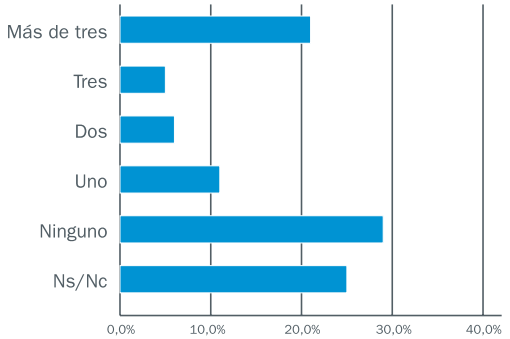
Se ha popularizado el uso de las líneas ADSL, pero en la mayoria de las ocasiones se contratan para uso profesional servicios que están diseñados para un uso domestico, y con un precio pensado para este uso.

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.



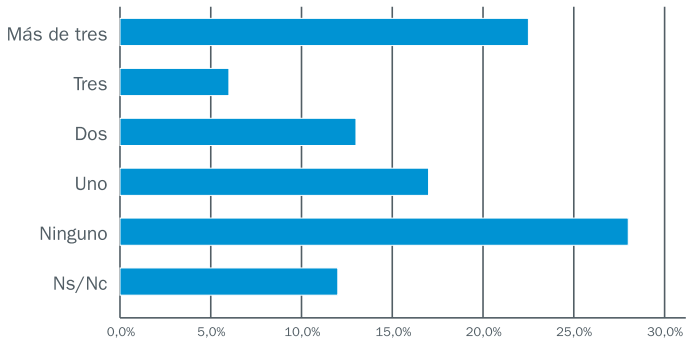
› Errores en el Software

En muchas ocasiones los errores de software no son tales, sino que más bien están provocados por un mal uso parte de los usuarios. Sin embargo si es cierto que existe un índice importante de incidencias debidas a carencias de los programas.



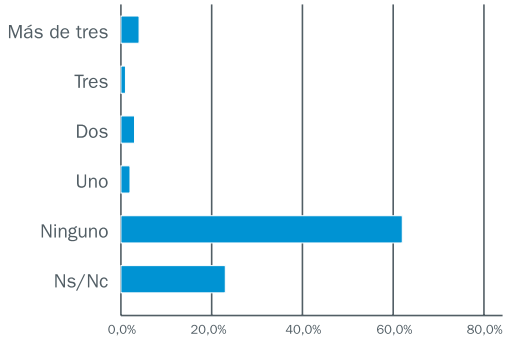
› Cortes en el suministro eléctrico

No es ningún secreto que el suministro eléctrico está dando muchos dolores de cabeza en nuestro país y en el mundo entero. No es fácil que esta situación mejore, por lo que las organizaciones deben comenzar a plantearse incorporar sistemas eléctricos de respaldo como Sistemas de Alimentación Ininterrumpida o, dependiendo de la criticidad de los procesos, incluso Grupos Electrógenos de generación de electricidad.



› Problemas de climatización

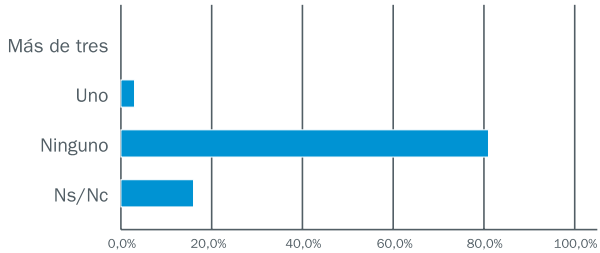
Este tipo de problemas toman especial relevancia en las organizaciones que disponen de un número importante de servidores instalados en una misma sala (a la que generalmente se denomina Centro de Proceso de Datos o CPD). En estos casos, el suministro de frió es crítico. Para las organizaciones que no disponen de este tipo de salas, la climatización suele ser más un tema relacionado con el confort del personal, que con el buen funcionamiento de sus sistemas.



› Incendios

Es habitual que cuando se le plantea a una organización que debe tomar precauciones para evitar incendios, responda que la probabilidad es tan baja que no merece la pena complicarse la vida con este tipo de medidas.

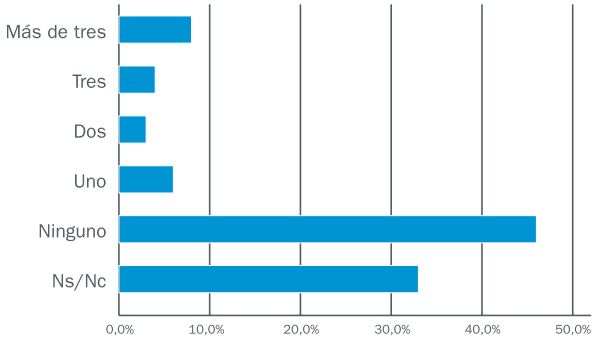
La oficina sin papeles sigue siendo un objetivo lejano, y a día de hoy suele concentrarse una carga de fuego importante en las instalaciones de las empresas, y como se aprecia en las respuestas obtenidas, la probabilidad es baja, pero los incendios se dan y sus consecuencias son muy relevantes.



› Errores de terceros

Desde la perspectiva de la seguridad de la información, los terceros son una fuente potencial de problemas que se debe analizar de cara a adoptar las medidas adecuadas (firma de acuerdos de confidencialidad, cláusulas de responsabilidad en los contratos, control de acceso físico, etc.).

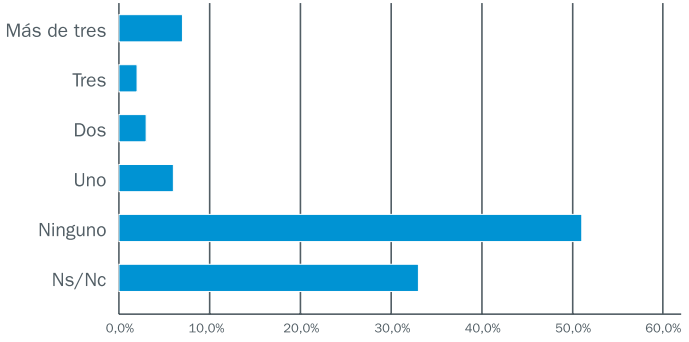
Habitualmente las organizaciones alegan que este tipo de medidas no son necesarias, porque los terceros no producen incidentes. Las respuestas obtenidas indican que esto no es así, y sí que se producen incidentes por errores de terceros.



› Errores de administradores

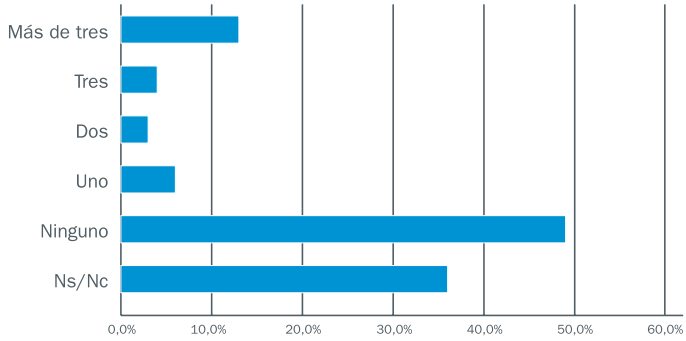
Los administradores de los sistemas de información tienen acceso absolutamente a todas las funciones e información que estén disponibles en el sistema, de ahí que los errores cometidos por estos usuarios pueden ser especialmente delicados.

La mejor forma de evitar este tipo de errores es invertir en la formación de los administradores, así como la definición de las funciones y responsabilidades de los mismos en materia de seguridad.



› Errores de usuarios

Los usuarios también provocan incidentes con sus errores. Una vez más la formación marca la diferencia.

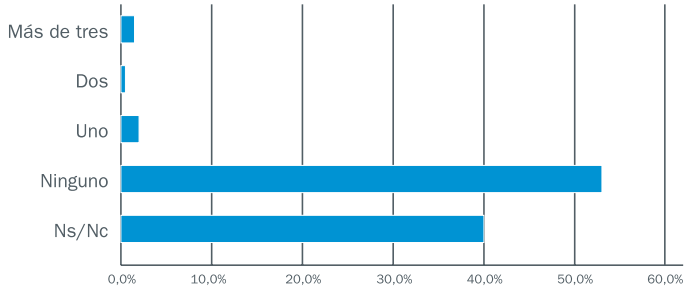


› Acceso físico no autorizado

Tradicionalmente la seguridad física y la informática se consideran mundos separados, adoptando las empresas medidas de protección en ambos entornos de forma aislada, es decir, sin tener en cuenta la relación que puede existir entre ambas.

El que no se controlen adecuadamente los accesos físicos a los recursos de la organización puede traer consigo problemas de seguridad con los sistemas de información, por lo que se deben alinear las estrategias de protección en los dos entornos.

Aunque el porcentaje de incidentes relacionados con accesos físicos no autorizados es escaso, lo cierto es que este tipo de incidentes se producen y se deben tener en cuenta a la hora de analizar los posibles problemas de seguridad en sistemas de información.

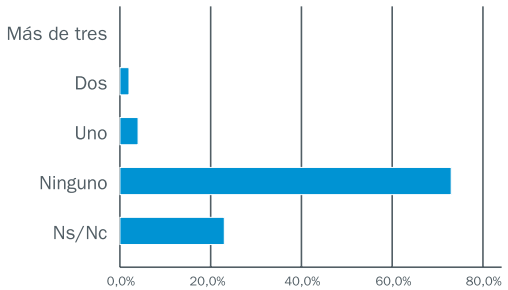


› Sabotaje de empleados

La amenaza que suponen los empleados desleales ha existido siempre. Hasta el momento las acciones que podían llevar a cabo estos empleados para perjudicar los intereses de la organización no habían tenido como objetivo los propios sistemas de información de la empresa, pero cada vez es más frecuente que se utilicen estos recursos para causar un perjuicio a la empresa.

El hecho de que en la mayoría de las ocasiones se trate de empresas pequeñas en las que generalmente se conocen todos los empleados, hace que se trabaje en un clima de confianza que por una parte hace que los empleados tengan una vinculación especial con la organización, pero por otra hace que se relajen las medidas de seguridad orientadas a evitar acciones de este tipo.

En cualquier caso la incidencia de este tipo de situaciones en la región es baja.

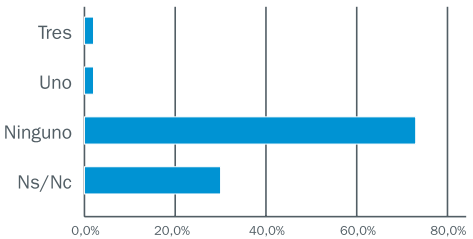


› Sabotaje de terceros

De forma similar a lo planteado en el punto anterior, la amenaza que suponen los proveedores descontentos también ha existido siempre.

En términos generales existe una relación de confianza con los proveedores que hace que no se analicen los riesgos que pueden suponer este tipo de acciones, por lo que dependiendo de la naturaleza de los procesos de la empresa se deberían analizar con más detenimiento.

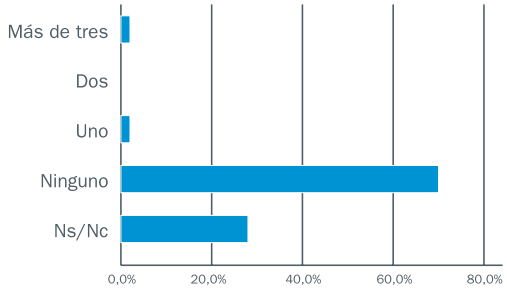
En cualquier caso la incidencia de este tipo de situaciones en la región también es baja.



› Robo de información

Los problemas que más relacionados están con los empleados, y sobre todo si se produce un despido, es el robo de información o de equipos.

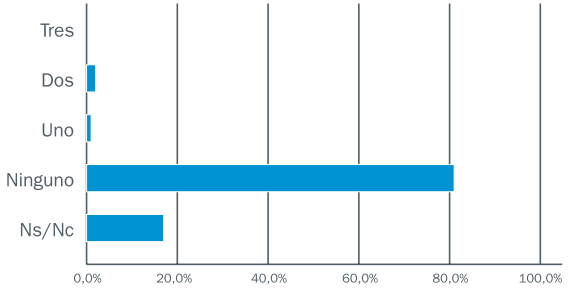
En el primer caso, es frecuente que el robo de información se produzca para su posterior utilización en la nueva empresa contratante, pero, para evitar este tipo de fraude, es importante que el empleado esté concienciado. Y esto parece cumplirse en las empresas riojanas ya que, de todas las encuestas contestadas, solamente en cinco casos se ha producido algún robo de información.



› Robo de equipos

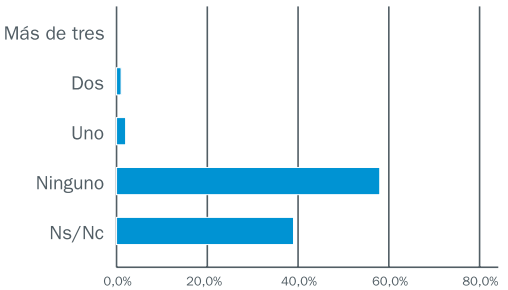
En el segundo caso, el robo de equipos, se va a producir más con un fin para uso personal que cualquier otro motivo, y, al igual que en el caso anterior, es importante la concienciación del empleado para evitarlo.

Este caso es más favorable que el anterior, puesto que en un 80,6% de las empresas no se ha producido este tipo de robo. Además, hay tres empresas en las cuales se han producido dos robos de equipos en el último año, que si se añade más del 17% restante del cual no se tienen datos, prácticamente se completa el 100% de la muestra.



Ataques de denegación de servicio o DoS

De momento este tipo de ataques van más orientados hacia empresas grandes, o con un número importante de servicios on line. De las respuestas obtenidas se desprende que la incidencia de este tipo de ataques es baja.



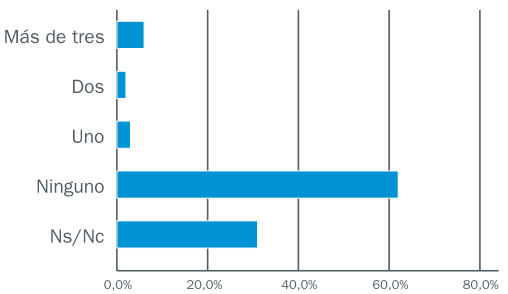
Ataques a la página web

El número de empresas que cuentan con una página web crece de forma constante, convirtiéndose generalmente en un escaparate de la propia empresa.

Los ataques a las páginas web de las empresas tienen varias posibles motivaciones:

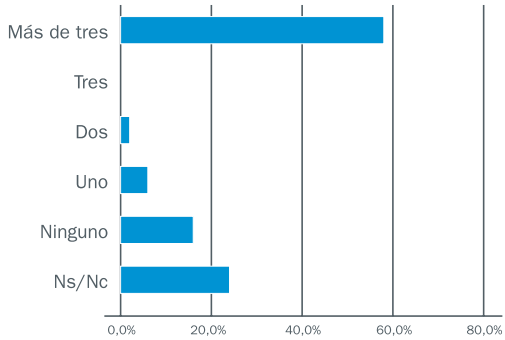
- Perjudicar a la empresa propietaria de la página web
- Infectar la página web para que a su vez infecte a los visitantes y obtener el atacante un beneficio indirecto
- Cada vez son menos frecuentes los ataques que no tienen una justificación clara (demostrar que se puede, entretenimiento, etc.).

También es importante reseñar que si la empresa no dispone de mecanismos que le permitan detectar este tipo de ataques, sólo va a percatarse de que su página web ha sido atacada en caso de que el ataque sea muy evidente (por ejemplo modificando contenidos o dejándola in operativa), o bien porque algún usuario le avise de que su página web está infectada. Esto hace pensar que aunque el número de empresas que han confirmado que han sufrido ataques a su página sea escaso, el número real pueda ser más elevado.



› Spam

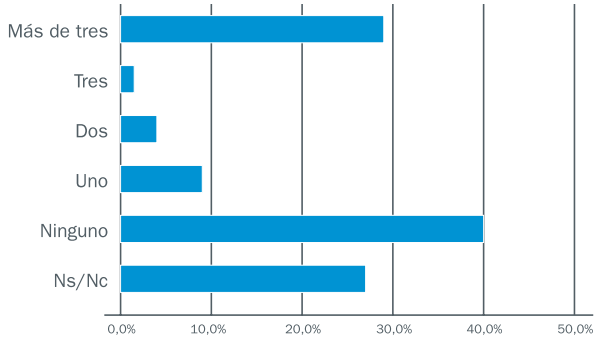
De las respuestas obtenidas de los encuestados, se concluye que el spam es un problema real en las empresas de la región, por lo que se deben apoyar decididamente medidas que ayuden a controlarlo.



› Virus

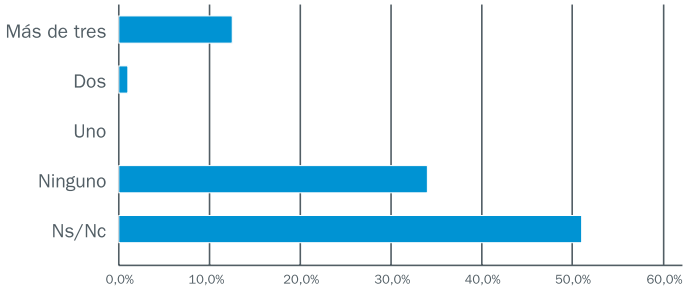
El elevado número de incidentes relacionados con virus, junto con el amplio despliegue de herramientas antivirus, sólo puede explicarse si estas herramientas no están adecuadamente instaladas, configuradas y/o mantenidas.

También ayuda a que se sigan produciendo tantos incidentes por virus el desconocimiento que existe a nivel general de los temas relacionados con la seguridad.



› Phishing

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.



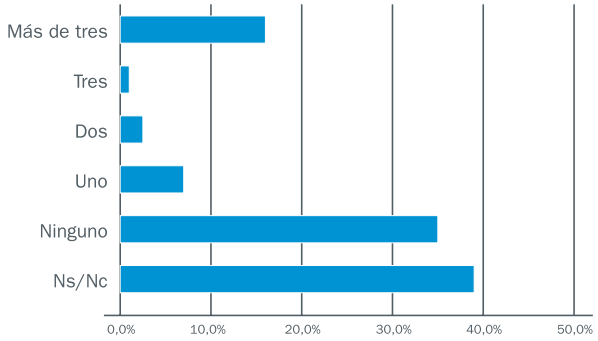
› Spyware y troyanos

En los últimos años la tendencia del código malicioso ha ido cambiando, pasando de intentar ser lo más destructivos posible, a ser lo más rentable posible. Esta tendencia ha multiplicado por cinco los ataques por programas espía o spyware, que ya no intentan destruir la información del ordenador, sino quedarse instalados recopilando información que pueda ser de utilidad (usuarios y contraseñas, datos bancarios, etc.) para obtener un beneficio económico.

También es frecuente que estos programas espía se instalen y permitan al atacante utilizar el ordenador infectado para hacer envíos masivos de correo, o incluso lanzar ataques desde ese ordenador contra otros.

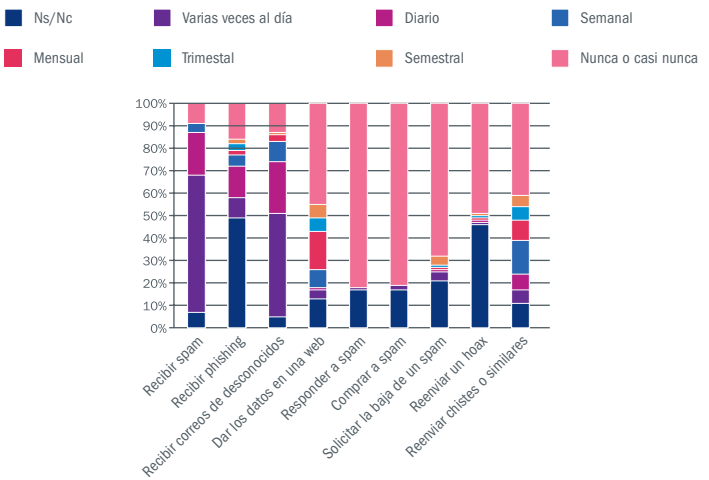
La mayoría de las herramientas actuales antivirus incorporan funcionalidades de antispyware, pero en muchas ocasiones no están adecuadamente configuradas, o simplemente están desactivadas.

El número de incidentes por spyware en la región es bastante elevado, lo que evidencia la necesidad de mejorar la protección de las empresas frente a esta amenaza.



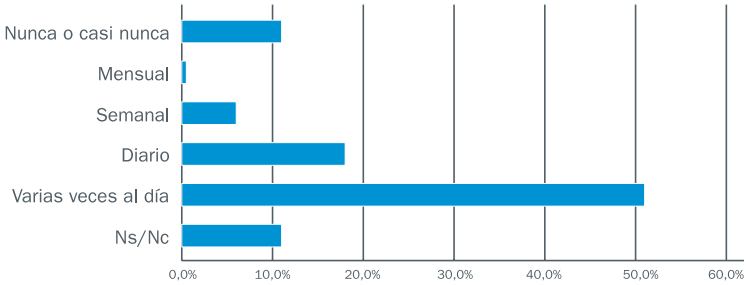
Frecuencias relacionadas con el correo

Una de las vías por las que se pueden producir mayores incidentes, y por lo tanto hay que aplicar mayor seguridad, es el uso del correo electrónico. Debido a esto, se planteó una pregunta que reflejaba distintas circunstancias relacionadas con su uso y la frecuencia de ocurrencia de cada una de las nueve situaciones que se propusieron. Los resultados obtenidos se pueden observar de forma resumida en la gráfica siguiente.



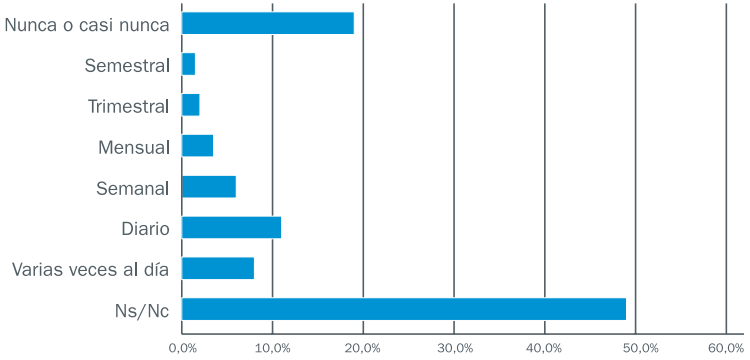
› Recibir spam

El spam se está convirtiendo en un problema general. Como se vio anteriormente, el porcentaje de organizaciones que cuentan con soluciones antispam es elevado, sin embargo, no están dando buenos resultados.



› Recibir Phishing

El phishing es uno de los ataques más rentables, puesto que los atacantes tratan de obtener información de los usuarios que les permita acceder fundamentalmente a sus cuentas bancarias o a sus tarjetas de crédito. El número correos de phishing que están recibiendo las empresas de la región es verdaderamente preocupante.

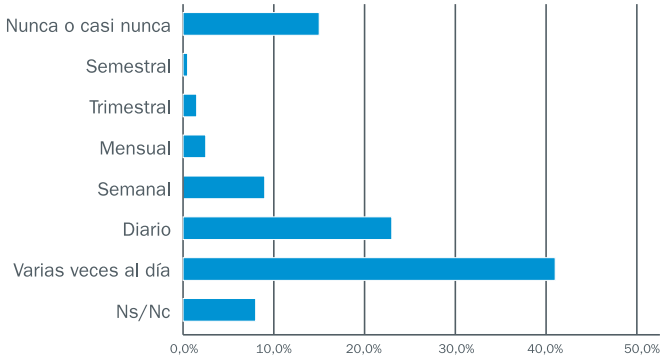


› Recibir correos de desconocidos

Como se ha comentado anteriormente, el correo electrónico lleva asociadas muchas de las amenazas más frecuentes para los sistemas de información (phising, virus, spyware, spam,etc.). Generalmente los correos que provocan este tipo de incidentes provienen de desconocidos, por lo que controlando los correos que se reciben de direcciones desconocidas se puede controlar una parte importante de la amenaza.

Sin embargo las empresas acostumbran a recibir correos electrónicos de desconocidos que son perfectamente legítimos (de potenciales clientes, proveedores, personas interesadas, ofertas de empleo, etc.) por lo que no se pueden descartar estos correos sin más.

Cuando casi un 65% de las empresas reciben correos de desconocidos a diario, la alternativa más eficaz que se puede adoptar es otra vez la formación para que el personal de la empresa pueda discernir qué correos borrar sin ni siquiera leerlos, y qué correos hay que leer aunque provengan de desconocidos.



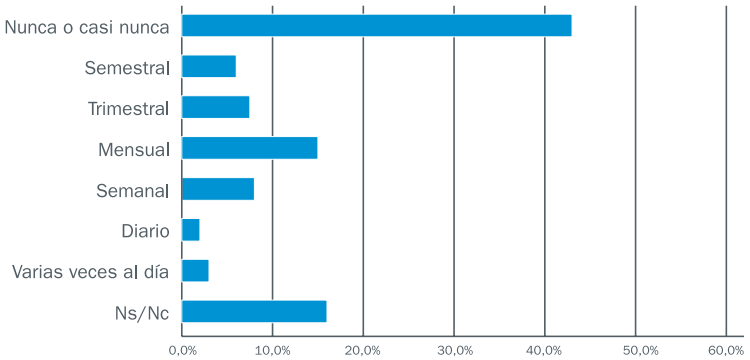
› Dar datos personales en las páginas web

Hay veces que el correo electrónico que se recibe no es de alguien completamente desconocido, si no que la propia persona ha facilitado los datos en alguna web para que le envíen información, y esto puede no ser conveniente a no ser que se esté seguro del tipo de web del que se trata.

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.

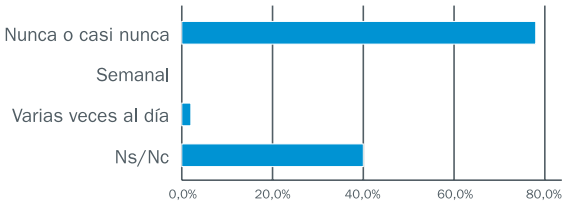
Aunque en España es ilegal enviar información comercial que no se ha solicitado expresamente, en la mayoría de los países no lo es, por lo que en ocasiones la información que se da en estas páginas es utilizada con fines publicitarios.

Lo mejor para evitar estos problemas es no dar datos personales en páginas web que no se tenga claro si el uso va a ser el que desea el usuario.



› Responder a spam

Los spammers necesitan verificar si las cuentas de correo a las que están enviando la información son válidas, por lo que en caso de que los usuarios respondan a los correos de spam, aunque sea para manifestar su queja por los correos recibidos, lo único que consiguen es que los spammers tengan constancia de que esa cuenta es válida, y se está leyendo.

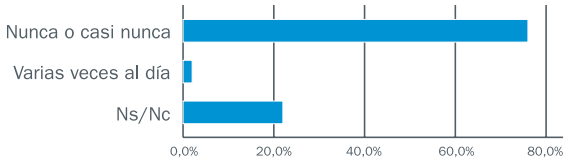


› Comprar a spam

El objetivo final del correo de spam es lograr que los usuarios compren los productos que están ofertando a través de estos correos, y conseguir así un retorno económico. Si en el caso anterior se indicaba que responder a un correo de spam es una forma de informar a los spammers que la cuenta de correo existe y que se lee, comprar a spam es una invitación a que continúen enviándonos este tipo de correos.

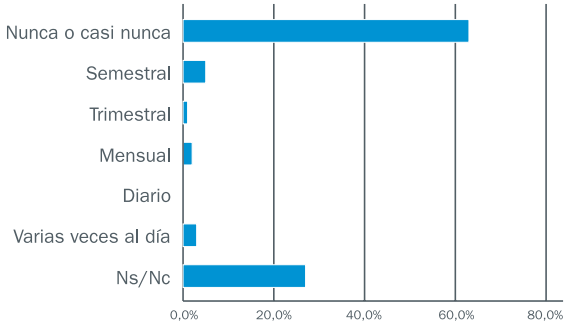
En este apartado la respuesta ha sido baja, pero el hecho de que un 1,6% de las empresas hayan comprado alguna vez a

un spam es en sí mismo una respuesta de porque hay tanto spam, Teniendo presente que el envío del spam prácticamente no tiene coste para los spammers, si logran un índice de respuesta de este orden de magnitudes, podemos entender que se trata de un técnica realmente fructífera.



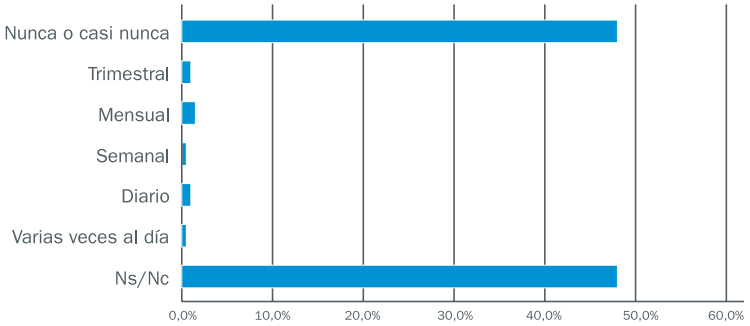
› Solicitar la baja a un spam

Algo que a priori puede parecer recomendable es solicitar la baja en el mismo. Sin embargo es otra forma de constatar al remitente que la cuenta es válida, por lo que lo único que se consigue es recibir más spam.



› Reenviar un hoax

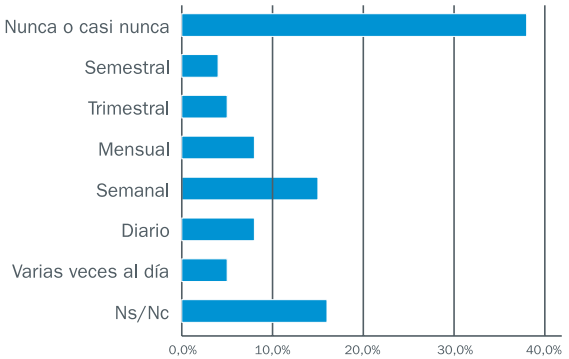
El envío de correos en los que se solicita ayuda para localizar a un menor, o en el que se informa de un supuesto problema informático al que el mismo correo le da la solución, es una forma de ocupar los sistemas informáticos, cuando no esconden algún tipo de código malicioso.



› Reenviar chistes, presentaciones o similares

Como se ha expuesto anteriormente, el correo es la vía más fácil para la recepción de virus y troyanos, la manera más popularmente utilizada son las "cadenas de correos" que contienen chistes o similares, por ese motivo resultó interesante incluirlo como la última circunstancia relacionada con el correo. Además de que esto puede supone una pérdida en la productividad del empleado que se entretiene con este tipo de distracciones, ocupando recursos tecnológicos de la empresa.

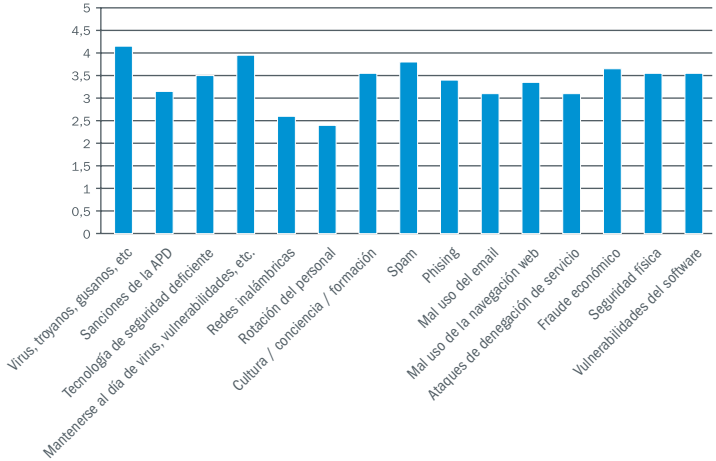
Esta respuesta nos da una idea del uso que se está haciendo de los sistemas informáticos de las organizaciones en tareas que no están relacionadas con el trabajo. Deja de manifiesto que un porcentaje muy alto de las empresas tienen personal que dedica parte de su tiempo y de los recursos de la empresa para fines personales y no relacionados con el trabajo. En sí mismo no tiene que ser un problema de seguridad, pero desde luego lo es de pérdida de productividad y de ocupación de los recursos de la empresa. También es conveniente tener en cuenta que en ocasiones estos correos esconden algún tipo de código malicioso incluido en los documentos que se reenvían.



Las mayores preocupaciones

Las personas actúan en base a las preocupaciones que tienen, y, en función de las mismas, van a tomar unas medidas u otras dependiendo del grado de la inquietud que tengan. Por ello, resulta interesante saber cuáles son las principales preocupaciones en lo concerniente a seguridad que tienen las empresas. Para ello, se realizó una pregunta en la que se recogían 15 posibilidades y se pedía que valorasen su grado de preocupación en función de unos valores facilitados.

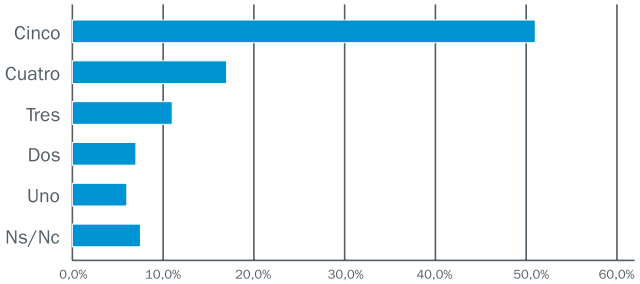
Como visión general se puede afirmar que la preocupación sobre los temas preguntados es bastante alta, y la muestra es bastante homogénea a la hora de valorarla.



› Virus, spyware y troyanos

En lo referente a los virus, troyanos, gusanos, etc., se puede decir que hay una gran preocupación, puesto que algo más de la mitad de la muestra (50,8%) puntúa estos elementos como “muy preocupado”. El resto de la muestra se ordena de forma ascendente en el grado de preocupación.

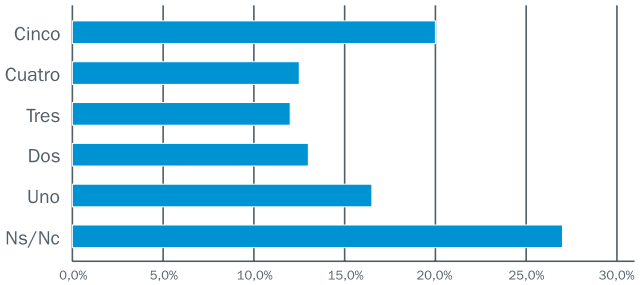
Una vez más queda de manifiesto que aunque la tecnología de protección de código malicioso está desplegada, lo cierto es que los usuarios no están tranquilos al respecto. Viendo la respuesta que se dio en el apartado de incidentes, es normal.



› Sanciones de la Agencia de Protección de Datos

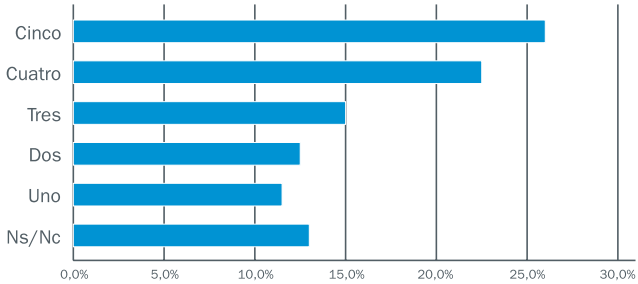
En lo referente a las posibles sanciones de la APD, no existe una gran preocupación, puesto que la frecuencia más alta corresponde al 20,2% que se situarían en "muy preocupado".

La Ley Orgánica de protección de Datos de Carácter Personal, y el miedo a las inspecciones y sanciones por parte de la Agencia de protección de Datos se ha esgrimido durante los últimos años como un argumento de peso para que las organizaciones adopten medidas en relación con la seguridad de los sistemas de información. Lo cierto es que, aunque la preocupación existe, es de las menos relevantes de entre las que se han planteado en el estudio.



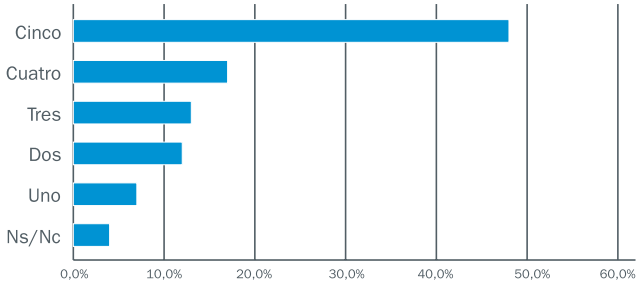
› Tecnología de seguridad insuficiente

Es obvio pensar que para que algo pueda avanzar, las tecnologías que le rodean tienen que hacerlo a la par, por lo que se cuestionó sobre si una tecnología de seguridad deficiente es una preocupación o no, de lo que se obtuvieron los siguientes datos.



› Mantengase al día

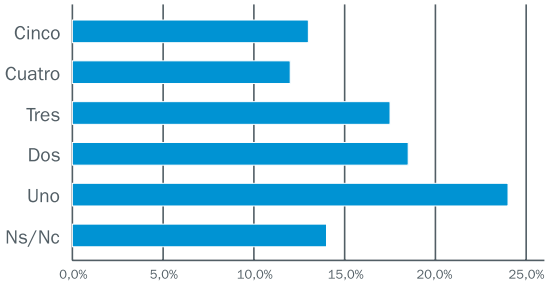
Para evitar ciertas debilidades que se pueden producir en la seguridad, es importante mantenerse al día en cuanto a los nuevos virus o nuevas vulnerabilidades que van surgiendo, por lo que esto debería ser una preocupación para las empresas, como así lo manifiestan, ya que la mitad de la muestra dice estar muy preocupado en este aspecto.



› Redes inalámbricas

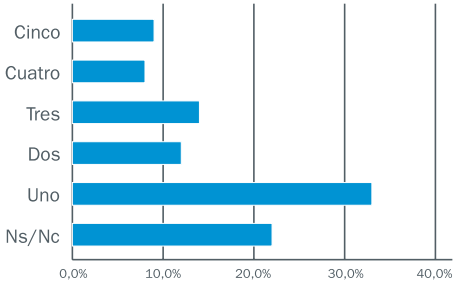
El establecimiento y uso de redes inalámbricas también puede ser un motivo de preocupación en lo referente a seguridad de la información, por lo que se decidió incluirlo aquí también. En este aspecto, una vez analizados los datos no parece existir una gran preocupación, ya que casi el 24% de la muestra dice no estar nada preocupado en este aspecto.

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 el que el acceso a la red inalámbrica este protegido por un algoritmo seguro; y por otra que el segmento donde se encuentra la red inalámbrica este debidamente aislado del resto de la red de la organización.



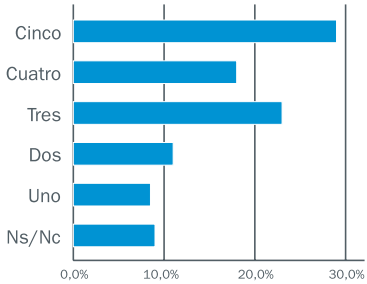
› Rotación del personal

La rotación de personal, con lo que implica en cuanto a la adaptación en el nuevo puesto, puede suponer un pequeño peligro para la seguridad de la información, motivo por el cual se incluyó también este ítem en el cuestionario. En la mayoría de los casos, esto no supone una gran preocupación, ya que un 46,4% no está preocupado o está poco preocupado.



› Falta de cultura, concienciación y divulgación

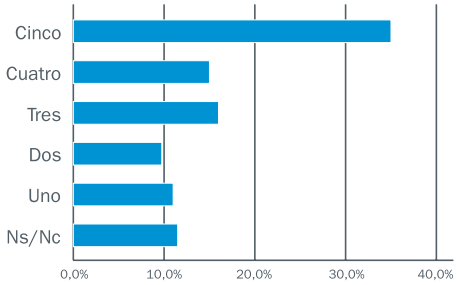
La falta de cultura puede suponer un impedimento para el desarrollo de la seguridad de la información, tal y como será planteado posteriormente, por eso, la cultura, la conciencia o la formación, pueden ser una preocupación para las empresas, y así lo demuestra el hecho de que el 48% de la muestra esté muy preocupado o bastante preocupado.



› Spam

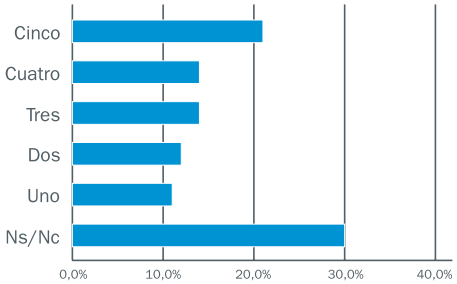
Antes se ha comentado que uno de los problemas que se repiten con mayor frecuencia son el spam o el phishing, por lo que resultó interesante preguntar sobre la preocupación que tienen sobre estos elementos.

El primero es el relacionado con el spam, del que un 35,3% dijo estar muy preocupado en este aspecto.



› Phishing

El segundo es el relacionado con el phishing, donde no se puede hablar de un acuerdo en lo referente a si es un elemento del cual hay existe mucha o poca preocupación, ya que el porcentaje más alto es el correspondiente al “no sabe/no contesta”.

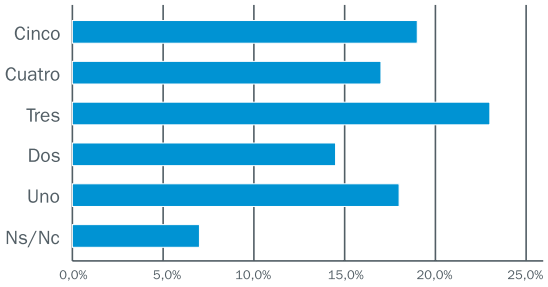


› Mal uso del email

El tercer elemento es el relacionado con el mal uso del e-mail, del cual se ha analizado una pregunta completa del cuestionario, pero la preocupación por un mal uso no supone una gran preocupación al no existir un claro acuerdo.

El principal problema de seguridad que se plantea con el uso del email es de confidencialidad de la información enviada mediante este medio de intercambio de información. El email no tiene ninguna característica de confidencialidad, por lo que se puede afirmar que la información que se envía por email sin proteger (por ejemplo con una contraseña o con técnicas de cifrado) no tiene garantizado que únicamente sea leída por el destinatario.

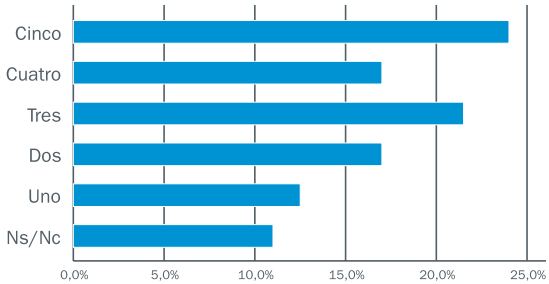
Por otra parte se da con una cierta frecuencia el enviar emails a direcciones equivocadas, especialmente si se utilizan las facilidades de auto completado de las direcciones de email que llevan incorporados los clientes de correo.



› Mal uso de la navegación web

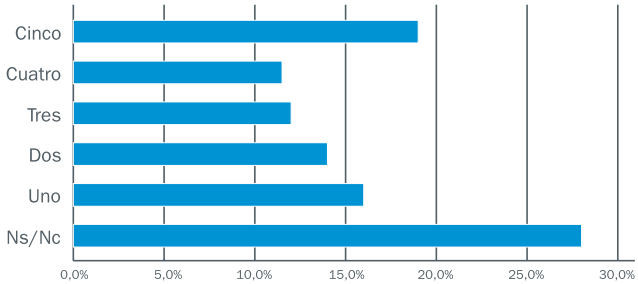
El cuarto elemento es el relacionado con el mal uso de la navegación web, ya que ésta puede incluir el acceso a páginas de Internet que pueden contener virus entre otras cosas.

Hacer un mal uso de la navegación web, además de redundar en una pérdida de productividad, puede provocar que la empresa se descargue código malicioso sin saberlo a través de la web. Aparte de que algún usuario pueda estar navegando por páginas que ética o moralmente no sean adecuadas.



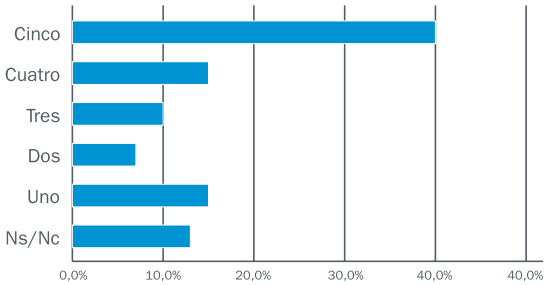
› Ataques de denegación de servicio

El quinto elemento, del cual ya se había preguntado anteriormente en el número de incidentes, son los ataques de denegación de servicio. En este caso hubo más de un 28% que no contestó a esta pregunta.



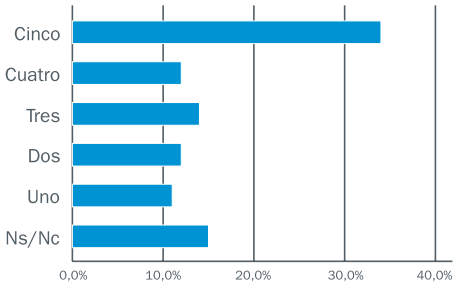
› Fraude económico

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.



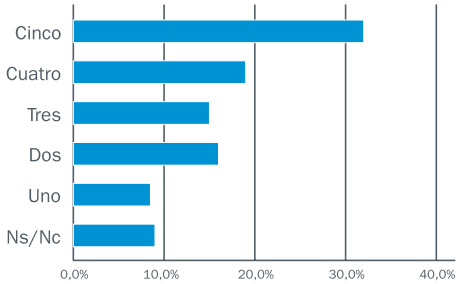
› Seguridad física

Algunos de los incidentes que se producen en las empresas son debidos a accesos físicos no autorizados, por lo que la seguridad física debe suponer una preocupación. En este caso, algo más de un tercio de la muestra dijo estar muy preocupado con este aspecto de la seguridad.



› Vulnerabilidades del software

Como último elemento se quiso saber el grado de preocupación que generan las vulnerabilidades del software.

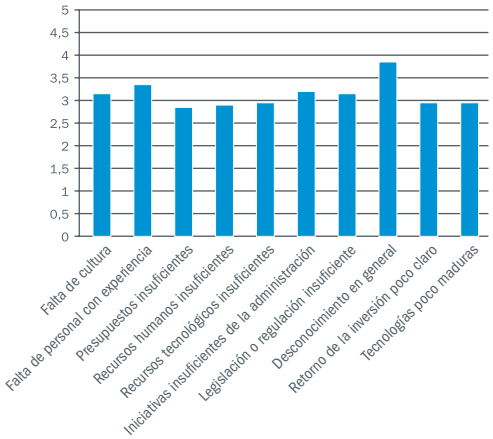


Los obstáculos para el desarrollo de la seguridad

Como se ha comentado anteriormente, las personas actúan en base a las preocupaciones que tienen, pero existen obstáculos que impiden actuar como se quisiera o debiera, por este motivo, se preguntó acerca de los obstáculos para el desarrollo de la seguridad.

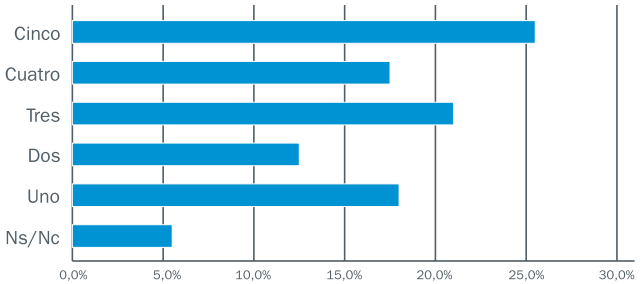
Esta pregunta incluye diez elementos que, según el propio criterio, pueden ser considerados como obstáculos; criterio que ha sido corroborado, puesto que para la mayoría de las empresas que han contestado al cuestionario, también los consideran así.

Todos los obstáculos tienen una media general superior a 3.50, lo que puede interpretarse como que las empresas son conscientes de los obstáculos que frenan el desarrollo de la seguridad.



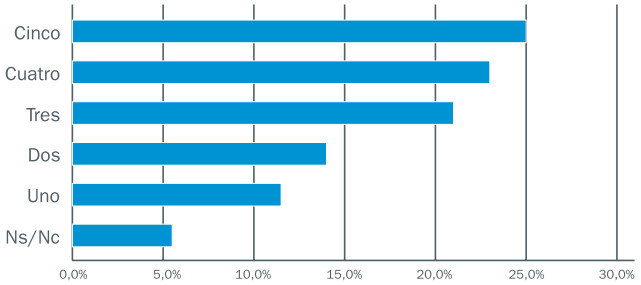
› Falta de cultura

El primer obstáculo del que se pidió información es de la falta de cultura. Este es uno de los más importantes puesto que no puede haber una preocupación en lo referente a la seguridad si no existe cultura ni conocimiento sobre el tema.



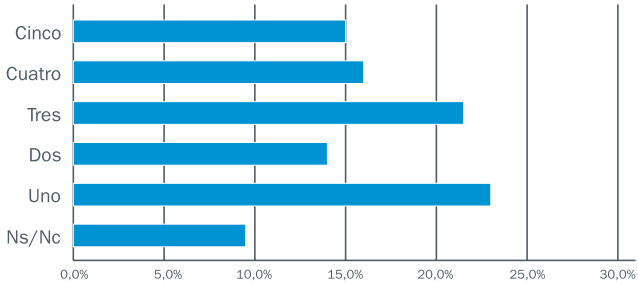
› Falta de personal formado y con experiencia

Parece que en las empresas tienen claro que el hecho de carecer de personal formado y con experiencia en el ámbito de la seguridad supone un obstáculo para el desarrollo de la misma, y así lo hacer ver la muestra, ya que casi un 48% opina que resulta un obstáculo importante.



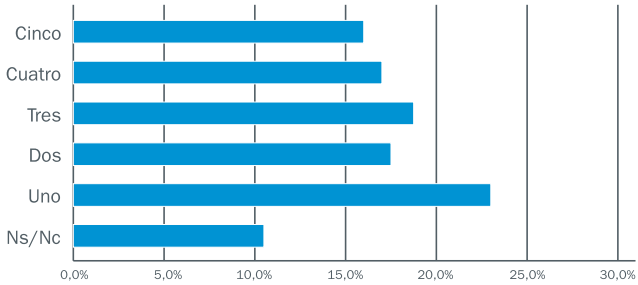
› Presupuestos insuficientes

Un posible motivo por el cual las empresas carecen de personal especializado en seguridad es por la falta de presupuesto o porque éste es insuficiente. Esta puede ser la visión que se tiene desde fuera de la empresa, pero ellas no lo perciben de la misma manera, y así lo demuestran los datos obtenidos.



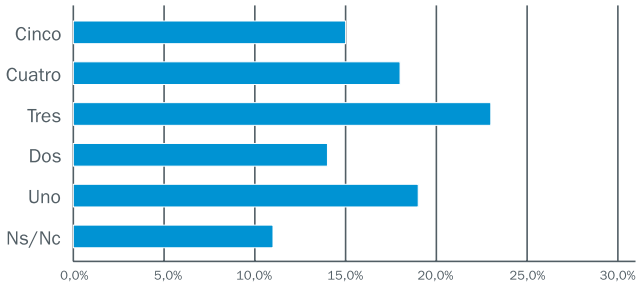
› RRHH insuficientes

Éste obstáculo es una variante de los dos anteriores. Hay que tener un presupuesto suficiente para tener recursos humanos formados y con experiencia.



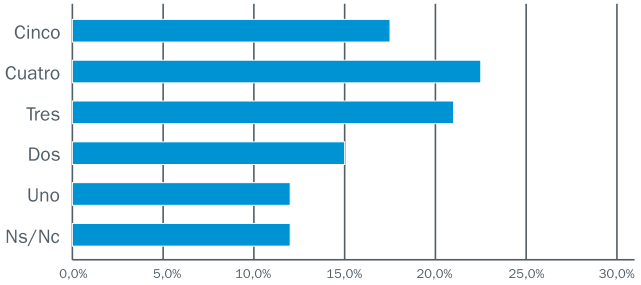
› Recursos tecnológicos insuficientes

Al igual que son importantes los recursos humanos, también lo son los recursos tecnológicos, ya que sin éstos poco puede hacerse.



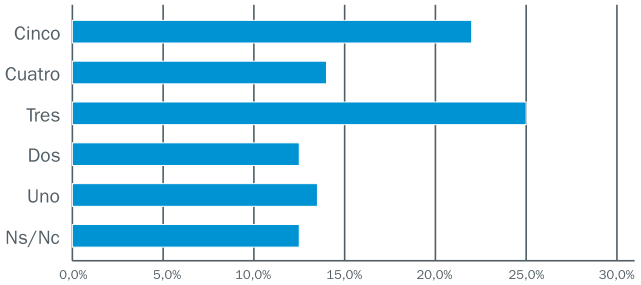
› Iniciativas insuficientes desde la administración pública

Actualmente, la seguridad de la información, así como la mayoría de las iniciativas tomadas al respecto, parten de instituciones privadas, por lo que se podría pensar que una mayor implicación en las iniciativas proveniente de la Administración Pública redundaría en un desarrollo más rápido y eficaz de la seguridad.



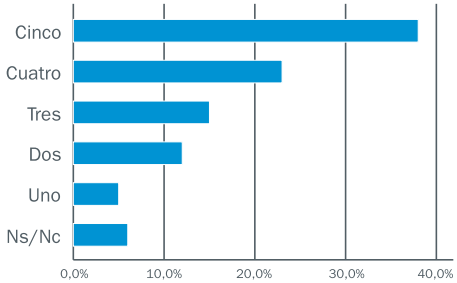
› Legislación o regulación insuficiente

En España existe una legislación clara que exige a las organizaciones implantar ciertas medidas de seguridad con respecto a la protección de sus datos, fundamentalmente la Ley Orgánica de Protección de Datos de Carácter Personal, la Ley de los Servicios de la Sociedad de la Información y el Comercio Electrónico, y la Ley de Firma Electrónica. Aun así, desde algunos foros especializados se considera que esta legislación puede resultar insuficiente. Si esto es así, podría suponer un obstáculo para su desarrollo, pero por las respuestas obtenidas, no es un claro obstáculo para la mayoría de las empresas.



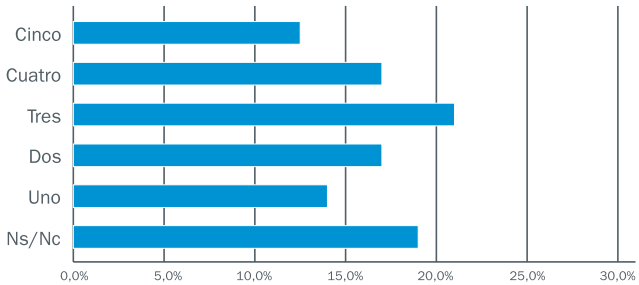
› Desconocimiento en general

Este elemento estaría relacionado con el primero, puesto que la falta de cultura puede influir en el desconocimiento general. Las empresas ven éste elemento como el mayor problema para el desarrollo de la seguridad, y así lo opina más de un 61% diciendo que es un obstáculo a tener en especial consideración.



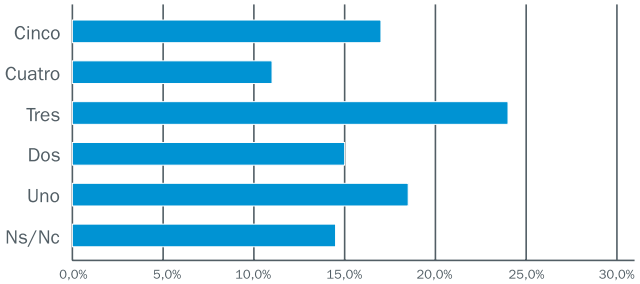
› Problemas para determinar el retorno de la inversión

Todo desarrollo en seguridad para una empresa supone una inversión, sin embargo el retorno de la misma o los beneficios que de ésta se puedan obtener no está tan claro para las mismas, por eso puede suponer un obstáculo de cara a conseguir que la dirección apruebe unos presupuestos para implantar medidas de seguridad, y que esto dificulte su desarrollo.



› Tecnologías poco maduras

El hecho de que las tecnologías relacionadas con la seguridad estén poco maduras pueden suponer un obstáculo para el desarrollo de la seguridad, por lo que se decidió incluir ésta como la última pregunta en cuanto a los obstáculos se refiere.



Las iniciativas que ayudarían a mejorar el desarrollo de la seguridad

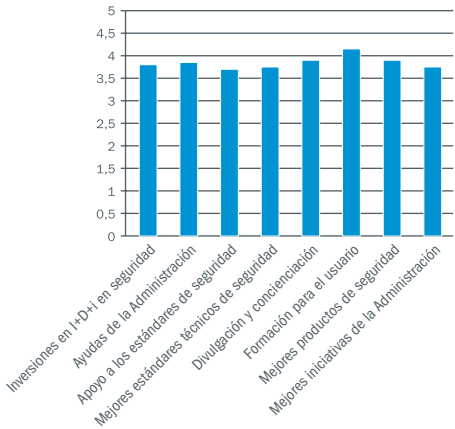
En las cuestiones anteriores, se preguntó acerca de las mayores preocupaciones y los obstáculos para el desarrollo de la seguridad. Una vez visto esto, es interesante la propuesta de iniciativas que ayudarían a mejorar el desarrollo de la seguridad en las empresas para evitar problemas.

Por ello, se incluyó en el cuestionario la siguiente cuestión referida a las iniciativas que más ayudarían a mejorar el desarrollo de la seguridad.

Como opciones, se dieron ocho de aquellas que los expertos coinciden en considerar que, llevándolas a cabo, la situación podría ser más favorable.

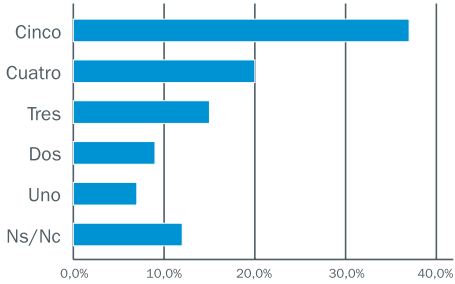
La mayoría de las empresas consideran que una de las mejores iniciativas que ayudarían al desarrollo de la seguridad sería la formación para el usuario, ya que, hoy en día, hay un gran desconocimiento en temas de seguridad entre todos los trabajadores, no sólo en los que se dedican más a este ámbito.

En general, las ocho opciones que se dan, son consideradas como una gran ayuda, siendo considerada la de menos ayuda la referida a inversiones en I+D+i en seguridad, pero con una puntuación lo suficientemente alta como para poder considerarla un elemento de apoyo.



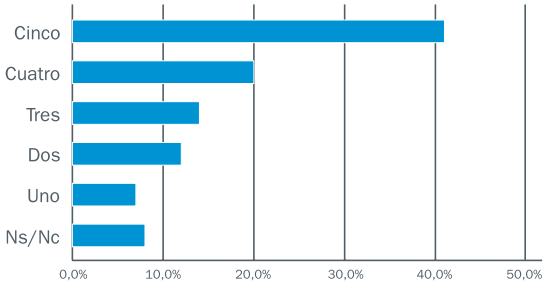
› Inversiones en I+D+I en seguridad

Se supone que la inversión en investigación y desarrollo ayuda a obtener mejores productos y servicios, y por tanto es positiva, y así lo podemos ver en los datos que obtenemos del análisis de la muestra.



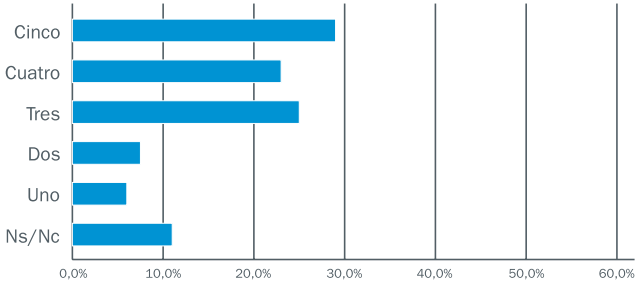
› Ayudas de la Administración pública

La mayoría de las empresas consideran que las ayudas de la administración para mejorar los sistemas podría resultar una gran iniciativa, y así lo consideran más del 60% de las organizaciones. Esto se puede entender como que el sector empresarial estima que la implicación de la Administración Pública en el tema de seguridad es mejorable.



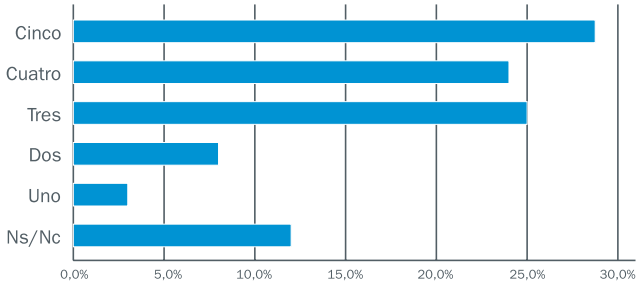
› Apoyos a los estándares de seguridad

Dentro de la seguridad, existen unos estándares técnicos. Se puede disponer de los mejores estándares, pero sin el apoyo a los mismos desde la administración y desde el sector privado, éstos no tendrán la difusión e implantación necesaria. Este apoyo ha sido considerado como una ayuda para mejorar el desarrollo de la seguridad, y así se demuestra en la distribución de los porcentajes.



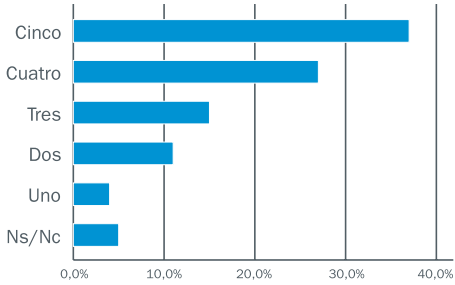
› Mejores estándares técnicos de seguridad

Relacionado con la pregunta anterior, existe la posibilidad de que el sector empresarial considere que los estándares técnicos de seguridad no fueran suficientes, necesitando mejorarlos. En este sentido de la respuesta obtenida se puede extraer la conclusión de que con el apoyo a los estándares no es suficiente, si no que se deben mejorar los existentes, y así lo considera el 52,8% de la muestra.



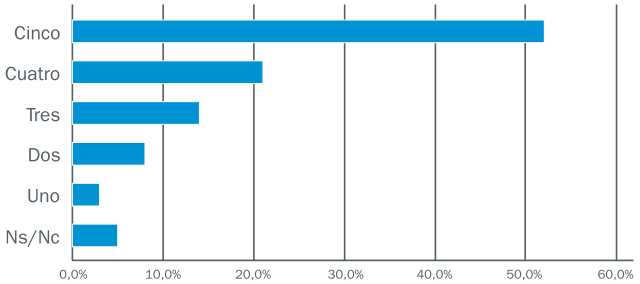
› Divulgación y concienciación

Uno de los elementos para aumentar la cultura y la información sobre seguridad en las empresas es una divulgación y concienciación eficaces en temas de seguridad, orientada a los distintos usuarios de las empresas. Los encuestados consideran ésta como una gran iniciativa y eso se refleja en que casi los dos tercios de la muestra opinan que esto sería una gran ayuda.



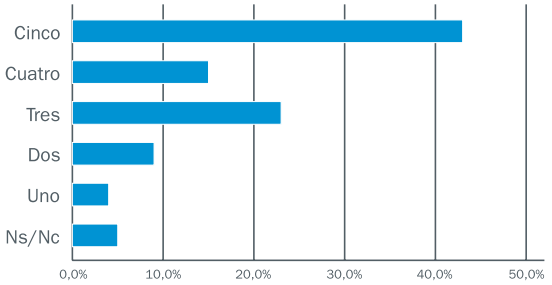
› Formación para el usuario

En relación con la cuestión anterior, hay pocos usuarios que estén formados en el marco de la seguridad y difícilmente se puede mejorar, si los usuarios no conocen ni los riesgos ni las soluciones. Así lo expresa el hecho de que un 73% de la muestra lo considere como una gran ayuda para mejorar el desarrollo de la seguridad.



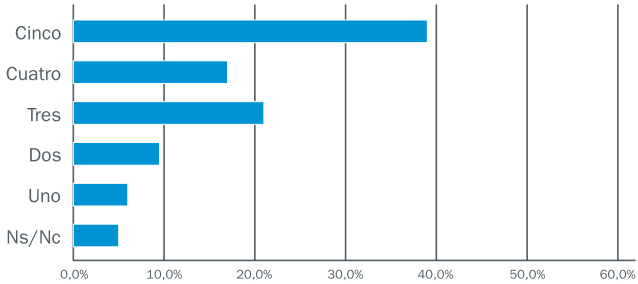
› Mejores productos de seguridad

Las empresas también se encuentran con el problema de que los productos de seguridad que existen actualmente en el mercado no tienen el nivel de fiabilidad al que están acostumbrados los usuarios en otros entornos, y se podrían mejorar. Hay una gran mayoría de encuestados que considera que la mejora de los productos de seguridad es una iniciativa que ayudaría de forma importante al desarrollo de la seguridad.



› Mejores iniciativas de la administración pública

La última pregunta incluida en el cuestionario que hace alusión a las iniciativas para ayudar al desarrollo de la seguridad es la referente a una mejora en las iniciativas procedentes de la Administración Pública. Se entiende, que además de subvencionar proyectos, podría tomar un papel más proactivo en relación con la problemática de la seguridad, impulsando otro tipo de iniciativas.



Análisis de las relaciones

Una vez realizados todos los análisis por bloques, resulta interesante observar las relaciones entre las distintas variables que se han solicitado a lo largo del cuestionario, para lo cual se hizo una selección de aquellas que podían resultar más interesantes. Como conclusión del análisis realizado sobre las relaciones se puede afirmar que las empresas tienen más o menos los mismos problemas de seguridad y preocupaciones, independientemente de su tamaño, tanto en facturación como en número de empleados.

Número de empleados

› Con respecto a los elementos de seguridad

Tras el análisis de los resultados obtenidos se observa que, en esta muestra, la relación existente entre estas variables es inversa y muy baja, no siendo significativa, es decir, que a más número de empleados se van a tener más elementos de seguridad, pero la relación es muy baja.

› Con respecto a los incidentes

En este caso, al igual que en el anterior, tampoco parece existir una relación importante, es más, esta relación es más pequeña que en el caso anterior.

Esta relación podría explicarse desde el punto de vista de que hay mayor número de personas que pueden cometer errores que son considerados como incidentes. En cualquier caso esta relación no es significativa.

› Con respecto a las preocupaciones

En concreto, esta relación es directa y muy baja, por lo que, cuantos más empleados tenga la empresa, mayor será su preocupación por la seguridad y los elementos relacionados con ella, pero nuevamente esta relación es muy baja.

Facturación en millones de euros al año

› Con respecto al os elementos de seguridad

En este caso, es esperable encontrar una relación baja entre estas variables, de tal forma que, cuando la facturación es mayor, el número de elementos de que dispone es mayor, siendo un resultado esperable puesto que puede tener mayor capital para invertir en seguridad.

› Con respecto a los incidentes

Se trata de una relación inversa y muy baja, que se puede interpretar como que a mayor facturación más incidentes. Además es una relación significativa, por lo que es esperable encontrar esta relación en la población.

› Con respecto a las preocupaciones

En lo referente a estas variables, se ha encontrado una relación prácticamente nula lo que indica que no hay relación entre estas variables.

La gestión de la seguridad

Otra de las relaciones que parece interesante observar es si el hecho de que la función de seguridad esté asignada va a influir sobre el número de incidentes, obteniendo como resultado que la relación existente es muy baja y directa.

En este caso, la relación directa resultante puede indicar que hay muchas empresas que no han contestado a esta cuestión puesto que lo esperable sería que aquellas empresas en las que las funciones de la gestión de la seguridad están asignadas deberían tener menos incidentes que aquellas en las que no están asignadas.

Las mayores preocupaciones

› Con respecto al número de servidores

En primer lugar y en lo referente al número de servidores operados por la organización, encontramos que la relación es directa, muy baja y no significativa, lo que quiere decir que a más servidores operados, mayor preocupación, pero esta relación es baja y no significativa, por lo que no es esperable que se produzca en el total de las empresas.

› Con respecto al número de puestos de trabajo

Y en segundo lugar, refiriéndonos al número de puestos de trabajo con ordenadores tipo PC, hay una relación inversa, muy baja y no significativa lo que se puede interpretar como que la preocupación será mayor cuando haya menos puestos de trabajo con ordenadores tipo PC, pero, al igual que en el caso anterior, esta relación es muy baja y no es significativa, por lo que no se va a producir en la población.

Líneas de actuación derivadas del estudio

Formación, concienciación y divulgación

A lo largo de todo el estudio se evidencia un desconocimiento importante en los temas relacionados con la seguridad de la información.

Es importante abrir una línea de trabajo orientada a cubrir esta necesidad, que aparte de los aspectos generales de la seguridad de la información, haga especial hincapié en los siguientes aspectos

- 1. Detección y eliminación de código malicioso.
- 2. Protección perimetral de los sistemas de información
- 3. Uso adecuado del correo electrónico
- 4. Protección frente a cortes de suministro eléctrico
- 5. Selección y uso de líneas de datos
- 6. Selección de herramientas de software

Se debe estudiar la posibilidad de crear una línea de comunicación relacionada con la seguridad de la información que incluya:

- 1. Constituir una línea de comunicación ambiciosa y persistente
- 2. Crear un portal que sirva de punto de referencia
- 3. Establecer un programa formativo para usuarios de las tecnologías de la información y otra para los profesionales de las mismas

Código malicioso

Aunque las organizaciones cuentan con herramientas de protección frente a código malicioso, lo cierto es que siguen sufriendo incidentes con bastante frecuencia.

Se debería elaborar una guía de buenas prácticas en lo referente a detección y eliminación de código malicioso.

Tecnologías de especial interés

Las organizaciones encuestadas han manifestado un especial interés por determinadas tecnologías, especialmente las siguientes:

- 1. Factura electrónica
- 2. Firma electrónica
- 3. Sistemas de detección de intrusos
- 4. Soluciones antispam

Es recomendable promover proyectos que faciliten la incorporación de estas tecnologías en los procesos de negocio de las organizaciones de la región.

Buenas prácticas

Promover las buenas prácticas en seguridad de la información, tanto en la administración autonómica, como en las organizaciones.

SEGURNET: PYME SEGURA RIOJA

Proyecto incluido dentro del Plan de Consolidación y
Competitividad de la Pyme. PCCP.
Expediente 2006/P/INF/00005.
Estudio elaborado 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:

pyE+ Plan de Consolidación y Competitividad de la Pyme