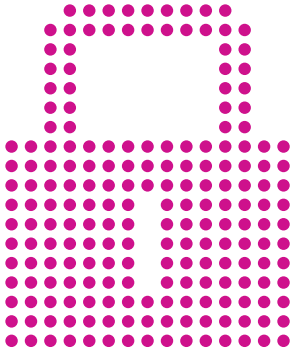


INFORME
DEL ESTUDIO DE
SEGURIDAD
THINKTIC 2016

Gobierno de La Rioja
think TIC Centro Nacional de Formación en Nuevas Tecnologías
Sistema Riojano de Innovación

Presentación

El Centro Nacional de Formación en Nuevas Tecnologías, Think-TIC, certificado el año 2015 como Centro de Referencia Nacional de Sistemas Informáticos y Telemática en el ámbito de la Formación Profesional, 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 2013 se realizó un estudio focalizado en la seguridad informática de las empresas riojanas que se encuentra disponible en la página web del Gobierno de La Rioja.

La Consejería de Desarrollo Económico e Innovación es consciente de la transformación digital que está viviendo la sociedad en general y las empresas en particular, independientemente del tamaño y sector. El incremento exponencial de la actividad de los empleados dentro de las organizaciones en entornos digitales y su uso intensivo en los procesos de negocio empresariales ha provocado en pocos años que la seguridad de la información constituya un factor estratégico decisivo para la continuidad de las empresas.

Con estas premisas, desde el comienzo de su actividad el Think-TIC han pasado por sus aulas más de 1.000 alumnos con el objetivo de mejorar su formación en las herramientas, procedimientos y prácticas más adecuadas en esta disciplina. Una labor de divulgación y comunicación para todo el tejido productivo riojano que también les acerca a las nuevas tendencias como el Big Data y a los medios necesarios para preservar seguros sus datos y sistemas informáticos.

El V Plan Riojano de I+D+I identifica en su línea estratégica “Sociedad innovadora” la necesidad de que la sociedad mantenga una alta cualificación en ciencia y tecnología. Incrementar la formación continua en las empresas convirtiéndola en factor de competitividad y una sociedad conectada utilizando las TIC’s como herramienta básica de la comunicación y de actividad económica. Dentro de esta línea se definen varios programas de trabajo que reflejan explícitamente los tres ejes verticales propuestos en la Agenda Digital de La Rioja en los que también se potenciará la vigilancia tecnológica y competitiva para analizar necesidades de formación en las empresas.

Se quiere destacar el trabajo conjunto realizado desde el Think-TIC con el Instituto de Estadística de La Rioja para la realización de las encuestas y también la contribución de AERTIC, miembro del Consejo Social del Centro de Referencia Nacional, que redunda en esa orientación práctica de una formación útil y de calidad para profesionales y empresas riojanas. Siempre con el fin último de mejorar la competitividad en aras de un mayor y mejor desarrollo económico y social de La Rioja.

Por último, agradecer la inestimable aportación en la dirección de este trabajo a Olof Sandstrom, uno de los mayores expertos nacionales en gestión de la seguridad de la información.

Leonor González Menorca

Consejera de Desarrollo Económico e Innovación

Gobierno de la rioja

Carta de aertic

Esta nueva versión del informe del estudio de seguridad ThinkTIC 2016, llega justo a tiempo ante la gran cantidad de noticias y sucesos ocurridos en el ámbito de la seguridad de la información en lo que llevamos de año 2017.

Los ataques informáticos son globales y se expanden de inmediato, muchos de ellos utilizando vulnerabilidades conocidas pero cuyos parches no han sido aplicados, o afectando a sistemas obsoletos para los que no hay un parche adecuado.

En estos momentos es crucial tomar una mayor conciencia con la seguridad en los sistemas informáticos y las comunicaciones. El desarrollo de la industria conectada y de los wearables, (dispositivos y maquinaria que se diseñan para que se conecten entre sí, bien para proporcionar información, o interactuar), hace fundamental el implantar una estrategia en seguridad. Un ataque a un simple dispositivo que esté integrado en una red global de una empresa puede infectar a esta empresa, además de propagarse por las empresas con las que tenga redes de confianza la organización infectada. Esto lo hemos visto en el reciente caso de Wannacry, en el que resultaron infectados un gran número de empresas que tenían redes de confianza con las multinacionales infectadas en primer término.

Por otro lado, tenemos que tomar conciencia de los peligros reales de no dotar a nuestras empresas de mecanismos de seguridad adecuados, ya que corremos riesgos como cese en la disponibilidad de los sistemas de información, secuestro de los datos, destrucción de la imagen, y perjuicio económico por la paralización de la organización, el posible pago de un rescate o las horas de técnicos de seguridad para restaurar el funcionamiento de la empresa. Además, es clave la posterior implantación de las medidas de seguridad adecuadas para prevenir futuros ataques.

Desde AERTIC recomendamos que las empresas auditen la seguridad de sus sistemas, implementen al menos las medidas básicas, y formen a sus trabajadores, algo fundamental en cualquier estrategia de aseguramiento de la continuidad de negocio.

Muchas empresas creen que, bien por la falta de personal especializado, bien por su pequeño tamaño, no pueden o no quieren dedicar recursos internos para implantar un plan de seguridad adecuado. Ante esta circunstancia recomendamos desde AERTIC que se doten de un acuerdo a largo plazo con una empresa especializada en este punto. Es importante la especialización en el asesoramiento tanto por el conocimiento a fondo de los sistemas empresariales, como por la mejora sostenida a lo largo del tiempo que solo puede brindar un experto en materia de seguridad de la información.

Consideramos que este informe es fundamental para la labor de divulgación y concienciación de toda la sociedad de nuestra comunidad ante una materia crítica en el futuro de nuestras empresas y organizaciones.

José Luis Pancorbo
Presidente de AERTIC

Indice

Introducción

El Centro de Referencia Nacional en Informática y Comunicaciones, en adelante Think-TIC, es un organismo dependiente de la Dirección General de Innovación, Trabajo, 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.

En el año 2014 el Think-TIC realizó un estudio sobre la situación de la seguridad informática en las empresas de La Rioja. Para ello se elaboró un estudio a lo largo del segundo semestre del año 2013. El informe del estudio realizado en 2014 está disponible en la página web del Gobierno de La Rioja.

A la vista de los resultados de este primer estudio desarrollado en el año 2014, el Centro consideró oportuno darle continuidad al mismo para disponer de una herramienta que permita valorar cómo evolucionan en La Rioja algunos de los aspectos relevantes de la seguridad informática. Por este motivo el Think-TIC ha realizado un nuevo estudio en el año 2016.

Como nota aclaratoria, indicar que cuando se hace referencia en el presente documento al concepto de "Seguridad", se debe entender como seguridad informática en cualquiera de sus dimensiones:

Confidencialidad: Únicamente tienen acceso a la información las personas autorizadas.

Integridad: La información es correcta y no ha sido modificada de forma no autorizada.

Disponibilidad: La información está disponible cuando es necesario acceder a ella.

Resumen ejecutivo

Tecnologías de seguridad utilizadas

Las tecnologías clásicas de seguridad (autenticación con usuario y contraseña, cortafuegos o firewalls, antivirus y antispam fundamentalmente) **están ampliamente implantadas, mientras que otras más avanzadas** (por ejemplo, IDS, cifrado o VPN) **tienen un nivel de implantación bajo.**

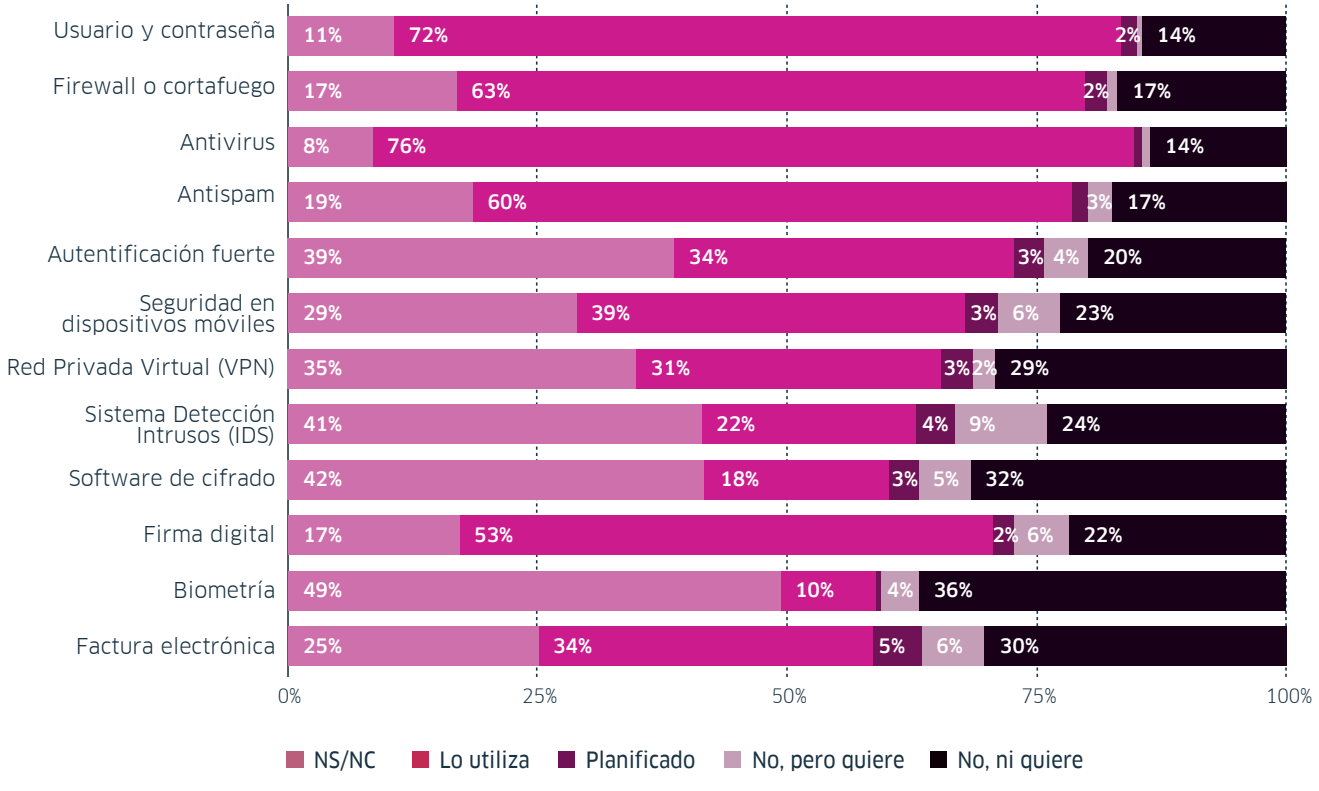
Un porcentaje significativo de empresas ha manifestado que usan, tienen planificado o quisieran implantar soluciones de firma digital (más de un 60%) y factura electrónica (cerca de un 45%).

Cabe destacar en este punto que, aunque las tecnologías de protección contra código malicioso tienen un elevado nivel de implantación, **más de un 30% de las organizaciones participantes en el estudio han sufrido incidentes relacionados con virus, spyware, etc.** Esto hace pensar que las soluciones, o la forma en la que están implantadas, no están siendo todo lo eficaces que sería deseable.

Es reseñable que casi un 39% de las organizaciones encuestadas utilizan actualmente sistemas de seguridad en dispositivos móviles, y aproximadamente otro 10% o tiene planificado instalarlos o le gustaría contar con ellos. Esto da una idea de la relevancia que está tomando el uso de dispositivos móviles en las organizaciones de la región.

Por último, es significativo el elevado porcentaje (por encima del 30%) de respuestas *No Sabe / No Contesta* para elementos de seguridad como autenticación fuerte, VPN, IDS, cifrado o biometría.

Indique si su organización utiliza actualmente alguno de los siguientes elementos



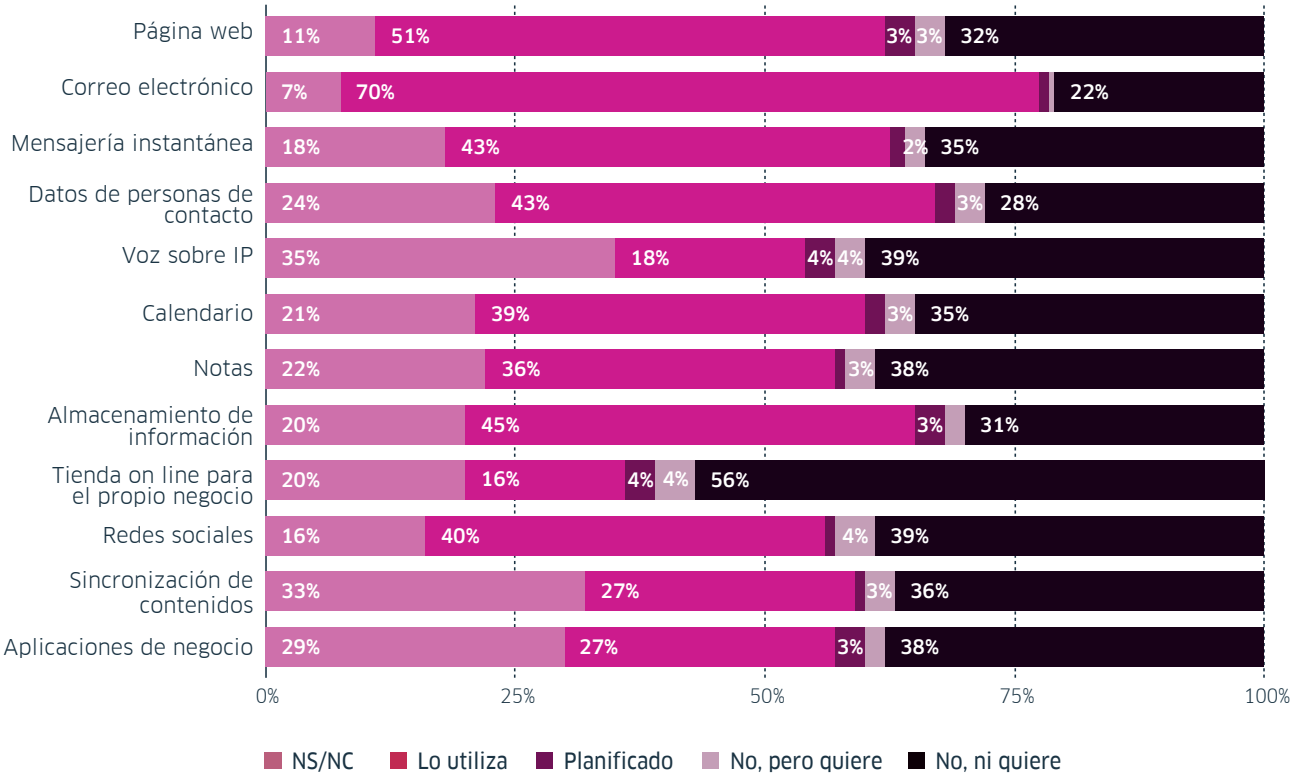
Uso de servicios a través de internet

El uso de servicios a través de Internet está ampliamente difundido.

Además de los servicios más evidentes como el correo electrónico o la página web, también hay un porcentaje significativo de organizaciones (más del 25%) que utilizan otros servicios como mensajería instantánea, contactos, calendario, notas, almacenamiento de información, redes sociales, sincronización de contenidos y aplicaciones de negocio.

En este apartado queremos destacar los bajos porcentajes de respuestas obtenidos para organizaciones que tienen planificado o quieren usar estos servicios a través de Internet. Las respuestas se concentran básicamente en *No Sabe / No Contesta*, Lo Utiliza o No, ni Quiere; es decir, **hay una fuerte polarización entre las organizaciones que ya utilizan estos servicios, y las que no quieren utilizarlos.**

Indique si su organización utiliza actualmente alguno de los siguientes servicios a través de Internet

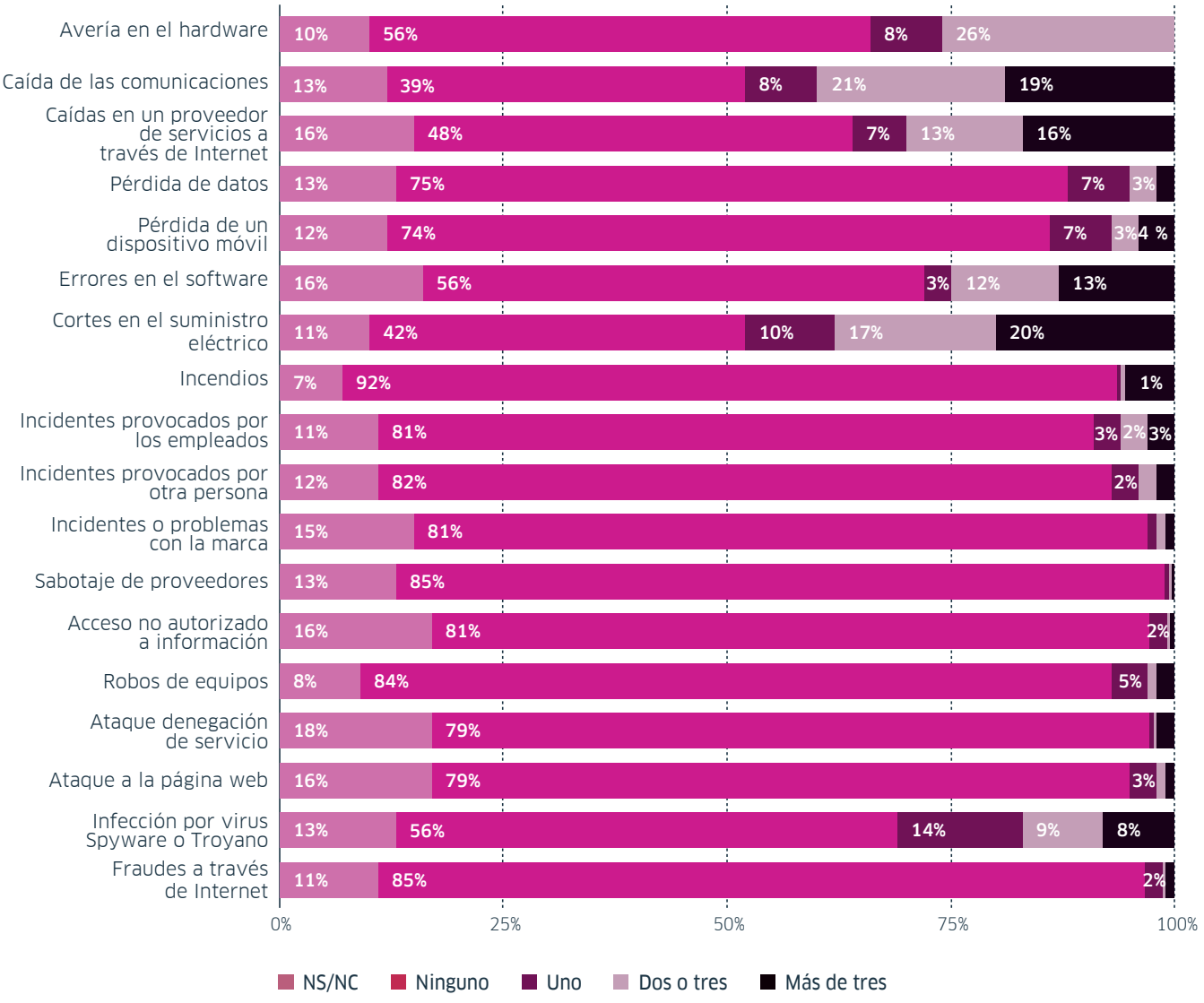


Incidentes

En este apartado cabe destacar que **casi el 50% de las organizaciones** que han participado en el estudio **han tenido cortes en los servicios de comunicaciones y de suministro eléctrico.** Son los dos tipos de incidentes más frecuentes en el estudio.

Alrededor de un 30% de las organizaciones también han sufrido incidentes debidos a averías de hardware, errores de software, infección por código malicioso o caídas del proveedor de servicios de Internet.

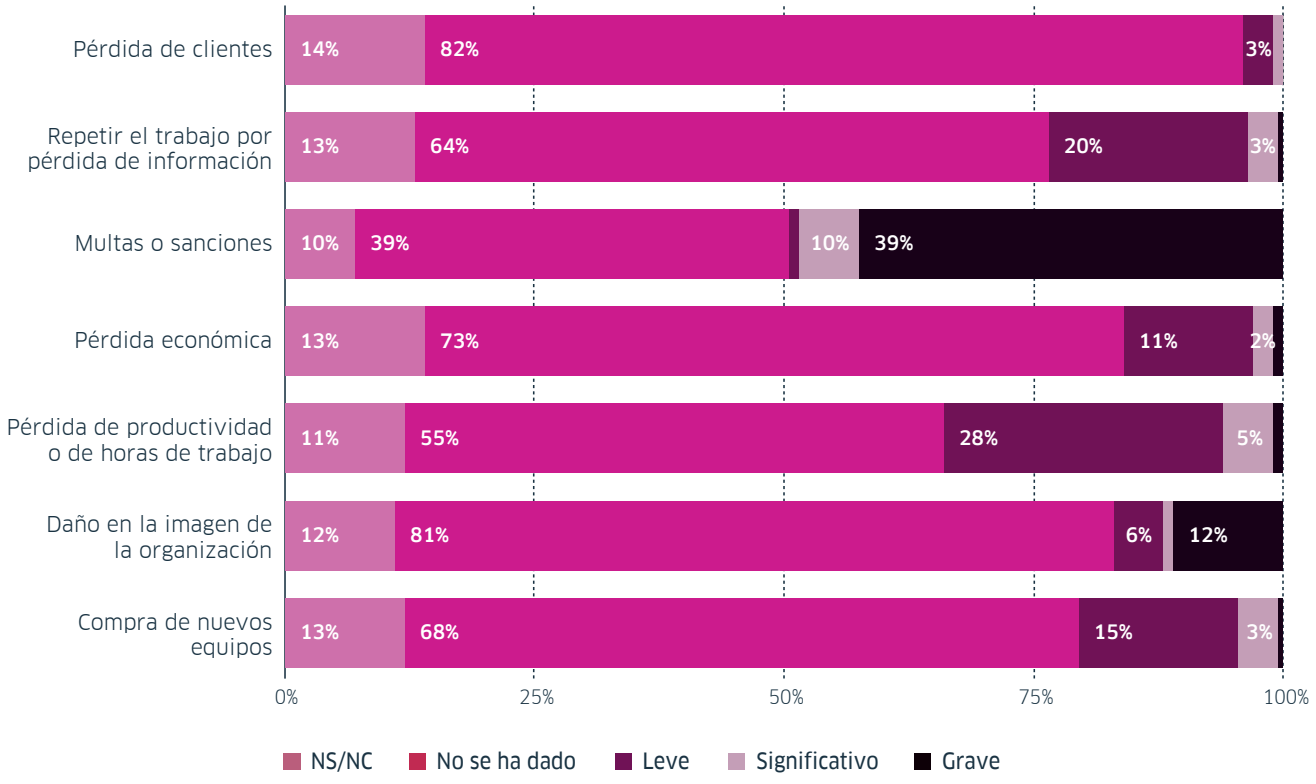
¿Cuántos incidentes de cada uno de los tipos siguientes ha sufrido en los últimos 12 meses?



En lo que respecta **al impacto de estos incidentes, las consecuencias más graves se dan cómo multas o sanciones,** o bien como daño a la imagen de la organización.

Además de los anteriores, también se consideran consecuencias significativas los incidentes relacionados 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, o la compra de nuevos equipos informáticos.

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

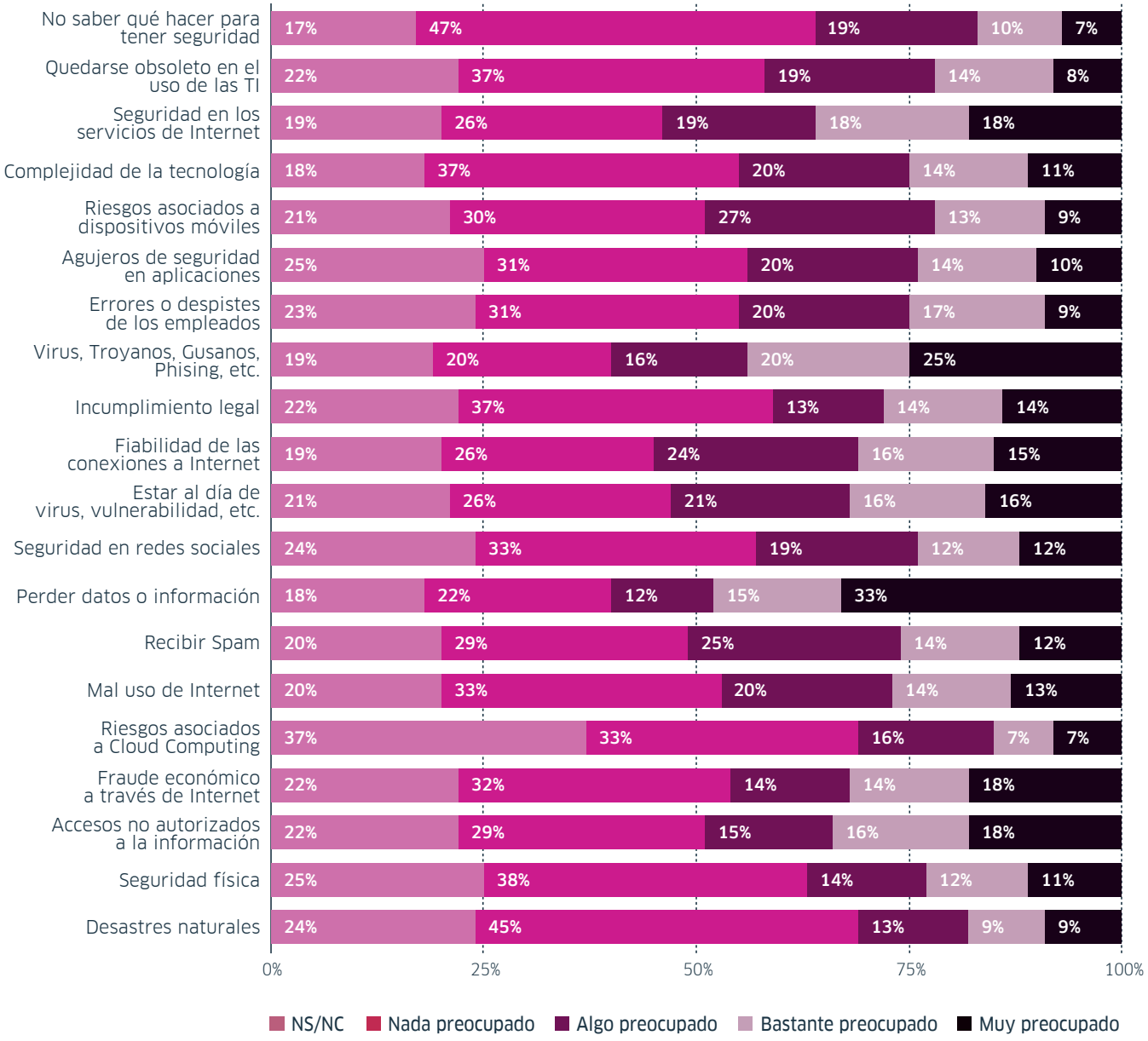


Preocupaciones en materia de seguridad

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

Aunque estos aspectos destacan sobre el resto, el nivel de preocupación es significativo para todos los elementos que se han incluido en la consulta, siendo **los desastres naturales y los riesgos asociados al Cloud Computing lo que menos preocupa** a los participantes en el estudio.

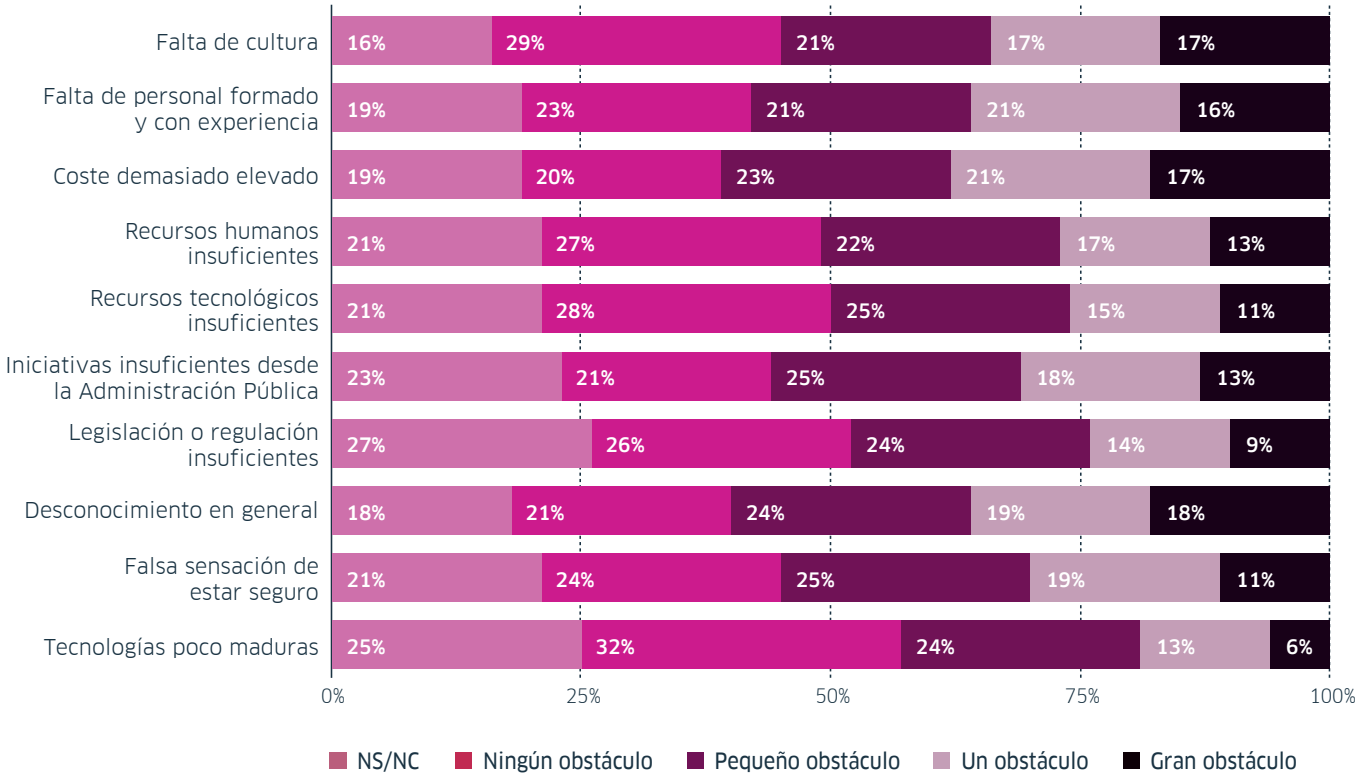
Valore cual es su grado de preocupacion con respecto a cada una de las siguientes circunstancias



Obstáculos para el desarrollo de la seguridad

De forma clara, los encuestados consideran que los mayores obstáculos para el desarrollo de la seguridad son **desconocimiento en general seguido de la falta de cultura, elevado coste de la seguridad además de una carencia de personal formado con experiencia.**

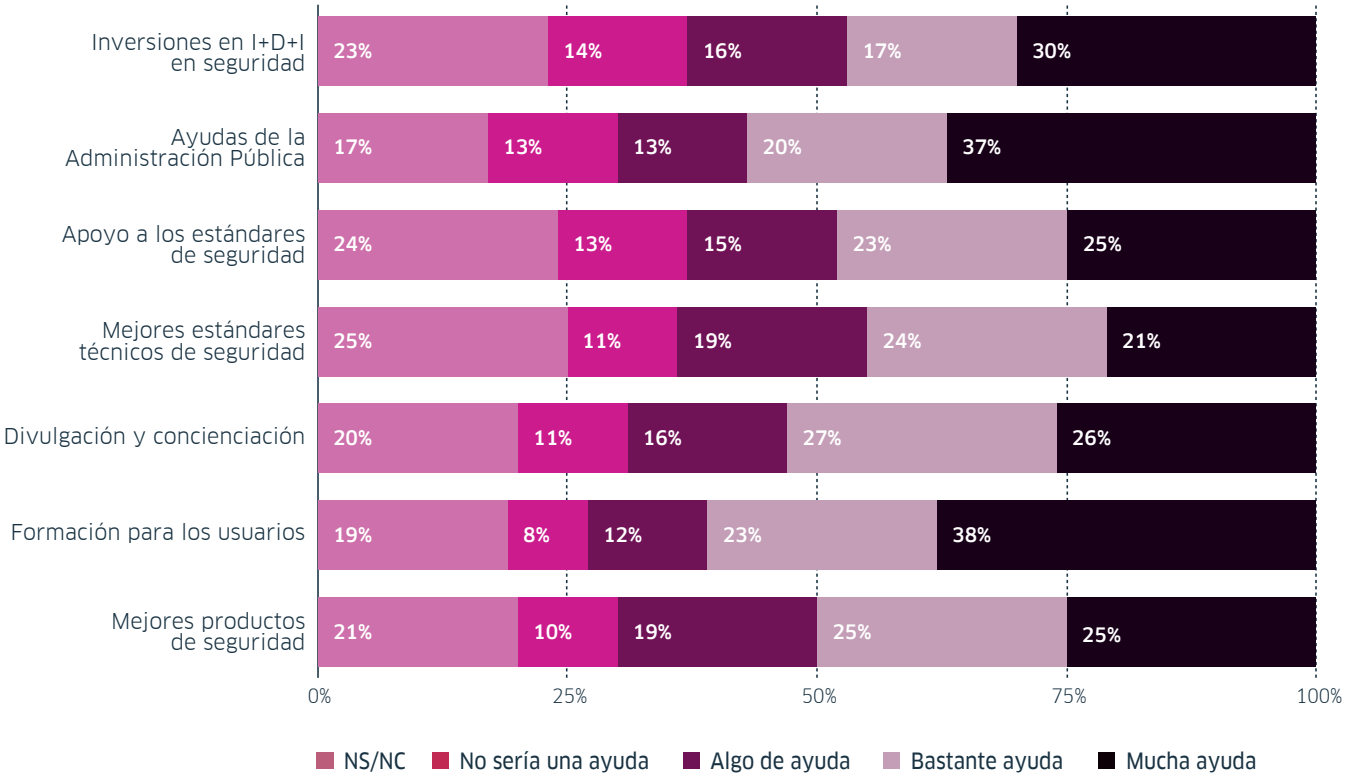
Valore la importancia de los siguientes obstáculos para disponer de un buen nivel de seguridad



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**, seguido de ayudas de la Administración Pública. Se destaca el alto porcentaje en divulgación y cocienciación.

Valore en que medida ayudarían a mejorar la seguridad cada una de las siguientes iniciativas



Conclusiones desde el Think-TIC

En una vista general de los resultados obtenidos, se observa que es necesario continuar trabajando de forma decidida en la formación en materia de seguridad informática e ir profundizando en su conocimiento, fundamentalmente dos aspectos corroboran dicha afirmación. En primer lugar, se sigue apreciando en la encuesta del 2016 que aproximadamente dos de cada tres organizaciones utilizan elementos de seguridad básicos como usuario y contraseña, cortafuegos, antivirus y antispam. De estas empresas, solo la mitad dicen disponer de sistemas con tecnologías un poco más avanzadas como pueden ser la autenticación fuerte o la seguridad en dispositivos móviles. Dichos valores se corresponden con las tendencias obtenidas en la encuesta de 2014.

Un segundo aspecto muy significativo es que más de un 30% de las organizaciones participantes han sufrido incidentes relacionados con infecciones por código malicioso (virus, spyware, etc.) y la mitad de ellas dicen haberlos sufrido varias veces. Este dato puede deberse a que solo el 76,3% de los entrevistados manifestaron que utilizaban una herramienta antivirus; a pesar de mejorar este dato respecto al obtenido en 2014, todavía hay un porcentaje elevado de entidades que no utilizan estas protecciones.

Por otro lado, cabe destacar que más de la mitad de las organizaciones (53,4%) están incorporando poco a poco la firma digital, y más de un tercio (34%), la factura electrónica como elementos de seguridad informática avanzados. Por el contrario, sorprende que exista un incremento respecto a 2014 de los encuestados que han manifestado que ni las usan ni las quieren usar, por lo que habrá que redoblar los esfuerzos para cambiar una resistencia al uso de las mismas con formación y divulgación.

Al igual que en el año 2014, en lo que se refiere a los incidentes, las empresas que han participado en el estudio de 2016 han sufrido incidentes de distinta naturaleza. Destacan por su frecuencia los debidos a interrupciones de suministro eléctrico, de comunicaciones y de servicios de Internet.

También han manifestado su preocupación por los aspectos que pueden comprometer la seguridad y en especial a las posibles pérdidas de datos o información, ratificando una inquietud de la encuesta de 2014.

En definitiva, las organizaciones que participaron en el estudio de 2016 siguen priorizando la formación en seguridad informática como herramienta para mejorar la situación actual. Estas conclusiones son similares a las obtenidas en el estudio del año 2014, por lo que **se considera necesario continuar trabajando desde el Think-TIC en las líneas de divulgación, concienciación y formación en materia de seguridad informática.**

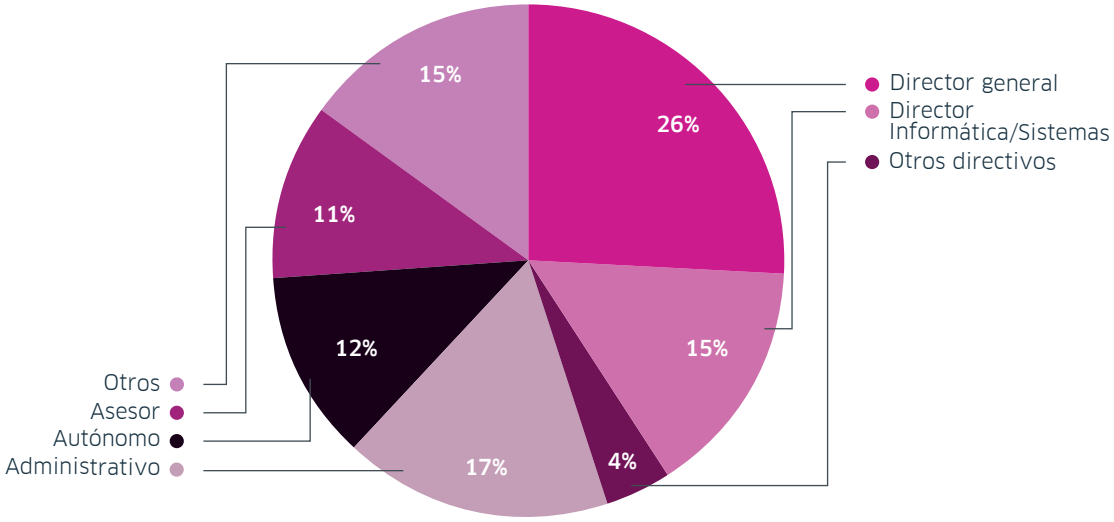
Datos generales de las organizaciones

Cargo de la persona que responde el test

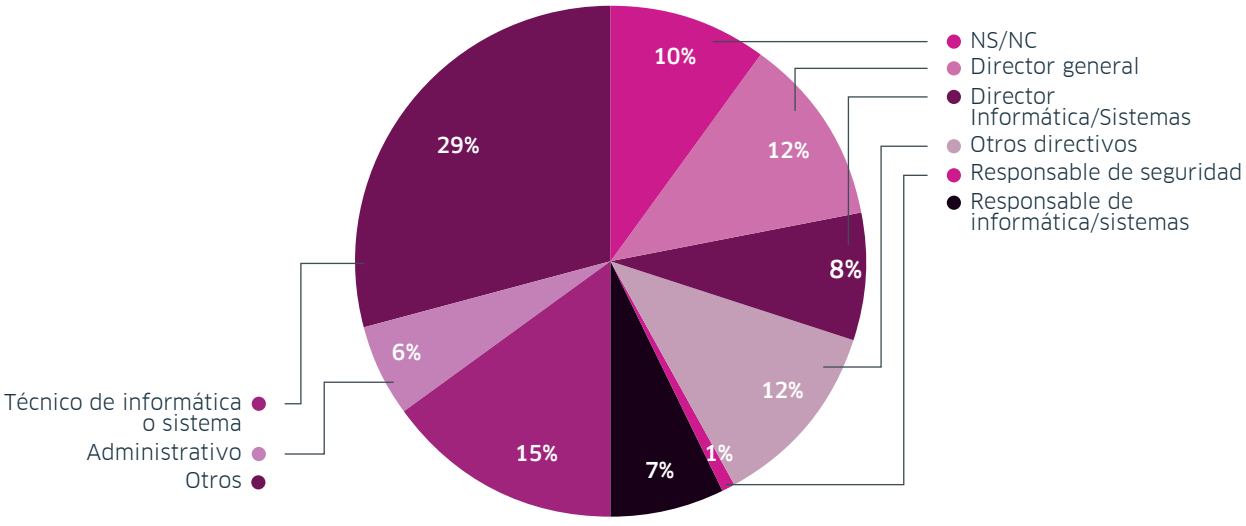
En el estudio realizado en el año 2016, las opciones contempladas para los cargos de las personas que respondían al test incluían algunas diferencias con respecto al estudio del año 2014. Con esta modificación se buscaba alinear las opciones disponibles para contestar esta pregunta a la realidad de las empresas de la región.

Cabe destacar que **un 45% de los encuestados pertenecen al equipo directivo** de las organizaciones.

Cargo de persona que responde al test



Cargo de persona que responde al test (Datos del estudio de 2014)

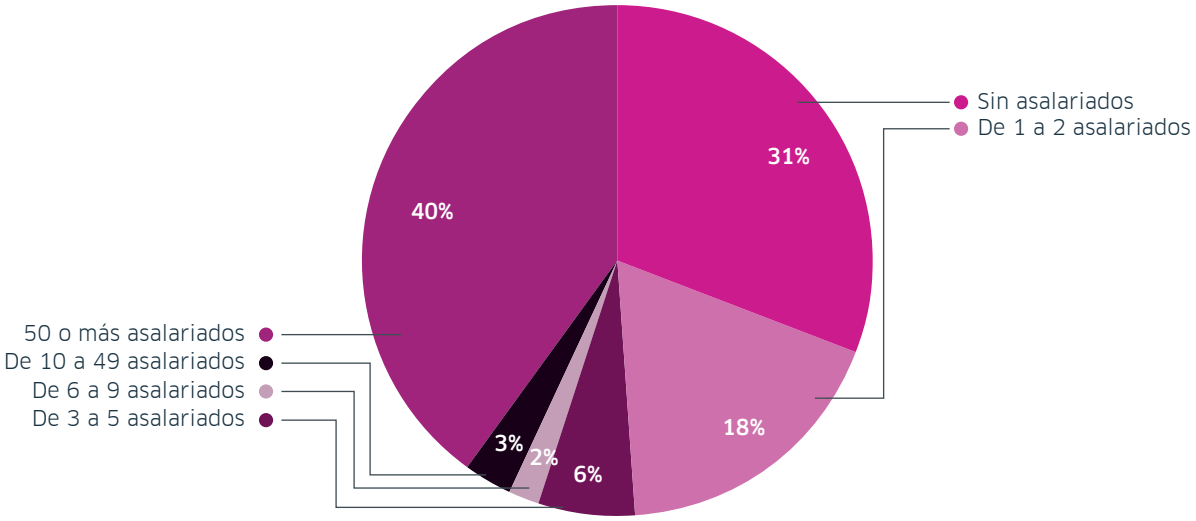


Número de empleados

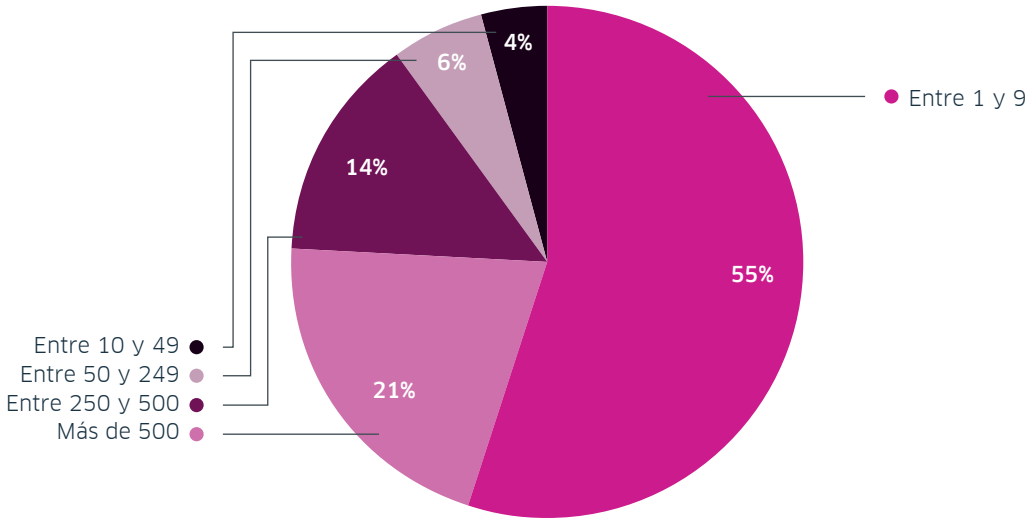
La distribución de las organizaciones en función del número de empleados en el estudio del año 2016, también se ha modificado con respecto al estudio del año 2014. El objetivo de esta modificación era disponer de una **mayor atomización** en las organizaciones de entre 1 y 10 empleados.

En este sentido, **el 57% de las organizaciones participantes tienen menos de 10 empleados.**

Estado de asalariados



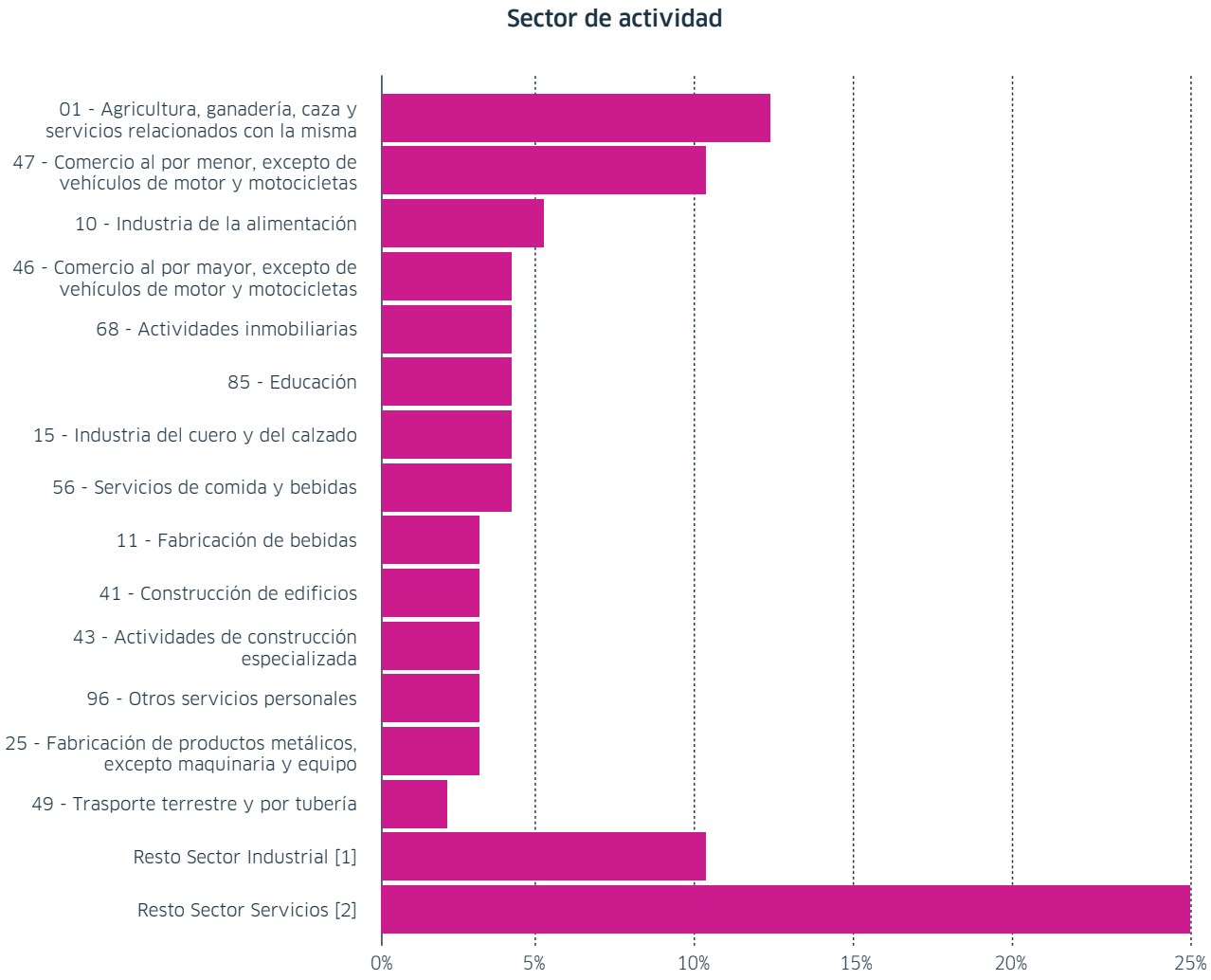
Número de empleados (Datos del estudio 2014)



Sector de actividad

En cuanto al sector de actividad de las empresas que respondieron al cuestionario, también se ha modificado la distribución de las organizaciones en el estudio del año 2016 con respecto al estudio del año 2014.

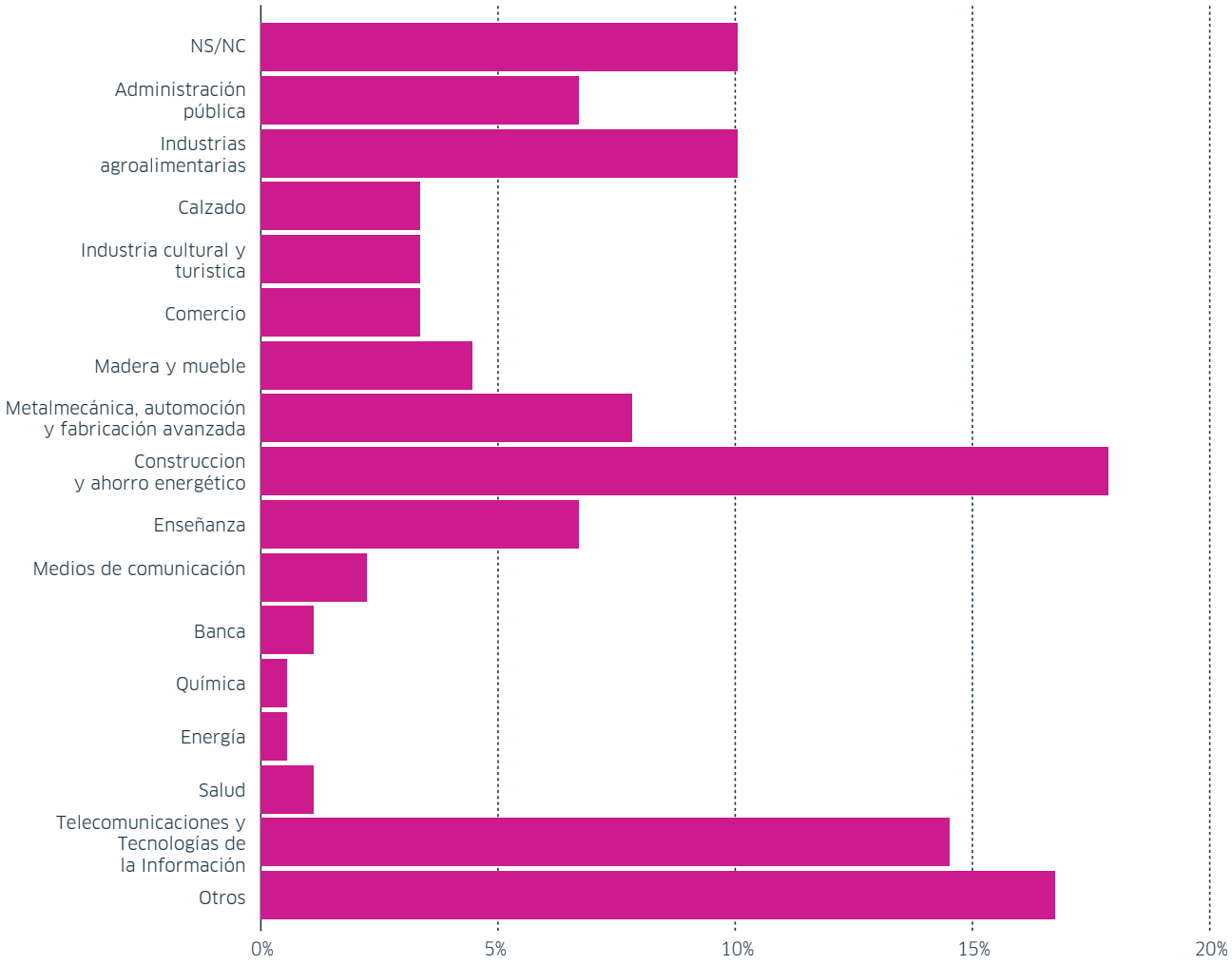
Al igual que en el estudio realizado en el año 2014, las organizaciones están bastante distribuidas por el sector de actividad buscando una atomización y alcance más detallado.



(1): Comprende las Divisiones: 12, 13, 14 16, 17, 18, 22, 23, 28, 29, 31, 33, 35 y 38

(2): Comprende las Divisiones: 45, 55, 58, 61, 64, 65, 66, 69, 70, 71, 72, 73, 74, 75, 78, 80, 81, 82, 86, 87, 88, 92, 93, 94, 95 y 97

Sector de actividad (Datos del estudio de 2014)

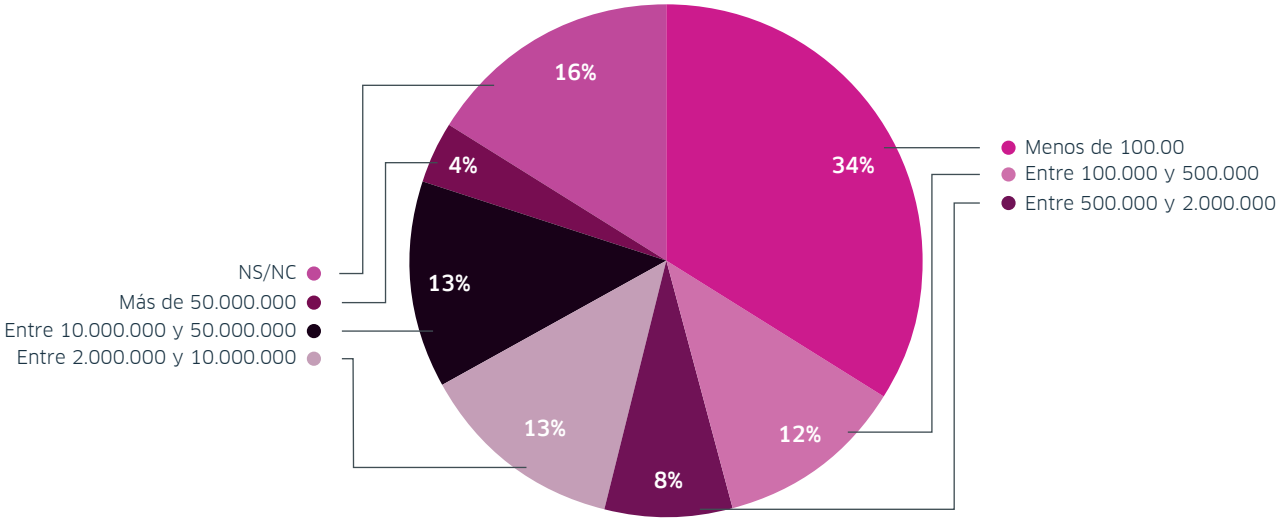


Facturación en millones de euros al año

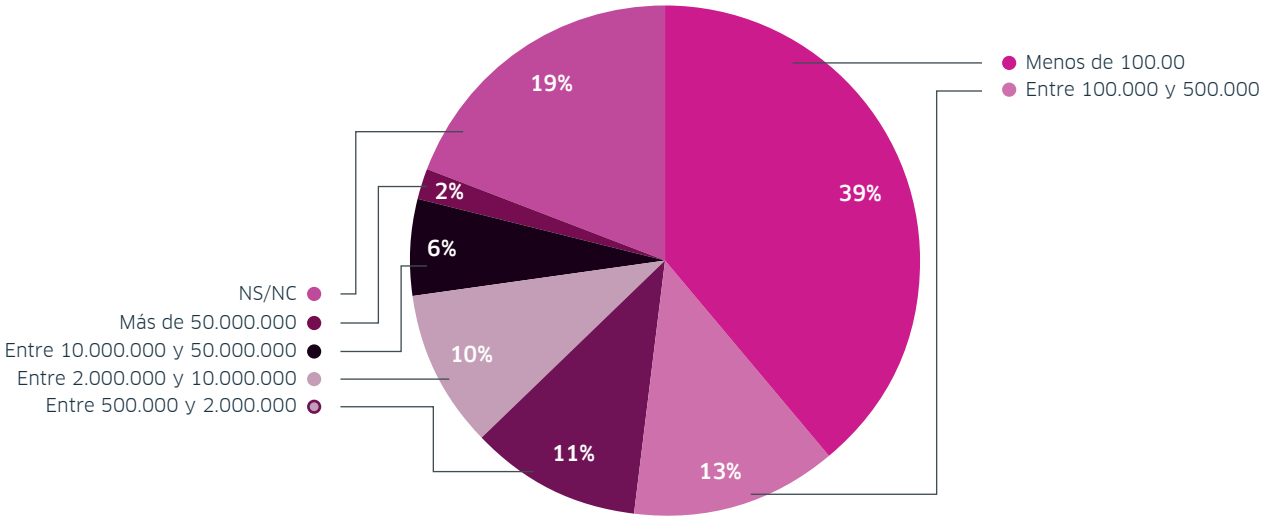
La distribución de las organizaciones en función de sus datos de facturación anual ha mostrado algunas diferencias con respecto al estudio realizado en el año 2014.

Se puede apreciar que, en la distribución de las organizaciones participantes en el estudio de 2016, los porcentajes correspondientes a organizaciones que facturan menos de 100.000 € al año son menores que en 2014.

Facturación en euros al año



Facturación en euros al año (Datos del estudio de 2014)



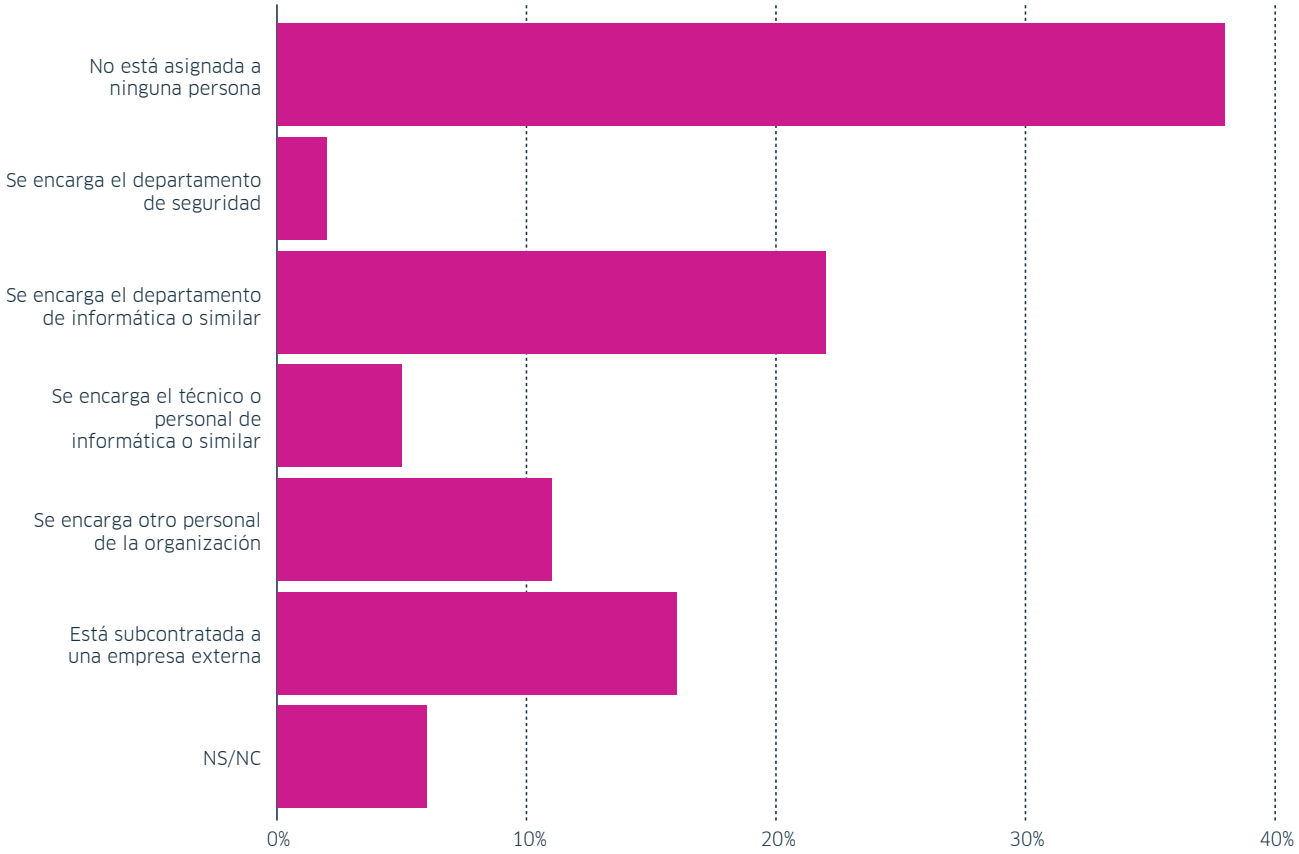
La gestión de la seguridad

Un indicador del grado de madurez de la seguridad es la asignación de recursos dentro de la organización a la función de seguridad, o al menos el reconocimiento de que esta función tiene un papel importante.

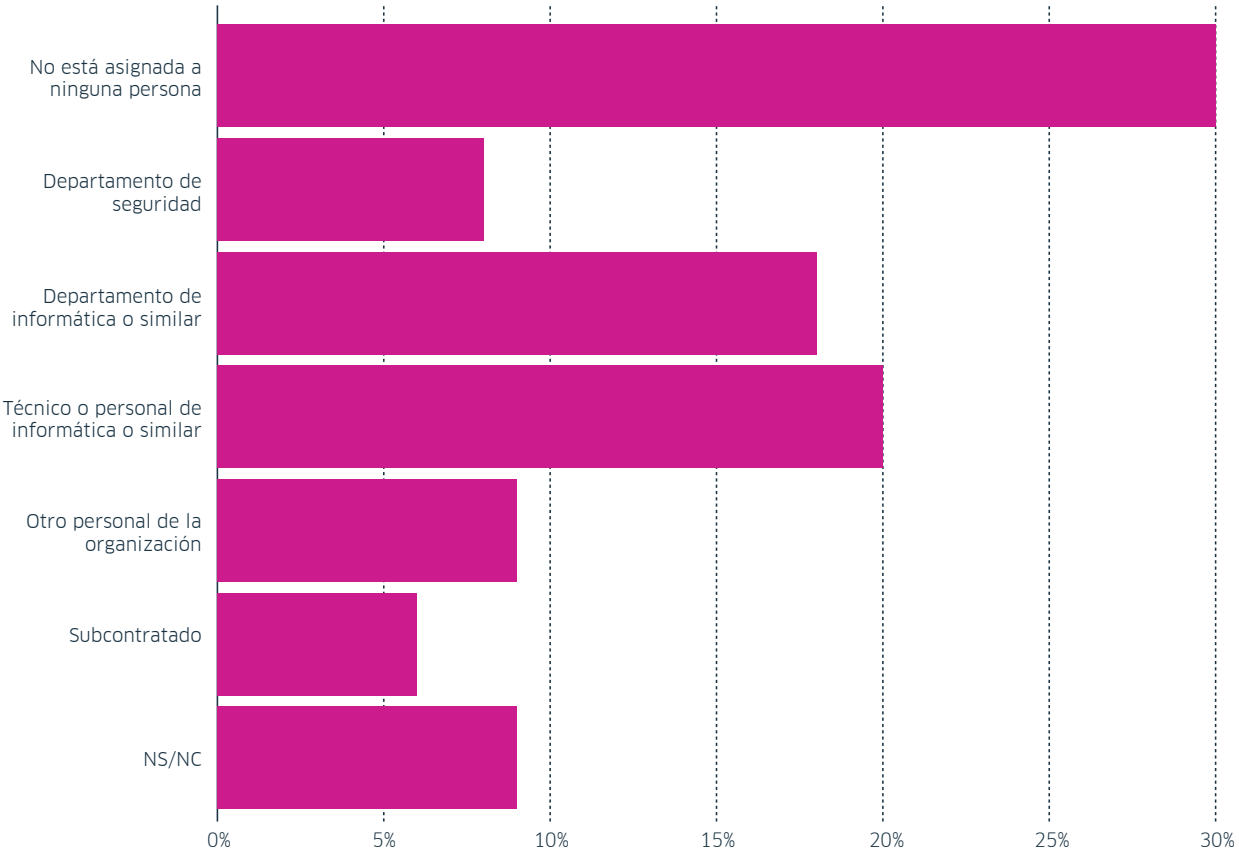
Los resultados obtenidos para la asignación de la función de gestión de la seguridad quedó como sigue:

- **En un 38% de los casos, la gestión de la seguridad no está asignada.** El porcentaje se puede considerar elevado, especialmente teniendo en cuenta que un 40% de los encuestados pertenecen a organizaciones con más de 50 empleados, y que un 30% facturan más de 2 millones de € al año.
- Solo el 2% de los encuestados manifiestan que sus organizaciones tienen asignada la seguridad a un departamento o área concreta de seguridad encargada de su gestión. Contrasta con el 8% resultante en el estudio de 2014.
- Otro 27% manifestó que la gestión de la seguridad está asignada al departamento o al personal de informática.
- Es destacable que en un 16% de los casos, las organizaciones han optado por subcontratar la gestión de la seguridad a empresas externas.

Gestión de la seguridad



Gestión de la seguridad (Datos del estudio de 2014)



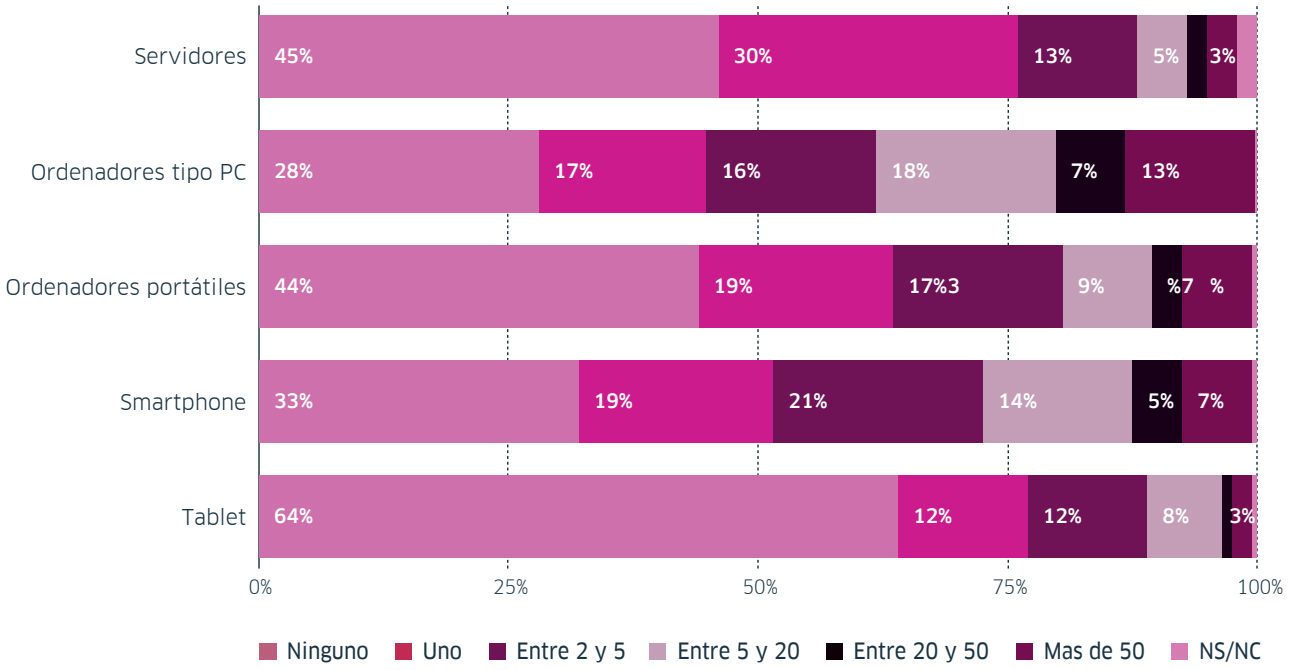
Número de equipos utilizados en la organización

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

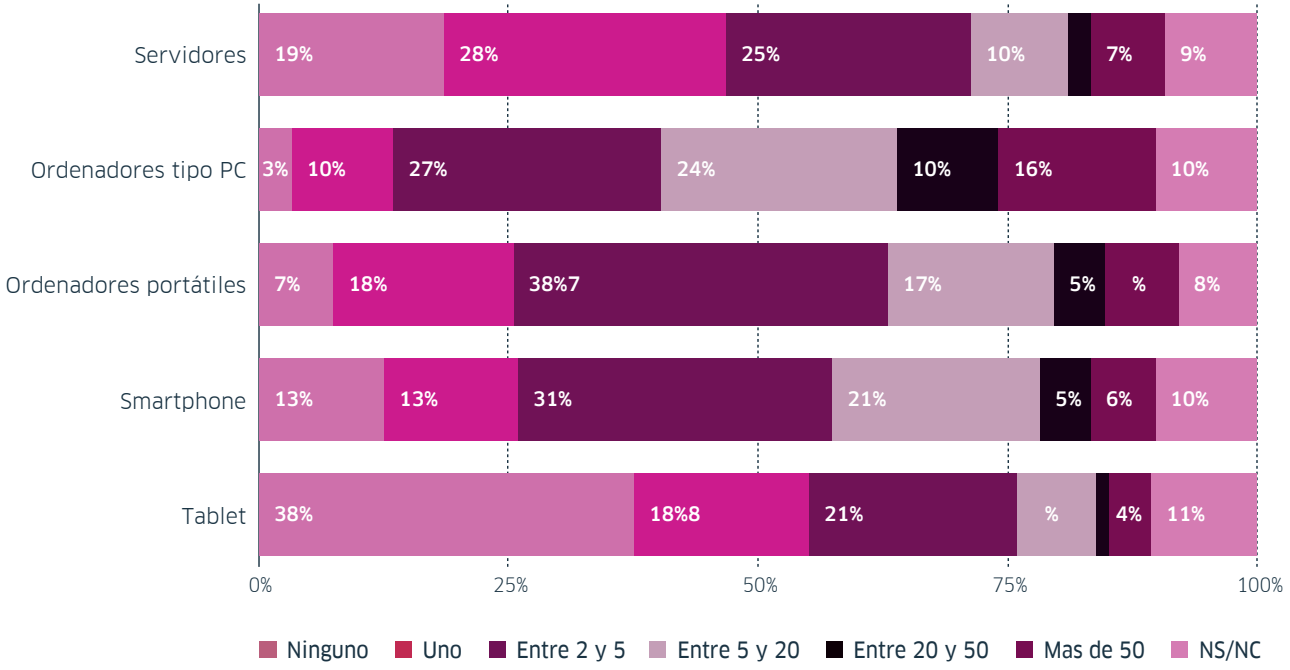
Así, el uso de servidores, ordenadores de sobremesa o PC, portátiles, teléfonos inteligentes o Smartphone, en las organizaciones que han participado en el estudio nos indica que se utilizan por más del 50% de las mismas.

Debido a la modificación del espacio muestral donde se han abierto sectores menos tecnologicos y una mayor atomización, la diferencia es significativa con respecto a los resultados del estudio de 2014, donde más del 80% de las organizaciones encuestadas los utilizaban. Por ejemplo, el 26% de los entrevistados en este estudio de 2016 indican que no tienen ningún ordenador tipo PC en su organización.

Indique el número de equipo informáticos de cada tipo que utilizan en su organización



Indique el número de equipo informáticos de cada tipo que utilizan en su organización (Datos del estudio de 2014)



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 la mitad 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.** Mientras que 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, en un ordenador portátil estas cuestiones de seguridad más obvias pueden resultar más complejas de lo que sería deseable.
  - **El 56% de las respuestas obtenidas indican que utilizan este tipo de ordenadores en el ámbito profesional.**
- **Teléfonos inteligentes o Smartphone**
  - Los teléfonos inteligentes o Smartphone se han popularizado en los últimos años, de forma que actualmente casi cualquier persona utiliza uno de estos equipos.
  - De las respuestas obtenidas se desprende que en **casi las dos terceras partes de las organizaciones entrevistadas** utilizan este tipo de teléfonos en el ámbito profesional.
  - Se trata de equipos desde los que generalmente se usa al menos el correo electrónico, agenda, contactos y servicios de mensajes o chats. Todas estas funcionalidades se suelen utilizar tanto a nivel profesional, como particular en el mismo terminal. Estos aspectos lo convierten en un sistema con unos ciertos requerimientos de seguridad.
  - 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 que 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 uso 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 equipos con respecto tanto al uso combinado profesional y particular, 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 esta tan extendido como el caso de los ordenadores portátiles y los Smartphone.**

Elementos de seguridad de los que dispone

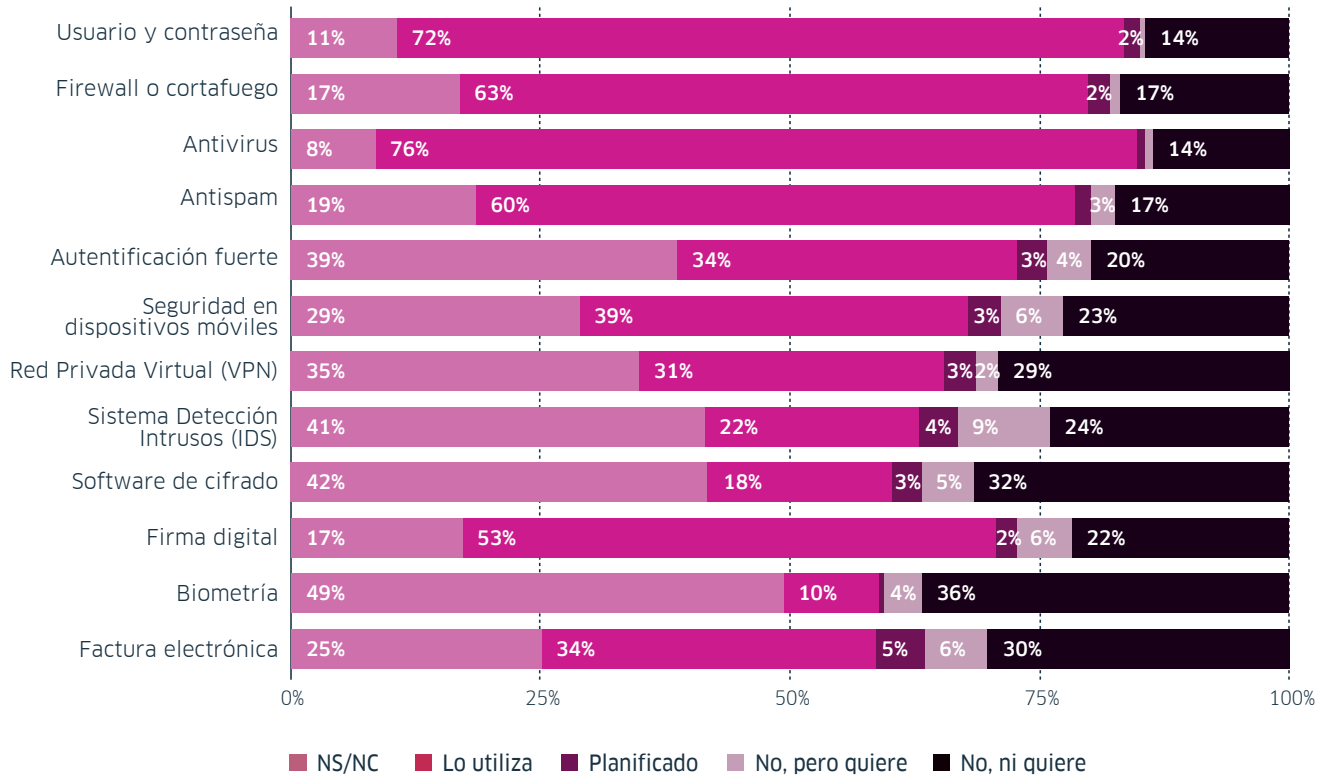
Este apartado del estudio nos da una idea bastante clara sobre el grado de implantación que tienen las tecnologías de seguridad más comunes en las organizaciones que han participado.

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.

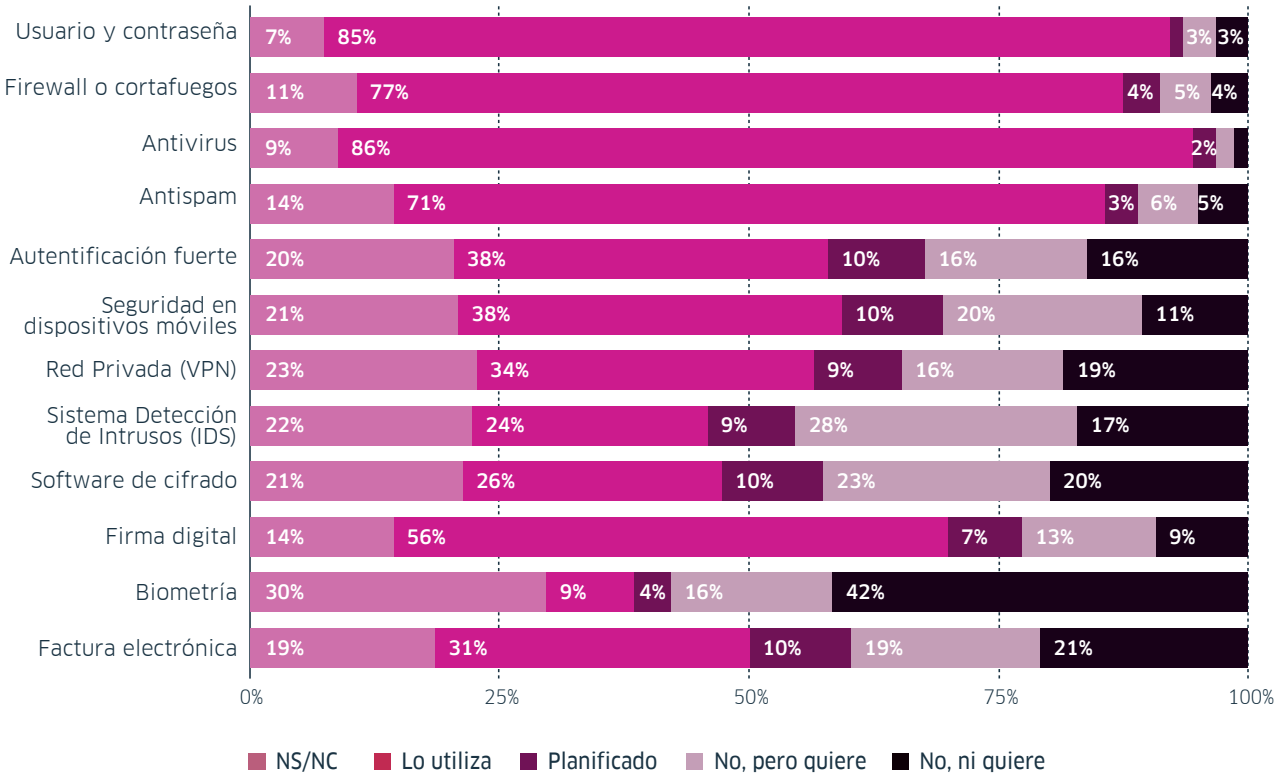
Cuando se trata de tecnologías un poco más avanzadas, el porcentaje de utilización disminuye considerablemente. Cabe destacar el número de organizaciones que no utilizan, pero que les gustaría hacerlo, tecnologías como la factura electrónica, sistemas de detección de intrusos, herramientas de cifrado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

También se puede apreciar como 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 elevado.

Indique si su organización utiliza actualmente alguno de los siguientes elementos



Indique si su organización utiliza actualmente alguno de los siguientes elementos (Datos del estudio de 2014)



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 75% de organizaciones utilicen usuario y contraseña.
  - Sin embargo, el hecho de **que un 14,4% de encuestados que ni lo usan, ni quieren usarlo, da una idea de la dimensión del problema cultural y de concienciación existente en materia de seguridad informática.**
- **Cortafuegos o firewall**
  - **Un 20%** de las organizaciones participantes en el estudio **no cuentan con una herramienta de protección elemental** frente a intentos de acceso no autorizado desde el exterior.
- **Antivirus**
  - Es importante resaltar nuevamente que, aunque más del **75%** de las organizaciones **disponen de soluciones antivirus**, los entrevistados han indicado en el apartado de incidentes que el número de incidentes relacionados con este tipo de amenazas es elevado.
  - En las respuestas obtenidas este año, **sorprende que un 13,6% de los encuestados hayan manifestado que ni lo usan ni quieren usarlo.**
- **Autenticación fuerte**
  - 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 al usuario y contraseña ("something that you have" o "algo que tienes") como puede ser un SMS enviado al teléfono móvil, un código compartido en una tarjeta de coordenadas, una llave USB, la huella digital, identificación facial, y un largo etc.

- Así, **frente al** dato del **14,4%** de organizaciones que **no utilizan ni quieren utilizar usuario y contraseña,** resulta muy interesante que **el 34%** de las organizaciones entrevistadas **ya estén utilizando algún método de autenticación fuerte.**

- **Seguridad en dispositivos móviles**
  - Los Smartphone incorporan algunas características de seguridad dentro del propio sistema, como el bloqueo con contraseña, la copia de seguridad, el borrado remoto, antivirus, etc.
  - Aunque el 67% de los encuestados indican que utilizan Smartphone, **solo el 39% han respondido que usan medidas de seguridad en dispositivos móviles.**
- **Red privada virtual o VPN**
  - Las comunicaciones a través de redes públicas (fundamentalmente Internet) no garantizan por sí mismas la confidencialidad de la información que se comparte.
  - Para securizar la información que se transmite es necesario cifrarla y esto se puede hacer utilizando páginas web HTTPS, o estableciendo la conexión a través de Redes Privadas Virtuales o VPN.
  - El que solo un 30% de las organizaciones utilice VPN no tiene porqué ser un mal dato. El que esté indicado o no el uso de VPN depende mucho de cómo utiliza cada organización sus conexiones a través de redes publicas.
- **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.
  - En este caso, **un 21,5%** de los encuestados **cuentan con sistemas de detección de intrusos**, y resulta interesante que un 3,8% tenga planificado implantarlo y otro 9,2% quiera utilizarlo.
- **Software de cifrado**
  - El cifrado es necesario para garantizar la confidencialidad de la información. Tanto de la información almacenada (en los servidores, PCs, portátiles, Dropbox, OneDrive, etc.) como de la enviada (por ejemplo, por correo electrónico).
  - **Las herramientas de cifrado siguen teniendo una implantación muy baja, sólo el 18,5%** de los encuestados han indicado que **las utilizan.**
- **Firma digital**
  - La firma digital es una tecnología que permite firmar electrónicamente los documentos, con la misma validez jurídica que tiene la firma manuscrita.
  - Probablemente el esfuerzo realizado desde las Administraciones Públicas para generalizar el uso de la firma digital ha ayudado a que **el 53,4%** de los encuestados **ya dispongan de esta herramienta.**

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.

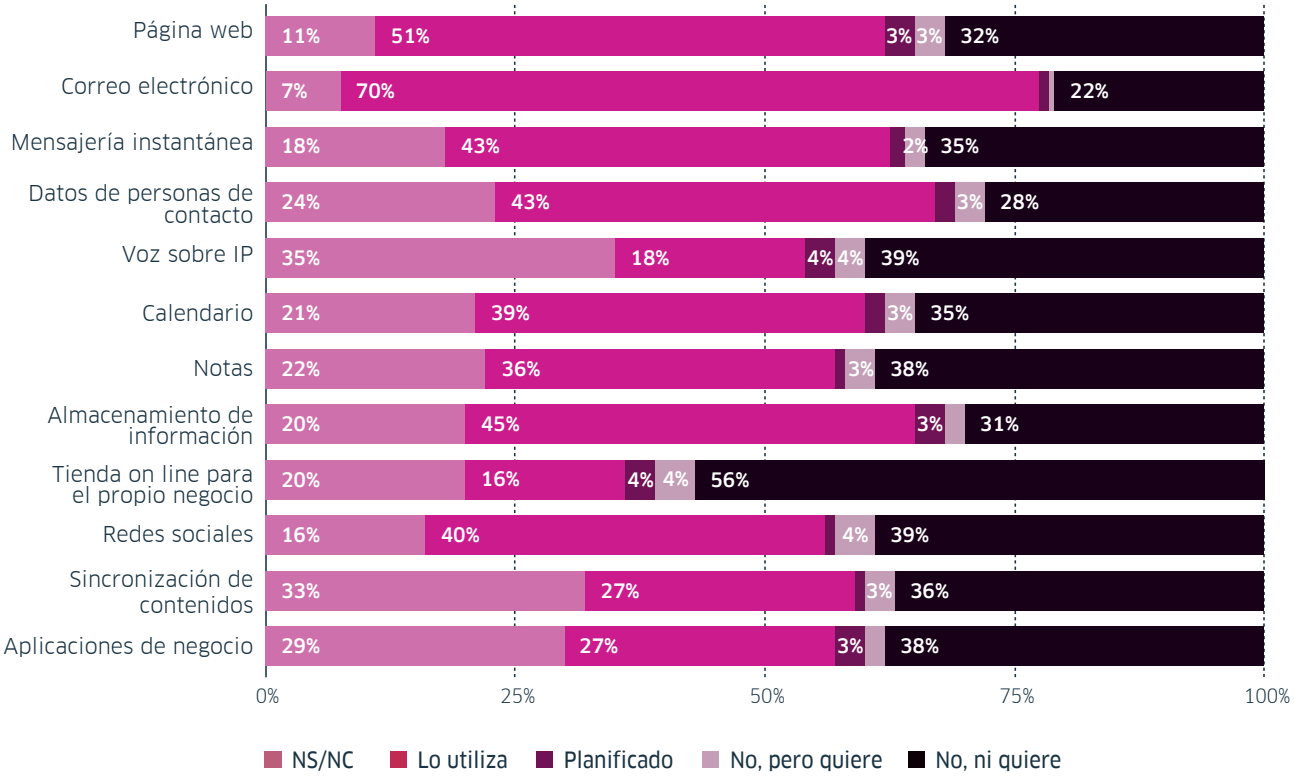
En este caso, **un porcentaje elevado** de las organizaciones participantes **utilizan en modo Cloud servicios como página web, correo electrónico, calendario, notas, o almacenamiento de información en Cloud.**

Probablemente hay una estrecha relación entre el uso de estos servicios y la progresiva implantación de Smartphones como herramienta de trabajo. Esto permite tener sincronizados los datos entre el PC, el Portátil, el Smartphone o la Tablet.

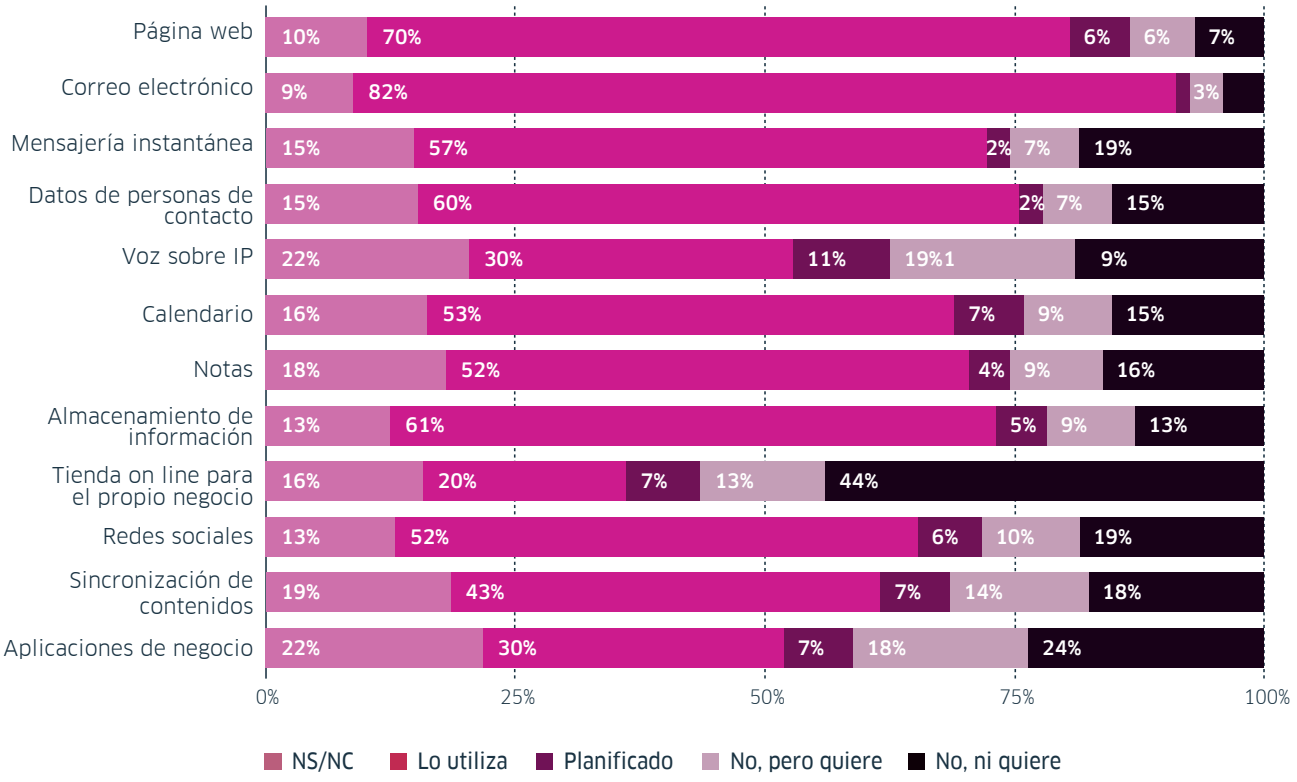
En cualquier caso, queda de manifiesto que más allá de los debates que puedan suscitarse con respecto al uso del Cloud, las organizaciones están haciendo uso de este tipo de servicios.

Una apreciación que no debería pasarse por alto es que en términos generales se aprecia que en el estudio de 2016 con respecto al de 2014 ha habido un aumento significativo de las organizaciones que no utilizan ni quieren utilizar servicios Cloud.

Indique si su organización utiliza actualmente alguno de los siguientes servicios a través de Internet



Indique si su organización utiliza actualmente alguno de los siguientes servicios a través de Internet (Datos del estudio de 2014)



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 telefonía.
  - En cualquier caso, **solo un 18,5%** de los entrevistados **ha contestado que lo utiliza.**
- **Almacenamiento de información**
  - Los servicios de almacenamiento de información en Cloud se están extendiendo rápidamente.
  - Ya un **45%** de los entrevistados manifiestan que **almacenan información en la nube.**
- **Tienda online para el negocio propio**
  - Probablemente este sea uno de los servicios más atractivos para las empresas, ya que les permite posicionar rápidamente su negocio en Internet y ampliar el espectro de clientes mas allá de los límites de un local y de un horario comercial
  - 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, **solo el 15,5%** de los entrevistados **utilizan este servicio**, y lo que podría ser más relevante, el **56% no quiere utilizarlo**

- **Redes sociales**

  - Aunque durante un tiempo se consideraron a las redes sociales como una herramienta orientada al uso particular, en los últimos dos años se ha consolidado su uso a nivel de organización

  - Esto queda de manifiesto por el hecho de que **un 39,5%** de los entrevistados **manifiestan utilizar las redes sociales**.

- **Aplicaciones de negocio**

  - **Las aplicaciones empresariales** para la gestión de recursos humanos, contabilidad, recursos operativos, gestión de clientes, 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 27%** de los entrevistados ya **están utilizando este tipo de servicios en modo Cloud.**

Incidentes

Las buenas prácticas comúnmente aceptadas en materia de gestión de la seguridad de la información **indican que las organizaciones deben realizar un análisis de riesgos formal** con el objeto de disponer de información real sobre los riesgos a los que se enfrentan y su potencial impacto en el desarrollo del negocio. Si no se cuenta con un análisis de riesgos formal, al menos si se debe disponer de información real sobre el número de incidentes que se producen.

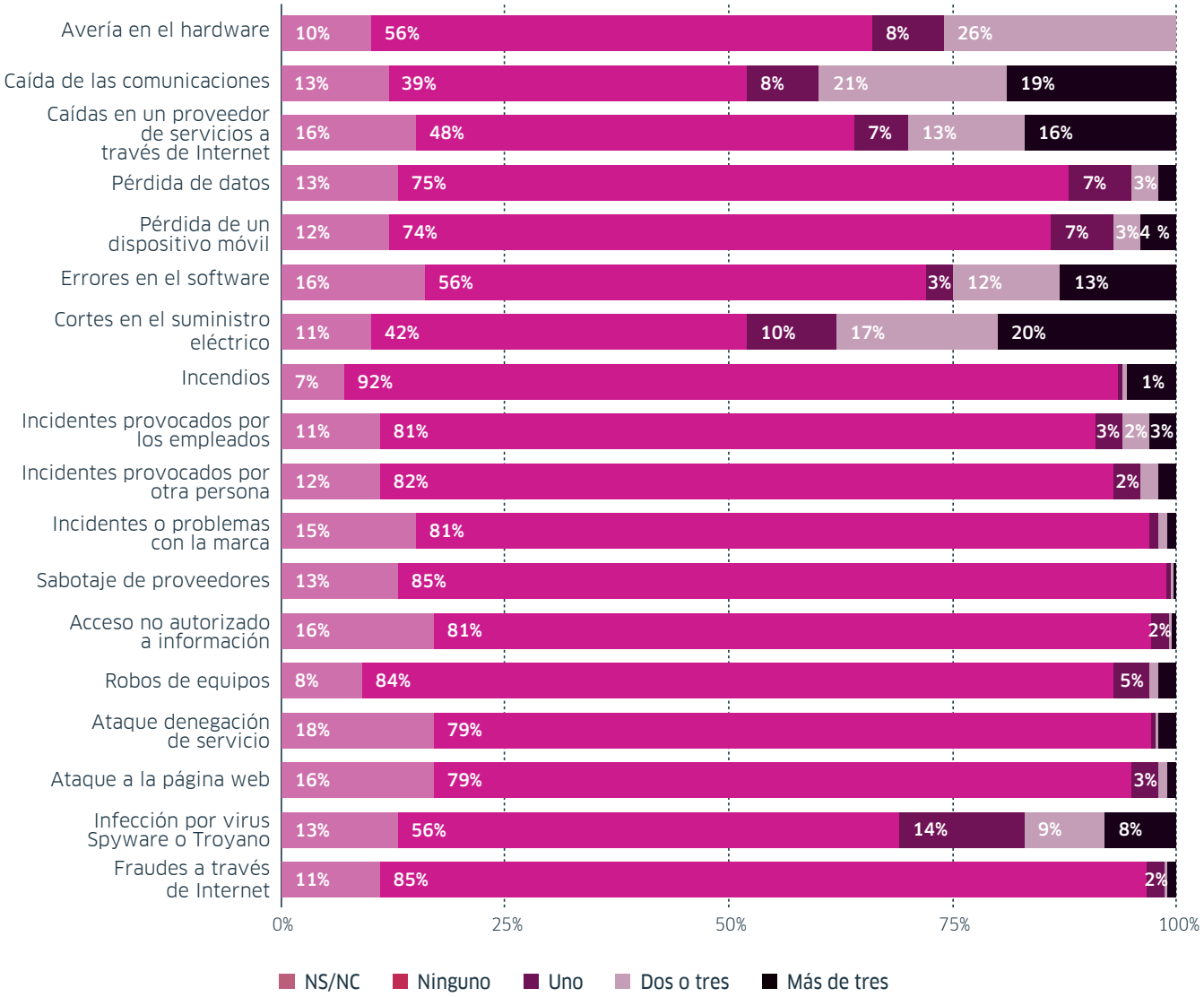
Para disponer de información sobre el número de incidentes que han sufrido las organizaciones, se ha incluido en la encuesta un apartado específico sobre el volumen de incidentes que han sufrido las organizaciones en el último año, y de qué tipo.

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

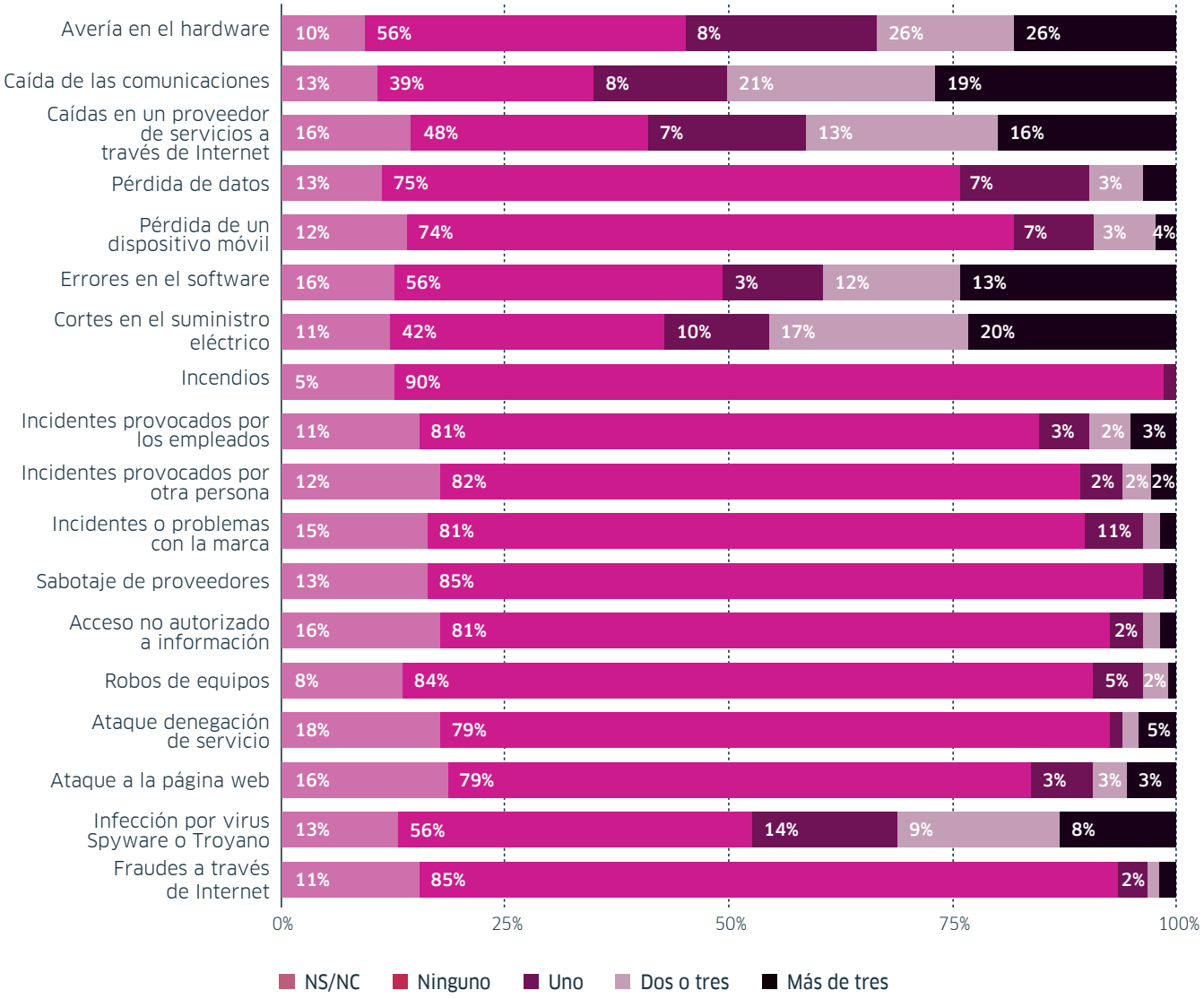
Cabe destacar que en algunos tipos de incidentes (averías en hardware, caídas de comunicaciones, caídas de servicios de Internet, errores en el software, interrupciones del suministro eléctrico o infecciones por virus), más de **una cuarta parte de los entrevistados se han visto afectados.**

Puede parecer una obviedad, pero la conclusión más evidente de este apartado del estudio, es que los incidentes ocurren. Muchas organizaciones piensan que este tipo de incidentes no son frecuentes y que la probabilidad que se den en su organización es muy baja.

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



¿Cuántos incidentes de cada uno de los tipos siguientes ha sufrido en los últimos 12 meses? (Datos del estudio de 2014)



En lo que se refiere a los tipos de incidentes que los entrevistados han manifestado haber sufrido durante los 12 meses anteriores, cabe destacar las siguientes conclusiones:

- **Infecciones por virus, spyware y troyanos**
  - Un **31%** de las organizaciones **ha sufrido infecciones por código malicioso,** y un 16,6% de ellas ha sufrido varios incidentes de este tipo.
  - Es conveniente interpretar este dato junto con la información de que **solo el 76,3%** de los entrevistados **manifestaron que utilizaban una herramienta antivirus.**
- **Caídas en las comunicaciones**
  - El día a día del trabajo tiene actualmente una dependencia importante de la disponibilidad de las comunicaciones (correo electrónico, compras online, aplicaciones en Cloud, etc.).

- En este sentido, las comunicaciones de datos se convierten cada vez mas en un servicio importante para el normal desarrollo de la actividad profesional.

- En muchas ocasiones, las organizaciones contratan los servicios de comunicaciones poniendo más la atención en el coste (típicamente se trata de líneas ADSL) y en el ancho de banda que en la estabilidad y calidad del servicio.

- **El hecho de que haya tantas caídas de las líneas de comunicaciones pone de manifiesto la necesidad de incidir en la calidad del servicio.**

- **Cortes en el suministro eléctrico**

  - Mas 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**

  - **El 12%** de las personas encuestadas **ha sufrido pérdida de datos.**

  - **Las copias de seguridad son la medida preventiva más extendida para evitar perdidas de datos,** pero en muchas ocasiones no se le presta la debida atención.

  - Es frecuente que no se haga 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.), o que no se verifique si las copias se han realizado correctamente, o si se pueden restaurar los archivos de la copia en un ordenador diferente.

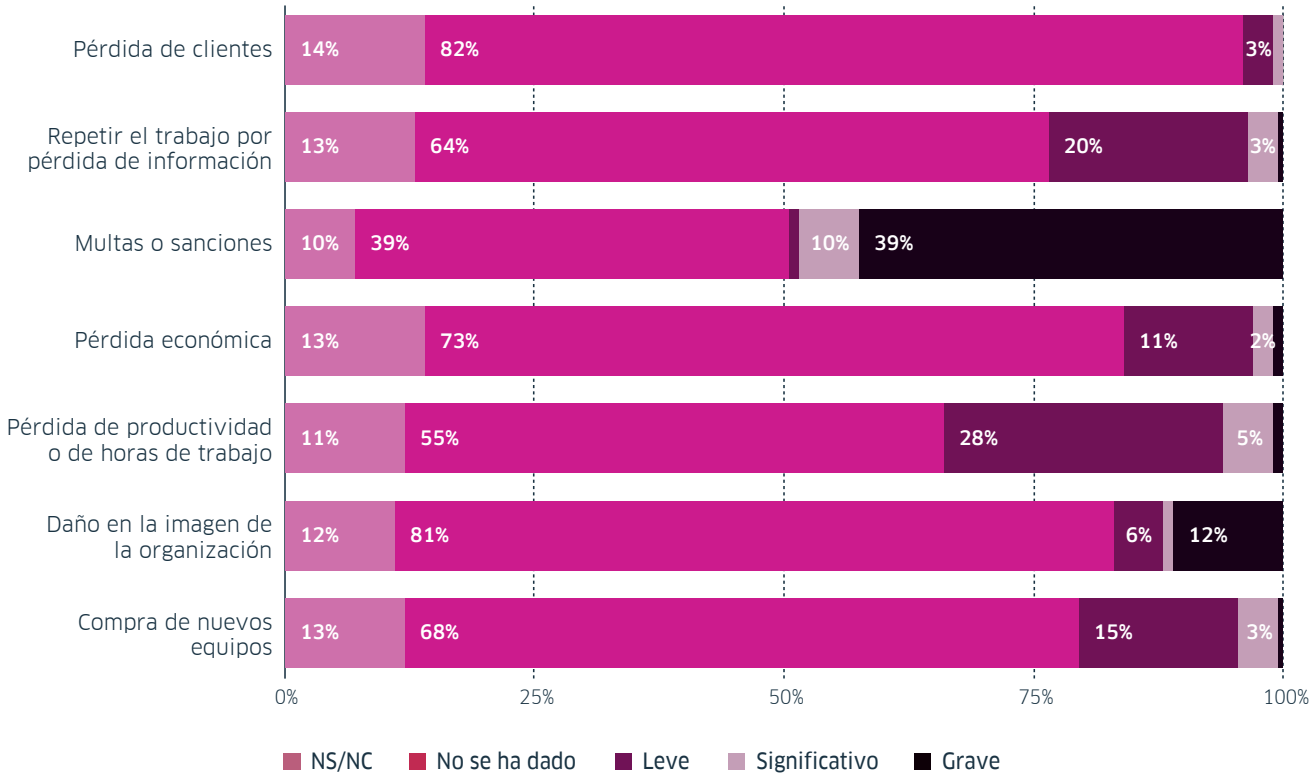
Consecuencias de los incidentes

Más allá del hecho de que los incidentes de seguridad ocurren, es importante tener una idea de cuáles son las consecuencias para la organización. Para tratar de obtener una visión más completa se ha incluido en el estudio un apartado para conocer cuál ha sido el impacto de estos incidentes.

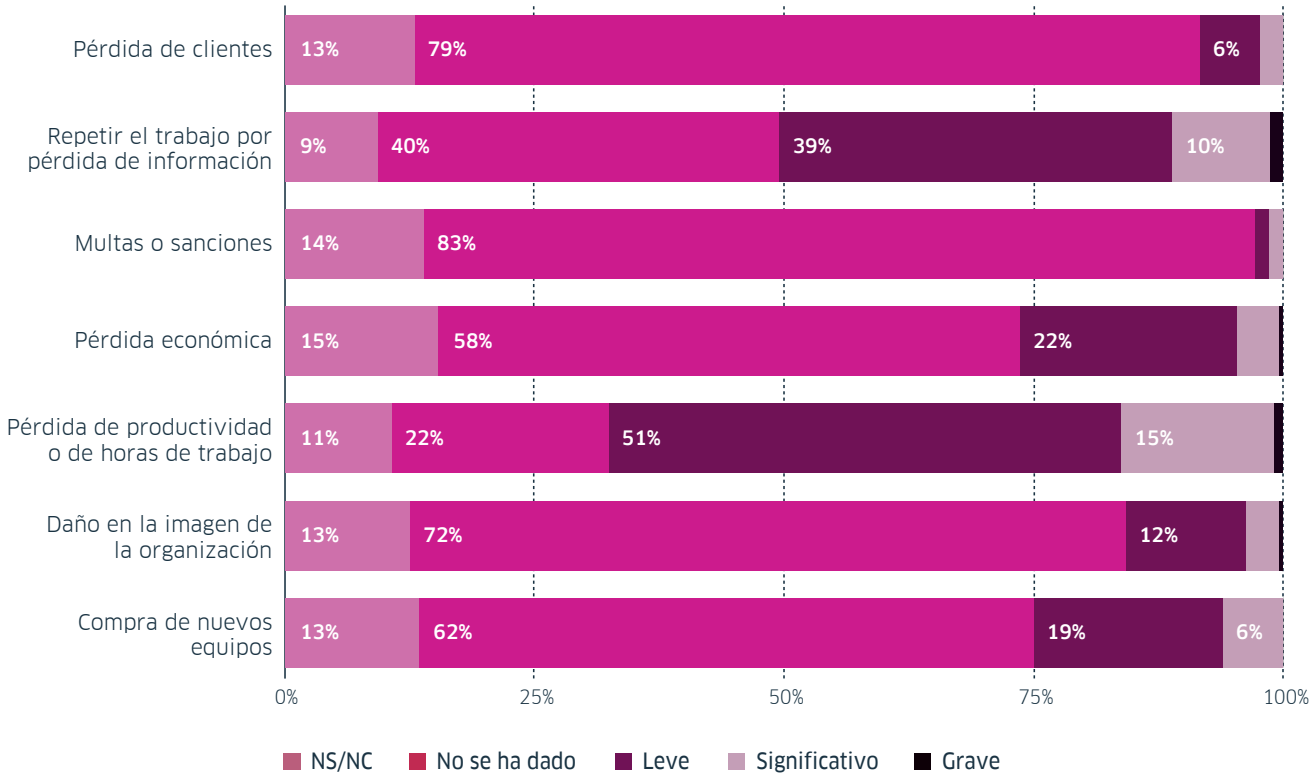
De las respuestas obtenidas cabe destacar el hecho de que **el mayor impacto se ve en el apartado de multas o sanciones, y en la pérdida de productividad.** También es relevante que **un 12%** de las organizaciones manifiesta que los incidentes de seguridad han supuesto un **daño grave en la imagen de la organización.**

Por otra parte, **uno de cada tres encuestados manifiesta que los incidentes de seguridad han supuesto una pérdida de productividad o de horas de trabajo.** Este dato es relevante teniendo en cuenta que la mejora de la productividad es un objetivo muy habitual para cualquier organización

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



Valore para cada uno de los siguientes supuestos cuáles han sido las consecuencias de los incidentes que ha sufrido (Datos del estudio de 2014)



Las preocupaciones

Los incidentes suponen la materialización de los riesgos de seguridad, pero el hecho de que un riesgo no se haya materializado aun en forma de incidente no implica que la organización esté a salvo de que estos riesgos se materialicen tarde o temprano.

Por este motivo, **los códigos de buenas prácticas de la gestión de la seguridad recomiendan encarecidamente a las organizaciones realizar un análisis de riesgos formal,** de forma que se disponga de información lo más realista posible sobre el nivel de riesgo que la organización está asumiendo en esta materia.

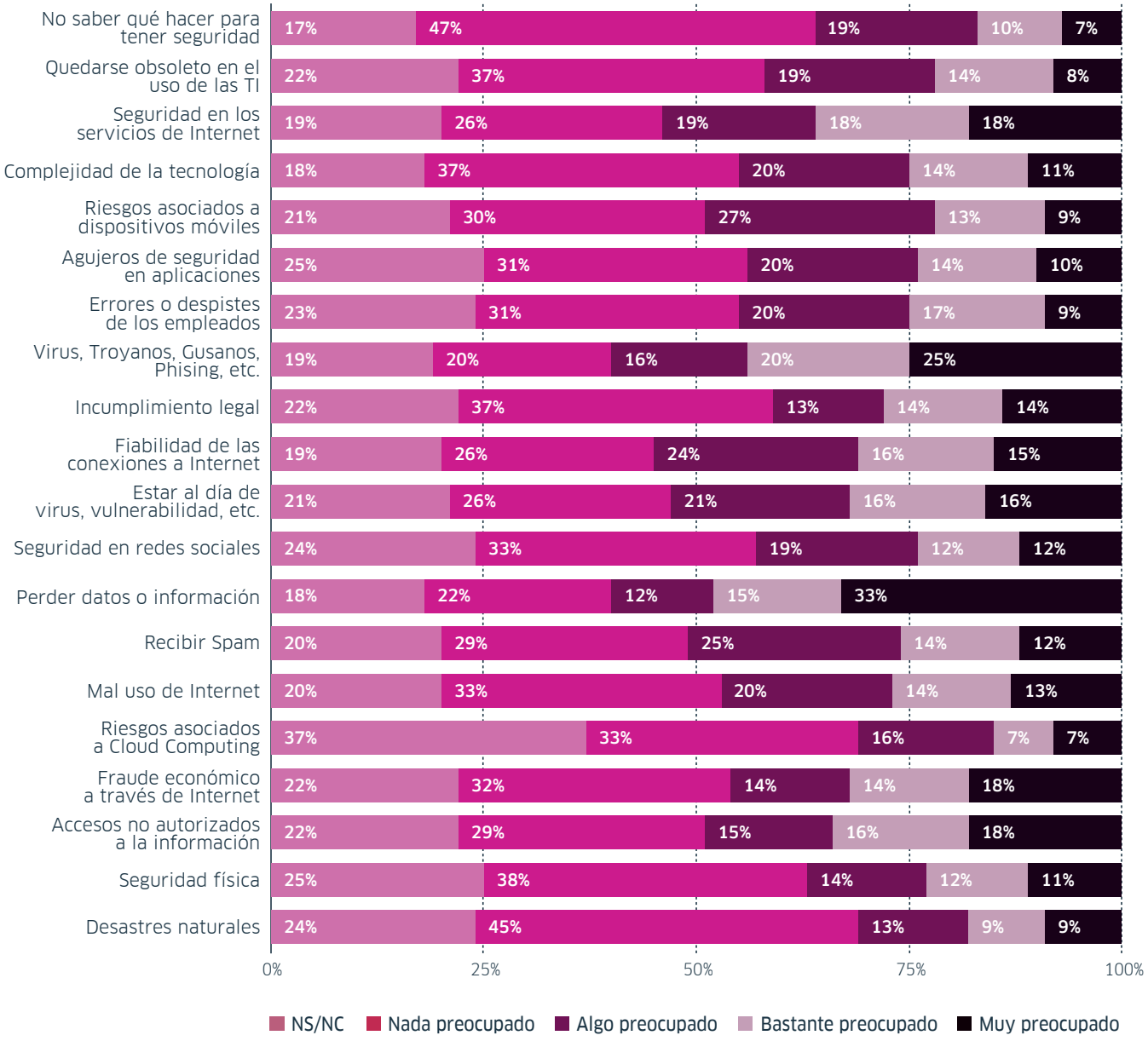
La mayoría de las organizaciones no realizan este análisis de riesgos, pero en el estudio se ha pretendido obtener, al menos, una visión sobre las preocupaciones que el personal de las organizaciones tiene en relación con algunas de las amenazas de seguridad mas frecuentes.

Por las respuestas obtenidas se aprecia, por una parte, que **el nivel de preocupación es bastante elevado** y, por otra, que el abanico de amenazas que preocupan a las organizaciones de la región es muy amplio.

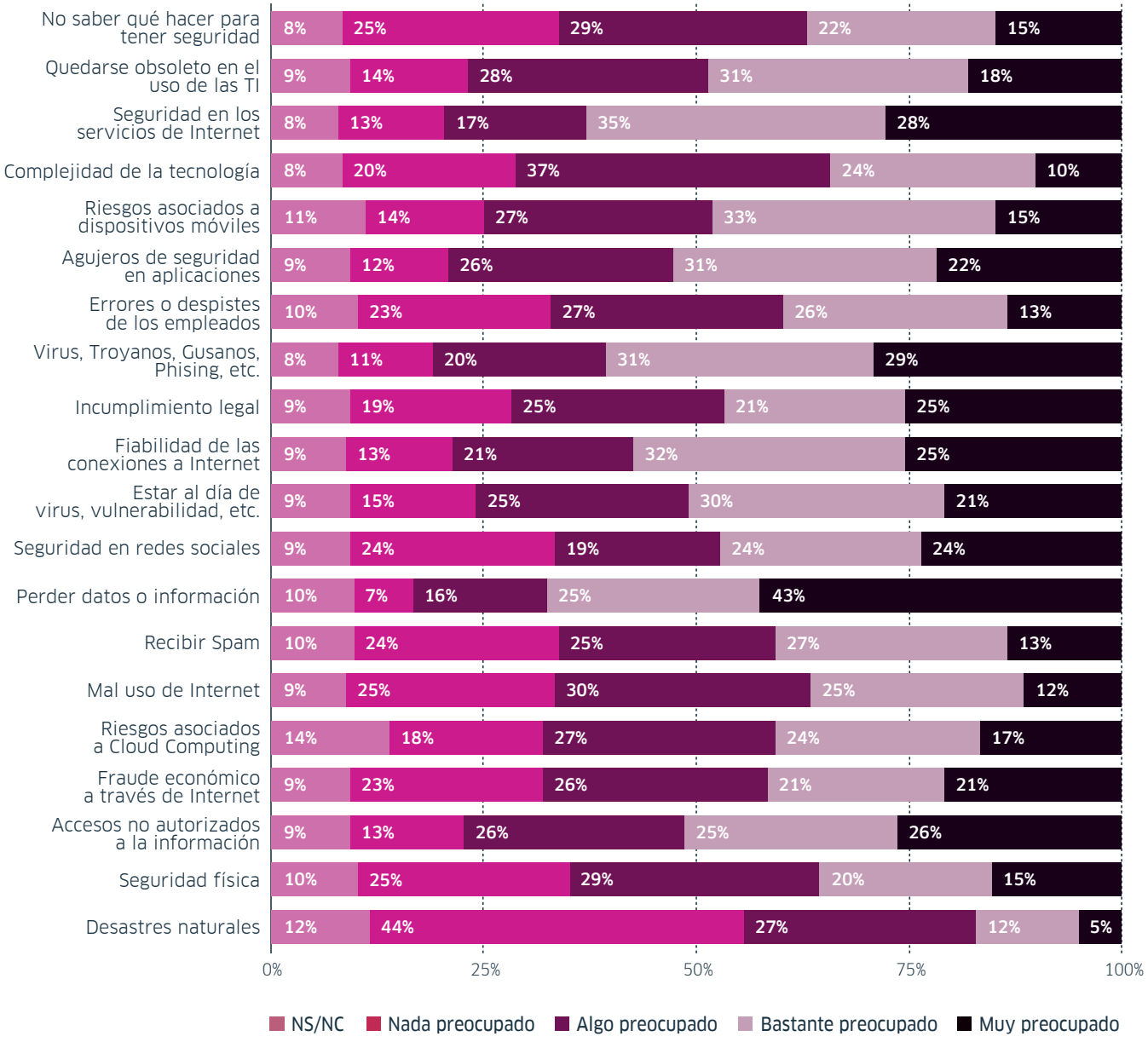
En términos generales, las personas entrevistadas están preocupadas por casi todas las amenazas contempladas en el estudio. **Se puede destacar la preocupación con respecto a las posibles pérdidas de datos o de información, así como al código malicioso** (virus, troyanos, etc.).

El grado de preocupación en esta edición del estudio de 2016 es menor al que se podía apreciar en el estudio realizado en 2014.

Valore cual es su grado de preocupacion con respecto a cada una de las siguientes circunstancias



Valore cual es su grado de preocupacion con respecto a cada una de las siguientes circunstancias (Datos del estudio de 2014)



En lo que se refiere a las amenazas por las que los entrevistados están muy preocupados, se destaca lo siguiente:

- **Perder datos o información**
  - **Este aspecto sigue siendo el más preocupante para las organizaciones,** lo cual pone de manifiesto que la información del negocio es uno de los activos más relevantes para cualquier organización.
- **Código malicioso**
  - Este elemento ya se ha comentado con anterioridad en otros apartados del estudio.
  - A pesar de ser uno de los temas sobre los que más tiempo se lleva trabajando, **continúa siendo una preocupación constante.**

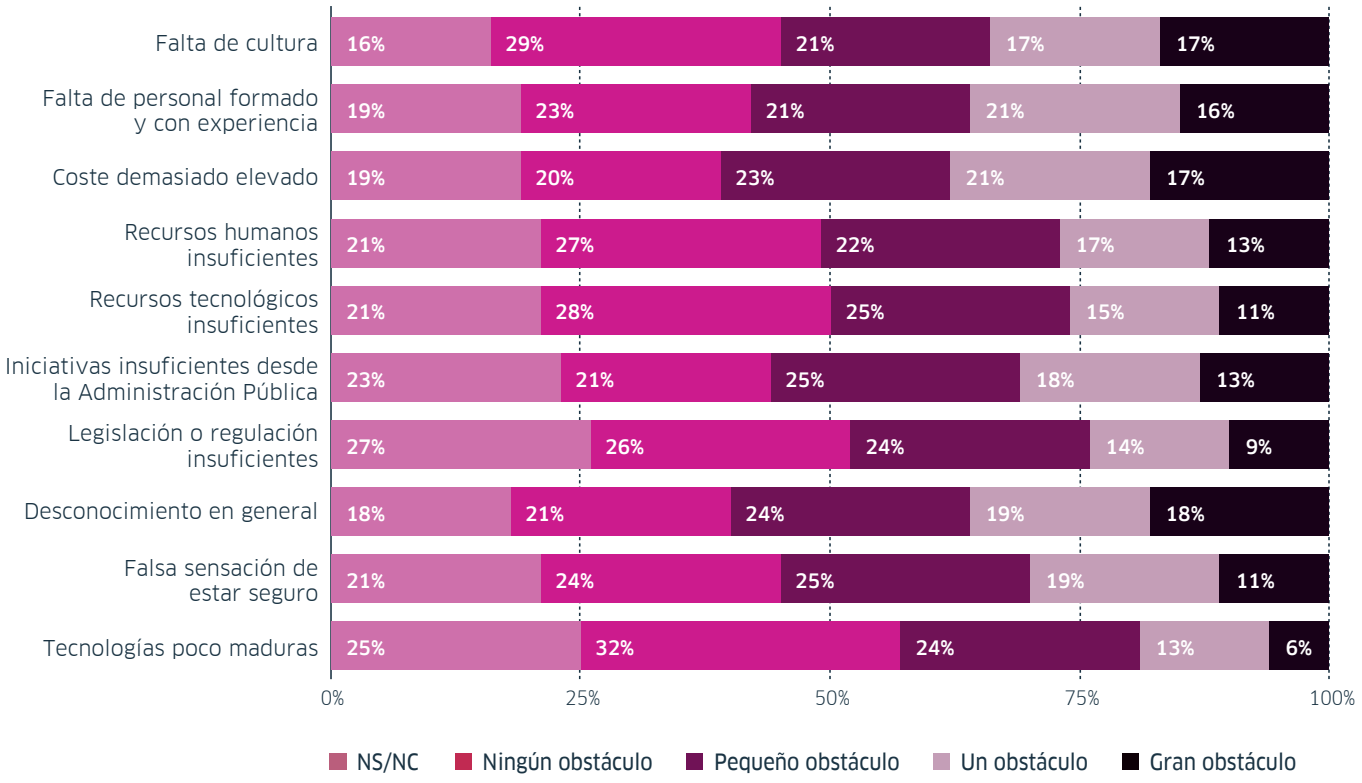
Obstáculos al desarrollo de la seguridad

De forma parecida a lo ocurrido en el apartado anterior, donde se valoraban las preocupaciones, en este caso también los entrevistados consideraban de forma general como tales los obstáculos contemplados dentro del estudio para el desarrollo de la seguridad.

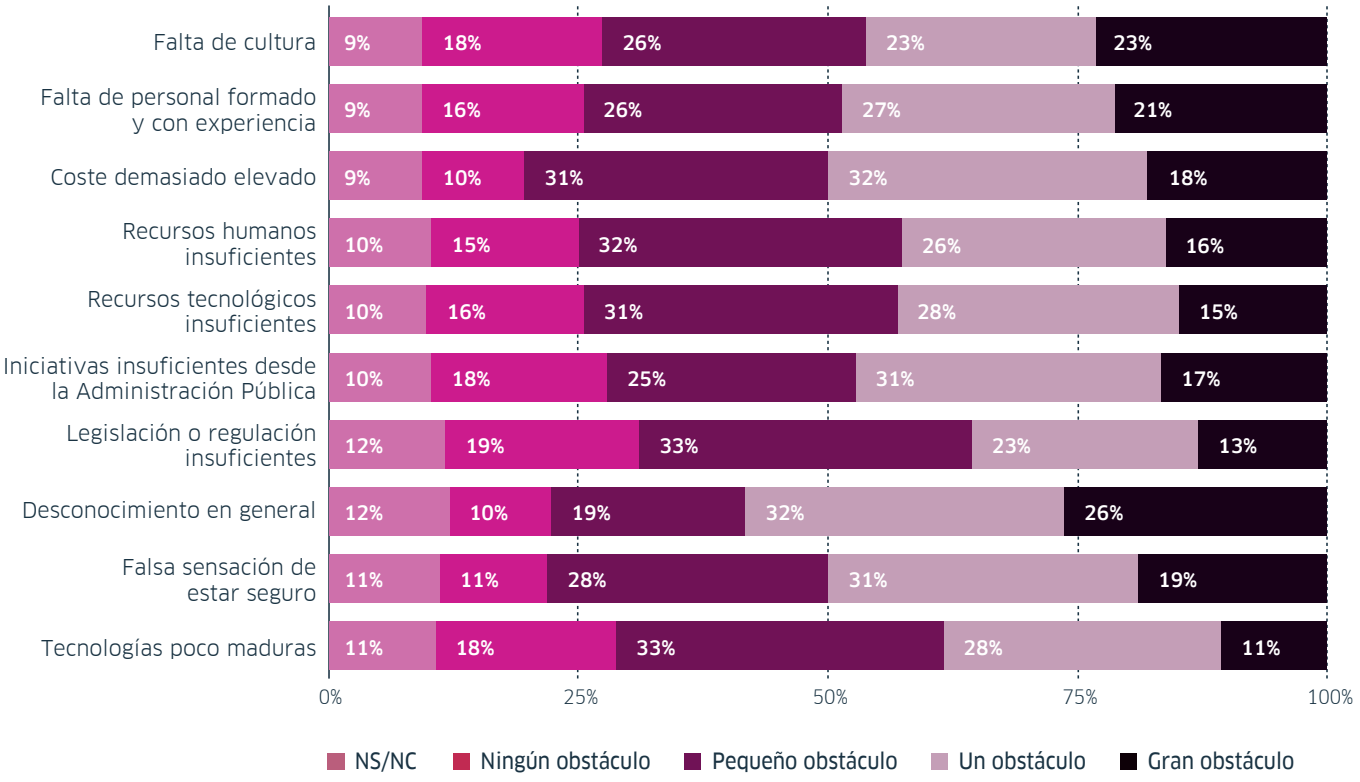
Independientemente de la importancia de cada uno de los obstáculos planteados, **se quiere resaltar que el desconocimiento general, la falta de personal formado y con experiencia, el coste de la seguridad y la falta de cultura destacan como grandes obstáculos.**

De forma similar a lo que se puede apreciar en el apartado de las preocupaciones, la valoración de la importancia relativa de estos obstáculos en esta edición del estudio es menor al que se indicaba en el estudio de 2014.

Valore la importancia de los siguientes obstáculos para disponer de un buen nivel de seguridad



Valore la importancia de los siguientes obstáculos para disponer de un buen nivel de seguridad (Datos del estudio de 2014)



Iniciativas para mejorar la seguridad

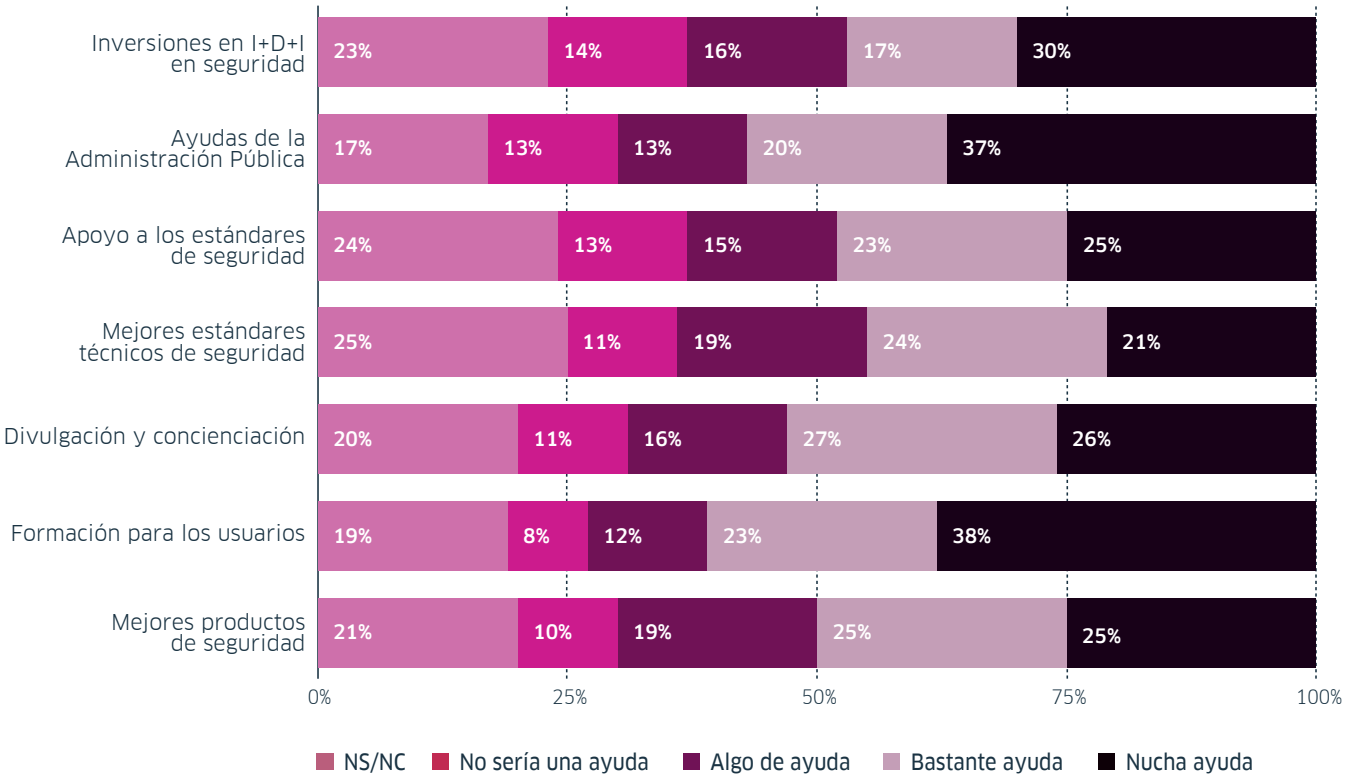
Por último, se consultó a los encuestados acerca de cuales son a su juicio las iniciativas que mejor podrían ayudar en el desarrollo de la seguridad.

Las respuestas obtenidas están alineadas con las que se obtuvieron en el apartado anterior referente a los obstáculos.

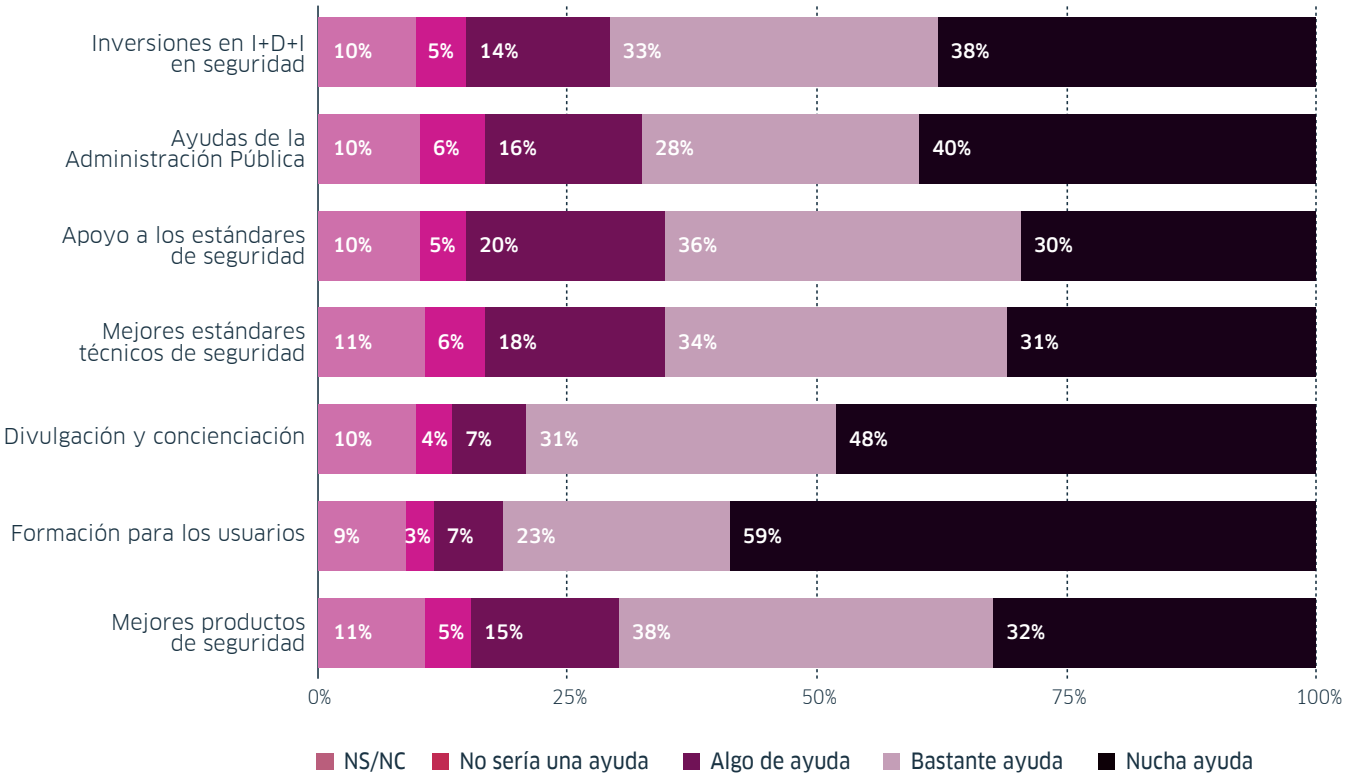
Por una parte, si se destacaban como obstáculos el desconocimiento general, la falta de personal formado y con experiencia, y la falta de cultura, **se considera que la formación para los usuarios ayudaría de una forma importante a mejorar la situación. Está iniciativa obtuvo el mayor porcentaje de respuestas como que sería de "Mucha ayuda".**

Por otra, si se destacaba el coste de la seguridad como obstáculo, se considera que las ayudas de la Administración Pública ayudarían también de una forma significativa en el objetivo final de mejorar la seguridad informática.

Valore en que medida ayudarían a mejorar la seguridad cada una de las siguientes iniciativas



Valore en medida ayudarían a mejorar la seguridad cada una de las siguientes iniciativas (Datos del estudio de 2014)



Análisis estadístico del cuestionario

A título informativo, se incluye en este apartado la información que se ha considerado relevante con respecto al análisis estadístico realizado.

Esta información pretende aportar una visión general sobre la naturaleza, notas metodológicas, medidas de calidad del cuestionario y errores de muestreo.

El número de empresas en La Rioja a 1 de enero de 2015, susceptibles de ser seleccionadas por pertenecer a alguno de los grupos de la CNAE-09 descritos anteriormente, es de 28.349.

Ámbitos de la encuesta

- **Ámbito temporal:**
  - La encuesta tiene una periodicidad bienal
- **Ámbito geográfico:**
  - El ámbito geográfico es la Comunidad Autónoma de La Rioja.
- **Ámbito poblacional:**
  - La población a la que va dirigida la encuesta es el conjunto de empresas riojanas pertenecientes a las secciones A, B, C, D, E, F, G, H, I, J, K, L, M, N, P, Q y R de la CNAE09. Se consideran todas las empresas de estas ramas de actividad, aunque no tengan asalariados.

Secciones	Descripción
Sección A	Agricultura, ganadería, silvicultura y pesca
Secciones B a N	Industria, suministro de energía eléctrica, gas, agua, construcción, comercio, trasporte, hostelería, información y comunicaciones actividades financieras, inmobiliarias, profesionales, científicas y técnicas actividades administrativas y servicios auxiliares
Sección P	Educación
Sección Q	Actividades sanitarias y de servicios sociales
Sección R	Actividades de juegos de azar y apuestas Actividades deportivas, recreativas y de entretenimiento

- Se excluyen las siguientes

Secciones	Descripción
Sección O	Administración Pública y defensa
Sección S	Actividades Asociativas Reparación de ordenadores, efectos personales y artículos de uso doméstico Otros servicios personales
Sección T	Actividades de los hogares como empleadores de personal doméstico; actividades de los hogares como productores de bienes y servicios para uso propio
Sección U	Actividades de organizaciones y organismos extraterritoriales

Marco de la encuesta

El marco de la Encuesta es el Directorio de Empresas del Instituto de Estadística de La Rioja.

Se trata de un registro organizado de información con datos de identificación, localización, distribución territorial y clasificación por tamaño y actividad económica de empresas y establecimientos.

El contenido del directorio procede de fuentes administrativas, y se actualiza y completa con información proveniente del Directorio Central de Empresas (DIRCE) del INE.

Diseño muestral

El número de empresas en La Rioja a 1 de enero de 2015, susceptibles de ser seleccionadas por pertenecer a alguno de los grupos de la CNAE-09 descritos anteriormente, es de 28.349.

Para la selección de la muestra se ha optado por un muestreo aleatorio estratificado según el tamaño de la empresa, combinado con un censo para las unidades de mayor tamaño. Esto permite valorar nuestro objetivo en los extremos de la población, desde empresas sin asalariados hasta empresas de 50 o más asalariados. Con esta técnica se obtiene una precisión estadística más elevada.

Se ha utilizado un muestreo estratificado no proporcionado, de forma que se garantice un mínimo error en cada estrato, ya que son de muy distintos tamaños.

Así, considerando un error del 5% y una confianza del 95% en cada grupo, se obtiene una muestra de 571 empresas que se distribuyen como sigue.

Etiquetas de fila	Total empresas	Muestra total	
Total (de la A hasta la R excepto O)	28.349	571	
Sin asalariados	16.093	217	
De 1 a 2	7.684	103	
De 3 a 5	2.360	32	
De 6 a 9	938	13	
De 10 a 49	1.082	15	
De 50 o más asalariados	192	192	

Tras la recogida de la información en el plazo considerado, se ha perdido representatividad, ya que han respondido el cuestionario un total de 371 empresas.

Si la pérdida de información es superior al 40% se pierde fiabilidad. Por esta razón se ha hecho un análisis con el total de empresas, ya que la pérdida por estrato de asalariados es como aparece reflejado en la siguiente tabla.

Etiquetas de fila	Total empresas	Muestra total	Muestra final	Pérdida de representatividad
Total (de la A hasta la R excepto O)	28.349	571	367	35,73%
Sin asalariados	16.093	217	112	48,39%
De 1 a 2	7.684	103	66	35,92%
De 3 a 5	2.360	32	21	34,38%
De 6 a 9	938	13	9	30,77%
De 10 a 49	1.082	15	12	20,00%
De 50 o más asalariados	192	192	147	23,44%

Así, a pesar de la pérdida en las empresas sin asalariados, se podría dar información sobre el total, sobre empresas con asalariados, o con empresas entre 1 y 49 asalariados y empresas con 50 o más asalariados. Así, el error para la muestra final es del 5.15%.

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 formada por 96 ítems.

Se ha realizado un análisis de fiabilidad calculando el índice Alpha de Cronbach, que permite cuantificar el nivel de fiabilidad de una escala de medida para la magnitud inobservable construida a partir de las "n" variables observadas.

El mayor valor teórico de Alpha es 1 y el resultado obtenido ha sido un Alpha de Cronbach de 0.9566, y Alpha Std de 0.9625.

Esto indica que el cuestionario aplicado a los encuestados es altamente fiable.

ANEXO 1 - ENCUESTA:

Evaluación sobre el estado de la seguridad de la información en las organizaciones de la rioja

Gestión de la seguridad

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

- No están asignadas a ninguna persona
- Departamento de seguridad
- Departamento de informática o similar
- Técnico o personal de informática o similar
- Otro personal de la organización
- Subcontratado a una empresa externa
- 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					
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					

	NS/NC	NO SE HA DADO	LEVE	SIGNIFICATIVA	GRAVE
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					
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					
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)					

Datos económicos

Facturación en euros al año

1. Menos de 100.000
2. De 100.000 a 499.999
3. De 500.000 a 1.999.999
4. De 2.000.000 a 9.999.999
5. De 10.000.000 a 49.999.999
6. Más de 50.000.000
7. No sabe o no contesta

Términos y definiciones

APD: Agencia de Protección de Datos (www.agpd.es).

Biometría: Es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos de una persona, para verificar su identidad o identificarlo.

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.

Dispositivo móvil: son equipos pequeños, con capacidad de proceso, con conexión de datos, en los que se pueden usar aplicaciones y que se pueden llevar con uno.

Algunos ejemplos son los ordenadores portátiles, Smartphones y los tablets.

Factura electrónica: Es una modalidad de factura en la que no se emplea el papel como soporte. Es un fichero que recoge la información relativa a una transacción comercial y sus obligaciones de pago y de liquidación de impuestos y cumple con todos los requisitos legales.

Firewall: O cortafuegos, es un elemento de hardware o software utilizado en una red para controlar las comunicaciones entrantes o salientes, permitiéndolas o prohibiéndolas según las políticas que se hayan definido.

Firma digital: 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.

Cadena de mensajes: Es un e-mail que intenta engañar haciendo creer que algo falso es real. Frecuentemente pide que se reenvíe el mensaje a todos sus contactos.

IDS: También conocido como sistema de detección de intrusos, es un programa usado para detectar accesos no autorizados a un ordenador o a una red.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Phishing: Es un tipo de ingeniería social, que busca conseguir de forma fraudulenta información confidencial como pueden ser contraseñas o información detallada sobre tarjetas de crédito u otra información bancaria.

Spam: O correo basura, son mensajes no solicitados, normalmente publicitarios, enviados en cantidades masivas.

Spyware: También conocido como programas espía, son aplicaciones que recopilan información de los ordenadores de una persona u organización sin su conocimiento.

TI: Las Tecnologías de la Información y la Comunicación agrupan los elementos y las técnicas usadas en el tratamiento y la transmisión de la información, aspectos tratados principalmente en la informática, la microelectrónica y las telecomunicaciones. Estas tecnologías destacan sobremanera en la red de redes: Internet.

Troyano: Es un programa malicioso que se aloja en los ordenadores y permite el acceso a usuarios externos, a través de una red local o de Internet, para recabar información o controlar remotamente la máquina.

Virus: Es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento normal del ordenador, sin el permiso o conocimiento del usuario

VPN: Es una tecnología de red que permite extender de forma segura la red local sobre Internet usando un canal cifrado.

Gobierno de La Rioja

think TIC Centro Nacional de Formación en Nuevas Tecnologías

Más información:

Desarrollo Económico e Innovación
Dirección General de Innovación, Trabajo, Industria y Comercio
Think-TIC
941 291 935
Av. Zaragoza, 21 Logroño
informacion.thinktic@larioja.org
larioja.org/thinktic