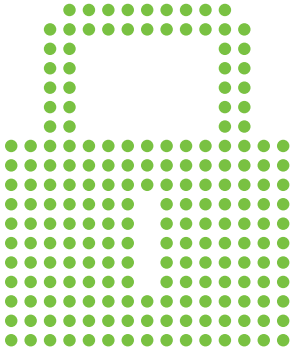


INFORME
DEL ESTUDIO DE
SEGURIDAD
THINKTIC 2014

13 de noviembre 2014

Gobierno de La Rioja | Industria, Innovación y Empleo

Sistema Riojano de Innovación

think TIC Centro Nacional de Formación en Nuevas Tecnologías

- Realización:
  Think TIC
- Diseño:
  Phics & Graphics
- Depósito Legal:
  LR-856-2014

PRESENTACIÓN

El Centro Nacional de Formación en Nuevas Tecnologías, Think TIC, como Centro de Referencia Nacional en Sistemas y Telemática, tiene entre sus objetivos observar la evolución y las necesidades de cualificación del sistema productivo y contribuir a la actualización y desarrollo de la formación profesional para adaptarla a dichas necesidades. En este marco nace este trabajo que ha sido posible gracias a las aportaciones de nuestros alumnos, a los que quiero agradecer su participación.

La seguridad de la información constituye actualmente un reto para el óptimo desempeño de las empresas y organizaciones, sobre todo teniendo en cuenta que cada vez disponemos de más dispositivos con los que gestionar y transferir la información que pueden dificultar considerablemente esta tarea.

La Consejería de Industria, Innovación y Empleo consciente de este reto desarrolla a través del Think TIC diferentes actuaciones en este ámbito con el objetivo de formar a los profesionales riojanos en las herramientas, procedimientos y prácticas más adecuadas. Concretamente, desde los inicios del Think TIC, en septiembre de 2007, hasta la fecha, se han impartido más de 1.000 horas de formación específica en cursos y jornadas relacionadas con la seguridad de la información, y sigue siendo actuación prioritaria dentro de la oferta formativa del Centro.

El IV Plan Riojano de I+D+i identifica en su línea estratégica "Sociedad innovadora" la necesidad de que la sociedad tenga un nivel formativo adecuado, siendo el papel de la administración clave para impulsar la socialización de la innovación. Por ello, una mayor interconexión de los agentes del Sistema Riojano de Innovación es fundamental para lograrlo tal y como el plan "Sociedad Conectada" define, para que esta interconexión se haga de una manera segura, es necesario que la sociedad riojana se forme de una manera planificada y sistemática.

Además, el trabajo conjunto realizado desde el Think TIC con AERTIC, partner principal en estas actividades formativas, redunda en esa orientación práctica de una formación de calidad y utilidad para profesionales y empresas riojanas de los principales sectores que sustentan la economía regional para conseguir la mejora de la competitividad que motiva la evolución del modelo productivo riojano y, en consecuencia, un mayor y mejor desarrollo económico y social de La Rioja.

Por último, agradecer la colaboración en la dirección de este trabajo de Olof Sandstrom. Es una suerte poder contar con uno de los mayores expertos nacionales en gestión de la información.

JAVIER ERRO URRUTIA
CONSEJERO DE INDUSTRIA, INNOVACIÓN Y EMPLEO
GOBIERNO DE LA RIOJA

EL RETO DE LA SEGURIDAD

Nuestra primera aportación a este informe en sus primeras líneas debe ser para agradecer al Centro de Referencia Nacional en Informática y Comunicaciones, dependiente de la Dirección General de Innovación del Gobierno de La Rioja, por esta excelente iniciativa de recoger en este estudio la opinión y las inquietudes de los profesionales riojanos acerca de la seguridad de la información.

Desde el sector TIC que represento, consideramos que este informe es muy necesario y valioso para poder conocer el estado de la cuestión en un ámbito cada día más complejo, tecnificado y que genera una mayor preocupación en las organizaciones.

Y debe ser así, porque estamos hablando de un tema crucial para el devenir, la actividad y la buena marcha de las organizaciones en unos mercados cada vez más competitivos, donde el poder de la información y la seguridad en torno a ella adquieren una dimensión inimaginable hace solo unos pocos años.

Además del equipo humano y profesional, las empresas debemos resguardar y proteger como un tesoro la información de la que disponemos sobre nuestra actividad, porque de ello se derivará en el presente y en el futuro nuestra posición en el mercado, la capacidad de competir y diferenciarnos y, en definitiva las posibilidades de éxito.

Sin embargo, las dificultades para este gran reto no son menores. De una parte, existe un desconocimiento bastante habitual sobre las herramientas a nuestro alcance y las posibilidades técnicas y de gestión que nos pueden facilitar el camino. La formación deber ser una asignatura permanente.

Por otro lado, la dimensión y estructura de pymes, micropymes y organizaciones muy reducidas hacen fundamental la colaboración de especialistas en materia de seguridad, sin los cuales el ingente patrimonio de conocimiento de una empresa corre un serio riesgo.

Y progresivamente, gracias al concurso del Think-TIC o de agentes activos como AERTIC, tenemos que seguir trabajando en una mayor concienciación y cultura de la seguridad en la sociedad. Creo que todos ganaremos. Las empresas, las organizaciones, nuestro entorno social y económico y, por supuesto, nuestra región, como modelo exportable y reconocible. El camino es amplio, pero la ilusión es el verdadero motor que nos mueve.

JOSÉ LUIS PANCORBO
PRESIDENTE DE AEI AERTIC

1. INTRODUCCIÓN

El Centro Nacional de Formación en Nuevas Tecnologías, en adelante Think-TIC, es un organismo dependiente de la Dirección General de Innovación, Industria y Comercio del Gobierno de La Rioja. Desde el comienzo de sus actividades ha tenido un foco claro en el ámbito de la Seguridad Informática, realizando durante todos estos años un esfuerzo muy relevante por mejorar la formación, divulgación y comunicación para con las empresas de La Rioja en temas relacionados con este ámbito.

El Think-TIC impartió en el año 2013 un total de 73 cursos relacionados con las tecnologías de la información en los que participaron un total de 1.447 alumnos, 6 de dichos cursos han estado directamente relacionados con el ámbito de la seguridad informática.

Desde el Centro se ha considerado necesario conocer la situación actual de la seguridad informática en las empresas de La Rioja, al objeto de programar actuaciones acordes a las necesidades detectadas. Se ha realizado un estudio a lo largo del año 2013, para ello se ha solicitado a las personas que han asistido a los cursos que cumplimentaran el cuestionario elaborado a tal efecto, con el resultado de 216 cuestionarios contestados.

Este cuestionario ofrece unas garantías científicas suficientes como para poder afirmar que los datos obtenidos son representativos de la situación de las empresas cuyos profesionales han participado en los cursos impartidos en el Centro.

El presente informe tiene como objetivo exponer las conclusiones a las que llega el estudio con respecto a la situación de la seguridad informática.

La intención del Think-TIC es actualizar estos datos periódicamente, de manera que sea posible hacer un seguimiento de la evolución de la seguridad informática en las organizaciones cuyo personal participa en los cursos celebrados en el Centro.

2. VALORACIÓN DE LA ENCUESTA

Tras un análisis de todos los datos obtenidos en el cuestionario, se han elaborado las siguientes notas metodológicas, medidas de calidad del cuestionario y errores de muestreo.

OBJETIVO DEL ESTUDIO

Conocer el estado de la seguridad de la información en las organizaciones de la región.

DISEÑO MUESTRAL

Se pueden plantear dos alternativas respecto al universo a estudiar, la primera es considerar que nuestra población objetivo comprende únicamente las empresas cuyos trabajadores han pasado por el Think-TIC en el periodo de estudio, es decir, 945 personas, o bien considerar que la población son todas las empresas de La Rioja cuya actividad está recogida entre las ramas de actividad objetivo (20.849). En la primera alternativa, los errores de muestreo que se comenten son inferiores, pero las conclusiones del estudio sólo harán referencia a este colectivo y no al total de empresas de La Rioja.

- Universo-1: Empresas riojanas cuyos trabajadores han asistido a cursos organizados por el Think-TIC durante 2013.
- Universo-2: Total de empresas riojanas

REPRESENTATIVIDAD

Para las encuestas la representativo es el 100% de las empresas ubicadas en La Rioja pues están incluidas en el marco muestral DIRCE 2013.

TAMAÑO DE LA MUESTRA

La muestra cuenta con 216 personas elegidas en forma intencionada, ya que se ha seleccionado para el estudio a aquellos trabajadores que han realizado algún curso en Think-TIC en el año 2013.

PROCEDIMIENTO DE MUESTREO

El sistema de muestreo aplicado es semi-probabilístico.

NIVEL DE CONFIANZA

El nivel de confianza obtenido es del 95%.

HETEROGENEIDAD

Los parámetros de heterogeneidad son los siguientes:

- P = 50%
- Q = 50%

ERROR MUESTRAL

El error cometido es de ± 2.7% considerando como población objetivo las empresas cuyos trabajadores han sido alumnos del Think-TIC.

INSTRUMENTO DE RECOLECCIÓN DE DATOS

Se diseñó un cuestionario electrónico con preguntas cerradas a cumplimentar por el encuestado. (Ver Anexo: Encuesta "Evaluación sobre el estado de la seguridad de la información en las organizaciones de la región").

TÉCNICA DE INVESTIGACIÓN

La técnica de investigación utilizada ha sido una encuesta por muestreo semi-probabilístico a las personas seleccionadas. Dicha encuesta está formada por 97 ítems, cuya fiabilidad, ha sido evaluada por técnicas psicométricas.

Se ha realizado un análisis de fiabilidad calculando el índice α de Cronbach, que permite cuantificar el nivel de fiabilidad de una escala de medida para la magnitud inobservable construida a partir de las variables observadas. No es un estadístico al uso, por lo que no viene acompañado de ningún p-valor que permita rechazar la hipótesis de fiabilidad en la escala; no obstante, cuanto más se aproxime a su valor máximo, 1, mayor es la fiabilidad de la escala.

El mayor valor teórico de α es 1 y el resultado obtenido ha sido un $\alpha = 0.995$, lo que indica que el cuestionario aplicado a los encuestados es altamente fiable.

3. RESUMEN EJECUTIVO

3.1. TECNOLOGÍAS DE SEGURIDAD UTILIZADAS

Las tecnologías clásicas de seguridad (autenticación con usuario y contraseña, firewalls y antivirus fundamentalmente) están ampliamente establecidas, mientras que otras más avanzadas tienen un nivel de implantación muy bajo. Cabe destacar en este punto que aunque las tecnologías de protección contra código malicioso tienen un elevado nivel de implantación, las empresas sufren con frecuencia incidentes relacionados con virus, spyware, etc. esto indica que las soluciones no están siendo eficaces.

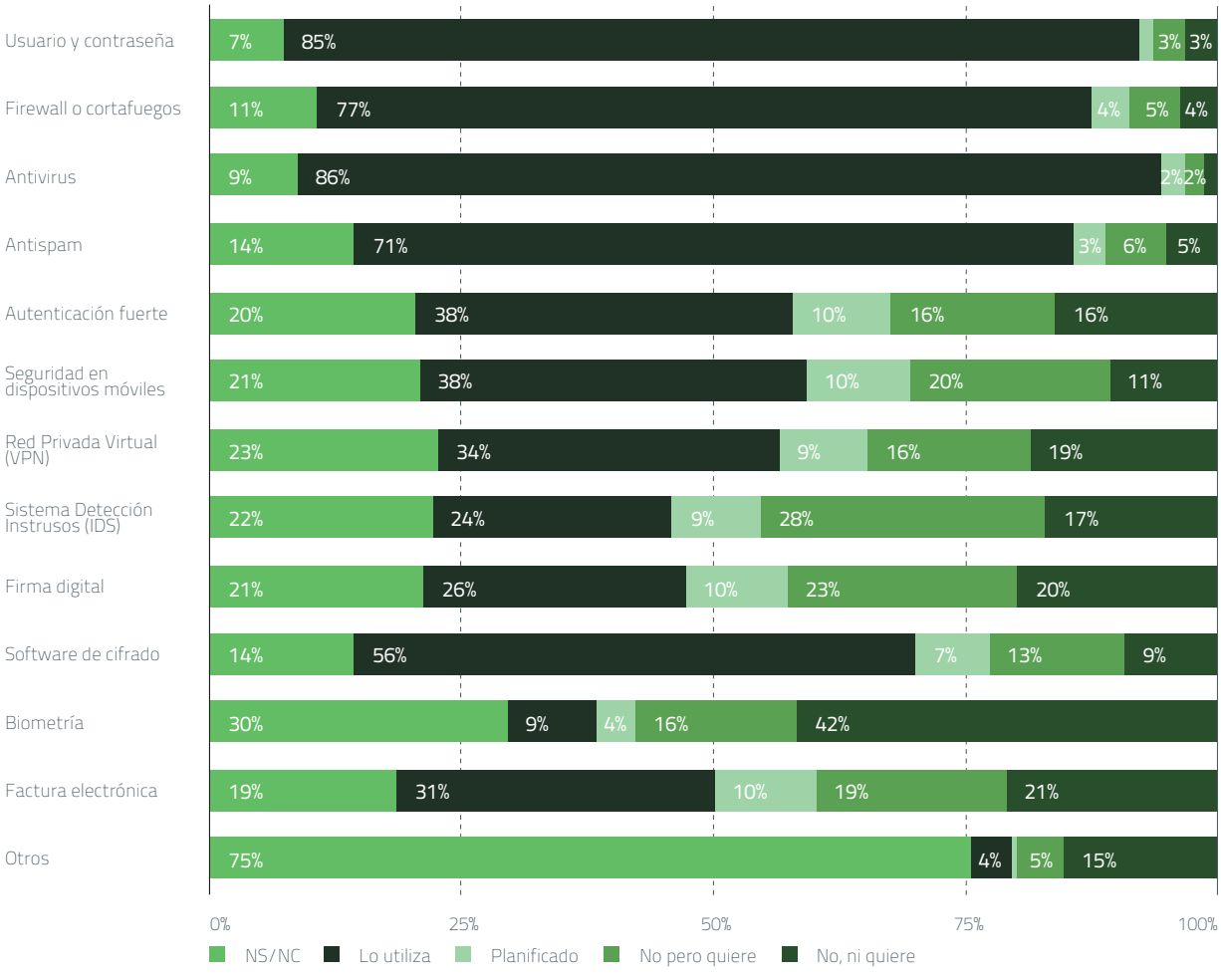
Un porcentaje significativo de empresas ha manifestado que tiene planificado o quiere implantar soluciones de factura electrónica y firma digital.

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.

También es relevante el interés que existe en dotar de elementos de seguridad a los dispositivos móviles.

Por último, atendiendo a las respuestas obtenidas, parece que las técnicas biométricas definitivamente no son del interés de las personas entrevistadas.

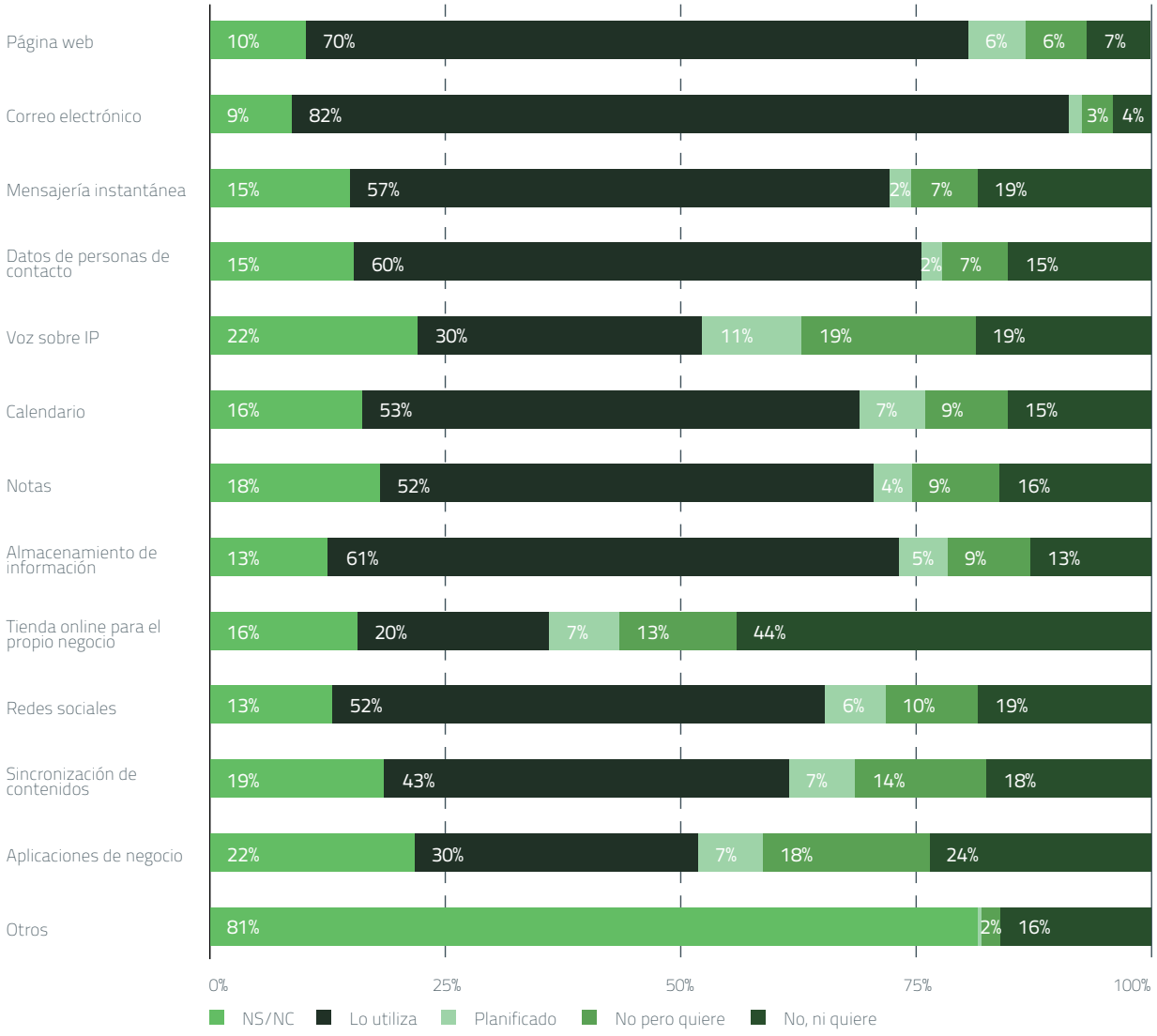
INDIQUE SI SU ORGANIZACIÓN UTILIZA ACTUALMENTE ALGUNO DE LOS SIGUIENTES ELEMENTOS



3.2. USO DE SERVICIOS A TRAVÉS DE INTERNET

El uso de servicios a través de Internet está ampliamente difundido. Además de los servicios más evidentes como el correo electrónico o las páginas web estándar, comienzan a ser cada vez de mayor interés para las organizaciones otros como la mensajería instantánea, voz sobre IP, tiendas online, almacenamiento online o, incluso, las aplicaciones de negocio.

INDIQUE SI SU ORGANIZACIÓN UTILIZA ACTUALMENTE ALGUNO DE LOS SIGUIENTES SERVICIOS A TRAVÉS DE INTERNET

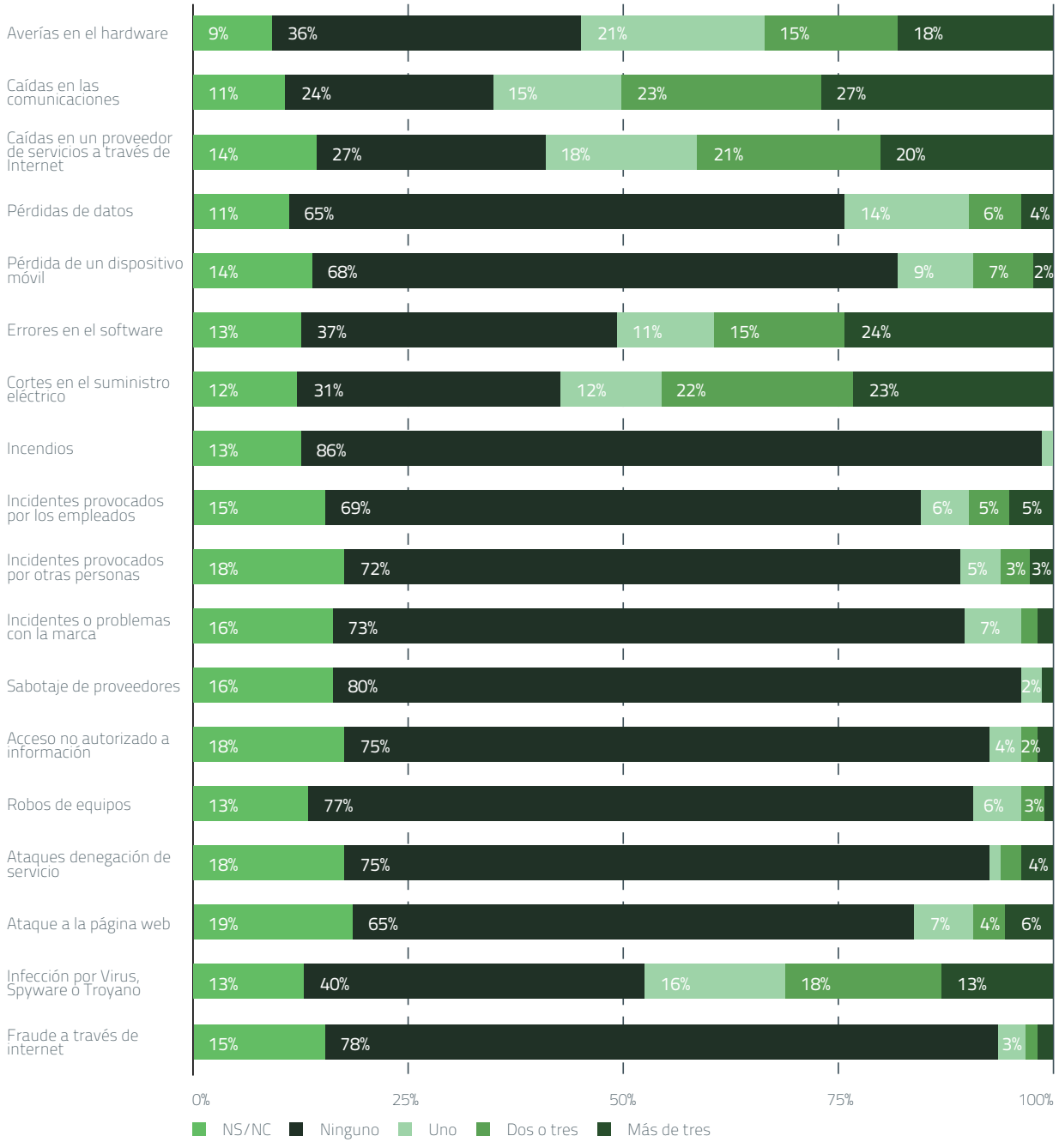


3.3. INCIDENTES

Además de los frecuentes incidentes relacionados con código malicioso, también son destacables los relacionados con interrupciones del suministro eléctrico, caídas de las comunicaciones, averías de hardware y errores en el software.

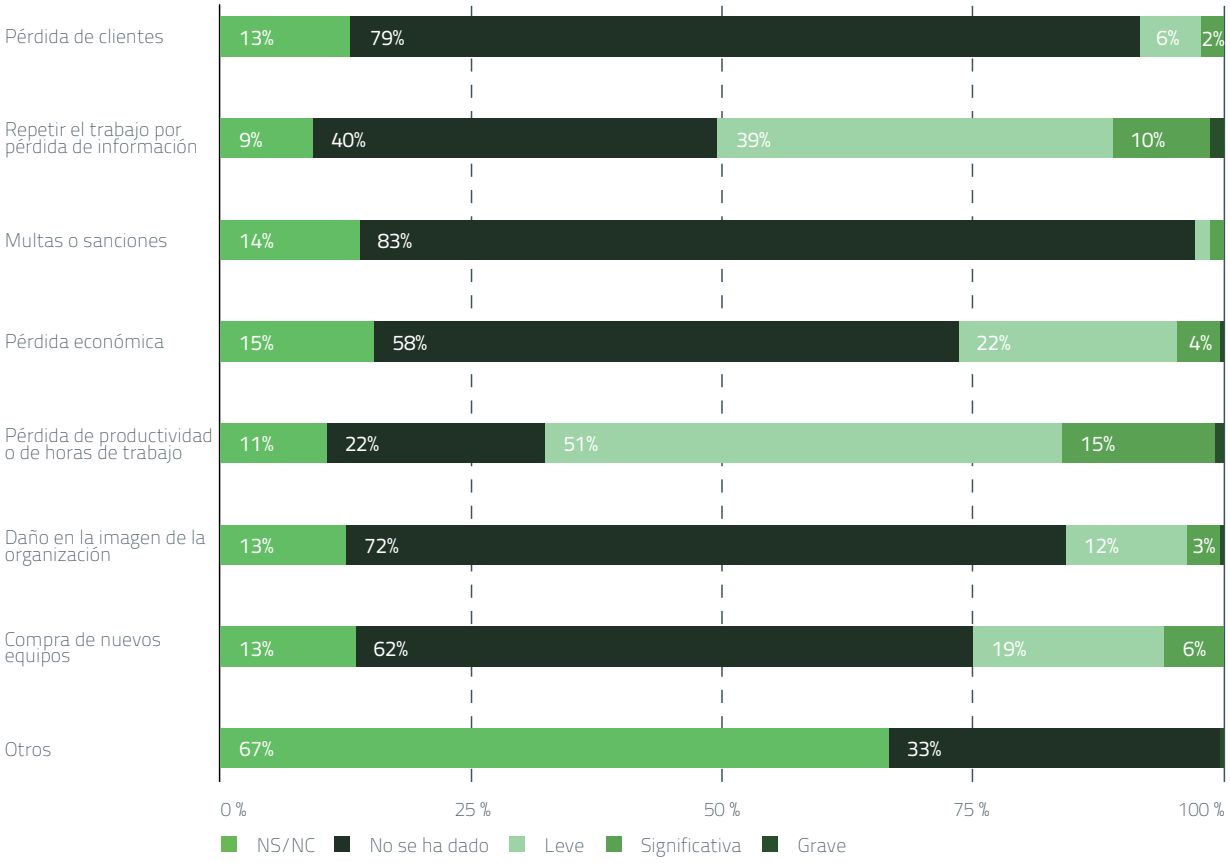
Los incidentes provocados por errores de empleados, administradores y proveedores también se dan, aunque con menor frecuencia.

¿CUÁNTOS INCIDENTES DE CADA UNO DE LOS TIPOS SIGUIENTES HA SUFRIDO EN LOS ÚLTIMOS 12 MESES?



En lo que respecta al impacto de estos incidentes, las consecuencias más habituales están relacionadas con la pérdida de productividad o de horas de trabajo, así como la necesidad de repetir el trabajo a consecuencia de la pérdida de información.

VALORE PARA CADA UNO DE LOS SIGUIENTES SUPUESTOS CUÁLES HAN SIDO LAS CONSECUENCIAS DE LOS INCIDENTES QUE HA SUFRIDO

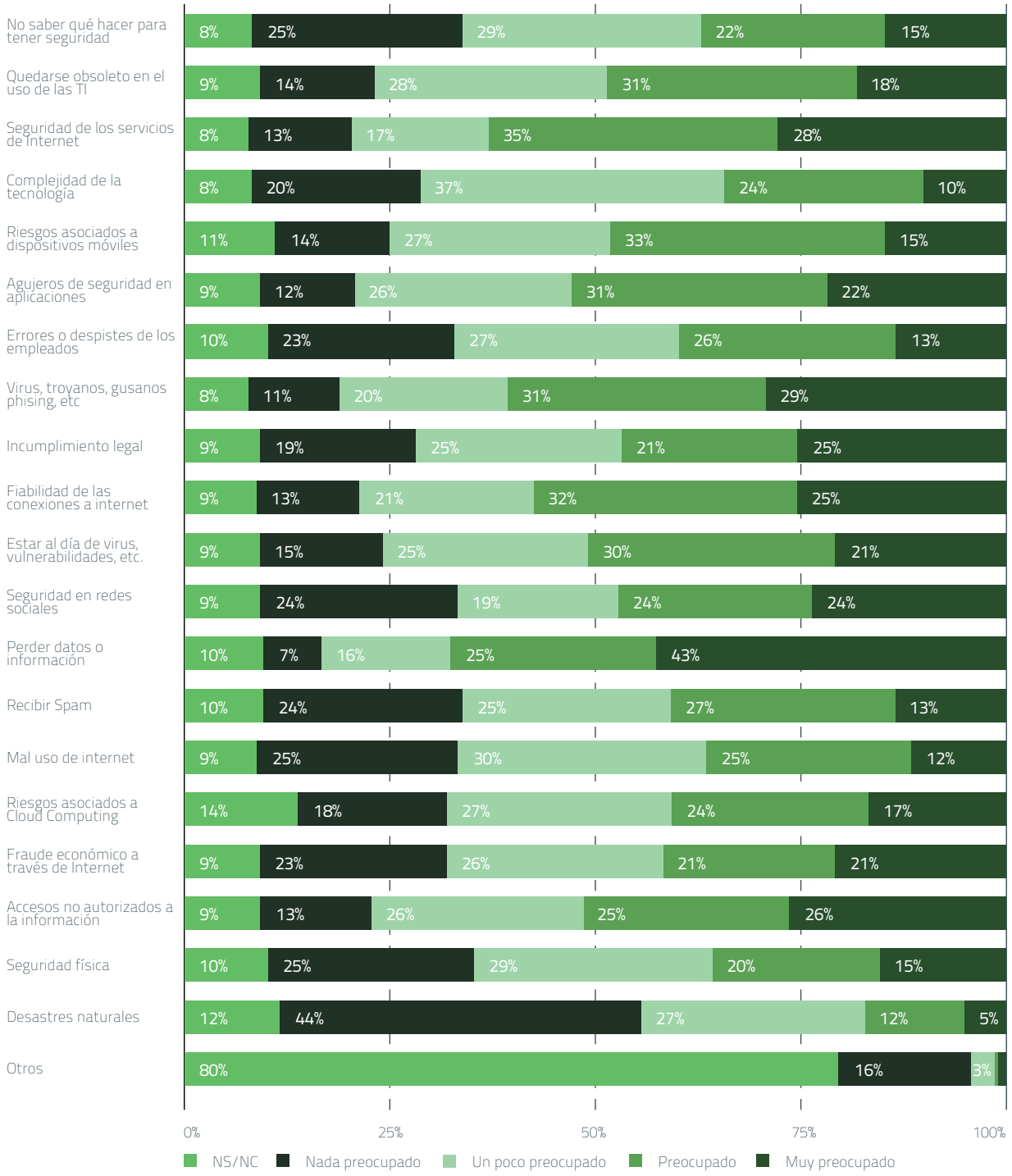


3.4. PREOCUPACIONES EN MATERIA DE SEGURIDAD

La mayor preocupación en materia de seguridad de las empresas es la posibilidad de perder datos o información, seguida de la seguridad de los servicios a través de internet y el código malicioso (virus, gusanos, troyanos, phishing, etc.).

Aunque estos aspectos destacan sobre el resto, el nivel de preocupación es elevado para todos los elementos que se han incluido en la consulta. El único que parece que no despierta significativamente la atención de los entrevistados son los desastres naturales.

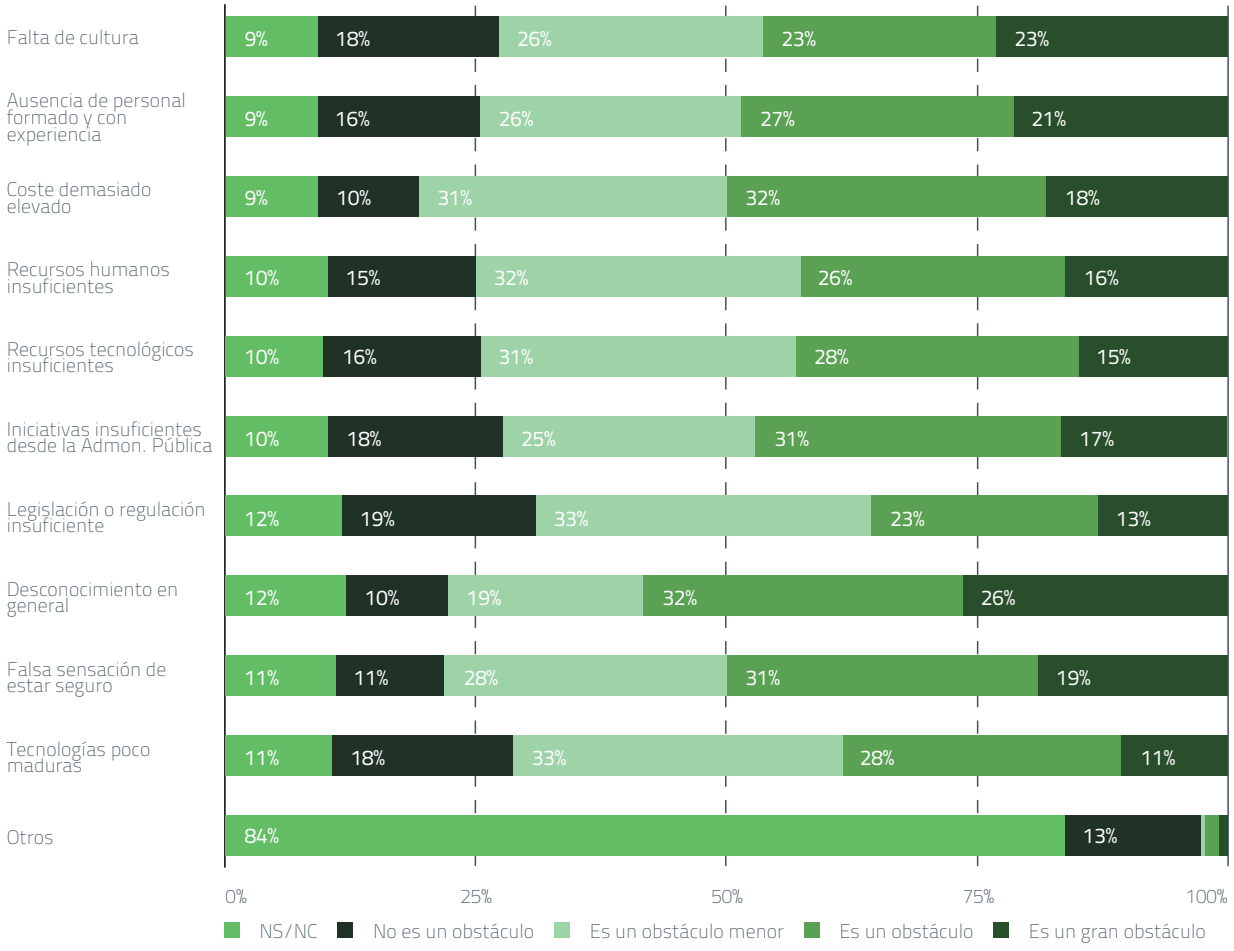
VALORE CUAL ES SU GRADO DE PREOCUPACIÓN CON RESPECTO A CADA UNA DE LAS SIGUIENTES CIRCUNSTANCIAS



3.5. OBSTÁCULOS PARA EL DESARROLLO DE LA SEGURIDAD

De forma clara, los encuestados consideran que el mayor obstáculo para el desarrollo de la seguridad es el desconocimiento general que existe sobre estos temas, seguido de cerca por la falta de cultura de seguridad, así como la ausencia de personal formado y con experiencia.

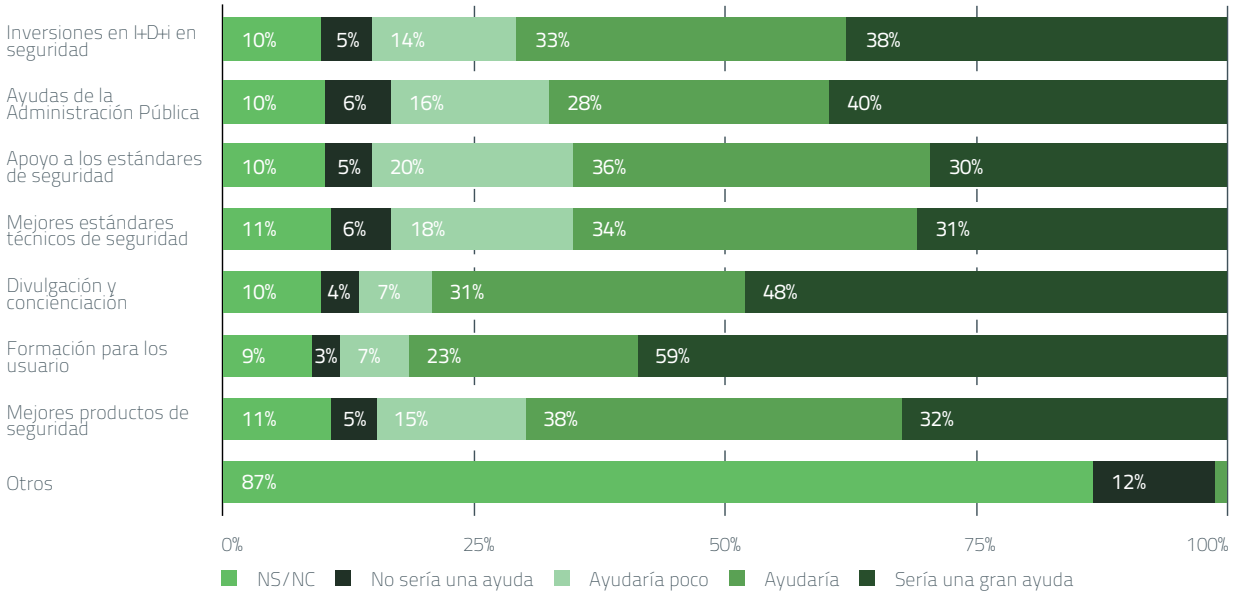
VALORE LA IMPORTANCIA DE LOS SIGUIENTES OBSTÁCULOS PARA DISPONER DE UN BUEN NIVEL DE SEGURIDAD



3.6. INICIATIVAS PARA MEJORAR LA SEGURIDAD

Es significativo que las empresas consideran que la iniciativa que más ayudaría a mejorar la seguridad es la formación para los usuarios, seguida de acciones de divulgación y concienciación.

VALORE EN QUE MEDIDA AYUDARÍAN A MEJORAR LA SEGURIDAD CADA UNA DE LAS SIGUIENTES INICIATIVAS



3.7. CONCLUSIONES DESDE EL THINK TIC

Como no puede ser de otra forma, el Think TIC toma buena cuenta de esta valoración, ya que precisamente la formación, divulgación y concienciación constituyen su principal área de actividad.

Haciendo una lectura global de los resultados obtenidos en los distintos apartados, se llega a la conclusión de que es necesario seguir insistiendo en la formación en materia de seguridad desde un punto de vista general.

Las organizaciones prácticamente están preocupadas por todo el abanico de posibles casos que se han planteado en el estudio, al tiempo que se ven afectadas por incidentes también de muy distinta naturaleza.

Este hecho hace conveniente la constitución de dos líneas de trabajo muy cercanas al día a día de las organizaciones riojanas.

Una de ellas centrada en la divulgación de una cultura de seguridad, con actuaciones continuadas en el tiempo que sigan una línea argumental clara alrededor de las buenas prácticas de la seguridad.

La otra línea de actuación estaría centrada en la formación en aspectos operativos y cotidianos teniendo muy presente que el 50% de las organizaciones que han participado en el estudio son de menos de 10 empleados. Esto se traduce en que estas actividades formativas deben ser eminentemente prácticas y enfocadas a la resolución de las necesidades específicas que en materia de seguridad tienen las organizaciones de La Rioja.

Por otra parte, y dada su rápida adopción como una herramienta de trabajo más, sería recomendable destacar la conveniencia de abordar acciones formativas relacionadas con la seguridad en dispositivos móviles como smartphones y tabletas.

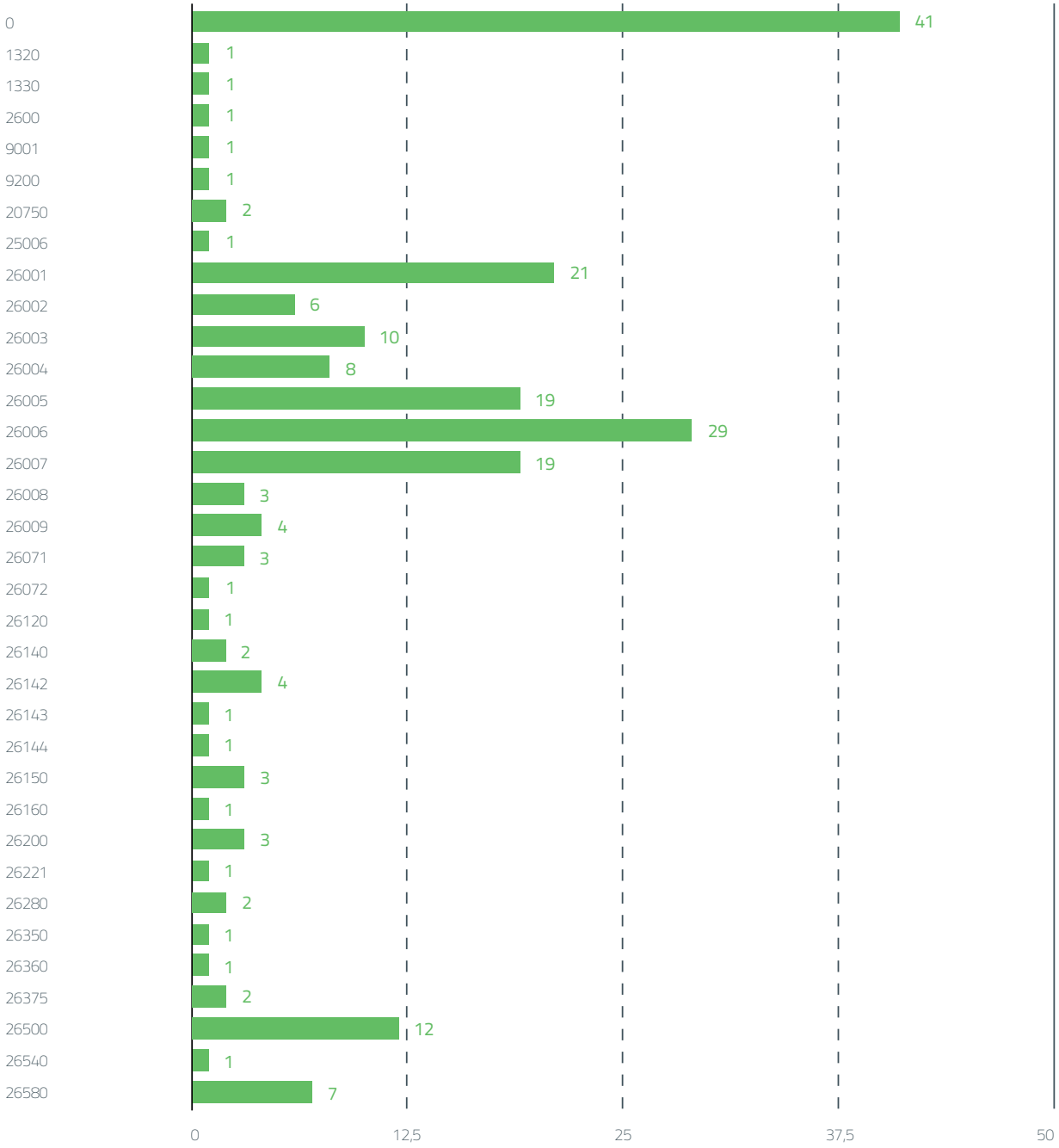
4. DATOS GENERALES DE LAS ORGANIZACIONES

4.1. CÓDIGO POSTAL

Uno de los objetivos por los cuales se solicitaba el código postal en el cual se hallaba ubicada la empresa, es observar si existen diferencias en cuanto a la instauración de elementos de seguridad así como de la propia opinión que tienen las empresas en función de si, por ejemplo, están ubicadas la ciudad de Logroño o lo están en alguna otra localización dentro de la Comunidad Autónoma de La Rioja.

Este objetivo no se ha podido contrastar puesto que el número de respuestas obtenidas para los distintos códigos postales no es lo suficientemente elevado como para extrapolar conclusiones estadísticamente significativas, rehusándose así el hacer la comparación.

CÓDIGO POSTAL

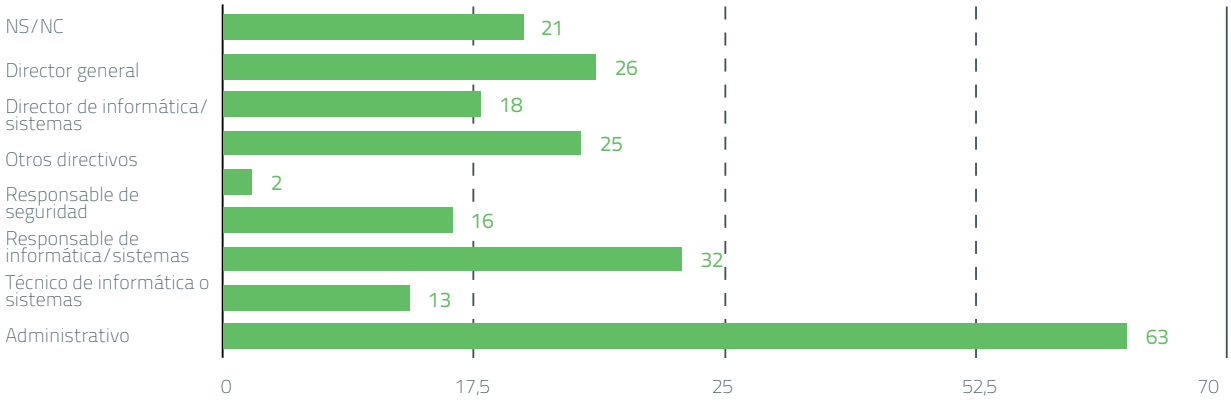


4.2. CARGO DE LA PERSONA QUE RESPONDE EL TEST

Se solicitaba el cargo de la persona que respondía el test, puesto que esta información podía dar alguna pista para ofrecer mayor o menor peso a los datos y opiniones facilitadas.

Un 32% de los encuestados pertenecen al equipo directivo de las organizaciones, y un 23% pertenecen a las áreas de seguridad o informática.

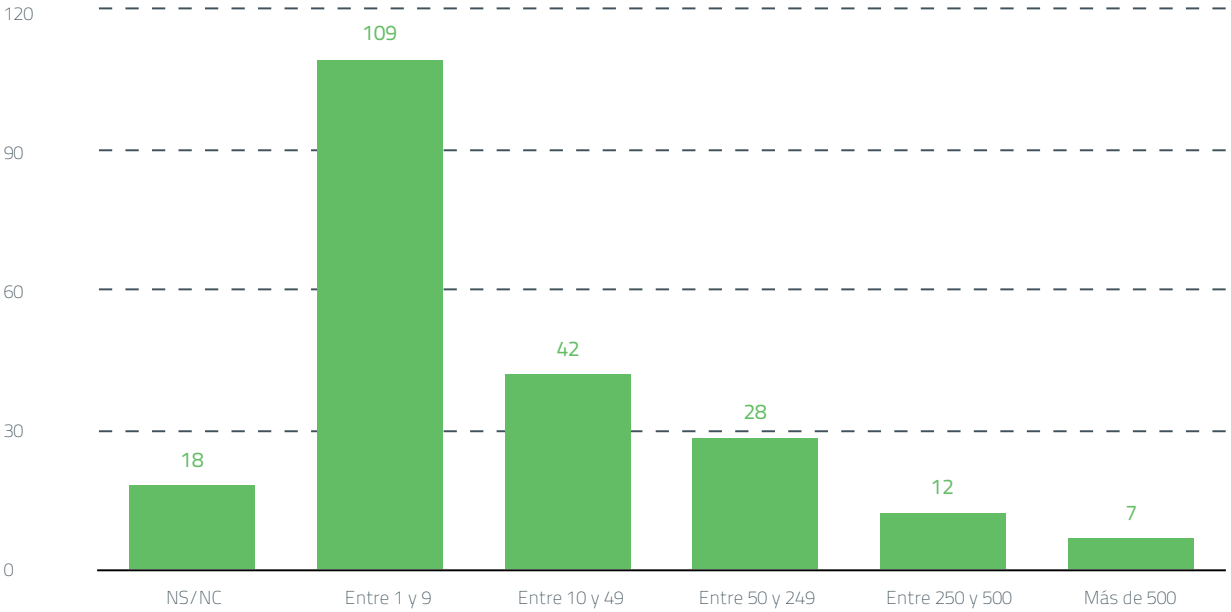
CARGO DE LA PERSONA QUE RESPONDE AL TEST



4.3. NÚMERO DE EMPLEADOS

Otro de los elementos solicitados era el número de empleados para saber si los datos utilizados como referencia pertenecen mayoritariamente a PYMES o a grandes empresas. En este sentido, la mitad de los cuestionarios recibidos pertenecen a empresas con menos de 10 empleados.

NÚMERO DE EMPLEADOS



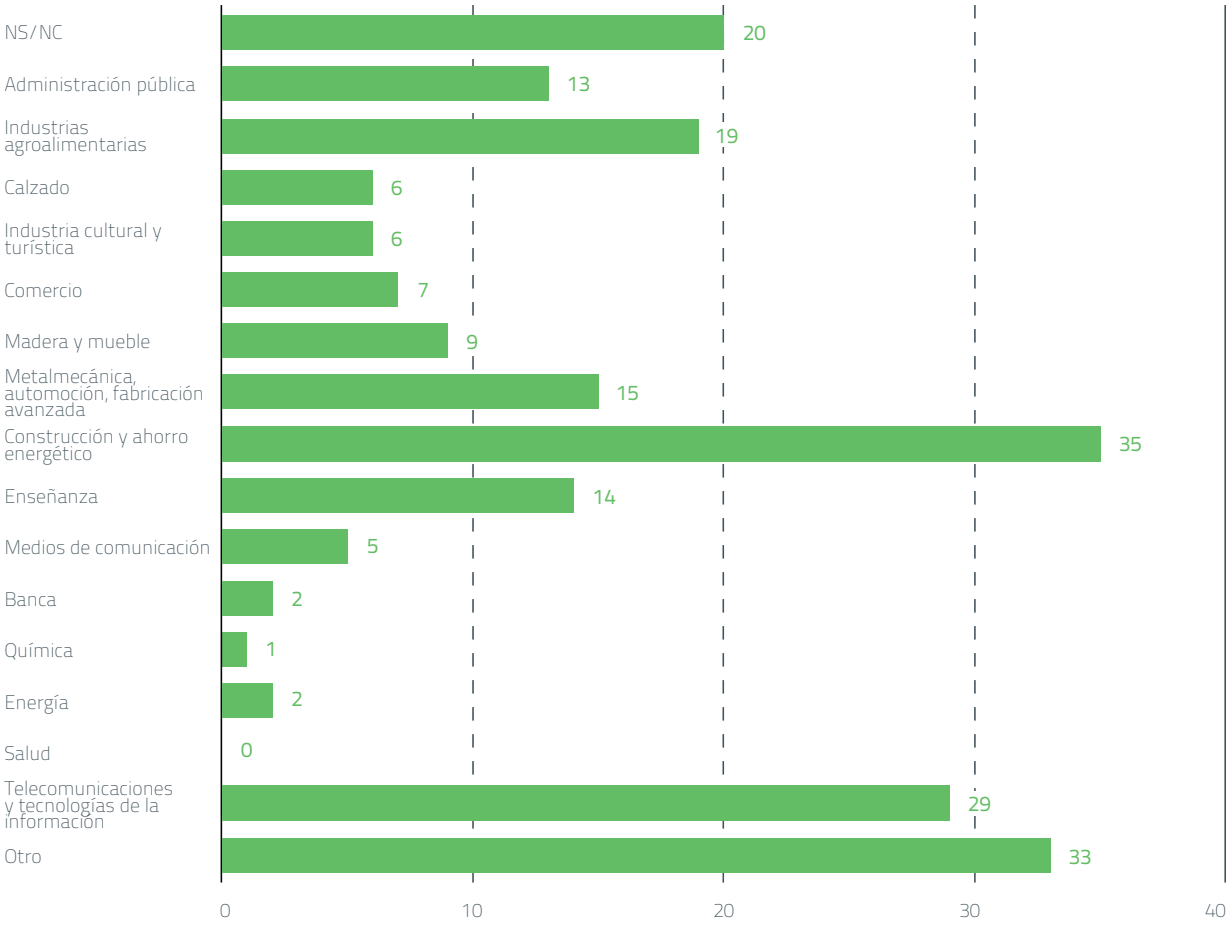
4.4. SECTOR DE ACTIVIDAD

En cuanto al sector de actividad de las empresas que respondieron al cuestionario, está bastante distribuido, aunque se pueden destacar los siguientes datos:

- El 16% pertenecen al sector de construcción y ahorro energético.
- Al sector de las telecomunicaciones y tecnologías de la información se corresponden el 13% de los cuestionarios.
- Un 9% se ubican dentro del sector de las industrias agroalimentarias.

Al ser ésta una de las variables de agrupamiento que se incluía en el estudio para la catalogación de las empresas, se comprobó si existían diferencias estadísticamente significativas tanto de los elementos que disponía la organización, como de los incidentes, del uso del correo, las preocupaciones, los obstáculos y las iniciativas para el desarrollo de la seguridad en función de pertenecer a un grupo u otro de actividad; sin embargo, esta prueba no resultó significativa, lo que quiere decir que las posibles diferencias encontradas no se debían a que realmente existían y podían ser tenidas en cuenta, sino a las propias diferencias no significativas de las empresas.

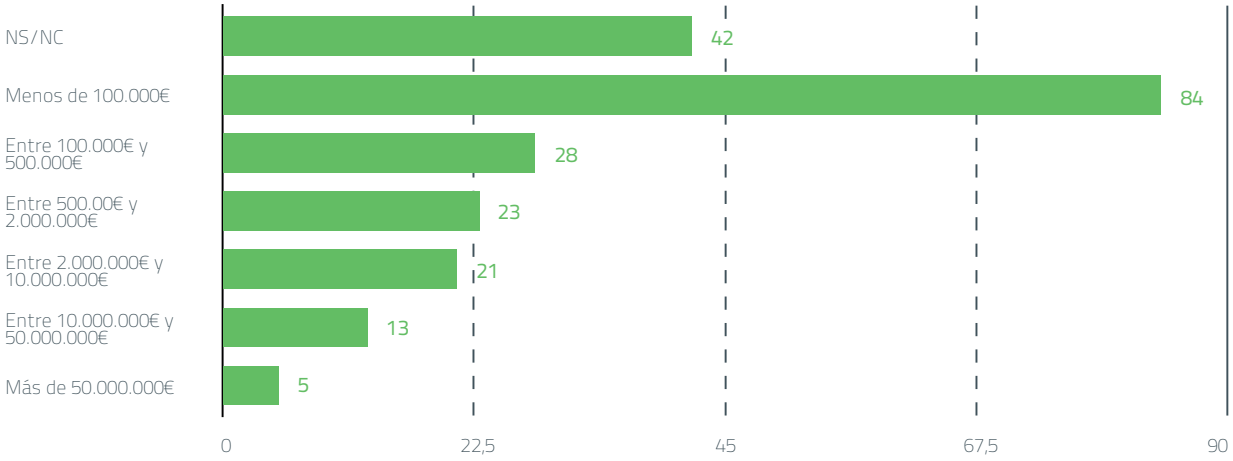
SECTOR DE LA ACTIVIDAD



4.5. FACTURACIÓN EN MILLONES DE EUROS AL AÑO

Además del número de empleados que tiene la empresa, para poder clasificarlas como PYMES o como grandes empresas, es necesario conocer la facturación anual de las mismas; dato que también fue solicitado y que quedó distribuido como se muestra en el siguiente gráfico.

FACTURACIÓN EN EUROS AL AÑO



4.6. LA GESTIÓN DE LA SEGURIDAD

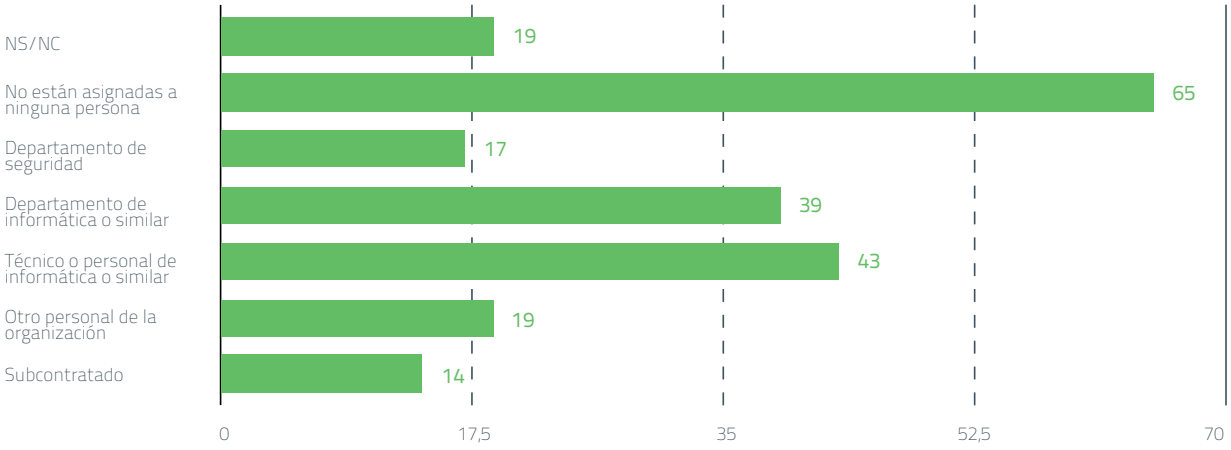
En lo referente a la seguridad de la información, es importante que su gestión esté asignada a una persona en concreto dentro de la organización.

Lo recomendable es que la realice alguien especializado en esa área puesto que estará al día de las mejoras que se realicen, de las nuevas tecnologías, así como de los nuevos requisitos legales o normativos que surjan.

Es importante tener claro que no es indispensable para la correcta gestión de la seguridad de la empresa que esta persona tenga dedicación exclusiva a la seguridad. Dependiendo del tamaño y la dependencia de las tecnologías de la información que tengan los procesos de negocio de la organización, es perfectamente válido que reparta su tiempo entre la gestión de la seguridad y otras funciones dentro de la empresa.

- El 8% de los encuestados trabajan en empresas que tienen un departamento o área concreta encargada de la gestión de seguridad.
- Un 18% indicó que la gestión de la seguridad está asignada al departamento o al personal de informática
- En el 9% de los casos, esta función era realizada por otro personal de la organización que no esta relacionado con las áreas de informática o sistemas
- Cerca del 6% han subcontratado la gestión de la seguridad a personas externas
- El resultado más llamativo es que en un 30% de los casos esas funciones no estaban asignadas
- También es interesante destacar que un 9% de las respuestas ha indicado que no sabe o no contesta quién se encarga de la seguridad dentro de su organización.

¿QUIÉN ASUMEN EN SU ORGANIZACIÓN LAS TAREAS RELACIONADAS CON LA SEGURIDAD DE LA INFORMACIÓN?



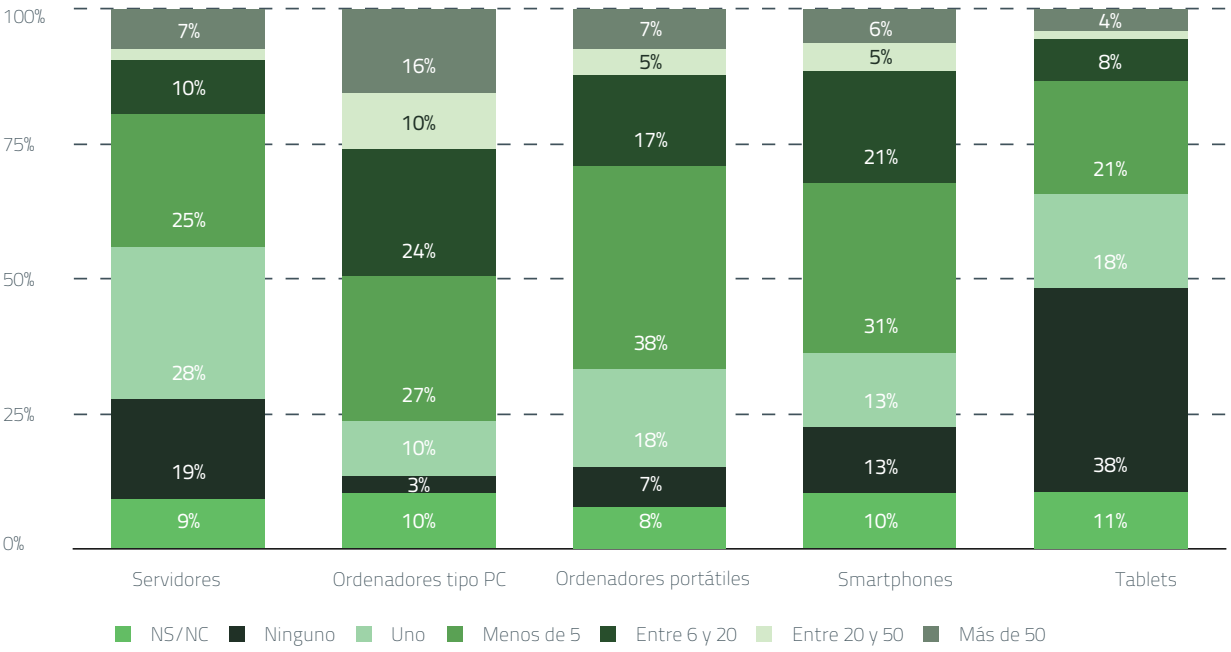
4.7. NÚMERO DE EQUIPOS UTILIZADOS EN LA ORGANIZACIÓN

El número y tipo de equipos informáticos que utiliza una organización es un factor determinante para entender sus necesidades en materia de seguridad informática.

Así, el grado de implantación en las organizaciones que han participado en el estudio de servidores, ordenadores de sobremesa o PC, portátiles, teléfonos inteligentes o Smartphone, y tabletas nos indica que, salvo en el caso de los Tablets, son dispositivos ampliamente utilizados.

Esto nos permite entender que se trata de organizaciones que realmente utilizan los sistemas informáticos y, por lo tanto, les afectan los aspectos relacionados con la seguridad informática objeto del estudio.

INDIQUE EL NÚMERO DE EQUIPOS INFORMÁTICOS DE CADA TIPO QUE UTILIZAN EN SU ORGANIZACIÓN



Con respecto a los diferentes tipos de equipos utilizados por las organizaciones, cabe destacar las siguientes conclusiones:

› Servidores:

Se trata de equipos que juegan un rol importante en la gestión de la información y de las aplicaciones que utiliza la organización para lograr sus objetivos de negocio. Como tales, conllevan unos requerimientos de seguridad más relevantes que los equipos personales que utilizan los empleados. En otras palabras, un problema de seguridad en un servidor afecta a un número significativo de empleados.

Casi tres cuartas partes de los entrevistados indican que en su organización se utilizan servidores.

› Ordenadores portátiles

Los ordenadores portátiles tienen unos requerimientos de seguridad diferentes a los que tienen los ordenadores de sobremesa.

Por su propia naturaleza "portátil" llevan implícita la movilidad y con ella la posibilidad de que se pierdan, los roben, se caigan y se averíen, etc.

Por otra parte, la forma de uso de estos equipos también introduce algunas complicaciones adicionales a la hora de gestionar su seguridad. En un ordenador de sobremesa parece más sencillo, por ejemplo, que el usuario no disponga de privilegios de administrador, que el antivirus esté actualizado o trabajar guardando los ficheros en una carpeta de un servidor; mientras que en un ordenador portátil estas cuestiones de seguridad de primer nivel pueden resultar más complejas de lo que sería deseable.

De las respuestas obtenidas se desprende que el uso de este tipo de ordenadores está desplazando progresivamente a los ordenadores tradicionales de sobremesa, también en el ámbito profesional.

› Teléfonos inteligentes o Smartphones

Los teléfonos inteligentes o Smartphones se han popularizado en los últimos años, de forma que actualmente cualquier persona utiliza uno de estos equipos. De las respuestas obtenidas se desprende que en casi las tres cuartas partes de las organizaciones de los entrevistados se usan este tipo de equipos.

Se trata de equipos desde los que generalmente se gestiona, al menos, el correo electrónico y la mensajería instantánea. Estos dos aspectos lo convierten en un sistema con unos ciertos requerimientos de seguridad, ya que de extraviarse o ser robados, podría estar comprometida toda la información del correo electrónico y de mensajería instantánea.

Debemos añadir, que con una cierta frecuencia se trata de terminales que son propiedad del usuario, no de la empresa. Esto implica que es el usuario el que decide como quiere utilizarlo y qué medidas de seguridad quiere adoptar en "su" terminal. La empresa debe ser consciente de las implicaciones que esto tiene y decidir si autoriza o no el uso de dispositivos personales para el trabajo profesional.

› Tabletas

Las tabletas están a mitad de camino entre un ordenador portátil y un teléfono inteligente.

Las implicaciones de seguridad son similares a las comentadas ya anteriormente para estos dos tipos de equipos con respecto tanto a la posibilidad de robo o extravío, como con respecto al hecho de que se trate de equipos que son propiedad del empleado y no de la empresa.

Sin embargo, a diferencia de todos los casos anteriores, en las respuestas se aprecia que su uso en el ámbito profesional no está tan extendido como el caso de los ordenadores portátiles y los Smartphones.

4.8. ELEMENTOS DE SEGURIDAD DE LOS QUE DISPONE

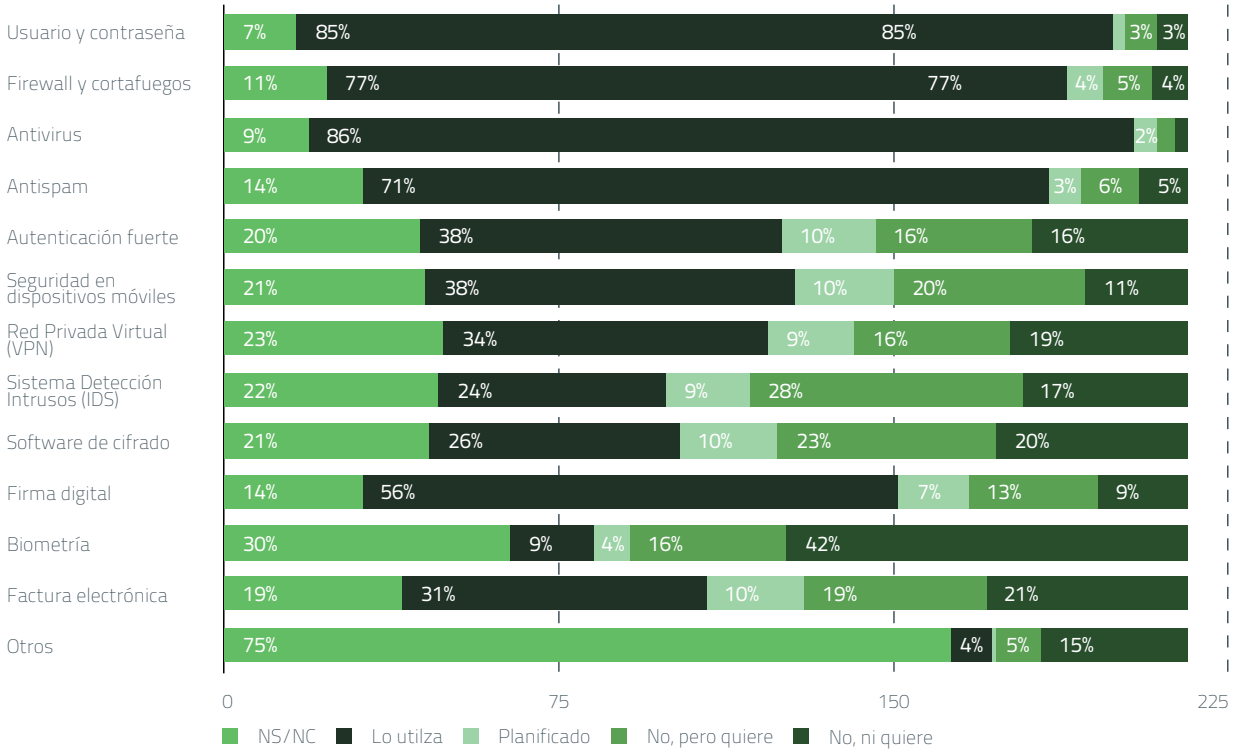
Este apartado del estudio nos da una idea bastante clara sobre el grado de implantación que tienen las tecnologías de seguridad más comunes en las organizaciones que han participado en el estudio.

Se puede apreciar que un porcentaje muy elevado de las organizaciones participantes utilizan elementos de seguridad básicos como usuario y contraseña, cortafuegos, antivirus y antispam.

Cuando se trata de tecnologías un poco más avanzadas, el porcentaje de utilización disminuye considerablemente. Cabe destacar el número de organizaciones que no utilizan, pero que les gustaría hacerlo, tecnologías como la factura electrónica, sistemas de detección de intrusos, herramientas de cifrado o sistemas de seguridad para dispositivos móviles.

También se puede apreciar cómo la biometría despierta muy poco interés en las organizaciones participantes en el estudio, ya que el porcentaje de organizaciones que ni la utilizan, ni la quieren utilizar es bastante alto.

INDIQUE SI SU ORGANIZACIÓN UTILIZA ACTUALMENTE ALGUNO DE LOS SIGUIENTES ELEMENTOS



En lo que se refiere a los elementos de seguridad con que cuentan las organizaciones que han participado en el estudio, cabe destacar las siguientes conclusiones:

› Usuario y contraseña

A primera vista podría interpretarse como un buen dato el que un 85% de organizaciones que utilizan usuario y contraseña para acceder a sus sistemas. Pero la realidad es que con todo lo que se ha andado en materia de seguridad, y con todos los incidentes que hay, el hecho de que continúe habiendo un 7% de empresas (1% que lo tiene planificado, 3% que quiere implantarlo y 3% que ni lo tiene ni lo quiere implantar) que no dispongan de algo tan básico como autenticación por usuario

y contraseña, da una idea de la dimensión del problema cultural y de concienciación existente en materia de seguridad informática.

› Cortafuegos o firewall

La lectura de que, actualmente, al menos un 13 % de las empresas entrevistadas no dispongan de cortafuegos, junto con el dato del alto porcentaje de organizaciones que utilizan servicios a través de internet, indican que más de un 10% de las organizaciones participantes en el estudio no cuentan con vías de protección elementales de sus sistemas frente a intentos de acceso no autorizado desde el exterior.

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

› Antivirus

Es importante resaltar nuevamente que, aunque más del 85% de las organizaciones disponen de soluciones antivirus, el número de incidentes relacionados con este tipo de amenazas es elevado, según han indicado los entrevistados en el apartado de incidentes. Esto sólo se puede entender como que las herramientas no están adecuadamente implantadas, mantenidas y actualizadas.

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

› Autenticación fuerte

Como ya se comento anteriormente en el apartado referente la utilización de usuario y contraseña para acceder a los sistemas informáticos y a la información, desde un punto de vista de seguridad, la identificación del usuario es uno de los puntos de partida.

En ocasiones, usuario y contraseña (lo que se conoce como "something that you know" o "algo que sabes") no es suficiente garantía para dar por válida esta identificación y se requiere de algún otro elemento adicional ("something that you have" o "algo que tienes") como puede ser una tarjeta chip, un código, una llave USB, la huella digital, identificación facial, y un largo etcétera.

Resulta muy interesante que el 38% de las organizaciones entrevistadas ya lo estén utilizando, que un 10% tenga ya planificado su implantación, y otro 16% esté interesado en su uso.

› Seguridad en dispositivos móviles

En el apartado de equipos informáticos utilizados por las organizaciones, se pudo ver como el uso de Smartphone estaba ampliamente difundido, así como los retos que el uso de estos equipos plantea desde la perspectiva de la seguridad.

Los Smartphones incorporan algunas características de seguridad dentro del propio sistema, como el bloqueo con contraseña, la copia de seguridad o el borrado remoto.

Sin embargo, muchas de estas características no se suelen activar, ya sea por desconocimiento o por la comodidad del usuario. Este hecho queda reflejado en que sólo el 38% de los entrevistados indican que utilizan este tipo de medidas de seguridad.

› 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 una garantía suficiente de 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 comprobar que un 34% de las organizaciones ya esté utilizando esta tecnología, y otro 25% quieran implantarla o bien tengan ya planificada su implantación.

› Sistema de detección y prevención de intrusiones o IDS / IPS

Estos sistemas suponen una medida de seguridad adicional a los cortafuegos, en materia

de protección de los sistemas informáticos, frente a intentos de acceso desde internet.

Cabe destacar que casi una cuarta parte de los encuestados utilizan esta tecnología de seguridad, pero es especialmente interesante el hecho de que un 9% lo contemple dentro de sus planes y otro 28% quiera utilizarlo.

- Firma digital

La firma digital es una tecnología que permite firmar electrónicamente los documentos, con la misma validez jurídica que tiene la firma manuscrita. Más de la mitad de los entrevistados indican que utilizan firma electrónica.

5. SERVICIOS CLOUD

En los últimos años se ha extendido la utilización de determinados servicios en modo Cloud, a la par que se ha mantenido abierto el debate sobre la seguridad de los mismos como uno de los frenos para su popularización.

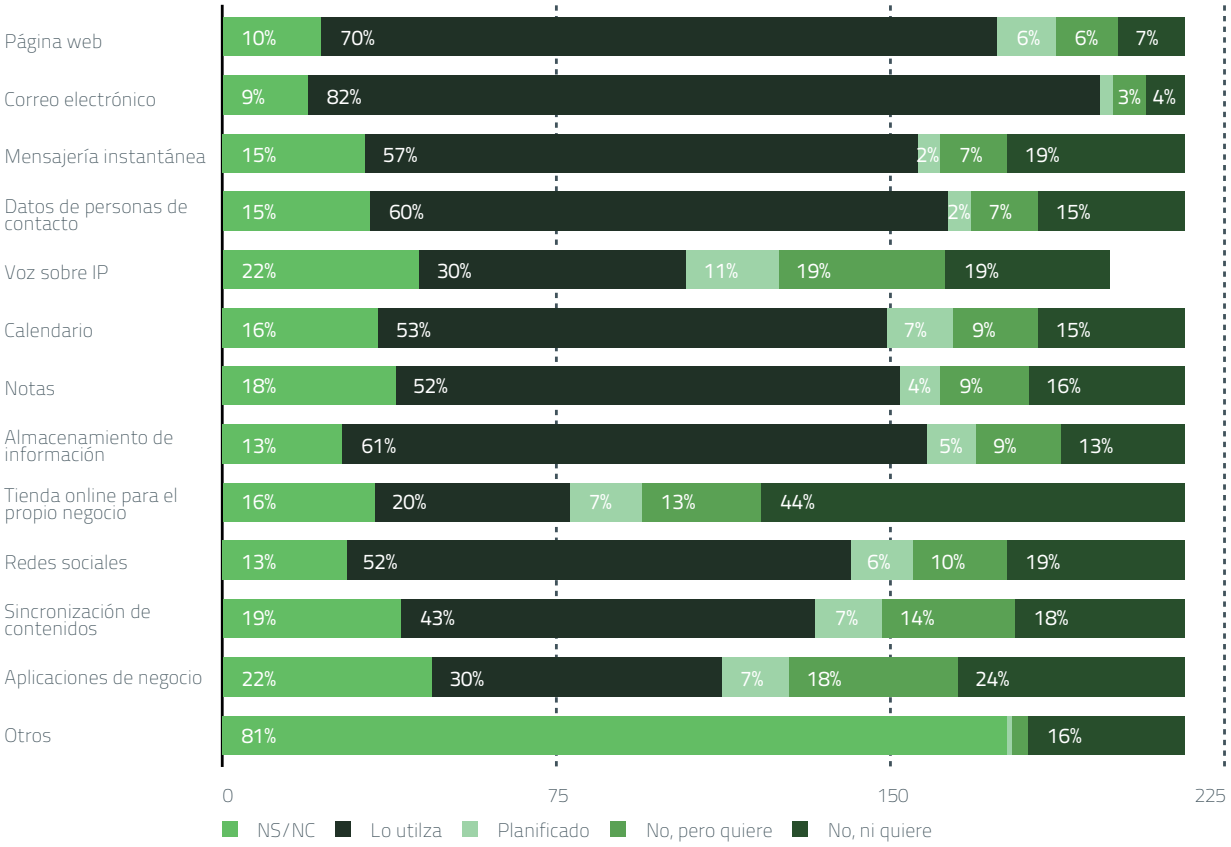
En el estudio se ha tratado de obtener una visión general sobre el grado de utilización de servicios en modo Cloud que están haciendo actualmente las organizaciones que han participado en el estudio.

En este caso, un porcentaje muy elevado de las organizaciones participantes utilizan en modo Cloud los servicios más habituales, como página web, correo electrónico, calendario, notas, o almacenamiento de información en Cloud.

Otros servicios como voz sobre IP, tienda online o aplicaciones de negocio tienen un nivel de implantación menor.

En cualquier caso, queda de manifiesto que más allá de los debates que puedan suscitarse con respecto al uso del Cloud, las organizaciones están haciendo un uso bastante amplio de este tipo de servicios.

INDIQUE SI SU ORGANIZACIÓN UTILIZA ACTUALMENTE ALGUNO DE LOS SIGUIENTE SERVICIOS A TRAVÉS DE INTERNET



En lo que se refiere a los servicios en modo Cloud que actualmente están utilizando las organizaciones que han participado en el estudio, cabe destacar las siguientes conclusiones:

› Voz sobre IP

El uso de sistemas de voz sobre IP se está popularizando, especialmente entre las organizaciones que mantienen relaciones frecuentes con terceros países. En estos casos, la voz sobre IP supone un ahorro sustancial en los costes de comunicaciones de voz con respecto a los servicios tradicionales de telefónica.

Aunque sólo un 30% de los entrevistados ha contestado que lo utiliza, casi otro 30 % más o lo tiene planificado, o quiere utilizarlo.

› Almacenamiento de información

Los servicios de almacenamiento de información en Cloud se están extendiendo rápidamente, un 61% de los entrevistados manifiesta que almacenan información en la nube.

› Tienda online para el negocio propio

Probablemente éste sea uno de los servicios más atractivos para las empresas, ya que les permite posicionar rápidamente su comercio en internet

La perspectiva de poder ampliar el negocio a un mercado mucho más amplio (incluso podría llegar a considerarse global) y sin limitaciones de horario, debería suponer un enorme atractivo para las organizaciones. Sin embargo, sólo el 20% de los entrevistados emplea este servicio, y lo que es más relevante, el 44% no quiere utilizarlo

› Redes sociales

Aunque durante un tiempo se consideraron a las redes sociales como una herramienta orientada al uso particular, en el último año se ha popularizado su uso a nivel de organización. Este hecho queda de manifiesto al constatar que el 52% de los entrevistados utiliza las redes sociales.

› Aplicaciones de negocio

Las aplicaciones empresariales para la gestión de recursos humanos, contabilidad, recursos operativos, etc. se están trasladando de forma progresiva a un modelo Cloud.

Aunque algunas organizaciones argumentan problemas de pérdida de control o de seguridad, lo cierto es que un 30% de los entrevistados ya están utilizando este tipo de servicios en modo Cloud.

6. INCIDENTES

Las organizaciones pueden asumir una serie de riesgos en materia de seguridad, de manera consciente o no, pero lo que realmente puede dar una visión objetiva de la relevancia de estos riesgos es el número de incidentes reales que se hayan producido.

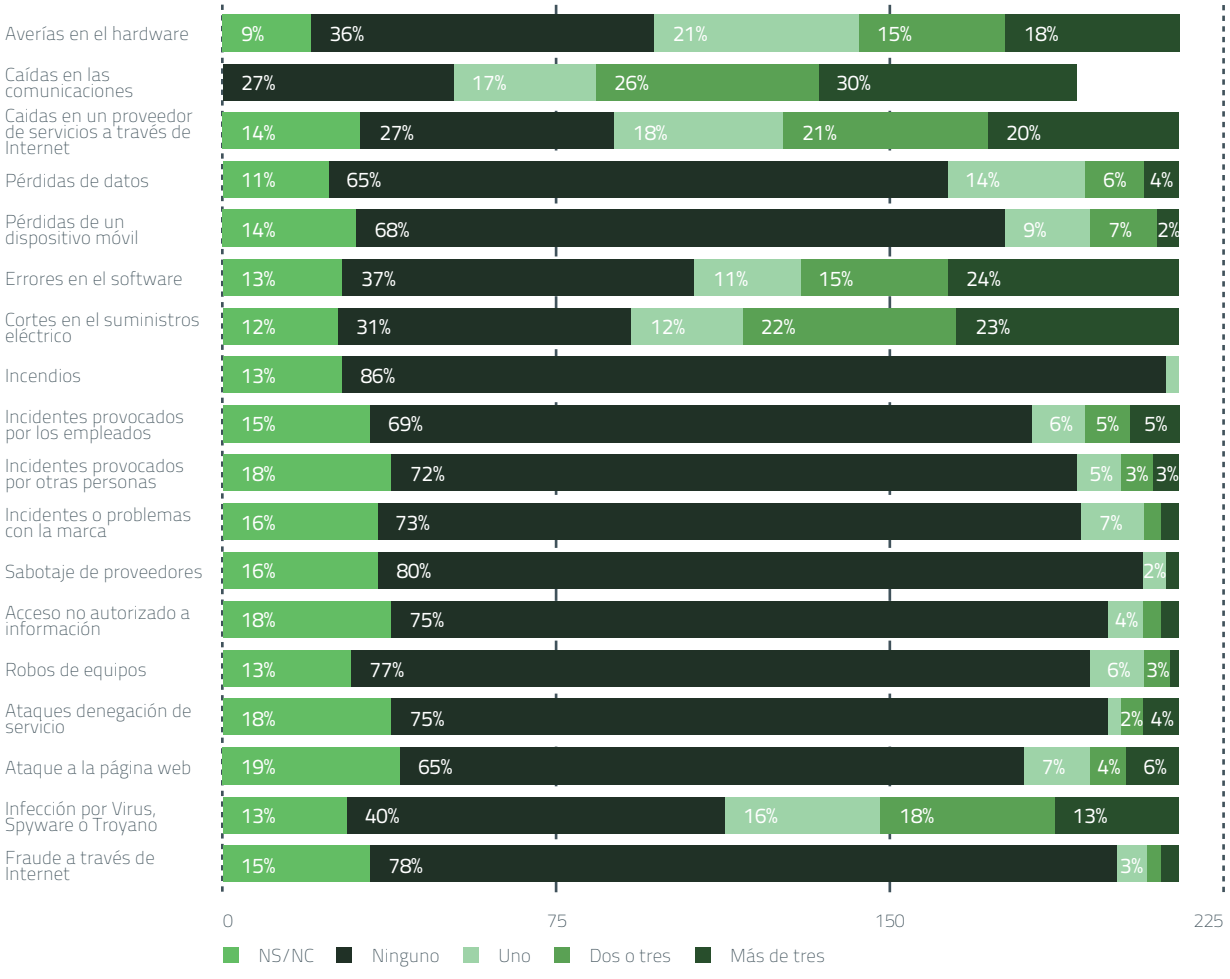
Para disponer de información real sobre este aspecto se ha incluido en el cuestionario un apartado específico para tratar de conocer el volumen de incidentes que han sufrido las organizaciones en el último año y de qué tipo han sido estos incidentes.

Los resultados de este apartado se deben valorar de forma conjunta con los del siguiente ítem, en el que se pregunta a los encuestados por el impacto de dichos percances.

Cabe destacar que algunos de estos incidentes (averías en hardware, caídas de comunicaciones, caídas de servicios de internet, errores en el software, interrupciones del suministro eléctrico o infecciones por virus) han afectado a más de la mitad de los entrevistados.

La conclusión más evidente de este apartado del estudio, es que los incidentes ocurren. No se trata de algo teórico, sino que se trata de circunstancias a las que se enfrentan habitualmente las organizaciones de la región.

¿CUÁNTOS INCIDENTES DE CADA UNO DE LOS TIPOS SIGUIENTES HA SUFRIDO EN LOS ÚLTIMOS 12 MESES?



En lo que se refiere a los tipos de incidentes que los entrevistados han manifestado haber sufrido durante los 12 meses anteriores, se subrayan los siguientes comentarios:

› Infecciones por virus, spyware y troyanos

Cerca del 50% de las organizaciones han sufrido sufrido infecciones por código malicioso y, alrededor de un 30%, han sufrido varios incidentes de este tipo.

Esta cifra no parece demasiado consistente con el dato de que cerca del 90% de los entrevistados manifestaron que utilizaban una herramienta antivirus.

El hecho de que se den tantos casos de infección, aun disponiendo de un antivirus, indica que o bien la herramienta de antivirus no está bien instalada o actualizada, o bien que no se están siguiendo las buenas prácticas para evitar infecciones (no abrir correos sospechosos, no navegar por páginas web poco fiables, abrir archivos sin pasarlos previamente por el antivirus, etc.)

› Caídas en las comunicaciones

El trabajo diario de las organizaciones, actualmente tiene una dependencia relevante de la disponibilidad de las comunicaciones. En este sentido, este aspecto debería considerarse como un elemento crítico para el normal desarrollo de la actividad profesional

En muchas ocasiones, las organizaciones contratan los servicios de comunicaciones haciendo más hincapié en el coste final de las líneas (típicamente se trata de líneas ADSL) que en la calidad del servicio del proveedor.

El hecho de que haya tantas caídas de las líneas de comunicaciones pone de manifiesto la necesidad de incidir de una forma más contundente en la calidad del servicio, aunque suponga un coste algo mayor.

› Cortes en el suministro eléctrico

Más allá del problema evidente de no poder utilizar los equipos informáticos, los cortes en el suministro eléctrico suelen redundar en averías en el equipamiento, así como en la pérdida de datos.

Disponer de un pequeño sistema de alimentación ininterrumpida para proteger el equipamiento informático frente a este tipo de situaciones, es una solución sencilla y económica.

› Pérdida de datos

Prácticamente una de cada cuatro personas entrevistadas manifiestan que han sufrido pérdida de datos.

Las copias de seguridad son la medida preventiva más extendida para evitar pérdidas de datos, pero en muchas ocasiones no se le presta la debida atención. En muchas ocasiones no se hace copia de seguridad de toda la información importante (correo electrónico, algunas bases de datos, ficheros guardados en ordenadores portátiles o en carpetas personales en los PC, etc.)

Para evitar pérdidas de datos es necesario tener la certeza de que se hacen copias de seguridad de toda la información importante para la organización, y verificar periódicamente que la información contenida en las copias se puede recuperar

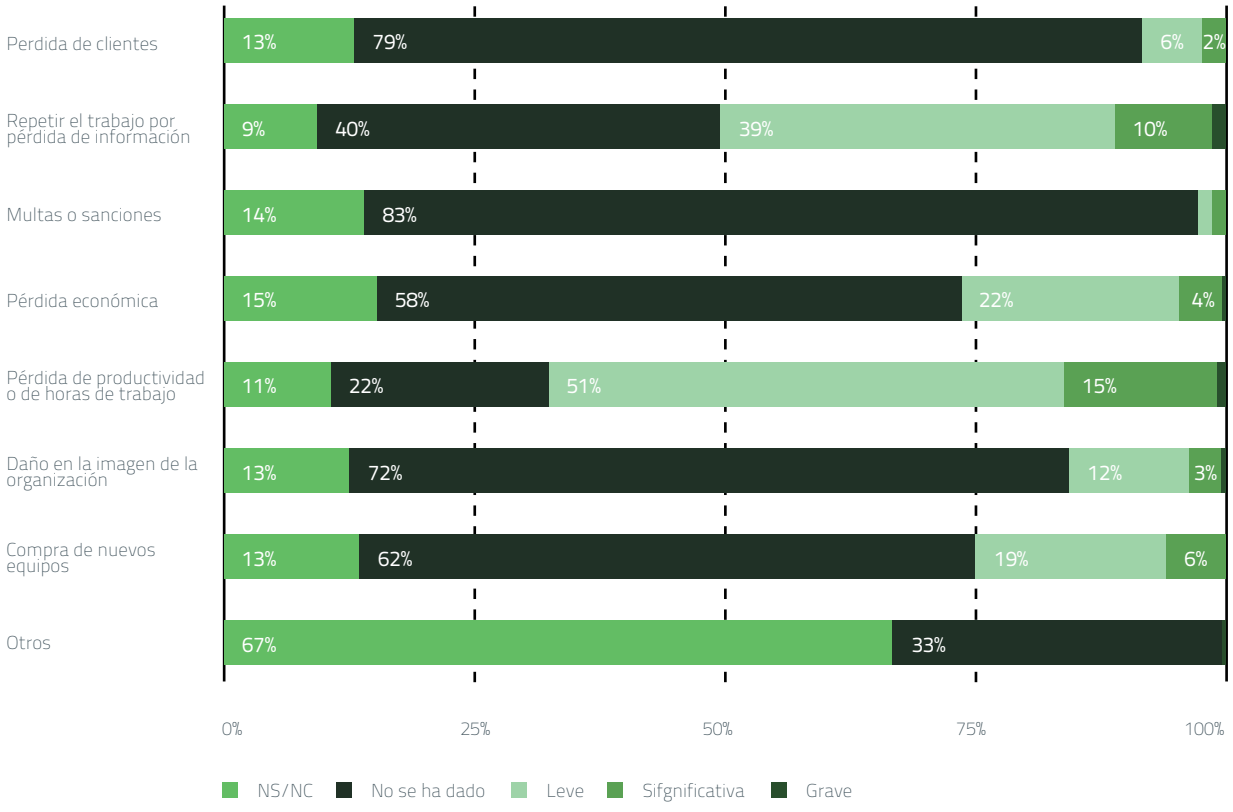
7. CONSECUENCIAS DE LOS INCIDENTES

Como ya se comentó en el apartado anterior, los incidentes de seguridad implican que estos percances ocurren. Otra cuestión es valorar cuáles son las consecuencias de estos incidentes para las organizaciones.

Por este motivo se ha incluido en el estudio un apartado para tratar de conocer cuál ha sido la dimensión del impacto que estos incidentes tienen en las organizaciones.

De las respuestas obtenidas cabe destacar el hecho de que el mayor impacto se ve en la necesidad de repetir el trabajo ya realizado, o en las pérdidas de productividad, teniendo una repercusión menor en lo referente a pérdidas económicas directas, pérdida de clientes o el daño a la imagen de la organización.

VALORE PARA CADA UNO DE LOS SIGUIENTES SUPUESTOS CUÁLES HAN SIDO LAS CONSECUENCIAS DE LOS INCIDENTES QUE HA SUFRIDO

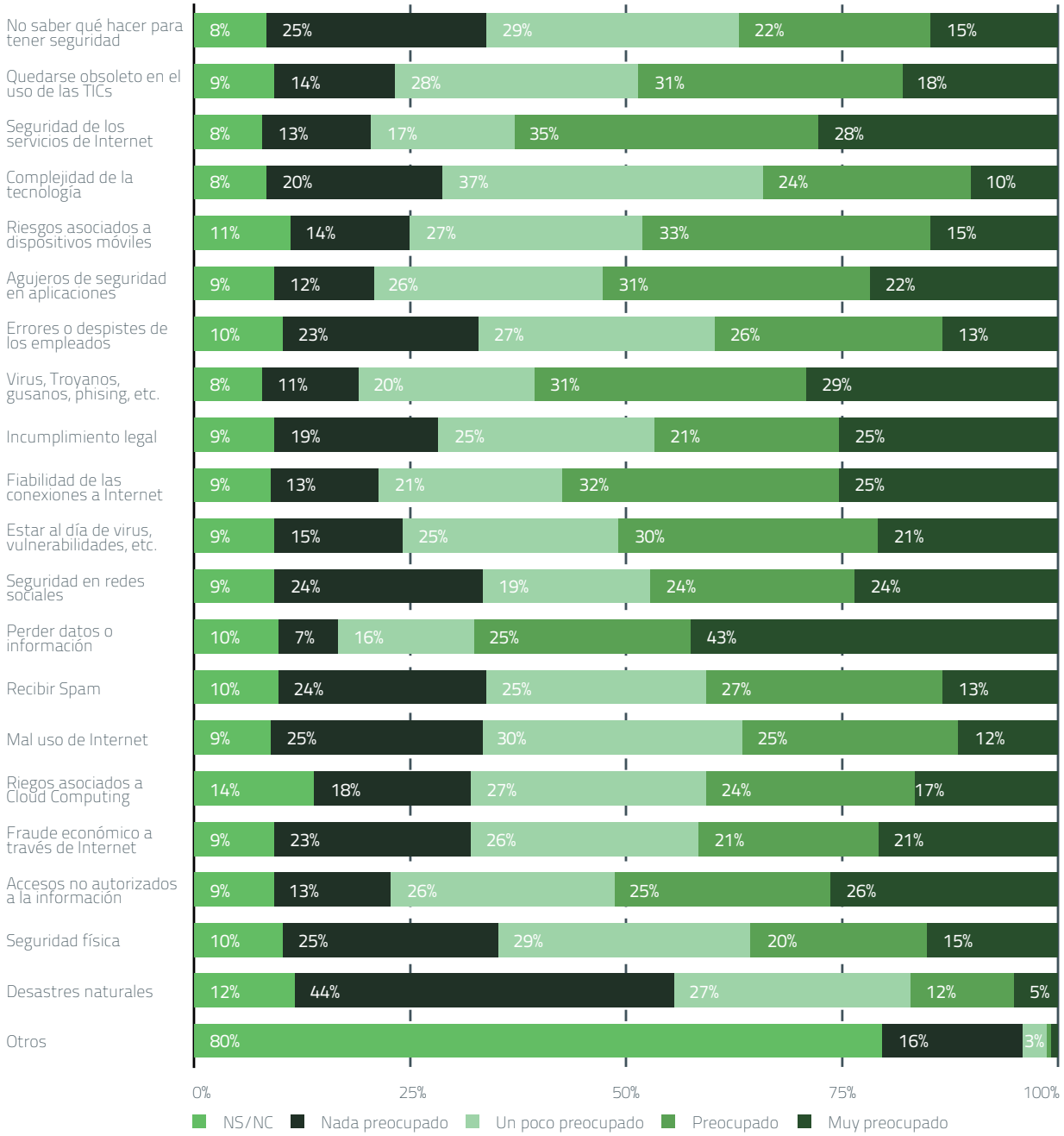


8. LAS PREOCUPACIONES

Independientemente de que los incidentes suponen la manifestación real de los problemas de seguridad, el personal de las organizaciones tiene una serie de preocupaciones relacionadas con estos posibles problemas de seguridad, que son importantes de valorar.

En este sentido, se aprecia por las respuestas obtenidas que existe un nivel de preocupación generalizado y bastante elevado. En términos generales, las personas entrevistadas están preocupadas por casi todos los aspectos contemplados en el estudio. Se puede destacar el temor con respecto a las posibles pérdidas de datos o de información.

VALORE CUÁL ES SU GRADO DE PREOCUPACIÓN CON RESPECTO A CADA UNA DE LAS SIGUIENTES CIRCUNSTANCIAS



Centrando los comentarios en aquellos eventos en los que los entrevistados están muy preocupados, se destaca

- Perder datos o información

Este aspecto sigue siendo el más preocupante para las organizaciones, además de coincidir con el hecho de que se produce un número significativo de incidentes relacionados con la pérdida de información

- Código malicioso

Este elemento ya se ha comentado con anterioridad en otros apartados del estudio y, aunque es uno de los temas sobre los que más tiempo se lleva trabajando, continúa siendo uno de los que está siempre presente.

- Seguridad en los servicios de Internet

En términos generales, la seguridad relacionada con los servicios en Internet sigue generando preocupación entre los usuarios de forma relevante.

Este aspecto está identificado de forma habitual, como un freno al desarrollo de estos servicios de forma masiva.

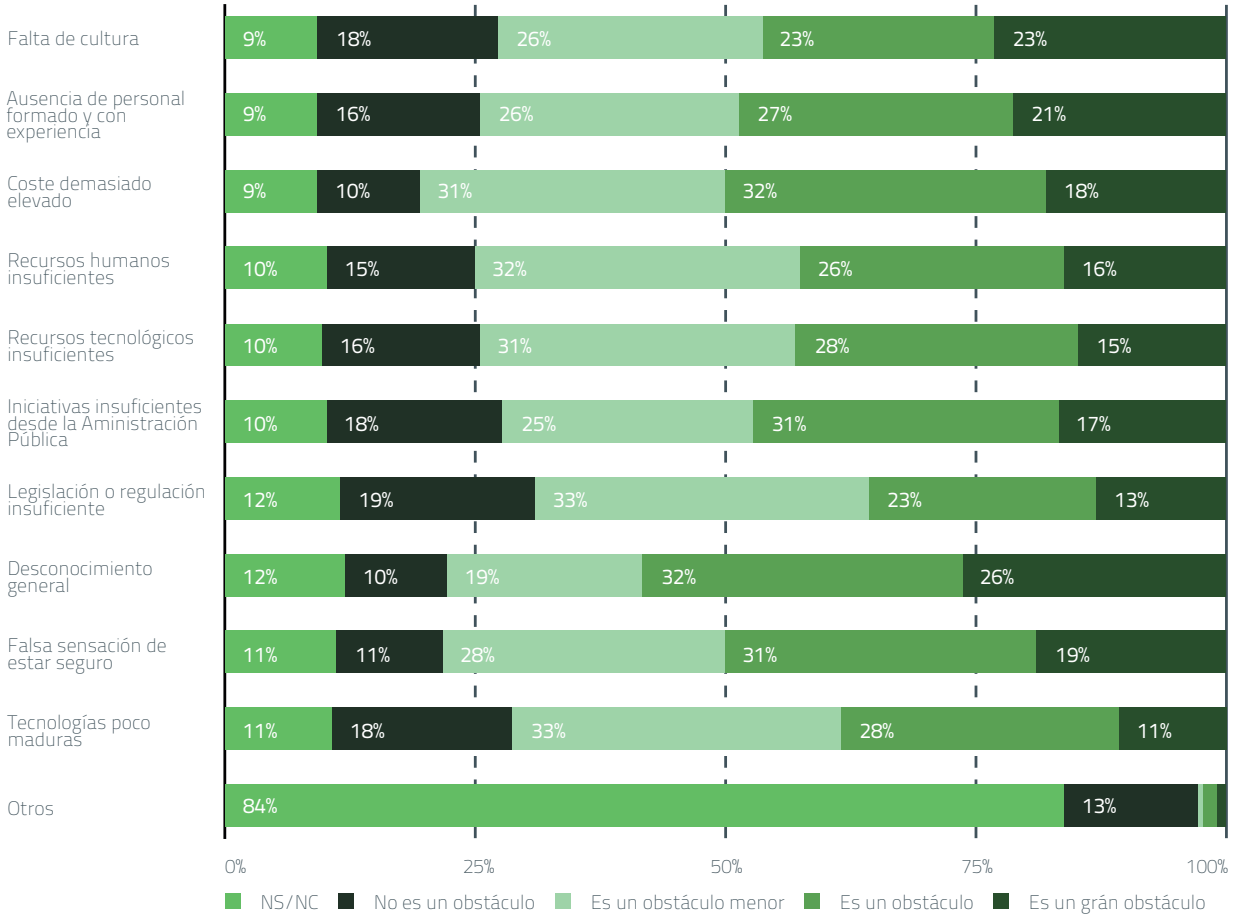
9. OBSTÁCULOS AL DESARROLLO DE LA SEGURIDAD

Se ha pedido a los alumnos que valorasen cuales son, a su juicio, los principales obstáculos para el desarrollo de la seguridad.

De forma parecida a lo ocurrido en el apartado anterior, donde se evaluaban las preocupaciones, en este caso también los entrevistados consideraban de forma general que los obstáculos contemplados dentro del estudio constituían un serio problema para el desarrollo de la seguridad.

Independientemente de la importancia de cada uno de los obstáculos planteados, se quiere destacar que el desconocimiento general y la falta de cultura en materia de seguridad son probablemente los más importantes.

VALORE LA IMPORTANCIA DE LOS SIGUIENTES OBSTACULOS PARA DISPONER DE UN BUEN NIVEL DE SEGURIDAD

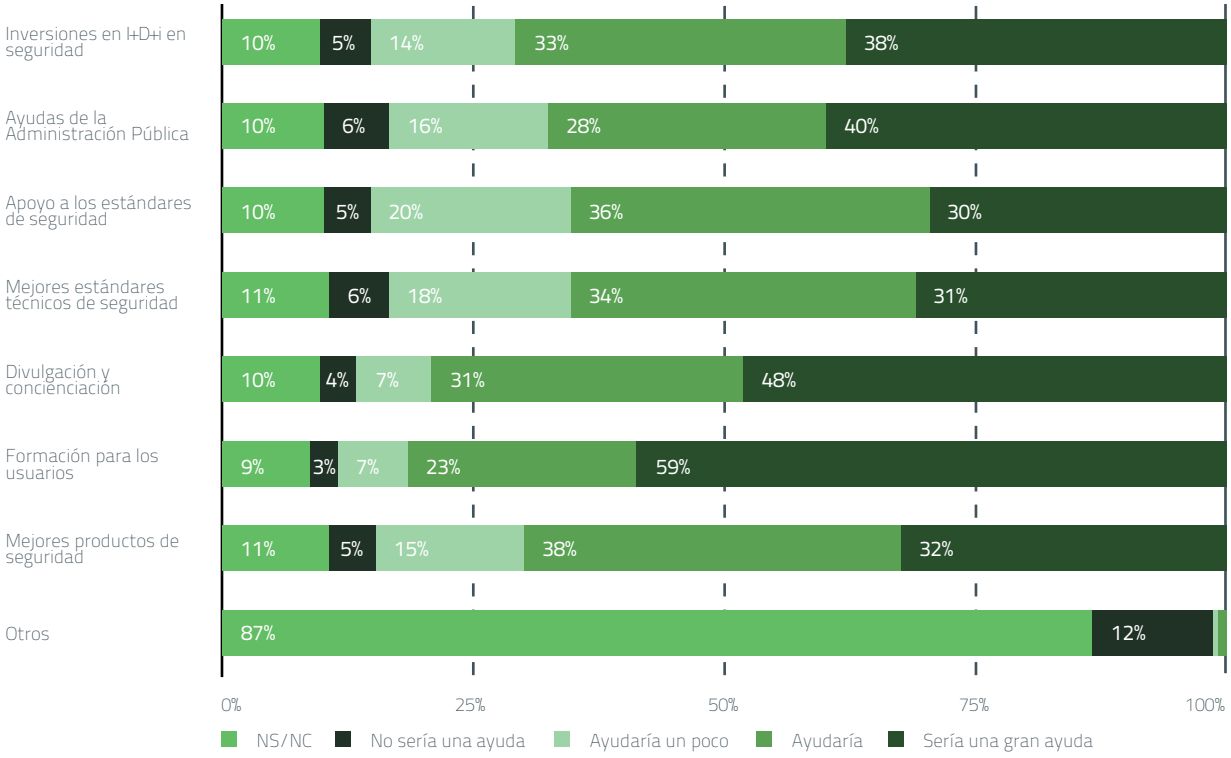


10. INICIATIVAS PARA MEJORAR LA SEGURIDAD

Vista cual es la situación respecto a la seguridad de la información, se consideró interesante incorporar al estudio la valoración de cuales son, a juicio de los entrevistados, las iniciativas más importantes para el desarrollo de la seguridad.

A partir de las respuestas obtenidas se llega a la conclusión de que tanto la divulgación y la concienciación, como la formación para los usuarios, serían las dos iniciativas que supondrían una mayor ayuda para mejorar los niveles de seguridad de las organizaciones, por delante incluso de otro tipo de actuaciones que a priori podrían parecer más importantes para las organizaciones como mayores inversiones en I+D+i, ayudas de la Administración Publica, o incluso la posibilidad de disponer de mejores productos de seguridad para proteger a las organizaciones.

VALORE EN QUE MEDIDA AYUDARÍAN A MEJORAR LA SEGURIDAD CADA UNA DE LAS SIGUIENTES INICIATIVAS



ANEXO-. ENCUESTA:

EVALUACIÓN SOBRE EL ESTADO DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES DE LA RIOJA

DATOS DE LA ORGANIZACIÓN

CÓDIGO POSTAL

Código postal: .....

CARGO DE LA PERSONA QUE RESPONDE AL TEST

1. Director general
2. Director de informática / sistemas
3. Otros directivos
4. Responsable de seguridad
5. Responsable de informática / sistemas
6. Técnico de informática o sistemas
7. Administrativo
8. No sabe o no contesta
9. Otro (indicar): .....

NÚMERO DE EMPLEADOS

1. Entre1y9
2. Entre 10 y 49
3. Entre 50 y 249
4. Entre 250 y 500
5. Más de 500
6. No sabe o no contesta

SECTOR DE ACTIVIDAD

1. Administración pública
2. Industrias Agroalimentarias
3. Calzado
4. Industria Cultural y Turística
5. Comercio
6. Madera y Mueble
7. Metalmecánica, Automoción y Fabricación Avanzada
8. Construcción y Ahorro Energético
9. Energía

10. Química

11. Enseñanza

12. Banca

13. Medios de comunicación

14. Telecomunicaciones y de las Tecnologías de la Información 15. Aseguradoras

16. Transporte

17. Salud

18. No sabe o no contesta

19. Otro (indicar): .....

FACTURACIÓN EN EUROS AL AÑO

1. Menos de 100.000

2. Entre 100.000 y 500.000

3. Entre 500.000 y 2.000.000

4. Entre 2.000.000 y 10.000.000

5. Entre 10.000.000 y 50.000.000

6. Más de 50.000.000

7. No sabe o no contesta

LA GESTIÓN DE LA SEGURIDAD

¿Quién asume en su organización las tareas relacionadas con la seguridad de la información?.

1. No están asignadas a ninguna persona

2. Departamento de seguridad

3. Departamento de informática o similar

4. Técnico o personal de informática o similar

5. Otro personal de la organización

6. Subcontratado a una empresa externa

7. NS/NC

EQUIPOS Y SERVICIOS

NÚMERO DE EQUIPOS INFORMÁTICOS

Indique el número de equipos informáticos de cada tipo que utiliza en su organización.

	NINGUNO	UNO	MENOS DE 5	ENTRE 6 Y 20	ENTRE 20 Y 50	MÁS DE 50	NS/NC
Servidores							
Ordenadores tipo PC							
Ordenadores portátiles							
Smartphones							
Tablets							

ELEMENTOS DE SEGURIDAD QUE USA

Indique si su organización utiliza actualmente alguno de los siguientes elementos, si tiene planificado empezar a usarlos en los próximos 12 meses, si no los usa pero le gustaría, o si ni los usa ni los quiere usar.

	NS/NC	LO UTILIZA	PLANIFICADO	NO, PERO QUIERE	NO, NI QUIERE
Usuario y contraseña					
Firewall o cortafuegos					
Antivirus					
Antispam					
Autenticación fuerte					
Seguridad en dispositivos móviles					
Red Privada Virtual (VPN)					
Sistema Detección Intrusos (IDS)					
Software de cifrado					
Firma digital					
Biometría					
Factura electrónica					
Otros (indicar)					

SERVICIOS EN CLOUD

Indique si su organización utiliza actualmente alguno de los siguientes elementos, si tiene planificado empezar a usarlos en los próximos 12 meses, si no los usa pero le gustaría, o si ni los usa ni los quiere usar.

	NS/NC	LO UTILIZA	PLANIFICADO	NO, PERO QUIERE	NO, NI QUIERE
Página web					
Correo electrónico					
Mensajería instantánea					
Datos de personas de contacto					
Voz sobre IP					
Calendario					
Notas					
Almacenamiento de información					
Tienda online para el propio negocio					
Redes sociales					
Sincronización de contenidos					
Aplicaciones de negocio					
Otros (indicar)					

LOS INCIDENTES

¿Cuántos incidentes de cada uno los siguientes tipos ha sufrido en los últimos 12 meses?

	NS/NC	NINGUNO	UNO	DOS O TRES	MÁS DE 3
Averías en el hardware					
Caídas en las comunicaciones					
Caídas en un proveedor de servicios a través de Internet					
Pérdida de datos					
Pérdida de un dispositivo móvil					
Errores en el software					
Cortes en el suministro eléctrico					
Incendios					
Incidentes provocados por los empleados					
Incidentes provocados por otras personas					
Incidentes o problemas con la marca					
Sabotaje de proveedores					
Acceso no autorizado a información					
Robos de equipos					

	NS/NC	NINGUNO	UNO	DOS O TRES	MÁS DE 3
Ataques denegación de servicio					
Ataque a la página web					
Infección por Virus, Spyware o Troyano					
Fraude a través de Internet					

LAS CONSECUENCIAS

Valore, para cada uno de los siguientes supuestos, cuáles han sido las consecuencias de los incidentes que ha sufrido

	NS/NC	NO SE HA DADO	LEVE	SIGNIFICATIVA	GRAVE
Pérdida de clientes					
Repetir el trabajo por pérdida de información					
Multas o sanciones					
Pérdida económica					
Pérdida de productividad o de horas de trabajo					
Daño en la imagen de la organización					
Compra de nuevos equipos					
Otros (indicar)					

LAS MAYORES PREOCUPACIONES

Valore cuál es su grado de preocupación con respecto a cada una de las siguientes circunstancias, siendo 1 nada preocupado y 4 muy preocupado.

	NS/NC	1	2	3	4
No saber qué hacer para tener seguridad					
Quedarse obsoleto en el uso de las TI					
Seguridad de los servicios de Internet					
Complejidad de la tecnología					
Riesgos asociados a dispositivos móviles					
Agujeros de seguridad en aplicaciones					

	NS/NC	1	2	3	4
Errores o despistes de los empleados					
Virus, troyanos, gusanos, phising, etc.					
Incumplimiento legal					
Fiabilidad de las conexiones a Internet					
Estar al día de virus, vulnerabilidades, etc.					
Seguridad en redes sociales					
Perder datos o información					
Recibir Spam					
Mal uso de Internet					
Riesgos asociados a Cloud computing					
Fraude económico a través de Internet.					
Accesos no autorizados a la información					
Seguridad física					
Desastres naturales					
Otros (indicar)					

LOS OBSTÁCULOS PARA LA SEGURIDAD

Valore la importancia de los siguientes obstáculos para disponer de un buen nivel de seguridad, siendo 1 no es un obstáculo y 4 es un gran obstáculo.

	NS/NC	1	2	3	4
Falta de cultura					
Ausencia de personal formado y con experiencia					
Coste demasiado elevado					
Recursos humanos insuficientes					
Iniciativas insuficientes desde la administración pública					
Legislación o regulación insuficiente					
Desconocimiento en general					

	NS/NC	1	2	3	4
Falsa sensación de estar seguro					
Tecnologías poco maduras					
Otros (indicar)					

LAS INICIATIVAS QUE AYUDARÍAN A MEJORAR LA SEGURIDAD

Valore en qué medida ayudarían a mejorar la seguridad, en su opinión, cada una de las siguientes iniciativas; siendo 1 no sería una ayuda y 4 sería de gran ayuda.

	NS/NC	1	2	3	4
Inversiones en ~~I+D+i~~ en seguridad					
Ayudas de la Administración Pública					
Apoyo a los estándares de seguridad					
Mejores estándares técnicos de seguridad					
Divulgación y concienciación					
Formación para los usuarios					
Mejores productos de seguridad					
Otros (indicar)					