Encuesta sobre confianza digital en las empresas

Octubre 2017

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

La encuesta sobre Confianza Digital en las Empresas ha sido elaborada por el ONTSI:

Alberto Urueña López

Luis Muñoz López

Pedro Antón Martínez

Este estudio y encuesta se ha realizado con la colaboración de las empresas ACAP (Asesores y Consultores en Administraciones Públicas) e I Claves

Con la colaboración asimismo de ODEC.

Este informe incluye recomendaciones e información del Instituto Nacional de Ciberseguridad, INCIBE

Índice

1 INTRODUCCIÓN

1.1 Objeto y alcance del estudio

Este informe responde al estudio de situación sobre confianza digital y seguridad de la información en las empresas españolas, elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de Red.es.

El objeto del estudio y encuesta es la situación de la seguridad TIC en las empresas españolas en el marco de la medida 13 denominada Esquema de indicadores para la confianza digital, contenida en el **Plan de confianza en el ámbito digital** de la Agenda Digital para España (ADpE), que persigue dar respuesta a los compromisos en materia de confianza digital establecidos por las estrategias, europea y nacionales de seguridad.

La Estrategia de Seguridad Nacional (ESN) integra entre sus objetivos el de garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques.

Por su parte los objetivos del Plan de confianza en el ámbito digital integrado en la ADpE son:

- Asegurar una experiencia digital segura.
- Generar capacidades para la resiliencia en materia de seguridad.
- Generar nuevas oportunidades para la industria y los profesionales.

En el marco del Plan, la medida 13 orientada a generar el **Esquema de indicadores para la confianza digital** constituye el medio de valoración de la consecución de los objetivos del Plan, y su evolución a lo largo del tiempo. El esquema ha sido elaborado con la colaboración del Foro Nacional para la Confianza Digital (FNCD).

Entre los **objetivos específicos del estudio** sobre confianza digital y seguridad TIC en las empresas cabe señalar los siguientes:

- Dar soporte a la obtención de la primera serie de indicadores relacionados con la confianza digital en empresas, asociados al esquema de indicadores de confianza digital, de forma que se asegure la obtención de los indicadores incluidos en dicho esquema.
- Caracterizar las empresas desde el punto de vista de los activos de información que utilizan y generan, así como desde la óptica del modelo de gestión de seguridad de dichos activos.
- Conocer la preparación de las empresas en materia de seguridad TIC.
- Conocer las herramientas y medidas de seguridad que implementan las empresas en el desarrollo de su actividad.
- Conocer los incidentes de seguridad que se producen y sus consecuencias desde el punto de vista del negocio de las empresas.
- Conocer el comportamiento de las empresas en materia de privacidad (protección de datos personales) y transacciones electrónicas.

2 ASPECTOS DESTACADOS

CARACTERIZACIÓN DE LAS EMPRESAS

Se entiende que los usos que las empresas realizan de las TIC y de Internet determinan los riesgos a los que se enfrentan en materia de seguridad TIC, siendo algunos aspectos destacados de su caracterización los siguientes:

- En términos generales, la presencia en Internet y el uso de servicios electrónicos es proporcional al tamaño de la empresa, exceptuando el caso del comercio electrónico. De esta manera, cuanto mayor es la empresa más indica tener presencia en Internet y usar servicios electrónicos como la firma digital o los servicios en la nube.
- Cabe resaltar, que las empresas que consideran la seguridad de la información como una prioridad elevada o máxima son las que gestionan más activos tecnológicos y de información. Todo ello parece indicar que cuanto mayor es el número de activos gestionados son más conscientes de la necesidad de gestionar la seguridad, mostrando estar más preparadas.
- La gran mayoría de las empresas han declarado tener sus sistemas operativos y herramientas actualizados. Estas empresas que indican mantener los sistemas operativos actualizados, declaran también utilizar en mayor medida servicios tales como la banca electrónica, la firma digital o servicios en la nube.

HERRAMIENTAS Y MEDIDAS DE SEGURIDAD

Desde el punto de vista de las herramientas y medidas de seguridad que mantienen las empresas las conclusiones más relevantes del estudio indican:

- Todavía hay un grupo muy importante de empresas que desconocen el beneficio que puede generar la formulación y ejecución de una política de seguridad en la gestión del impacto que pueden tener los incidentes de seguridad desde el punto de vista económico y del negocio. Así, el porcentaje de empresas con una política de seguridad TIC formalmente definida todavía es bajo, aunque mayor que el registrado en la "ETICce" 2014-15[1].
- Entre las empresas que mantienen una política de seguridad TIC, la mayoría han declarado haberla revisado en los últimos 12 meses. Cabe mencionar, además, que las microempresas han declarado revisar sus sistemas de seguridad con más asiduidad que en otras ocasiones ("ETICce" 2014-15), lo que sin duda significa una evolución positiva.
- Los datos obtenidos indican que la obtención de certificados ISO 27001 está vinculada con el mercado. De esta forma, es posible que si no existiera esta demanda del mercado las empresas no optarían por abordar por si solas el proceso de certificación.
- Por el contrario, la definición de una estrategia de continuidad de negocio, está ligada a factores internos. De este modo, se entiende que supone la reacción de las empresas a los problemas

[1] "*Encuesta sobre el uso de las tecnologías de la información y las comunicaciones y del comercio electrónico en las empresas*" realizada por el Instituto Nacional de Estadística INE 2014-2015.

de seguridad que pudieran haber sufrido en el pasado, constituyendo su implantación una reacción a incidencias de seguridad pasadas.

- Existe una relación proporcional entre el tamaño de la empresa y la seguridad en sus conexiones inalámbricas, de manera que las grandes y medianas empresas utilizan el protocolo WPA o WPA2 en mayor proporción que las pequeñas. Esto concuerda con el nivel de desconocimiento del tipo de protección de la red wifi, ya que es inversamente proporcional al tamaño de las empresas, es decir, cuanto menor es la empresa mayor es el desconocimiento sobre el tipo de protección de su red wifi.
- En lo que a valoración de las características de los servicios se refiere, las empresas de menor tamaño valoran más la accesibilidad del producto, probablemente por la falta de tiempo o de personal especializado para abordar las cuestiones relativas a la seguridad. Esto podría indicar que buscan soluciones fáciles de gestionar.
- Las medianas y grandes empresas valoran proporcionalmente más el servicio postventa y la garantía, así como la calidad y efectividad del producto.

INCIDENTES DE SEGURIDAD

- Cuanto mayor es la empresa mayor grado de conocimiento muestra de las consecuencias que los incidentes de seguridad pueden tener para su negocio.
- El porcentaje de empresas que declaran haber sufrido algún incidente de seguridad ha aumentado respecto al registrado en 2012[2]. No obstante, lejos de ser un elemento negativo, estas respuestas podrían mostrar cómo ha evolucionado la capacidad de las empresas de identificar la ocurrencia de los distintos incidentes, lo que supondría en consecuencia una mayor capacidad de respuesta.
- Cuantos más activos tecnológicos y de información gestione una empresa y más presencia en Internet haya desarrollado mediante el uso de servicios o la realización de transacciones electrónicas, la empresa indica que aborda más riesgos e incidentes de seguridad. La creciente declaración sobre el uso de activos y servicios electrónicos parece indicar que las empresas se exponen a crecientes problemas de seguridad, por lo que en un entorno como el actual, la seguridad TIC de la empresa se convierte en un elemento esencial para la estabilidad del negocio de las empresas.
- Al contrario de lo que cabría esperar, las empresas que tienen definida una política de seguridad también sufren más incidentes de seguridad, lo que probablemente tiene que ver con la existencia de registros específicos que permiten su gestión, una mayor capacidad de aminorar sus consecuencias y una mayor consciencia de la ocurrencia concreta de los incidentes.

  Se puede concluir que la existencia de una política de seguridad no disminuye necesariamente la existencia de incidentes, sino que permite una adecuada gestión de los mismos, aminorando su impacto.

[2] "*Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*" INTECO 2012. (Actualmente INCIBE).

- Las grandes empresas mencionan que sufren un menor número de consecuencias negativas derivadas de incidentes de seguridad. De esta forma, el hecho de que las grandes empresas sufran mayor número de incidentes de seguridad y, por el contrario, denoten menores consecuencias, refuerza la idea de que su mayor preparación ante los incidentes minimiza las consecuencias negativas que estos tienen para su negocio.
- Se ha detectado un bajo porcentaje de empresas que declaran haber cuantificado el impacto económico que han tenido los incidentes de seguridad. Esta sin duda parece una tarea pendiente para el futuro.
- Al contrario de lo que cabría imaginar, existe una relación inversamente proporcional entre el tamaño de las empresas y la cuantificación del impacto económico producido por los incidentes de seguridad, así, las microempresas son las que declaran haber cuantificado los daños económicos en un mayor porcentaje, 44%, seguidas de las pequeñas empresas con un 31%, medianas empresas 29% y, finalmente, grandes empresas 27%.
- El cambio de hábitos como consecuencia de haber sufrido un incidente de seguridad presenta diferencias según el tamaño de la empresa, de manera que: las microempresas y pequeñas empresas han manifestado en mayor proporción dejar de usar determinados servicios de Internet y haber comenzado a realizar copias de seguridad, mientras las medianas y grandes empresas indican en mayor medida que establecen protocolos y procedimientos de seguridad más estrictos, o bien contratan servicios de auditoría externos.

POLÍTICAS DE PRIVACIDAD

- Existe una relación proporcional entre las políticas de privacidad en las empresas y su tamaño. Cuanto mayor es la empresa es más frecuente que manifieste mantener la declaración sobre la política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web. Igualmente, también indican en mayor proporción mantener conocimiento sobre la LOPD, y estar adecuados a dicha normativa en todos sus requerimientos.
- La labor de sensibilización parece que debe incidir fundamentalmente en las microempresas y las pequeñas y medianas empresas.

TENDENCIAS TECNOLÓGICAS EN LA PRIVACIDAD Y LA SEGURIDAD

- Para un porcentaje bastante alto de las empresas consultadas el uso de dispositivos personales para el acceso a datos e información, y la movilidad y el acceso remoto a sus sistemas y datos supone un riesgo de seguridad añadido y creciente.
- Esto representa un reto para la seguridad TIC ya que la tendencia al uso de dispositivos personales en el ámbito laboral y el acceso remoto a los sistemas y datos, parece que pueden exponer a la empresa a sufrir en mayor medida incidentes de seguridad no controlados.

3 RESUMEN EJECUTIVO

CARACTERIZACIÓN DE LAS EMPRESAS

Los activos tecnológicos y de información en las empresas

- Las empresas consultadas manifiestan gestionar una media de cinco tipos de activos tecnológicos y de información. Un 93,5% menciona los equipos informáticos de sobremesa, un 86,9% software y aplicaciones informáticas, un 84,6% portátiles, dispositivos móviles y tabletas, un 75,4% ficheros de datos personales, y un 74,4% equipos y redes de comunicaciones.
- Se ha observado una relación proporcional entre el número de activos tecnológicos y de información que gestionan las empresas y su tamaño, de manera que cuanto más grande es la empresa más tipos de activos tecnológicos y de información manifiesta gestionar.

Presencia en Internet y servicios electrónicos

- El 72,8% de las empresas consultadas tienen página web.
- El 89,7% de las empresas afirman utilizar la firma digital: el 88,9% de las empresas afirman utilizar la firma digital para relacionarse con la Administración Pública y el 27% para relacionarse con clientes y proveedores.
- El 16,3% de las empresas consultadas afirman realizar ventas por Internet y un 11,4% de las empresas ha declarado que algún problema de seguridad TIC o protección de datos ha obstaculizado realizar ventas a través de Internet.
- Por otra parte, el 66,6% de las empresas ha manifestado utilizar servicios en la nube. El 58,7% de las empresas utiliza servicios de alojamiento de correo electrónico y/o página web en la nube, el 36,1% utiliza servicios de almacenamiento y acceso de datos y un 22,7% contrata aplicaciones de software como servicio en la nube.
- En términos generales, la presencia en Internet y el uso de servicios electrónicos es proporcional al tamaño de la empresa para todos los casos, exceptuando el comercio electrónico, de manera que cuanto más grande es la empresa más indica tener presencia en Internet y usar servicios electrónicos como la firma digital o los servicios en la nube.
- Los sectores de actividad que destacan en la presencia en Internet y el uso de servicios electrónicos son el de Información y comunicaciones, Actividades administrativas y servicios auxiliares y Actividades profesionales, científicas y técnicas.

Preparación de las empresas

- La mayoría de las empresas consultadas consideran la seguridad de la información como una cuestión de máxima o elevada prioridad para su empresa y manifiestan tener sus sistemas operativos y herramientas de seguridad actualizadas, con un 86,9%, y un 87,3% de la respuesta respectivamente.

- Existe una relación proporcional y positiva entre la preparación de las empresas y el tamaño, de manera que cuanto más grande es la empresa más indica que considera la seguridad de la información como una prioridad y más afirma tener sus sistemas operativos y herramientas de seguridad actualizados.
- Las empresas que consideran la seguridad de la información como una prioridad son las que gestionan más activos tecnológicos y de información.
- Las empresas que no tienen actualizados sus sistemas operativos y herramientas de seguridad utilizan menos Internet como usuario y proveedor de determinados servicios electrónicos en comparación con las empresas que se mantienen actualizadas. En concreto, los servicios menos utilizados por las empresas que no están actualizadas con los de banca electrónica y firma digital.

HERRAMIENTAS Y MEDIDAS DE SEGURIDAD

Políticas y estrategias de seguridad

- El 43,4% de las empresas consultadas afirma tener definida formalmente una política de seguridad TIC. Solo el 5,7% de las empresas consultadas afirma estar certificada por la ISO 27001 y el 41% de las empresas consultadas ha afirmado que disponen de una estrategia de continuidad de negocio.
- Existe una relación proporcional entre definir políticas y estrategias de seguridad y el tamaño de la empresa, así las medianas y grandes empresas que tienen definida formalmente una política de seguridad TIC, están certificadas en mayor proporción en la ISO 27001, y afirman tener definida una estrategia de continuidad de negocio, más que las microempresas y pequeñas empresas y apuntan también a definir más riesgos en su política de seguridad.
- Las empresas que pertenecen al sector de Información y comunicaciones son las que más indican mantener una política de seguridad TIC. Del mismo modo, mantienen en mayor medida certificación ISO 27001 y estrategias de continuidad de negocio. Las empresas cuya respuesta ha sido peor pertenecen al sector de Servicios de comidas y bebidas.
- Las empresas consultadas revisan su política de seguridad con asiduidad: el 69,3% de las empresas ha indicado haber revisado su política de seguridad en los últimos 12 meses, el 21% entre los últimos 12 y 24 meses y el 9,7% hace más de 24 meses.
- A pesar de que las medianas y grandes empresas son las que más definen políticas y estrategias de seguridad, son las microempresas y pequeñas las que revisan su política de seguridad con más continuidad según la respuesta obtenida.
- El riesgo más definido por las empresas consultadas en su política de seguridad es el de destrucción o corrupción de datos con un 82,8%. El 52,2% de las empresas consultadas ha definido en su política el riesgo de revelación de datos confidenciales y el 51,3% la falta de disponibilidad de servicios TIC.
- En cuanto a las razones o los motivos que han llevado a las empresas a definir una política de seguridad TIC, el 76,5% de las empresas consultadas manifiesta cuatro o más razones: el 96,2% de las empresas indica implantar políticas de seguridad para

asegurar la integridad de los datos y la información. El segundo motivo para implementar la política de seguridad es garantizar la disponibilidad de las operaciones de negocio y la disponibilidad de los servicios en caso de crisis, con un 73,9% de las respuestas. La protección contra el robo de activos de la empresa con un 70,3% es otro de los motivos más mencionados.

Sistemas y soluciones de seguridad

- Las empresas medianas y grandes han manifestado en mayor proporción que las microempresas y pequeñas empresas haber implantado sistemas internos de seguridad, productos de seguridad, medidas de seguridad en dispositivos móviles, servicios especializados de seguridad y protocolos de seguridad en sus conexiones inalámbricas.
- Respecto a los sistemas internos de seguridad que han implantado las empresas, el sistema que más han indicado las empresas haber implantado es el de autenticación con contraseña segura con un 86,9%. El segundo sistema interno más utilizado por las empresas consultadas es el backup de datos externos con un 81,1% de las respuestas. En tercer lugar, las empresas han afirmado utilizar protocolos para el análisis de incidentes de seguridad con un 26%.
- Los tres sistemas internos de seguridad más utilizados se justifican por las mismas razones: proteger contra el robo sus activos, garantizar la disponibilidad de las operaciones de negocio/servicios en caso de crisis y la ventaja competitiva. La diferencia la encontramos entre las empresas que han indicado utilizar protocolos para el análisis de incidentes de seguridad que han afirmado, además, estar motivadas por el cumplimiento de requerimientos regulatorios/legales, así como por experiencias negativas anteriores relacionadas con la interrupción de las operaciones.
- En cuanto a los productos de seguridad que han implantado las empresas, los productos antivirus/anti espía son los más indicados por las empresas consultadas con un 97,8%. A continuación, los cortafuegos y filtros de contenidos web representan el segundo producto más utilizado por las empresas consultadas con un 76,1%. Finalmente, el 71,4% de las empresas manifiestan utilizar herramientas de contingencia y continuidad.
- En relación a las medidas de seguridad que más utilizan las empresas en sus dispositivos móviles, el 90% ha indicado utilizar acceso mediante código pin, el 75,2% contraseña de desbloqueo. Les siguen las actualizaciones de software automáticas con un 46,4% y los programas antivirus con un 41,2%.
- Respecto a cuáles son los servicios especializados de seguridad que más han indicado utilizar las empresas, en primer lugar, encontramos los servicios de cumplimiento de la legislación (LOPD) con un 72,2%, un 51,8% de las empresas consultadas ha indicado que su negocio utiliza servicios de formación y un 36,6% manifiesta utilizar servicios de planificación e implantación de estructuras.
- En lo que a seguridad en las conexiones inalámbricas se refiere, el 77,3% de las empresas consultadas indica que protege la red wifi utilizando el protocolo WPA, WPA2. Tan sólo el 4,5% de las empresas consultadas todavía afirma contar con protección WEP y

un residual 0,2% de las empresas tienen la red wifi abierta sin protección. El 13% asegura que mantiene protección, pero desconoce el sistema.

Valoración y necesidad de soluciones de seguridad

- El 93,5% de las empresas consultadas valoran positivamente la efectividad del producto y un 93% valoran positivamente la calidad del producto. Las características que menos valoradas en general son el acceso a su contratación y la facilidad de instalación.
- Vista la distribución de las respuestas cabe indicar que para las microempresas y pequeñas empresas el acceso a la contratación y la facilidad de instalación son aspectos proporcionalmente más relevantes que otros, estando su respuesta por encima de las empresas medianas y grandes.
- Las empresas de menor tamaño valoran más la accesibilidad del producto, probablemente por la falta de tiempo o de personal especializado para abordar las cuestiones relativas a la seguridad, lo que podría indicar que buscan soluciones fáciles de gestionar. Por otro lado, las medianas y grandes empresas valoran proporcionalmente más el servicio postventa y la garantía, así como la calidad y efectividad del producto.
- El servicio más valorado como necesario es el de cumplimiento de la legislación (LOPD). En segundo lugar, un 74,4% de las empresas considera necesarios los servicios de formación, mientras un 72,3% considera la necesidad de servicios de contingencia y continuidad de negocio. Por otro lado, el servicio especializado de seguridad que se considera más prescindible es la externalización de servicios de gestión de la seguridad, dado que lo consideran necesario solo un 37,5%.
- Respecto a la existencia de alguna relación determinante entre considerar necesario un servicio y el tamaño de la empresa, cabe indicar que es directamente proporcional al tamaño para todos los servicios especializados menos en el caso de la externalización de servicios, donde las respuestas no guardan una relación proporcional.

Barreras a la implementación de medidas y soluciones de seguridad

- Se ha detectado cierta disparidad de criterios a la hora de percibir barreras a la implementación de medidas y soluciones de seguridad. El 62,2% de las empresas han realizado tan solo una mención, el 24,7% percibe dos barreras y el restante 14% tres barreras o más. Cabe resaltar, además, que un alto porcentaje de empresas ha declarado no percibir ninguna barrera a la implementación de medidas de seguridad (36,7%).
- Las barreras a la implementación de medidas y soluciones de seguridad más mencionadas por las empresas son el precio y la falta de presupuesto para un 36,1%. La falta de tiempo para el 28,8% y la falta de personal cualificado para abordar el proceso, para el 25,4%, son también barreras relevantes.
- Resulta llamativo que sean las grandes empresas las que observen la falta de personal cualificado como una barrera en mayor proporción que el resto, especialmente que las microempresas, lo

que sin duda tiene que ver con la mayor conciencia que pueden tener estas grandes empresas sobre la complejidad que supone abordar la seguridad y las capacidades que debe mantener el personal dedicado a ello en un ámbito complejo como son estas organizaciones.

INCIDENTES DE SEGURIDAD

Incidentes de ciberseguridad y consecuencias

- Las empresas españolas están bastante concienciadas de cuáles son los incidentes de seguridad y las consecuencias negativas que se pueden derivar de ellos ya que el 94,8% ha declarado conocer las consecuencias de más de cuatro incidentes.
- Las consecuencias negativas más conocidas por las empresas son las derivadas del virus con un 96,7%, seguida muy de cerca por el correo basura con un 94,6% y los troyanos con un 94,3%.
- Las medianas y grandes empresas tienen mayor conocimiento sobre las consecuencias negativas que tienen los incidentes de seguridad para su negocio que las microempresas y pequeñas empresas.
- La mayoría de las empresas consultadas ha sufrido algún tipo de incidente de seguridad a lo largo del último año. Un 30% declara no haber sufrido incidentes. El incidente de seguridad más común ha sido la afectación por código dañino con un 46,5%, en segundo lugar, la caída de los sistemas de las aplicaciones ha afectado al 28,2% de las empresas consultadas y, en tercer lugar, la caída de sistemas de soporte ha sido sufrida por el 23,4% de las empresas. Un 19,8% ha sufrido ataques informáticos.
- Existe una relación proporcional entre la frecuencia de incidentes de seguridad y el tamaño de empresa, de manera que cuanto mayor son las empresas más incidentes de seguridad manifiestan sufrir. Las PYME manifiestan en menor proporción que las grandes sufrir incidentes, lo que confirma que las grandes empresas son más conscientes de los incidentes que sufre su empresa, dado que, por lo general, cuentan con departamentos de informática y monitorizan dichos procesos.
- Además, los sectores de actividad que más han indicado haber sufrido incidentes de seguridad también son los más preparados y conscientes de los ataques que puedan sufrir, estos son el de Información y comunicaciones, el de Actividades profesionales, científicas y técnicas y el sector de Actividades administrativas y auxiliares.
- Se ha observado que cuantos más activos tecnológicos y de información gestione una empresa y más presencia en Internet haya desarrollado mediante el uso de servicios o la realización de transacciones electrónicas, la empresa abordará más riesgos de sufrir incidentes de seguridad. El propio uso de activos y servicios electrónicos expone a las empresas a los problemas de seguridad, por lo que en un entorno como el actual la seguridad TIC de la empresa se convierte en un elemento esencial para la estabilidad del negocio de las empresas.
- Por otro lado, se ha detectado que la existencia de una política de seguridad no supone que se declare que se sufren menos incidentes de seguridad, más bien al contrario, las empresas que

tienen definida una política de seguridad también sufren más incidentes de seguridad, lo que probablemente tiene que ver con la existencia de registros específicos que permiten su gestión, una mayor capacidad de aminorar sus consecuencias y una mayor consciencia de la ocurrencia concreta de los incidentes.

- Para el 61,6% de las empresas consultadas la pérdida de tiempo de trabajo fue una de las consecuencias de los incidentes de seguridad más sufrida. En segundo lugar, los problemas de conexión o de redes han sido identificados como consecuencias de los incidentes para el 31,2%, seguida de la pérdida de archivos y datos con un 30,6% de la respuesta.
- Las grandes empresas mencionan que sufren un menor número de consecuencias negativas derivadas de incidentes de seguridad. De esta forma, el hecho de que las grandes empresas sufran mayor número de incidentes de seguridad y, por el contrario, denoten menores consecuencias, refuerza la idea de que su mayor concienciación y preparación ante los incidentes minimiza las consecuencias negativas que estos tienen en su sistema.

Impacto y repercusión de los incidentes de ciberseguridad

- El impacto de los incidentes de seguridad está bastante focalizado ya que el 87% de las empresas concentra su respuesta en un solo tipo de impacto. El 94,7% de las empresas consultadas ha manifestado que las consecuencias derivadas de los incidentes tuvieron un impacto operativo en su negocio. Solo el 13,2% ha indicado haber sufrido un impacto económico-financiero, siendo poco relevantes el impacto en la imagen/reputación de la empresa (5,8%) y el impacto legal/contractual (1%).
- Se ha analizado la relación entre la percepción de consecuencias negativas de los incidentes y su impacto en las empresas, de lo que se desprende que los problemas de conexión y redes han tenido en mayor proporción un impacto en la imagen/reputación de la empresa en comparación con las demás consecuencias negativas.
- De las empresas que identificaron impacto económico de sus incidentes, tan solo el 32% manifiesta haberlo cuantificado.
- Respecto a la distribución por tamaño de las empresas y la repercusión económica de los incidentes de seguridad, existe una relación inversamente proporcional, de manera que las microempresas son las que cuantifican los daños económicos en un mayor porcentaje, 44%, seguidas de las pequeñas empresas con un 31%, frente a 29% y 27% de medianas y grandes respectivamente, si bien parecería lógico que fuesen las empresas de mayor tamaño las que estuvieran más avanzadas en la determinación del impacto económico de los incidentes que sufren.
- El grueso de las empresas ha cuantificado el perjuicio económico ocasionado por los incidentes en menos de 5.000 euros ya que el 62,8% de las empresas sitúa sus pérdidas entre menos de 1.000 euros y 5.000 euros. El 23,2% de las empresas cuantifica sus pérdidas económicas en una cifra superior a 5.000 euros.

Respuesta a los incidentes de ciberseguridad y cambio de hábitos

- El 56,5% de las empresas consultadas ha resuelto la incidencia a través de personal interno de la empresa y el 54,6% ha llamado a su proveedor local de sistemas informáticos para resolver la incidencia. En un segundo plano, las empresas han manifestado haber localizado un experto de seguridad externo a la empresa o haber llamado al proveedor de Internet en un 22,2% y un 21,3% respectivamente.
- Las empresas de mayor tamaño y del sector de Información y comunicaciones son las que más indican resolver los incidentes con personal interno mientras las pequeñas y microempresas pertenecientes al sector Servicios de alojamiento recurren a su proveedor local de sistemas informáticos en mayor proporción que las medianas y grandes.
- En lo que a cambio de hábitos como consecuencia de incidentes de seguridad se refiere, el 58,2% de las empresas ha establecido protocolos de seguridad más estrictos tras sufrir un incidente de seguridad, el 40,9% ha instalado nuevas herramientas y actualizado programas y un 37,7% ha cambiado sus contraseñas.
- Las empresas que han manifestado dejar de usar determinados servicios de Internet y haber comenzado a realizar copias de seguridad pertenecen en mayor proporción a microempresas y pequeñas empresas. Mientras, establecer protocolos y procedimientos de seguridad más estrictos y contratar servicios de auditoría externos parece ser más característico de medianas y grandes empresas.

PRIVACIDAD Y TENDENCIAS

Políticas de privacidad

- En cuanto a los servicios disponibles en la página web, el 63% de las empresas ha manifestado que su página web cuenta con una declaración política de intimidad, salvaguarda de la privacidad o certificación relacionada con la seguridad.
- Existe una relación proporcional entre las empresas que manifiestan contar con una declaración política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web y el tamaño de la empresa, de manera que cuanto mayor es la empresa, crece la afirmación de cumplir con la normativa o certificación web. Cabe destacar el porcentaje tan alto de microempresas que no saben cuál es la situación de su página web (40,2%), lo que indica el desconocimiento que mantienen este tipo de empresas sobre los requerimientos normativos.
- Las empresas que más han manifestado contar con una declaración política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web, pertenecen al sector de Actividades inmobiliarias con un 70,6% y al sector de Información y comunicaciones con un 70%.
- Por otro lado, el 88,1% de las empresas ha manifestado tener conocimiento sobre la Ley Orgánica de Protección de Datos, el 81,9% ha indicado conocer su sujeción a dicha normativa en caso de disponer de ficheros de datos personales y el 67,9% de las

empresas con ficheros de datos personales declaran disponer de documento de seguridad.

- Según su tamaño se ha observado una relación proporcional y positiva de manera que las medianas y grandes empresas han manifestado en mayor proporción que conocen la ley y su adecuación a la normativa sobre protección de datos que las pequeñas y microempresas.
- Para finalizar, el 93,6% de las empresas manifiestan informar sobre la existencia de datos personales, cumpliendo con el deber de información de la LOPD. El 90,2% de las empresas consultadas requiere el consentimiento expreso para el tratamiento de los datos personales. Y el 88,9% afirma que mantiene un procedimiento para facilitar y garantizar el derecho de acceso, rectificación, cancelación y oposición sobre los datos personales.
- La labor de sensibilización debe incidir fundamentalmente en las microempresas y las pequeñas y las medianas empresas, ya que el análisis de la distribución de respuesta sobre el conocimiento y cumplimiento de las obligaciones derivadas de la norma por tamaño de empresa indica que cuanto mayor es la empresa mayor es la proporción de empresas que manifiestan cumplir sus obligaciones.

Tendencias tecnológicas en la privacidad y la seguridad

- Se ha pretendido valorar la tendencia creciente en las relaciones laborales a orientar las tareas a la consecución de objetivos más que a la presencia física en una oficina, por lo que se ha detectado que en el ámbito laboral se utilizan cada vez más los dispositivos personales, lo que supone un creciente riesgo ya que pueden encontrarse más expuestos a ciberamenazas.
- Así lo confirma que un 73,2% de las empresas ha manifestado que el uso de dispositivos personales para el acceso a datos e información corporativos supone un riesgo que se intenta evitar.
- En este sentido, se ha identificado una tendencia a trabajar desde Internet que se ha contrastado con la percepción de las empresas de que la movilidad y el acceso remoto a los sistemas y datos corporativos desde múltiples dispositivos está incrementando la vulnerabilidad de sus activos y hace más compleja la gestión de la seguridad.
- Respecto a la irrupción del Big Data en el mundo empresarial, el 48,4% de las empresas consultadas considera que el análisis de macro datos y el uso masivo de datos representa un riesgo creciente para la privacidad de las personas y la seguridad de la información corporativa.
- En lo que respecta a los servicios en la nube, las empresas han manifestado en un porcentaje muy similar recurrir a A.N.S (acuerdos de nivel de servicio) con proveedores y adaptar su propia política de seguridad para controlar la privacidad y la seguridad de los activos de información y servicios que mantienen en la nube. No obstante, un 41,6% de las empresas consultadas todavía considera que la implementación de soluciones en la nube es un riesgo añadido para la privacidad y la seguridad de los activos de información.
- Por último, cabe resaltar positivamente que un porcentaje elevado de empresas mantienen una estrategia de análisis de datos

asociados al acceso y uso a nuestros sistemas de información, que nos ayuda a mejorar nuestra seguridad y conocer nuestras vulnerabilidades (44,3%).

- Para un porcentaje bastante alto de las empresas consultadas el uso de dispositivos personales para el acceso a datos e información, y la movilidad y el acceso remoto a sus sistemas y datos supone un riesgo. Esto supone un reto para la seguridad TIC ya que la tendencia al uso de dispositivos personales para trabajar y el acceso remoto a los sistemas y datos desde otros lugares pueden exponer a la empresa a sufrir incidentes de seguridad imprevistos.

TABLA RESUMEN PARA EL ESQUEMA DE INDICADORES DE CONFIANZA DIGITAL

A continuación, se presentan los valores obtenidos en esta encuesta del ONTSI, gran parte de ellos para completar y actualizar el Esquema de Indicadores de Confianza Digital en las Empresas.

En el caso de los indicadores incluidos y actualizados en encuestas de INE, ninguno de los valores obtenidos en la presente encuesta del ONTSI sustituye a los mismos de dicha fuente oficial.

TABLA 1: TABLA RESUMEN PARA EL ESQUEMA DE INDICADORES DE CONFIANZA DIGITAL

CIBERSEGURIDAD EN LAS EMPRESAS					
Herramientas y medidas de seguridad	**Valor total**	**Microempresas**	**Pequeñas**	**Medianas**	**Grandes**
30. Barreras a la implementación de medidas de seguridad					
Falta de personal cualificado	25,4	22,7	25,2	24,4	28,8
Falta de presupuesto	36,1	36,3	33,7	36,7	37,9
Falta de tiempo	28,8	30,8	30,1	23,9	31,2
No es de interés para la dirección	10,3	8,8	9	11,4	11,7
No lo considero económicamente rentable	4,4	7,1	6,7	3,1	1,3
No percibe ninguna barrera	36,7	33,2	35,2	41,8	35,5
Dificultad para encontrar soluciones adecuadas para mi negocio	14,9	14,2	17,2	13,3	14,9
31. Nivel de utilización del antivirus (declarado)					
Dispone	97,8	95,3	97,2	99,1	98,9
No dispone	2,2	4,7	2,8	0,9	1,1

Incidentes sobre ciberseguridad [3]	Valor total	Microempresas	Pequeñas	Medianas	Grandes
32. Incidentes de seguridad					
Ataque informático	19,8	13,3	15,8	20,5	28,5
Baja de personal crítico	4,9	2	1,6	5,1	10,5
Caída de mis sistemas/aplicaciones	28,2	17,3	20,9	33,6	38,2
Caída de sistemas de soporte	23,4	11,2	15,8	30,2	33,3
Daño físico en instalaciones/equipos	2	0,7	1,6	2,4	3,2
Falta de servicio por parte de proveedores	15,2	8,5	10,9	17,9	22
Inundación, terremoto, incendio	2,7	2	2,6	2,7	3,2
La compañía no ha sufrido ningún incidente	30	51,7	36,2	21,5	15,9
Multas, sanciones	0,8	1,4	0	1	1,1
Otros	0,4	-	0,5	0,7	0,3
Pérdida o copia de datos de negocio críticos	11,8	6,5	12,4	13,3	13,7
Afectación por código dañino	46,5	26,9	40,8	54,1	59,4
Robo de equipos	12,9	3,4	4,4	14	28
33. Consecuencias derivadas de los incidentes de seguridad					
Daños en la imagen/reputación de su negocio	3,8	3,5	2,8	4,3	4,2
Daños en mi equipo (Hardware)	17,9	22,5	22,3	15,1	15,3
Multas, sanciones	0,7	0,7	0	0,9	1
Ninguna situación de importancia	23	19	18,6	22,5	28,8
Otros	1,1	0,7	0,8	1,5	1
Pérdida de archivos y datos	30,6	26,1	38,5	28	29,1
Pérdida de tiempo de trabajo (horas)	61,6	62	65,2	62,2	58,1
Problemas de conexión/redes	31,2	35,9	30	33,2	27,8
Pérdida de confianza en los medios electrónicos	7,2	9,2	7,3	8,3	5,1
Fraude con perjuicio económico	2,2	1,4	1,6	1,8	3,5

[3] Véase "*Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*" INCIBE 2017. https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

34. Repercusión económica de las incidencias de seguridad					
Se han sufrido pérdidas económicas, pero no se han calculado	9,0	9,9	11,7	6,8	8,7
Se han sufrido pérdidas económicas y se han calculado	4,2	7,7	5,3	2,8	3,2
35. Grado de conocimiento de las incidencias de seguridad					
Correo basura	94,6	90,1	92,8	96,9	97,3
Virus	96,7	94,2	95,9	97,1	99,2
Programas espía	78,6	70,1	68,3	85,3	88,5
Troyanos	94,3	90,1	91,5	96,9	97,6
Fallos técnicos	79,4	68,7	70,9	85,7	89,8
Pérdidas de datos	87,3	79,6	83,0	91,5	93,0
Fraudes	82,4	73,8	75,5	87,2	91,2
Phising	72,2	56,1	55,4	82,6	90,9
Robos de información	74,9	60,9	64,4	83,1	87,7
Robos de identidad	75,5	66,7	64,9	80,2	88,2
Denegación de servicios	60,0	40,8	36,9	73,2	84,5
Bombas lógicas	33,8	16,7	18,3	42,8	53,6
Pharming	31,6	15,6	16,5	39,4	51,2
No conocía las consecuencias de ninguno	1,8	2,7	3,1	1,2	0,5
Preparación de empresas	**Valor total**	**Microempresas**	**Pequeñas**	**Medianas**	**Grandes**
36. Empresas que han definido formalmente una política de seguridad TIC	43,4	21,4	28,1	51,9	67,2
37. Empresas que utilizaban sistemas internos de seguridad como					
Autenticación mediante contraseña segura	86,9	76,6	82,4	93,0	93,1
Identificación de usuario y autenticación mediante elementos hardware	24,0	20,7	21,9	26,1	26,5
Identificación de usuario y autenticación mediante elementos biométricos	12,0	5,4	7,8	14,8	18,5
Backup de datos externos	81,1	69,6	75,6	85,7	91,0
Protocolos para el análisis de incidentes de seguridad	26,0	11,7	16,1	30,8	42,6

38. Riesgos que se incluyen en la política de seguridad TIC					
Destrucción o corrupción de los datos debido a un ataque o incidente inesperado	82,8	60,9	81,3	86,0	86,2
Revelación de información confidencial debido a intrusión, pharming, phising o por accidente	52,2	34,4	42,9	55,2	58,3
Problemas de funcionamiento de los servicios TIC debido a ataques externos	51,3	21,9	36,6	55,7	61,4
Ninguna	13,5	34,4	16,1	10,0	10,2
39. Estado de actualización del sistema operativo y de las herramientas de seguridad, declarado					
Ns/Nc	9,1	14,0	13,1	4,9	5,6
Actualizado	87,3	83,3	83,4	90,6	91,0
No actualizado	3,6	2,7	3,5	4,5	3,4
PRIVACIDAD DE EMPRESAS					
Relativos a la protección de datos personales	**Valor total**	**Microempresas**	**Pequeñas**	**Medianas**	**Grandes**
40. Servicios disponibles en la página web: Declaración de la política de intimidad o certificación relacionada con la seguridad del sitio web	62,7	48,8	57,0	63,9	74,0
41. Empresas con ficheros de datos personales que declaran disponer de Documento de Seguridad					
No	32,1	45,4	43,8	24,9	17,6
Sí	67,9	54,6	56,2	75,1	82,4
42. Conocimiento LOPD					
No	11,9	15,4	14,5	9,0	9,7
Sí	88,1	84,6	85,5	91,0	90,3
43. Deber de información					
No	6,4	13,0	10,4	4,0	2,2
Sí	93,6	87,0	89,6	96,0	97,8

TRANSACCIONES ELECTRÓNICAS EMPRESAS					
Relativos a las transacciones electrónicas de las empresas	**Valor total**	**Microempresas**	**Pequeñas**	**Medianas**	**Grandes**
45. Porcentaje de empresas que han realizado ventas por comercio electrónico	16,3	11,4	11,6	21,1	19,6
46. Porcentaje de empresas que utilizó firma digital para: relacionarse con sus clientes y/o proveedores	88,9	81,3	86,9	92,5	92,9
46. Porcentaje de empresas que utilizó firma digital para: relacionarse con la Administración Pública	27,0	11,4	18,6	32,2	42,6
47. Porcentaje de empresas cuyos siguientes obstáculos limitó o impidió realizar ventas a través de la web: Problemas relacionados con la seguridad TIC	9,6	7,7	9,3	9,4	11,6
47. Porcentaje de empresas cuyos siguientes obstáculos limitó o impidió realizar ventas a través de la web: Problemas relacionados con la protección de datos	8,9	6,0	8,5	8,9	11,6

4 CARACTERIZACIÓN DE LAS EMPRESAS

En este capítulo se realiza una aproximación a la realidad de las empresas españolas desde el punto de vista de los activos tecnológicos y de información que mantienen, de su comportamiento en Internet, y de su percepción de la relevancia de la seguridad TIC para sus negocios. Esta caracterización es determinante desde el punto de vista de las contingencias o incidentes de ciberseguridad, así como desde el punto de vista del establecimiento de medidas de protección de los activos y la demanda de herramientas de seguridad.

ACTIVOS TECNOLÓGICOS Y DE INFORMACIÓN

EQUIPOS INFORMÁTICOS DE SOBREMESA

93,5%

SOFTWARE Y APLICACIONES INFORMÁTICAS

86,9%

PORTÁTILES, DISPOSITIVOS MÓVILES Y TABLETS

84,6%

FICHEROS DE DATOS PERSONALES

75,4%

EQUIPOS Y REDES DE COMUNICACIONES

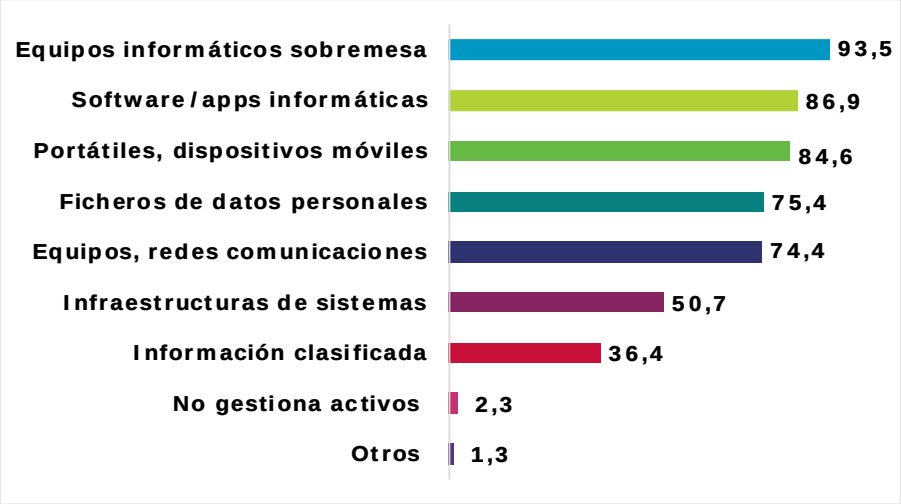
74,4%

4.1 Los activos tecnológicos y de información en las empresas

Un activo en el ámbito de la seguridad de la información, se refiere a cualquier información, sistema relacionado con su tratamiento, o soporte tecnológico que tenga valor para la organización. Son activos de información desde los dispositivos electrónicos de distinta naturaleza que contienen datos e información, hasta las personas que gestionan dicha información, así como los propios datos e información que genera la empresa en su actividad diaria. Desde el punto de vista de la seguridad, en una empresa, todos los activos deberían estar claramente identificados, con el fin de gestionar las vulnerabilidades y amenazas que se puedan derivar.

La información es una parte fundamental de toda empresa para tener un alto nivel de competitividad y desarrollo. Así lo demuestran las empresas españolas, que gestionan una media de cinco tipos de activos tecnológicos y de información, lo que acentúa el peso de los contenidos y los soportes digitales en las organizaciones. Los más mencionados son: Equipos informáticos de sobremesa (93,5%), el software y las aplicaciones informáticas (86,9%), Portátiles, dispositivos móviles y tabletas, con un 84,6%, Ficheros de datos personales (75,4%) y Equipos y redes de comunicaciones (74,4%).

FIGURA 1. PRESENCIA DE ACTIVOS TECNOLÓGICOS Y DE INFORMACIÓN EN LAS EMPRESAS. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501 P1

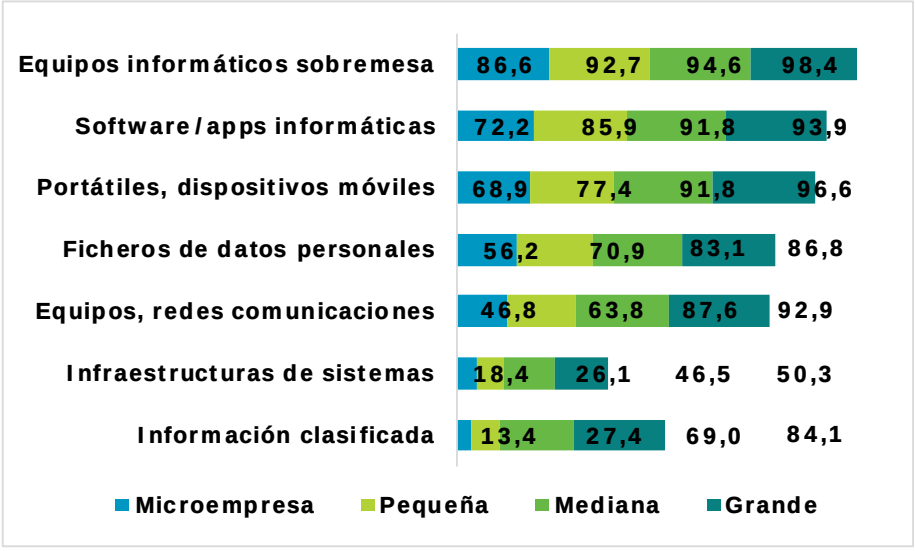
Entre los activos que aparecen con menor frecuencia se encuentran los relacionados con instalaciones e infraestructuras de sistemas (CPD), 50,7%, lo que parece lógico dado que son infraestructuras complejas que solo se desarrollan en empresas de cierto tamaño.

Igualmente, sólo un 36,4 % de las empresas menciona mantener información clasificada, sensible o confidencial, respuesta que parece escasa si se entiende que cualquier empresa podría considerar tener este tipo de información, siempre que se considere como tal, por ejemplo, la información sobre los clientes.

¿Cuál es el nivel de ciberseguridad de su empresa? Puede conocer el nivel de riesgo de sus activos con la herramienta de autodiagnóstico: https://adl.incibe.es/

Respecto a la relación entre el número de activos tecnológicos y de información que gestionan las empresas y su tamaño, se ha observado que la media de menciones de las empresas va aumentando cuanto mayor es la empresa. De manera que las microempresas señalan una media de 3,7 activos tecnológicos y de información, las pequeñas tienen 4,5 menciones, las medianas 5,7, y finalmente las grandes empresas mencionan que gestionan una media de 6,1 activos.

FIGURA 2: PRESENCIA DE ACTIVOS TECNOLÓGICOS Y DE INFORMACIÓN EN LAS EMPRESAS POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P1

El sector de actividad no es significativo para determinar si las empresas gestionan muchos tipos de activos tecnológicos y de información. Existen, no obstante sectores que están por debajo de la media en todos los activos tecnológicos y de información menos en lo que se refiere a Software y aplicaciones informáticas y Equipos informáticos de sobremesa. Estos sectores son el de la Construcción, los Servicios de comidas y bebidas, y las Actividades inmobiliarias.

4.2 Presencia en Internet y servicios electrónicos

Si los activos son los elementos objeto de protección desde el punto de vista de la seguridad, la forma en que se utiliza Internet también determina las necesidades relacionadas con la seguridad TIC.

De esta forma, la presencia web de las empresas, el comercio electrónico, o el uso de servicios en la nube, puede implicar riesgos añadidos sobre los activos en caso de que su despliegue no se realice de forma segura. Igualmente, el uso de certificados y la firma digital en las comunicaciones evita nuevos riesgos.

Es por ello que se ha preguntado a las empresas por el tipo de servicios que han desarrollado o utilizan en Internet.

PRESENCIA WEB

72,8% DE LAS EMPRESAS TIENEN PÁGINA WEB

Presencia web

Una página web es una fuente de información adaptada para la World Wide Web (WWW) y accesible mediante un navegador de Internet. Esta Información se presenta generalmente en formato HTML y puede contener hiperenlaces a otras páginas web, constituyendo la red enlazada de la World Wide Web. La existencia de una página web en una empresa permite deducir que puede sufrir determinadas amenazas derivadas de su presencia en Internet.

Las empresas españolas tienen una presencia web relevante ya que el 72,8% declaran tener una página web. El valor de este indicador obtenido en la "Encuesta sobre el uso de las tecnologías de la información y las comunicaciones y del comercio electrónico en las empresas" realizada por el Instituto Nacional de Estadística INE para el año 2015, es idéntico al obtenido en este estudio.

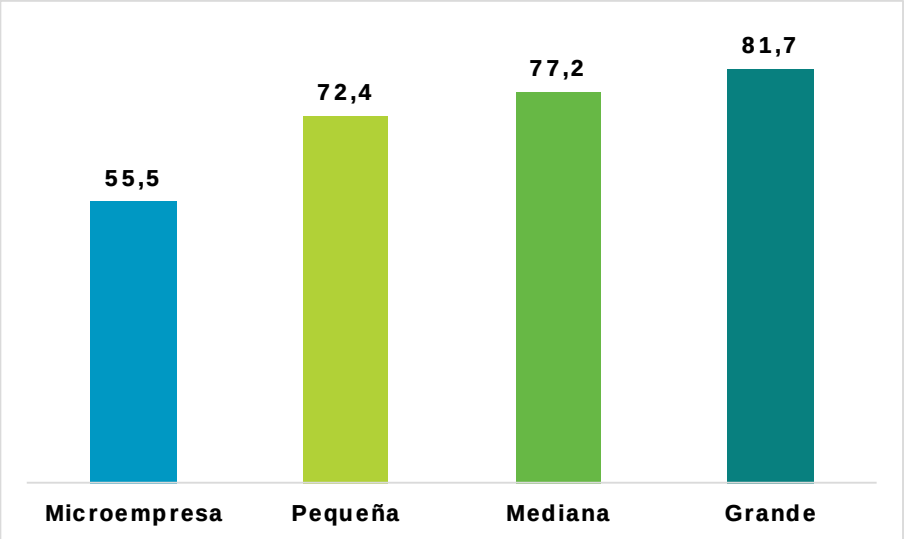
La web es su tarjeta de presentación, puede protegerla adecuadamente:
https://www.incibe.es/protege-tu-empresa/blog/tu-web-tu-tarjeta-presentacion-protegela
Además puede consultar el dosier específico:
https://www.incibe.es/protege-tu-empresa/que-te-interesa/protege-tu-web

Respecto a la presencia web por tamaño de empresa, parece haber una relación positiva entre la presencia web y el número de trabajadores de la empresa. Así, las empresas de menos de 50 trabajadores tienen una presencia web por debajo de la media. Las microempresas (menos de 10 trabajadores) manifiestan que su presencia web es 20 puntos porcentuales por debajo de la media.

Los datos desagregados por tamaño no son comparables con los indicados por el INE por los motivos metodológicos relacionados con el universo al que va dirigido el estudio.[4] El indicador del INE recoge la siguiente distribución por tamaño de la presencia web: Microempresa 31,4%, Pequeña 74,8%, Mediana 89,5% y Grande 95,2%.

[4] El INE recoge un porcentaje bastante menor de microempresas con presencia web, dato que posiblemente es consecuencia de la inclusión de los autónomos en la muestra.

FIGURA 3: PRESENCIA WEB POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P2

SECTORES QUE MÁS HAN INDICADO TENER PRESENCIA WEB

INFORMACIÓN Y COMUNICACIONES

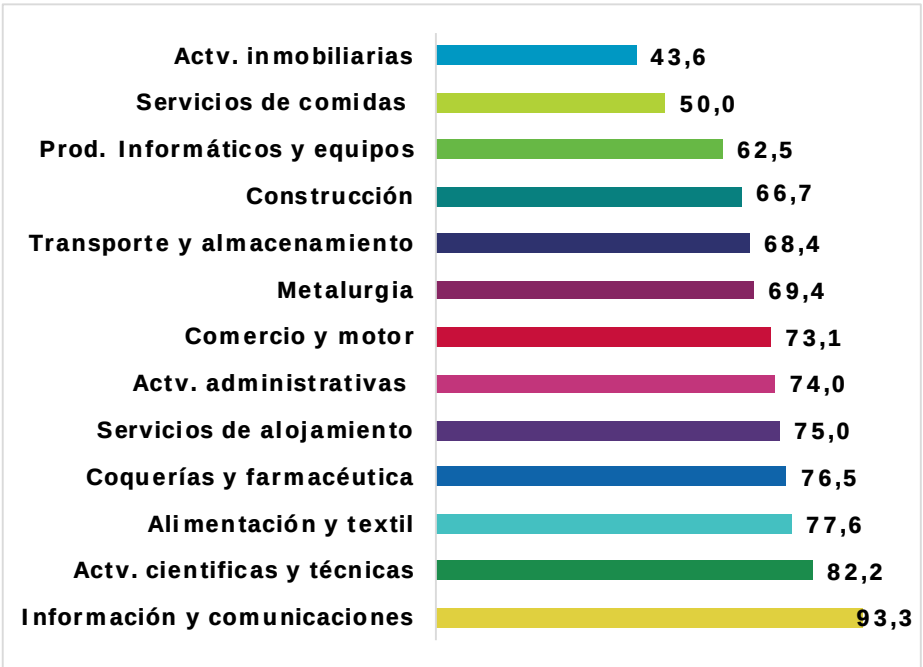
93,3%

ACTIVIDADES PROFESIONALES, CIENTÍFICAS Y TÉCNICAS

82,2%

A continuación, se muestra la respuesta sobre la presencia web distribuida por sector de actividad de las empresas.

FIGURA 4: PRESENCIA WEB POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104. P2

SECTORES QUE MENOS HAN INDICADO TENER PRESENCIA WEB

ACTIVIDADES INMOBILIARIAS

43,6%

SERVICIOS DE COMIDAS Y BEBIDAS

50%

Todos los sectores empresariales están expuestos a riesgos de ciberseguridad. Es importante conocer los aspectos de seguridad que afectan a su sector: https://www.incibe.es/protege-tu-empresa/blog/conoces-los-aspectos-ciberseguridad-tu-sector-ahora-puedes

Los sectores que muestran una presencia web más elevada son el sector de Información y comunicaciones, con un 93,3% de empresas con página web, y el sector de Actividades profesionales, científicas y técnicas con un 82,2%. Por otra parte, los sectores con menos presencia web son el sector de Actividades inmobiliarias con un 43,6% y el de Servicios de comidas y bebidas, con un 50%.

Firma digital

Empresas que utilizan firma digital en alguna comunicación de la empresa, para relacionarse con la Administración Pública o para relacionarse con clientes/proveedores (Indicador 46 en el "Esquema de Indicadores de Confianza Digital en España", en adelante EICDE)

La firma digital es una información cifrada que identifica al autor de un documento electrónico y autentifica su identidad. Al igual que las firmas manuales, es única y específica de un usuario y o un ordenador. El uso de la firma digital en una empresa indica el grado de madurez de la organización en lo que se refiere al uso de documentos electrónicos como alternativa al papel.

El uso de la firma digital forma parte del área de indicadores relativos a las transacciones electrónicas de las empresas en el esquema EICDE. Este indicador se viene recogiendo en la "Encuesta sobre el uso de las tecnologías de la información y las comunicaciones y del comercio electrónico en las empresas"[5], realizada por el INE desde 2001, aunque los datos obtenidos en este caso no son plenamente comparables debido a las diferencias metodológicas entre la encuesta del INE y la de este estudio[6].

El indicador obtenido por la encuesta del INE está desagregado por tamaño, por un lado el dato total para pequeñas, medianas y grandes

[5] "*Encuesta sobre el uso de las tecnologías de la información y las comunicaciones y del comercio electrónico en las empresas*" INE 2015-16. http://www.ine.es/dynt3/inebase/es/index.htm?type=pcaxis&path=/t09/e02/a2015-2016&file=pcaxis&dh=0&capsel=0

[6] La diferencia en los valores de indicadores obtenidos por el INE se debe a que esta encuesta utiliza un filtro dicotómico al preguntar por las empresas que utilizan la firma digital en alguna comunicación enviada por su empresa, para después preguntar por las que se dirigen a la Administración Pública y a clientes o proveedores. En el caso del presente estudio, sin embargo, en aras de simplificar la formulación y precisar la respuesta, los datos se han recogido mediante una pregunta multirespuesta dirigida a una batería de servicios relativos a las transacciones electrónicas y el uso de servicios electrónicos por parte de las empresas. Esta diferencia metodológica impide la comparabilidad exacta de los datos obtenidos por el INE y los obtenidos por el ONTSI, por lo que el indicador que ha de servir de referencia es el generado por el INE.

empresas, y del otro para microempresas, de esta forma, el 75,06% de las pequeñas, medianas y grandes empresas utilizaron la firma electrónica para alguna comunicación enviada desde su empresa, de estas el 98,85% la dirigió a la Administración Pública y el 27,26% utilizó la firma con clientes proveedores. De otro lado, el 44,2% de las microempresas manifestaron utilizar la firma electrónica para alguna comunicación enviada desde su empresa, el 98,1% la dirigió a la Administración Pública y el 15,5% a clientes o proveedores.

En lo que se refiere a los resultados de la encuesta que da soporte a este estudio, se ha obtenido el indicador para el total de empresas, por un lado, y el indicador desagregado por tamaño de empresa por otro.

USO FIRMA DIGITAL

Así, el 89,7% del total de las empresas afirman utilizar la firma digital para relacionarse con la Administración o con clientes y proveedores.[7]

89,7%

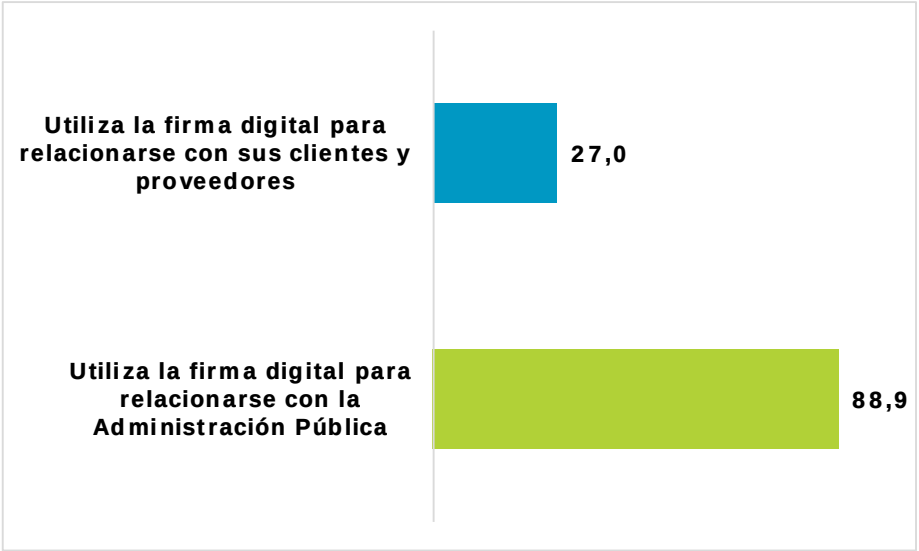
DE LAS EMPRESAS AFIRMA UTILIZAR LA FIRMA DIGITAL:

PARA RELACIONARSE CON LA ADMINISTRACIÓN PÚBLICA

88,9%

A pesar de la obligatoriedad de las empresas con personalidad jurídica propia de relacionarse con la Administración a través de la firma digital, solo un 88,9% declara utilizar este servicio, lo que podría estar relacionado con que, en muchos casos, las empresas subcontratan los servicios vinculados a la relación electrónica con la Administración (Declaraciones tributarias periódicas, cotizaciones a la Seguridad Social, etc.). Por otra parte, un 27% utiliza este servicio con clientes y/o proveedores.

FIGURA 5: USO DE LA FIRMA DIGITAL. RESPUESTA EXPRESADA EN %



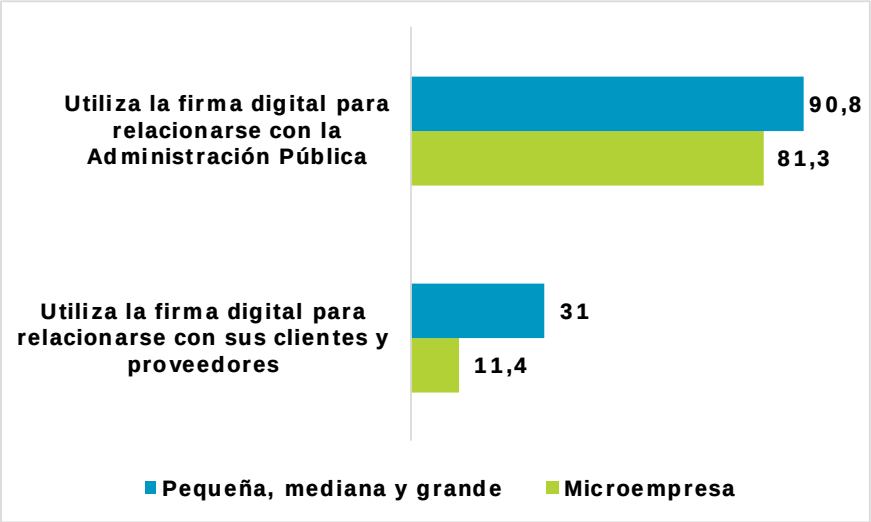
Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501 P2

En cuanto a los datos desagregados por tamaño, el 91,8% de las pequeñas, medianas y grandes empresas consultadas indican utilizar la firma electrónica. A su vez el 90,8% la utilizan en sus relaciones con la Administración Pública, siendo algo inferior el dato (8 puntos porcentuales) al ofrecido por el INE. Por el contrario, el 31% la utiliza en sus relaciones con clientes y proveedores, siendo en este caso el dato 4 puntos porcentuales superior al ofrecido por el INE.

[7] Este indicador recoge la suma de las empresas que se han referido a alguna de las opciones de respuesta relacionadas con la firma digital. No se corresponde y no es comparable con el indicador relacionado con la pregunta dicotómica del INE sobre si la empresa utiliza la firma digital en alguna comunicación de la empresa.

De otro lado, el uso de la firma digital es menor entre las microempresas, siendo el 82,9% las que indican utilizarla. En este caso el 81,3% indica que lo hace en las relaciones con la Administración pública, dato bastante inferior al recogido por el INE, mientras que el 11,4% la utiliza para relacionarse con clientes o proveedores, dato que se aproximaría algo más al indicador ofrecido por la encuesta del INE.

FIGURA 6: USO DE LA FIRMA DIGITAL POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña, mediana y grande 1.202. P2

El secreto de la robustez de los certificados digitales es que el propietario o suscriptor del certificado debe ser el único en conocer su clave privada, ya que de no ser así no se podría asegurar la identidad del mismo. La firma digital permite identificarse, a usted o su empresa, de forma unívoca: https://www.incibe.es/protege-tu-empresa/blog/certificado-digital-identificar

EL SECTOR QUE UTILIZA MÁS LA FIRMA DIGITAL ES EL DE ACTIVIDADES ADMINISTRATIVAS Y SERVICIOS AUXILIARES

95,2%

EL SECTOR QUE MENOS UTILIZA LA FIRMA DIGITAL ES EL DE SERVICIOS DE COMIDAS Y BEBIDAS

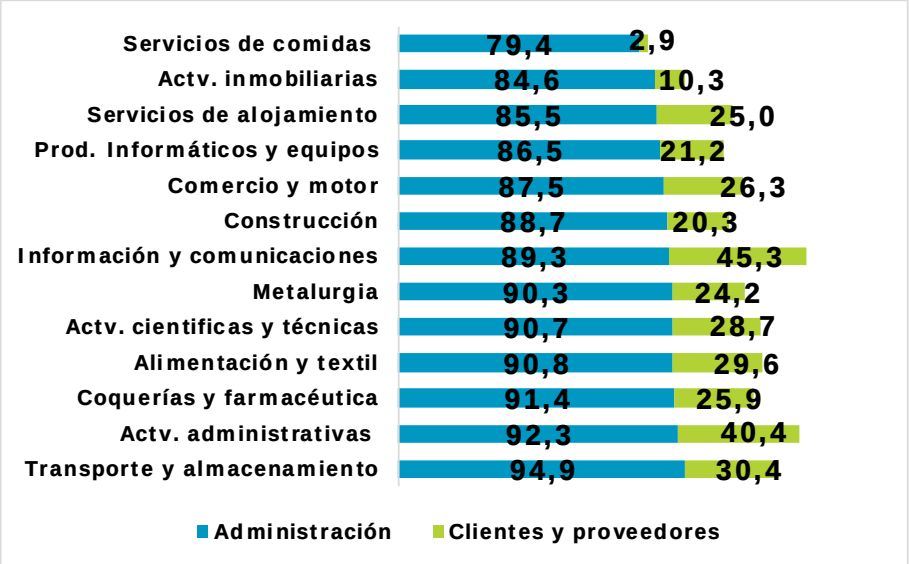
79,4%

No existen diferencias sectoriales que supongan una relación significativa entre el tipo de actividad que desarrolla la empresa y el uso de la firma electrónica.

El sector que más utiliza la firma digital es el de Actividades administrativas y servicios auxiliares con un 95,2% y el sector que menos la utiliza es el de Servicios de comidas y bebidas con un 79,4%.

El siguiente gráfico muestra la distribución sectorial del uso de la firma electrónica para relacionarse con la Administración y para relacionarse con clientes y proveedores.

FIGURA 7: USO DE LA FIRMA DIGITAL POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P2

EL SECTOR QUE UTILIZA MÁS LA FIRMA DIGITAL **PARA RELACIONARSE CON LA ADMINISTRACIÓN** ES EL DE TRANSPORTE Y ALMACENAMIENTO

94,9%

EL SECTOR QUE MÁS UTILIZA LA FIRMA DIGITAL **PARA RELACIONARSE CON CLIENTES O PROVEEDORES** ES EL DE INFORMACIÓN Y COMUNICACIONES CON UN

45,3%

El uso de la firma electrónica para relacionarse con la Administración es más homogéneo entre sectores en comparación con el uso para relacionarse con clientes y proveedores lo cual está relacionado con la obligatoriedad del uso con la Administración. El sector que más utiliza la firma electrónica para relacionarse con la Administración es el de Transporte y almacenamiento con un 94,9%, por el contrario, el que menos la utiliza es el sector de Servicios de comidas y bebidas con un 79,4%. Además, este último es también el sector que menos utiliza la firma electrónica para relacionarse con clientes y proveedores.

Por otra parte, el sector que más utiliza la firma electrónica para relacionarse con clientes y proveedores es el de la Información y comunicaciones (45,3%), seguido por las empresas del sector de Actividades administrativas y auxiliares (40,4%).

Comercio electrónico

VENTAS POR COMERCIO ELECTRÓNICO

16,3%

DE LAS EMPRESAS HAN REALIZADO VENTAS POR COMERCIO ELECTRÓNICO

Empresas que han realizado ventas por comercio electrónico (Indicador 45 en EICDE)

La venta a través del comercio electrónico forma parte también del área de indicadores relativos a las transacciones electrónicas de las empresas en el esquema de EICDE. Este indicador fue medido por la Encuesta 2015-16 del INE, en adelante "ETICce", de forma desagregada por tamaño, de un lado, pequeñas, medianas y grandes y del otro, microempresas, de igual forma que el indicador de firma electrónica descrito en el apartado anterior.

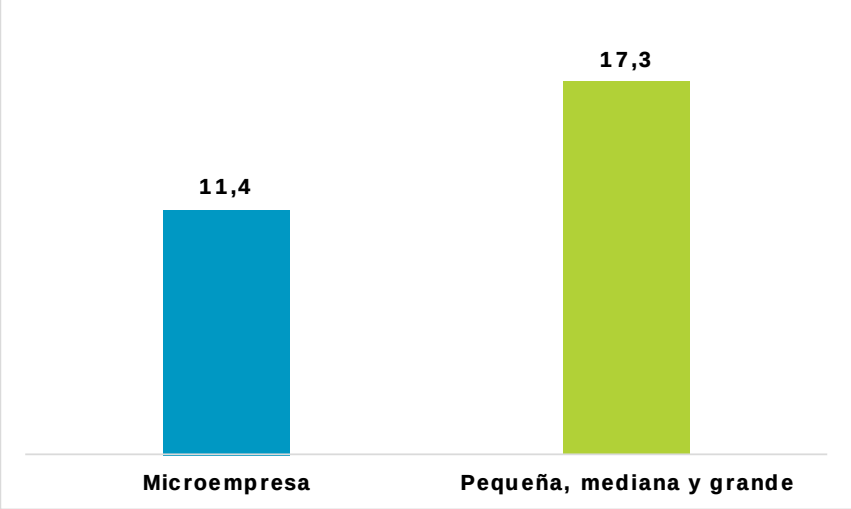
El resultado del INE fue que un 20,4% de las pequeñas, medianas y grandes empresas manifestó realizar ventas por comercio electrónico, en contraste con el 4,2% de las microempresas.

En el estudio que nos ocupa, se ha obtenido en primer lugar el dato para el total de empresas consultadas, de forma que, el 16,3% ha manifestado realizar ventas por comercio electrónico.

El comercio electrónico adquiere cada vez más importancia en muchas empresas, por esta razón es conveniente introducir al empresario en las medidas de seguridad necesarias, que toda tienda de comercio electrónico debe tener. INCIBE dispone de una guía que recoge los aspectos más importantes para proteger su tienda online: https://www.incibe.es/protege-tu-empresa/guias/guia-ciberseguridad-comercio-electronico

En lo referente a los datos desagregados por tamaño, el 17,3% de las pequeñas, medianas y grandes empresas ha declarado realizar ventas por comercio electrónico, dato muy similar al obtenido por el INE (20,4%). Sin embargo, el 11,4% de las microempresas ha manifestado realizar ventas a través del comercio electrónico, dato sensiblemente superior al obtenido por el INE (4,2%). De nuevo esto puede deberse a las diferencias metodológicas, concretamente a la formulación de la pregunta[8].

FIGURA 8: VENTAS POR INTERNET POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña, mediana y grande 1. 202.P2

LAS EMPRESAS QUE MÁS HAN MANIFESTADO REALIZAR VENTAS POR COMERCIO ELECTRÓNICO PERTENECEN A LOS SECTORES DE

SERVICIOS DE ALOJAMIENTO

42,1%

COMERCIO Y MOTOR

24,4%

INFORMACIÓN Y COMUNICACIONES

22,7%

En lo que a la distribución sectorial se refiere, el sector que más ventas por comercio electrónico realiza es el de Servicios de alojamiento (42,1%), lo que podría explicarse por el peso que han

[8] En la encuesta del INE se pregunta si la empresa recibió pedidos/reservas de bienes o servicios a través de comercio electrónico mediante páginas web o aplicaciones móviles y especifica el enunciado "excluyendo correos electrónicos escritos manualmente", mientras que en la encuesta que nos ocupa se pregunta por las ventas sin concretar el medio ni precisar el modo. Esta diferencia obliga a reconsiderar la formulación de la pregunta en un futuro.

estado adquiriendo en los últimos años las reservas *online*. En segundo lugar, se sitúa el sector de Comercio al por mayor, al por menor y venta y reparación de vehículos de motor (24,4%) y a continuación el sector de la Información y comunicaciones (22,7%). El sector de la Información y comunicaciones se muestra especialmente ligado al comercio electrónico ya que además de ser uno de los que más vende por Internet también es el que más compras realiza.

FIGURA 9: VENTAS POR INTERNET POR SECTOR. RESPUESTA EXPRESADA EN %

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P2

Es importante estar al día acerca de las amenazas de Internet. Con el servicio de avisos de seguridad para empresas de INCIBE, es posible: https://www.incibe.es/protege-tu-empresa/blog/estar-al-dia-las-amenazas-ciberseguridad-nuestro-servicio-avisos

EMPRESAS PARA LAS QUE ALGÚN PROBLEMA DE SEGURIDAD TIC O PROTECCIÓN DE DATOS OBSACULIZÓ REALIZAR VENTAS A TRAVÉS DE INTERNET

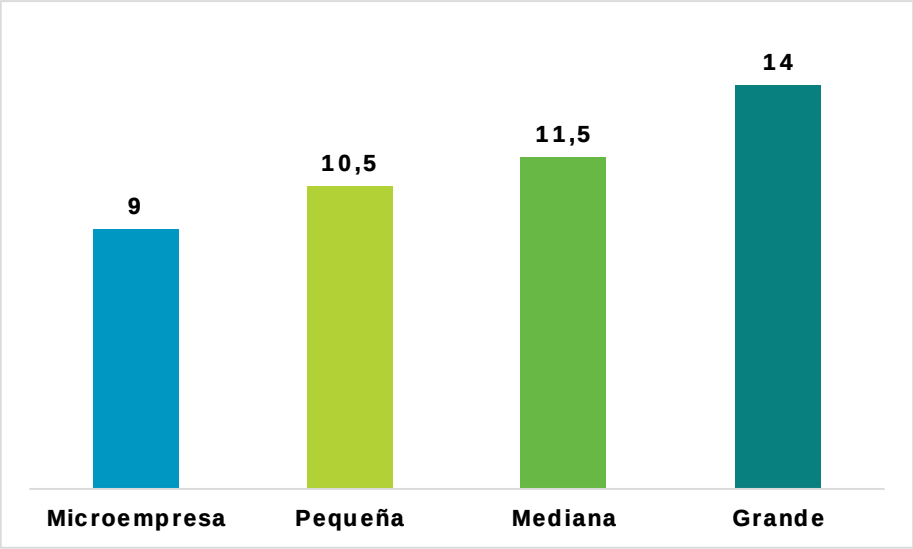
11,4%

Porcentaje de empresas para las que algún problema de seguridad TIC o protección de datos limitó u obstaculizó realizar ventas a través de Internet (Indicador 47 en EICDE)

La seguridad TIC y la protección de datos no limitan a la generalidad de las empresas a la hora de realizar ventas por Internet, un 11,4% de las empresas declara que ha experimentado alguna vez algún problema relacionado con Seguridad TIC o protección de datos que haya limitado u obstaculizado sus ventas.

Por otra parte, cuanto mayor es la empresa más manifiesta que algún problema de seguridad TIC o protección de datos ha limitado u obstaculizado sus ventas a través de Internet, lo que puede deberse a que las empresas más grandes son las que más realizan ventas a través de Internet y, por tanto, estarían expuestas en mayor proporción a posibles problemas.

FIGURA 10: EMPRESAS POR TAMAÑO PARA LAS QUE ALGÚN PROBLEMA DE SEGURIDAD TIC O PROTECCIÓN DE DATOS LIMITÓ U OBSTACULIZÓ REALIZAR VENTAS A TRAVÉS DE INTERNET EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378.P3.1.1 y P3.1.2

Uso de servicios en la nube

USO DE SERVICIOS EN LA NUBE

66,6%

DE LAS EMPRESAS UTILIZAN SERVICIOS EN LA NUBE

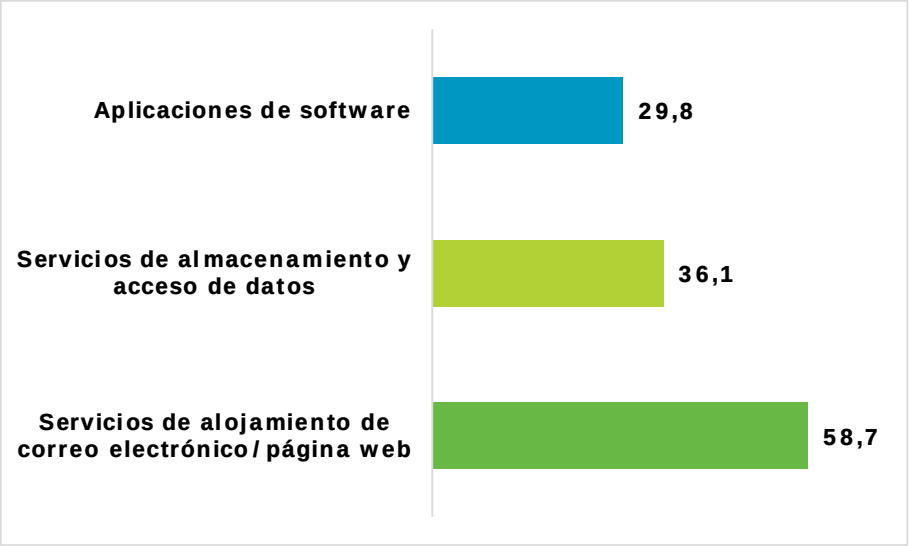
Los denominados servicios en la nube se refieren a los servicios TIC que son usados mediante el alojamiento en servidores de Internet para tener acceso a software, capacidad de computación, capacidad de almacenamiento, etc.

Los servicios en la nube suponen una fuente de ahorro para las empresas ya que ofrecen un modelo de consumir tecnología como servicio (aplicaciones, computación y almacenamiento) sin necesidad de realizar una gran inversión y evitando dedicar tiempo al mantenimiento y actualización de su infraestructura tecnológica. Es por ello que la seguridad TIC y la accesibilidad en este tipo de servicios se tornan sustanciales.

El 66,6% de las empresas españolas utiliza servicios en la nube. Estos se han dividido en tres grupos atendiendo al tipo de servicio que ofrecen con el objetivo de precisar la respuesta.

Los servicios “en la nube” son cómodos y accesibles, e incluso en caso de pago por uso o no-gratuitos, permiten evitar importantes inversiones en hardware, software y personal técnico propio, no obstante, se ha de conocer los detalles antes de contratarlos: https://www.incibe.es/protege-tu-empresa/blog/12-preguntas-seguridad-antes-contratar-cloud

FIGURA 11: USO DE SERVICIOS EN LA NUBE. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501 P2

58,7%
DE LAS EMPRESAS UTILIZA SERVICIOS DE ALOJAMIENTO DE CORREO ELECTRÓNICO Y/O PÁGINA WEB EN LA NUBE

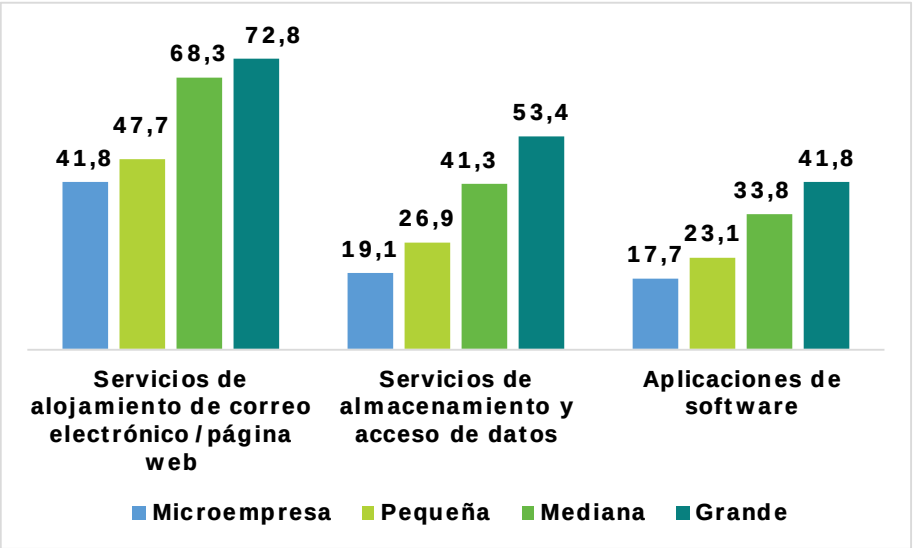
36,1%
UTILIZA SERVICIOS DE ALMACENAMIENTO Y ACCESO DE DATOS

29,8%
CONTRATA APLICACIONES DE SOFTWARE COMO SERVICIO EN LA NUBE

El servicio más utilizado por las empresas es el de Alojamiento de correo electrónico y/o página web con un 58,7%. En segundo lugar, el 36,1% contrata servicios en la nube de almacenamiento, de acceso de datos y contenidos de información, en remoto. Y, por último, el 29,8% contrata aplicaciones de software como servicio en la nube.

En lo que a tamaño de empresa se refiere, se ha observado que cuanto mayor es la empresa más utiliza servicios en la nube, ya sea servicios de alojamiento, almacenamiento o aplicaciones.

FIGURA 12: USO DE SERVICIOS EN LA NUBE POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P2

Cabe sin embargo indicar que es posible que la respuesta de algunas empresas y especialmente las microempresas esté desvirtuada, en la medida que no sean conscientes de que utilizan servicios de este tipo.

Se da el caso por ejemplo que existen servicios de correo electrónico gratuitos en la nube, que no se contratan conscientemente dado que son de carácter gratuito. Lo mismo ocurre con servicios de almacenamiento, por ejemplo, Google Drive o Dropbox.

En cuanto al uso de servicios en la nube por sector de actividad existen diferencias según el tipo de servicio que se analice. En el uso de los servicios de alojamiento de correo electrónico y/o página web no existen grandes variaciones por sector en comparación con los otros dos tipos de servicios que son más dispares.

LAS EMPRESAS QUE MÁS HAN INDICADO UTILIZAR SERVICIOS EN LA NUBE PERTENECEN A LOS SECTORES DE

INFORMACIÓN Y COMUNICACIONES

55,5%

ACTIVIDADES ADMINISTRATIVAS Y SERVICIOS AUXILIARES

54,5%

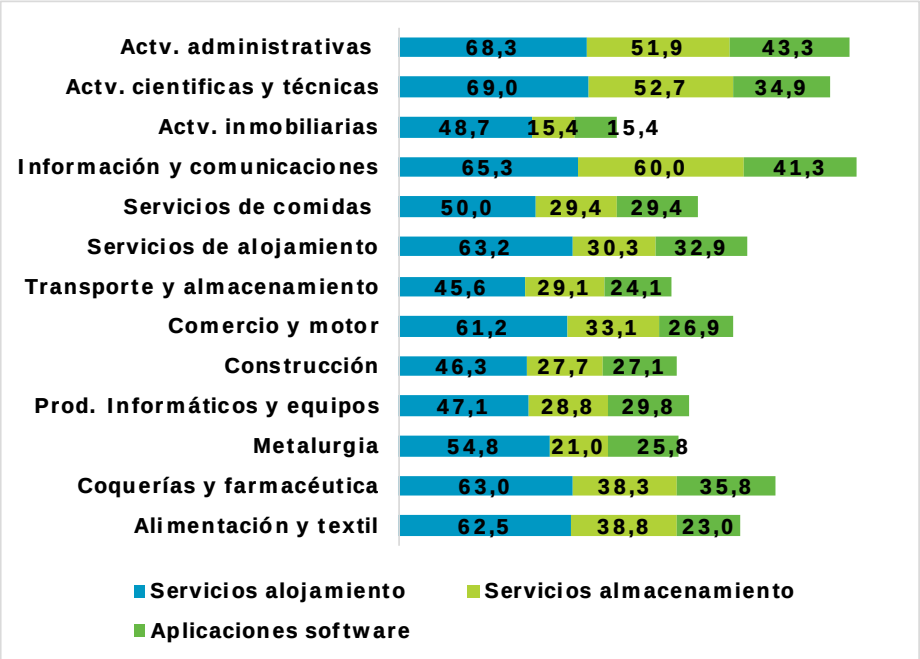
ACTIVIDADES PROFESIONALES, CIENTÍFICAS Y TÉCNICAS

52,2%

Los sectores que más usan servicios de alojamiento son: Actividades profesionales, científicas y técnicas (69,0%), Actividades administrativas y servicios auxiliares (68,3%) e Información y comunicaciones (65,3%). Los sectores que menos utilizan estos servicios son los de: Transporte y almacenamiento (45,6%), Construcción (46,3%) y Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor (47,1%).

Los sectores que más utilizan servicios de almacenamiento son: Información y comunicaciones (60,0%), Actividades profesionales, científicas y técnicas (52,7%) y Actividades administrativas y servicios auxiliares (51,9%). Los que menos utilizan servicios de almacenamiento son los sectores de las Actividades inmobiliarias (15,4%), de la Metalurgia y fabricación de productos metálicos (21,0%) y el de la Construcción (27,7%).

FIGURA 13: USO DE SERVICIOS EN LA NUBE POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P2[9]

[9] La categoría Servicios alojamiento se refiere a los servicios de alojamiento de correo electrónico y/o página web y la categoría Servicios de almacenamiento a la de servicios de almacenamiento y acceso de datos.

Por último, los sectores que más utilizan aplicaciones de software como servicio en la nube son: Actividades administrativas y servicios auxiliares (43,3%), Información y comunicaciones (41,3%) y Actividades profesionales, científicas y técnicas (34,9%). Por el contrario, los que menos usan estas aplicaciones son: Actividades inmobiliarias (15,4%), Metalurgia y fabricación de productos metálicos (25,8%) y Comercio al por mayor, al por menor y venta y reparación de vehículos de motor (26,9%).

En resumen, los sectores que más utilizan servicios en la nube, tanto de alojamiento como de almacenamiento y de aplicaciones software son: Información y comunicaciones, Actividades administrativas y servicios auxiliares y Actividades profesionales, científicas y técnicas. Los sectores que menos utilizan servicios en la nube son el de Actividades inmobiliarias, Transporte y almacenamiento y el de la Construcción.

En términos generales, la presencia en Internet y el uso de servicios electrónicos es proporcional al tamaño de la empresa para todos los casos, exceptuando el comercio electrónico, de manera que cuanto más grande es la empresa más indica tener presencia en Internet y usar servicios electrónicos como la firma digital o los servicios en la nube.

Los sectores de actividad que destacan en la presencia en Internet y el uso de servicios electrónicos son el de Información y comunicación, Actividades administrativas y servicios auxiliares y Actividades profesionales, científicas y técnicas.

4.3 Preparación de las empresas

PRIORIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

29%

DE LAS EMPRESAS CONSIDERAN QUE LA SEGURIDAD DE LA INFORMACIÓN ES UNA MÁXIMA PRIORIDAD EN SU EMPRESA

57,9%

CONSIDERA QUE TIENE UNA PRIORIDAD ELEVADA

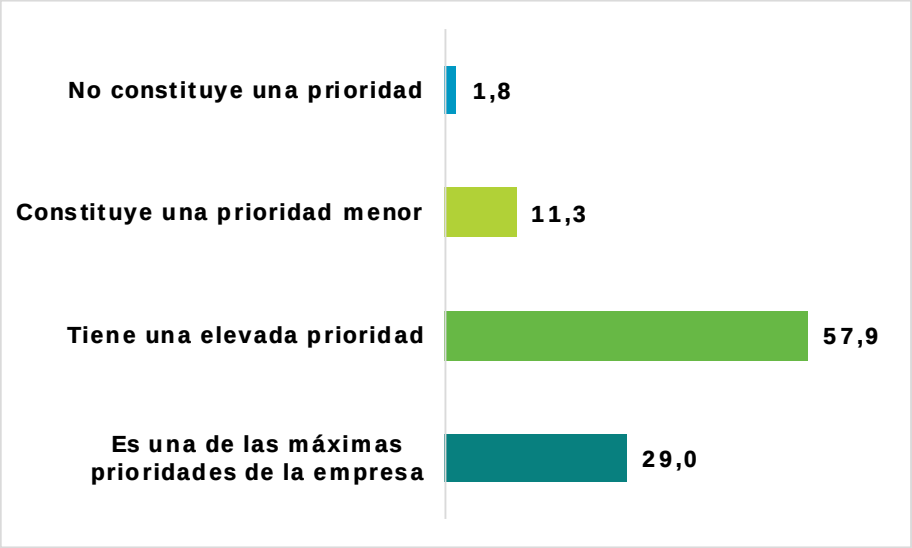
La seguridad de los activos tecnológicos y de información, así como la gestión de los incidentes que se puedan producir están determinados por la preparación de las empresas para prevenir su ocurrencia, los riesgos y contingencias, y abordar su solución, lo que entre otras cosas requiere reconocer que se pueden producir estos problemas de ciberseguridad, y por tanto integrar la seguridad TIC como ámbito de gestión y actuación por parte de la empresa.

Para valorar la preparación de las empresas españolas en lo que se refiere a abordar estas situaciones, cada vez más complejas relacionadas con la seguridad TIC, en el ámbito de la sociedad de la información y el conocimiento, se ha preguntado a las empresas por su percepción de la relevancia de la seguridad TIC y de la protección de los activos de la empresa y por el estado de actualización de sistemas operativos y programas.

Percepción de la relevancia de la seguridad TIC y de la protección de los activos de la empresa

Para la mayoría de las empresas españolas la seguridad de la información constituye una prioridad, ya que el 29% afirma que constituye una de las máximas prioridades de su empresa y el 57,9% asegura que la seguridad de la información tiene una elevada prioridad para su empresa.

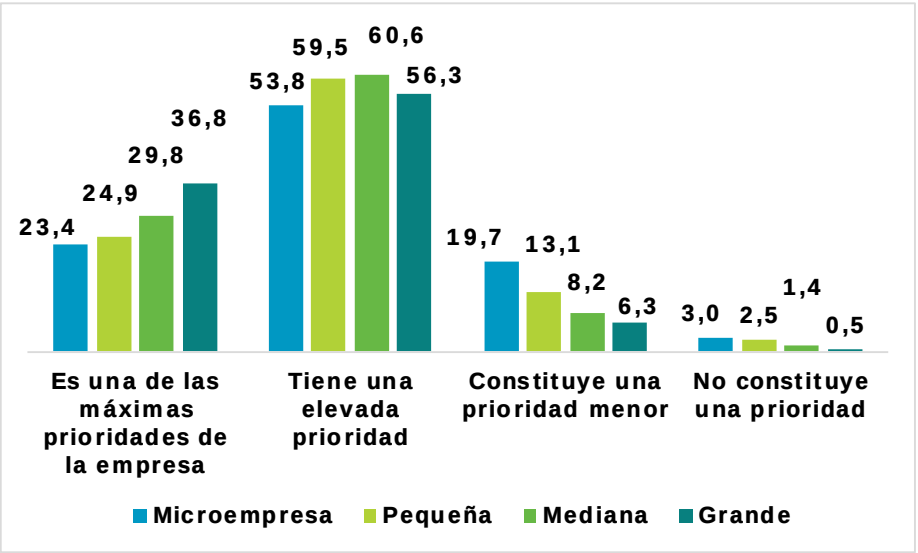
FIGURA 14: GRADO DE PRIORIDAD DE LA SEGURIDAD DE LA INFORMACIÓN. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501 P3

Que la seguridad TIC sea una de las máximas prioridades de la empresa está relacionado de manera significativa y proporcional con el tamaño de la empresa, de manera que las grandes y medianas empresas lo consideran una prioridad máxima en mayor medida que las microempresas y las pequeñas empresas. Conforme va disminuyendo el tamaño de la empresa va aumentando la consideración de que la seguridad TIC constituye una prioridad menor.

FIGURA 15: GRADO DE PRIORIDAD DE LA SEGURIDAD DE LA INFORMACIÓN POR TAMAÑO. RESPUESTA EXPRESADA EN %

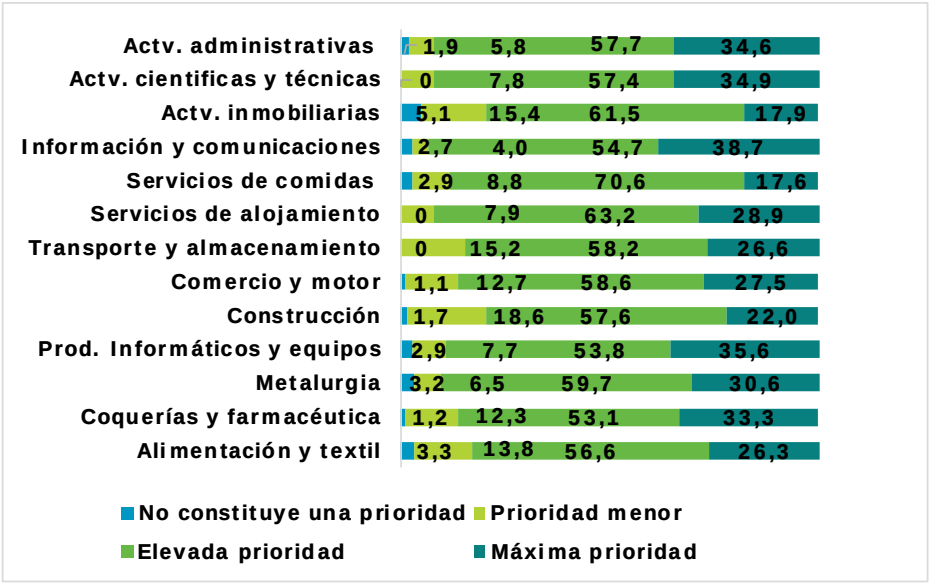


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P3

Se puede afirmar que existe una relación proporcional y positiva entre considerar la seguridad TIC como una prioridad y el tamaño de la empresa.

La ciberseguridad es una inversión a futuro.
Si quiere conocer su nivel de riesgo y si el asegurar sus activos está entre sus prioridades, puede realizar un rápido análisis con la herramienta de autodiagnóstico de INCIBE:
https://adl.incibe.es/

FIGURA 16: GRADO DE PRIORIDAD DE LA SEGURIDAD DE LA INFORMACIÓN POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base ya referida. P3

EL SECTOR QUE MÁS CONSIDERA LA SEGURIDAD DE LA INFORMACIÓN COMO MÁXIMA PRIORIDAD CON UN

38,7%

ES EL DE INFORMACIÓN Y COMUNICACIONES

Y UN

18,6%

DEL SECTOR SE LA CONSTRUCCIÓN LO CONSIDERA UNA PRIORIDAD MENOR

El análisis del grado de prioridad de la seguridad de la información por sectores de actividad evidencia un comportamiento similar entre sectores con la creencia generalizada de que la seguridad de la información es una prioridad para la empresa.

Entre los sectores que consideran que la seguridad TIC es una máxima prioridad en la empresa destaca el de Información y comunicaciones (38,7%) y entre los que consideran que tiene una elevada prioridad el de Servicios de comidas y bebidas representa el porcentaje más alto con un 70,6%. El sector que otorga menos prioridad a la seguridad de la información es el de la Construcción con un 18,6%.

La prioridad en la seguridad de la información está directamente relacionada con el número de activos tecnológicos y de información que gestiona una empresa, de manera que cuantos menos activos tecnológicos y de información dice gestionar menos considerará la seguridad de la información como una prioridad.

Las empresas que consideran la seguridad de la información como una prioridad elevada o máxima son las que gestionan más activos tecnológicos y de información. Todo ello parece indicar que son las empresas más conscientes en lo que se refiere a los activos que gestionan, las que muestran estar más preparadas.

ESTADO DE ACTUALIZACIÓN DE LOS SISTEMAS OPERATIVOS Y HERRAMIENTAS DE SEGURIDAD

87,3%

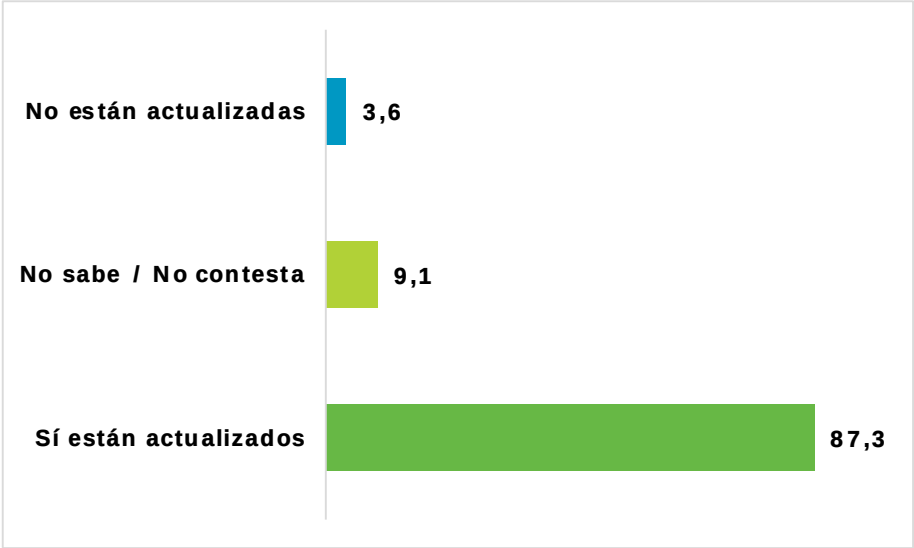
DECLARA TENERLOS ACTUALIZADOS

Estado de actualización de sistemas operativos y programas (Indicador 39 en EICDE)

Un sistema operativo es un programa o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes. La mayoría de aparatos electrónicos que utilizan microprocesadores para funcionar, llevan incorporado un sistema operativo (teléfonos móviles, reproductores de DVD, ordenadores, radios, enrutadores, etc.). La actualización del sistema operativo permite disminuir la vulnerabilidad de los dispositivos electrónicos.

El resultado del indicador es que el 87,3% de las empresas declaran tener los sistemas y programas actualizados. Por otra parte, llama la atención que haya un porcentaje mayor de empresas que "No saben o no contestan", que de empresas que afirman no tener los sistemas operativos y las herramientas actualizadas, de lo que se desprende que un volumen sustancial de las empresas desconoce si sus sistemas están debidamente actualizados.

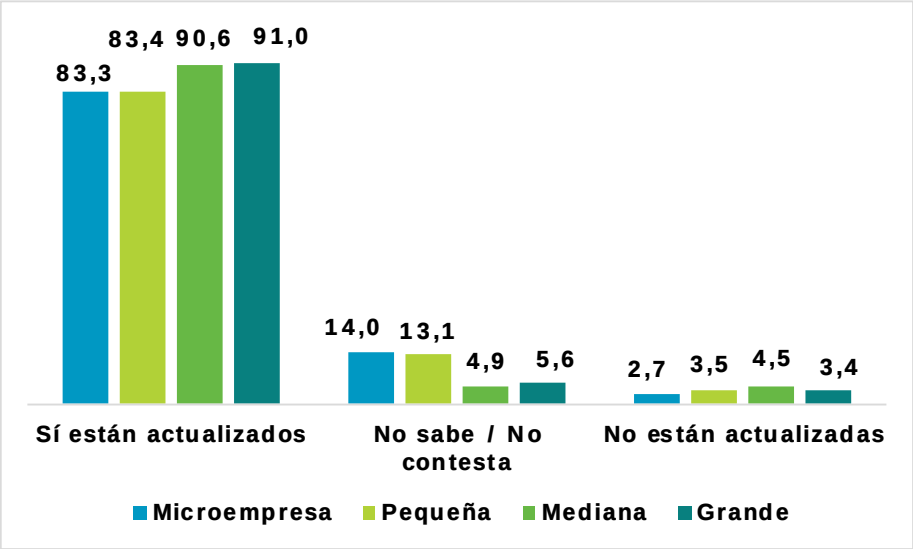
FIGURA 17: GRADO DE ACTUALIZACIÓN DE SISTEMAS OPERATIVOS Y HERRAMIENTAS DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501 P5

El grado de actualización de los sistemas operativos y las herramientas de seguridad correlaciona con el tamaño de la empresa. Existe una brecha de casi siete puntos porcentuales entre el comportamiento de microempresas y pequeñas empresas, por un lado, y medianas y grandes empresas por otro, de manera que microempresas y pequeñas empresas tienen actualizados sus sistemas operativos en menor proporción que las medianas y grandes empresas.

FIGURA 18: GRADO DE ACTUALIZACIÓN DE SISTEMAS OPERATIVOS Y HERRAMIENTAS DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P5

Por otra parte, los datos muestran como las microempresas y las pequeñas empresas desconocen la situación de sus sistemas operativos y de sus herramientas de seguridad en mayor medida que medianas y grandes empresas.

El "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas" de 2009[10] recogió el indicador para estas dos poblaciones y estableció que un 88,9% de las empresas tenían su sistema operativo y herramientas de seguridad actualizados, mientras un 6,7% declaraban no tenerlos actualizados y un 4,4% optaban por la opción no sabe / no contesta.

Si se comparan los datos de la encuesta de este año 2016, específicamente para las microempresas y pequeñas empresas, con los datos del estudio de 2009, parece que la actualización de los sistemas operativos y las herramientas de seguridad en las empresas españolas de este tamaño ha disminuido en cinco puntos porcentuales. Sin embargo, cabe destacar que al mismo tiempo las empresas que afirman no tener sus sistemas actualizados se han reducido a la mitad en el transcurso de estos años, de 6,7% a 3,1%.

La disminución de empresas que afirman tener sus sistemas actualizados ha podido verse afectada por el aumento de empresas que desconoce cuál es la situación de sus sistemas operativos y herramientas, que ha pasado de 4,4% en 2009 a 13,6% en 2016.

[10] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009 (Actualmente INCIBE)

FIGURA 19: GRADO DE ACTUALIZACIÓN DE SISTEMAS OPERATIVOS Y HERRAMIENTAS DE SEGURIDAD 2016 VS. 2009. PEQUEÑAS Y MICROEMPRESAS. RESPUESTA EXPRESADA EN %

LAS EMPRESAS QUE MÁS HAN INDICADO TENER SUS SISTEMAS ACTUALIZADOS PERTECENEN AL SECTOR DE

METALURGIA

93,5%

INFORMÁTICA Y ELECTRÓNICA

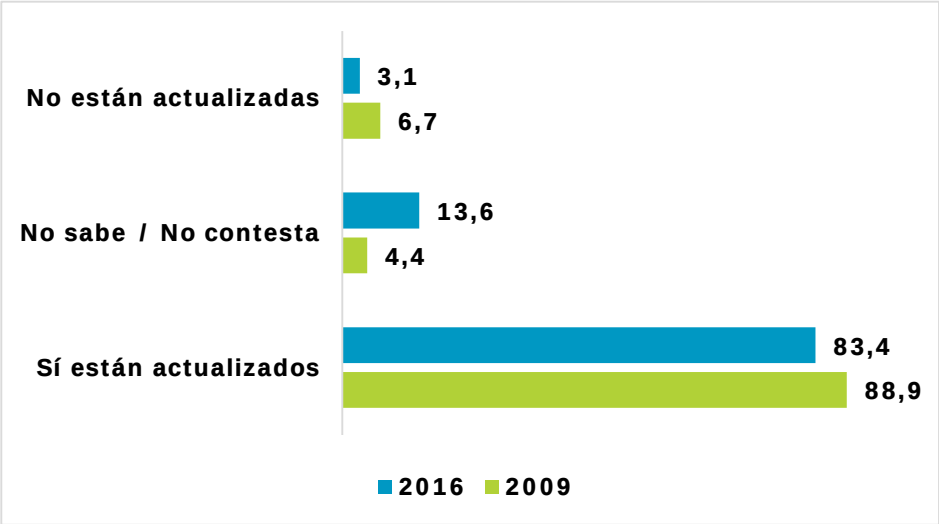
91,3%

ACTIVIDADES PROFESIONALES, CIENTÍFICAS Y TÉCNICAS

90,7%

ACTIVIDADES ADMINISTRATIVAS Y SERVICIOS AUXILIARES

90,4%



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa y Pequeña empresa 697. P5; y Estudio de INTECO (actual INCIBE) sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas 2009.

Los sectores que indican que tienen los sistemas más actualizados son el de Metalurgia y fabricación de productos metálicos (93,5%), Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor (91,3%), Actividades profesionales, científicas y técnicas (90,7%) y Actividades administrativas y servicios auxiliares (90,4%).

Entre los sectores que indican en mayor proporción que no están actualizados figuran el de Servicios de alojamiento (7,9%) y el de Alimentación, textil, madera y papel (5,3%).

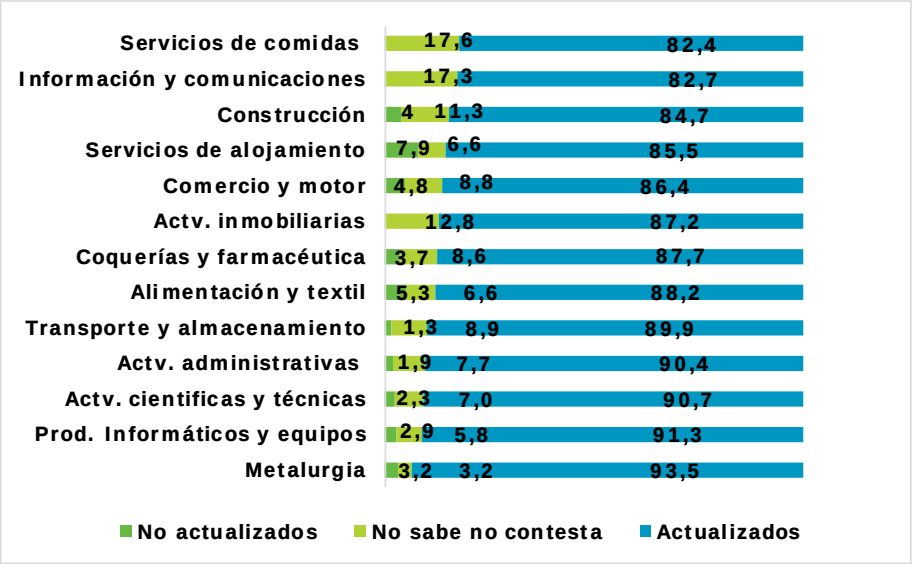
En cuanto a los sectores que más desconocen cuál es la situación de sus sistemas y herramientas de seguridad están los Servicios de comidas y bebidas (17,6%) e Información y comunicaciones (17,3%), lo que sin duda resulta llamativo en este último caso.

Para terminar con este apartado, se ha creído oportuno cruzar el grado de actualización de los sistemas operativos con los servicios electrónicos que utilizan las empresas, con la hipótesis de que aquellas empresas que utilizan más servicios electrónicos tendrán sus sistemas más actualizados, dado el riesgo al que se exponen.

Los resultados no son del todo significativos ya que muy pocas empresas han manifestado no tener sus sistemas actualizados, sin embargo, cabe resaltar que las empresas que no tienen actualizados sus sistemas operativos y herramientas de seguridad utilizan menos internet como usuario y proveedor de determinados servicios electrónicos en comparación con las empresas que se mantienen actualizadas, como por ejemplo los servicios de banca electrónica, la firma digital, y servicios en la nube.

Las empresas que no tienen sus sistemas actualizados son menos propensas a utilizar este tipo de servicios en comparación con las empresas que tiene sus sistemas operativos y herramientas de seguridad debidamente actualizados.

FIGURA 20: GRADO DE ACTUALIZACIÓN DE SISTEMAS OPERATIVOS Y HERRAMIENTAS DE SEGURIDAD POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P5

TABLA 2: USO DE INTERNET COMO USUARIO Y PROVEEDOR DE SERVICIOS Y GRADO DE ACTUALIZACIÓN

Uso de internet como usuario y proveedor de servicios	Sí, están actualizados	No están actualizados
Utiliza servicios de banca electrónica	86,7%	75,9%
Utiliza la firma digital para relacionarse con la Administración Pública	90,2%	79,6%
Utiliza la firma digital para relacionarse con clientes y proveedores	27,8%	22,2%
Contrata servicios en la nube de almacenamiento	37,3%	33,3%
Contrata aplicaciones de software como servicio en la nube	31%	18,5%

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Cruce P5 Y P2.[11]

[11] En la tabla solo se recogen los datos referentes a las empresas que han declarado estar actualizadas y utilizan en mayor medida internet como usuario y proveedor de servicios.

5 HERRAMIENTAS Y MEDIDAS DE SEGURIDAD

La Seguridad de la Información tiene como fin la protección de la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Se puede definir como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener su confidencialidad, disponibilidad e integridad.

El concepto integra la seguridad informática, pero es más amplio, dado que los riesgos asociados a la información van más allá del medio informático, pues pueden estar vinculados a las personas, o a otros soportes tradicionales.

En este capítulo se describe el comportamiento de las empresas en lo que se refiere al establecimiento de medidas de seguridad de la información y el uso de herramientas de seguridad.

Igualmente se analizan las características de las medidas establecidas y las razones que han llevado a las empresas a desarrollar esas medidas, así como las distintas tipologías de herramientas y/o servicios de seguridad que se utilizan, asociadas en algunos casos a distintos tipos de activos.

Finalmente, se aborda la valoración de las herramientas de seguridad, así como la percepción de la existencia de posibles barreras a la implementación de medidas y soluciones de seguridad en la empresa.

5.1 Políticas y estrategias de seguridad

La política de seguridad TIC de una organización constituye el marco de referencia que permite la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad asociados al uso de las tecnologías y la información de la organización.

La política de seguridad TIC queda constituida por tanto como el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro, o acceso no autorizado. Generalmente se instrumenta a través de un plan de seguridad, o plan de acción para afrontar riesgos de seguridad, o a través de un conjunto de reglas para el mantenimiento de cierto nivel de seguridad.

La política de seguridad se expresa en un documento que denota el compromiso de la dirección de la empresa con la seguridad de la información. La política de seguridad se materializa generalmente en la existencia de un Sistema de Gestión de la Seguridad que en algunos casos puede estar certificado bajo la norma ISO 27001. De esta forma el Sistema de Gestión de Seguridad de la Información (SGSI) es el concepto central sobre el que se construye ISO 27001 que da soporte a un proceso de gestión de la seguridad sistemático, documentado y conocido por toda la organización.

Puede conocer cuáles son los elementos principales para la ciberseguridad en su empresa, desde la creación de un plan director de seguridad hasta la contratación de servicios, en los diversos contenidos y herramientas de la siguiente página Web de INCIBE: https://www.incibe.es/protege-tu-empresa/que-te-interesa

Un elemento complementario a los dos anteriores es el de estrategia de continuidad de negocio que integra un conjunto de tareas que permiten a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. La estrategia de continuidad de negocio da respuesta a los incidentes que ponen en riesgo la actividad de las organizaciones. De esta forma, la estrategia permite garantizar que se puede dar una respuesta planificada ante cualquier fallo de seguridad.

Empresas que han definido formalmente una política de seguridad TIC (Indicador 36 en EICDE)

EMPRESAS CON UNA POLÍTICA DE

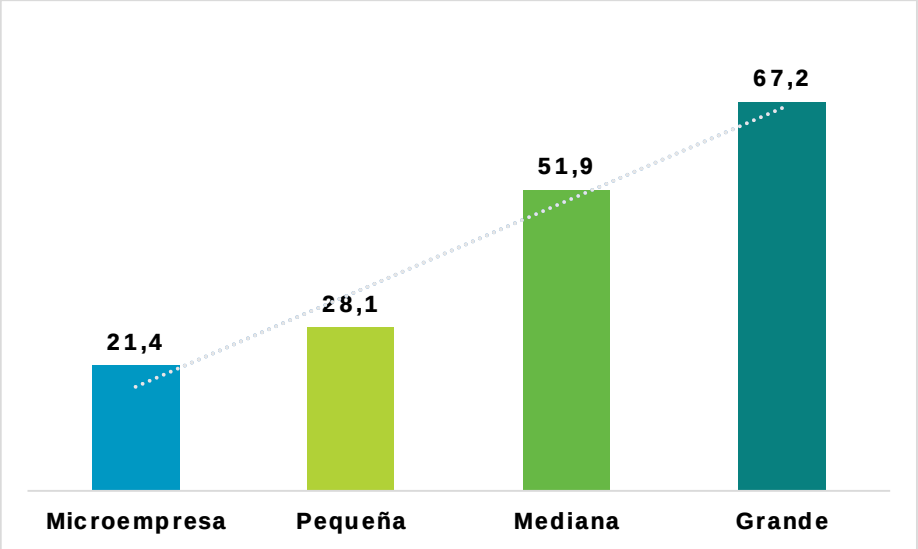
43,4%

TIENEN DEFINIDA FORMALMENTE UNA POLÍTICA DE SEGURIDAD TIC

El 43,4% de las empresas consultadas afirman tener definida formalmente una política de seguridad TIC. Este indicador muestra que todavía hay un grupo muy relevante de empresas que desconocen el beneficio que puede generar la formulación y ejecución de una política de seguridad en la gestión del impacto que pueden tener los incidentes de seguridad desde el punto de vista económico y del negocio.

En lo que a su distribución por tamaño se refiere, existe una relación directa y prácticamente lineal entre definir una política de seguridad y el tamaño de la empresa, así las medianas y grandes empresas tienen definida formalmente una política de seguridad en mayor proporción que las microempresas y las pequeñas empresas.

FIGURA 21: POLÍTICA DE SEGURIDAD TIC DEFINIDA POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P6

EL PORCENTAJE DE EMPRESAS CON UNA POLÍTICA DE SEGURIDAD TIC FORMALMENTE DEFINIDA HA AUMENTADO RESPECTO AL VALOR REGISTRADO POR LA ETICCE 2014-15

El dato que recogió el INE en su encuesta 2014-15 fue algo menor al obtenido en el presente estudio; el 37% de las pequeñas, medianas y grandes empresas declararon tener definida formalmente una política de seguridad TIC, mientras el 10% de las microempresas mantenían tenerla definida.

El porcentaje de empresas con una política de seguridad TIC formalmente definida ha aumentado desde la "ETICce" 2014-15, donde el 37% de las pequeñas, medianas y grandes empresas declararon tener definida formalmente una política de seguridad TIC, y el 10% de las microempresas mantenían tenerla definida. Mientras, en el presente estudio el 48,8% de las pequeñas, medianas y grandes y el 21,4% de las microempresas consultadas han declarado tener definida una política de seguridad TIC.

LAS EMPRESAS QUE MÁS HAN INDICADO TENER UNA POLÍTICA DE SEGURIDAD TIC DEFINIDA PERTENECEN A LOS SECTORES DE

INFORMACIÓN Y COMUNICACIONES

68%

ACTIVIDADES PROFESIONALES, CIENTÍFICAS Y TÉCNICAS

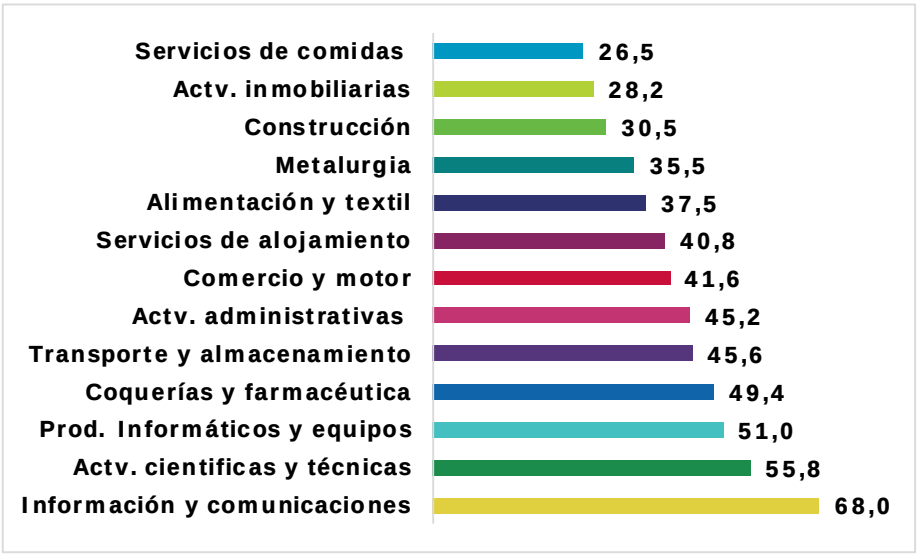
55,8%

PRODUCTOS INFORMÁTICOS Y EQUIPOS

51%

En cuanto a la distribución sectorial, las empresas cuya actividad principal está más relacionada con las tecnologías de la información son las que, en mayor medida, tienen definida formalmente una política de seguridad TIC.

FIGURA 22: POLÍTICA DE SEGURIDAD TIC DEFINIDA POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P6

El sector que ocupa el primer lugar en cuanto a la definición de una política de seguridad TIC es el de la Información y comunicaciones, con un 68%, le sigue el sector de Actividades profesionales, científicas y técnicas (55,8%) y finalmente el sector de Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor (51%).

Entre los sectores que menos tienen definida una política de seguridad TIC, a priori los menos adaptados a las tecnologías de la información, destaca el sector Servicios de comidas y bebidas con un 26,5%, seguido muy de cerca por el sector de las Actividades Inmobiliarias con un 28,2% y el de la Construcción con un 30,5%.

INCIBE cuenta con un servicio de Itinerarios Interactivos, en base a diez sectores de actividad, con el que puede ponerse al día, de manera entretenida, acerca de qué políticas ha de implementar en su sector
https://itinerarios.incibe.es/

Revisión de la política de seguridad TIC

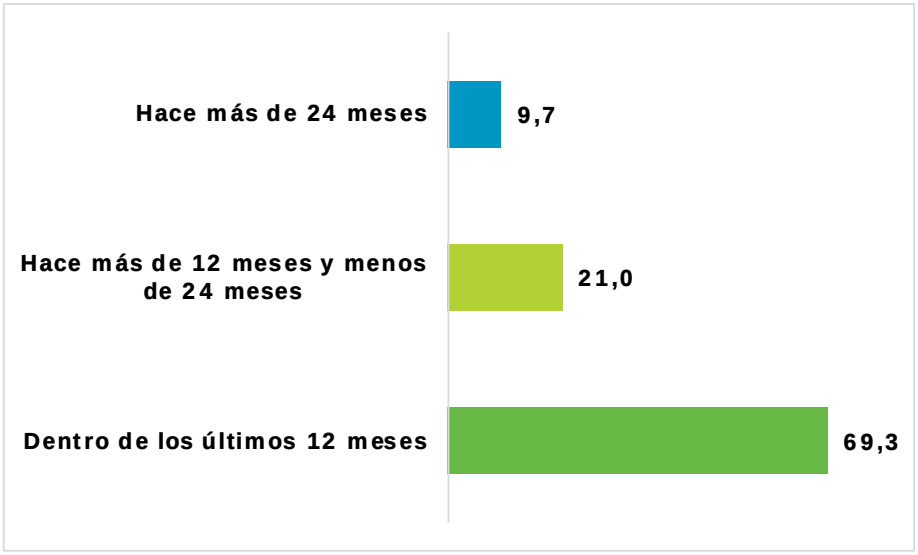
REVISIÓN DE LA POLÍTICA DE SEGURIDAD TIC

69,3%

EN LOS ÚLTIMOS 12 MESES
(% SOBRE EL TOTAL DE EMPRESAS CON POLÍTICA DE SEGURIDAD)

Con el objetivo de conocer el grado de revisión que las empresas consultadas mantienen de su política de seguridad TIC, se ha preguntado a las empresas consultadas por la última revisión de la política de seguridad que han hecho. El resultado permite indicar que en 2016 las empresas españolas han revisado su política de seguridad con cierta asiduidad, ya que el 69,3% de las empresas que han afirmado tener una política de seguridad definida, declaran que la han revisado en los últimos 12 meses, el 21% en los últimos dos años y el 9,7% hace más de dos años.

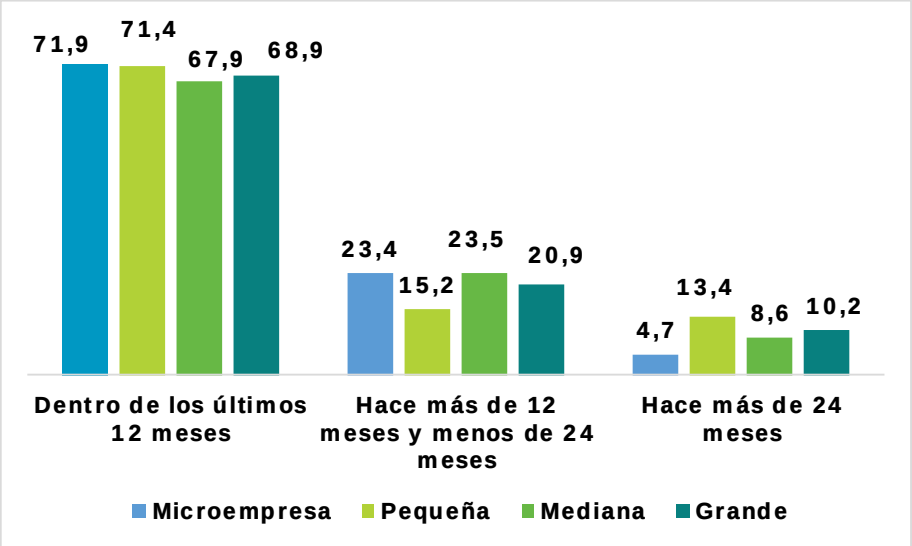
FIGURA 23: REVISIÓN DE LA POLITICA DE SEGURIDAD TIC. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 651 (Empresas que han declarado mantener formalmente una política de seguridad).P6.1

En cuanto a la distribución de la revisión de la política de seguridad por tamaño de empresa la situación es muy similar de forma que no existen grandes diferencias entre las respuestas. En cualquier caso, resulta destacable que las microempresas y pequeñas empresas son las que indican que revisan su política de seguridad con más asiduidad, con respuestas del 71,9% y un 71,4% respectivamente.

FIGURA 24: REVISIÓN DE LA POLITICA DE SEGURIDAD TIC POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 64, Pequeña 112, Mediana 221, Grande 254 (Empresas que han declarado mantener formalmente una política de seguridad). P6.1

Los datos que recogió el INE en su encuesta 2014-15 se mueven en una estructura de cifras similares para el conjunto de pequeñas, medianas y grandes empresas ya que, de las empresas que tienen definida política de seguridad TIC, un 65,8% declararon haber revisado la misma en los últimos meses (en el presente estudio 69%), un 26,7% entre los últimos 12 y 24 meses (20,7% en el presente estudio) y un 13,6% hace más de 24 meses (frente a un 9,7% en el estudio de este año).

La situación de las microempresas parece que ha cambiado algo más durante el último año, de manera que han declarado revisar sus sistemas de seguridad con más asiduidad que en la encuesta de 2014-15 del INE, lo que sin duda es un aspecto positivo.

LAS EMPRESAS QUE MÁS HAN AFIRMADO HABER REVISADO SU POLÍTICA DE SEGURIDAD RECIENTEMENTE (EN LOS ÚLTIMOS 12 MESES) PERTENECEN A LOS SECTORES DE:

TRANSPORTE Y ALMACENAMIENTO

86,3%

Y COQUERÍAS Y FARMACÉUTICA

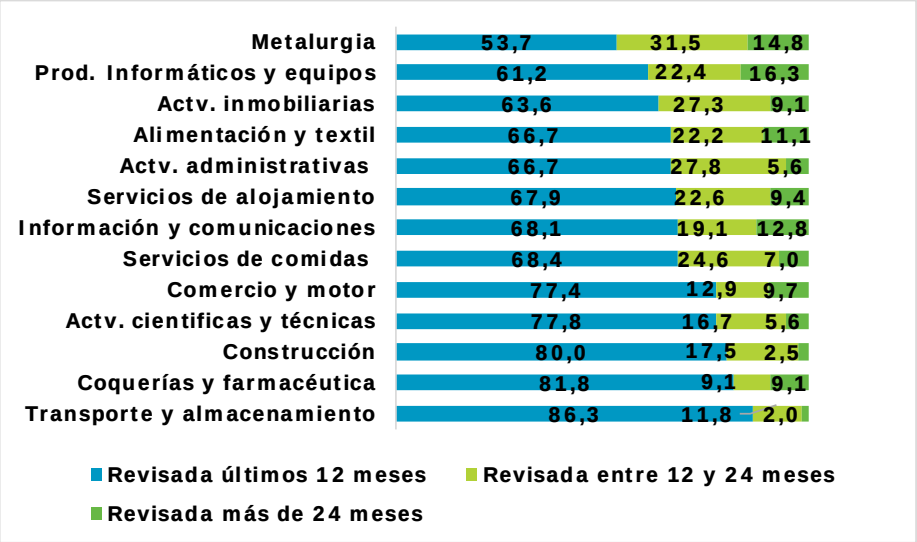
81,8%

El 61,3% de las microempresas que disponen de ella declararon haber revisado su política de seguridad en los últimos 12 meses, frente a un 71,9% en el año anterior, mientras un 14,9% manifestaba haber revisado su política de seguridad hace más de 24 meses frente a tan solo un 4,7% de las microempresas en el presente estudio.

Desde una perspectiva sectorial, las empresas que más han indicado haber revisado su política de seguridad en los últimos 12 meses pertenecen a los sectores de Transporte y almacenamiento (86,3), Coquerías, productos farmacéuticos, caucho y plásticos (81,1%) y Construcción (80%).

Entre las empresas que menos han revisado su política de seguridad en los últimos 12 meses figuran, aparte de las de Metalurgia, las pertenecientes al sector de Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor, así como el sector de información y comunicaciones, pudiendo resultar paradójico que estos dos últimos sectores, más afines a las TIC, no se encuentren entre los que revisan su política con mayor frecuencia.

FIGURA 25: REVISIÓN DE LA POLITICA DE SEGURIDAD TIC POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 57, Coquerías y farmacéutica 40, Metalurgia 22, Informática y mecánica 53, Construcción 54, Comercio y motor 147, Transporte y almacenamiento 36, Alojamiento 31, Servicios de comidas 9, Información y comunicaciones 51, Actividades inmobiliarias 11, Actividades científicas y técnicas 72, Actividades administrativas 47 (Empresas que han declarado mantener formalmente una política de seguridad). P6.1

RIESGOS DEFINIDOS EN LA POLÍTICA DE SEGURIDAD

82,8%
DESTRUCCIÓN O CORRUPCIÓN DE DATOS

52,2%
REVELACIÓN DE DATOS CONFIDENCIALES

51,3%
FALTA DE DISPONIBILIDAD SERVICIOS TIC

13,5%
NO TIENEN NINGUNO DE ESTOS RIESGOS

Riesgos que se incluyen en su política de seguridad TIC (Indicador 38 en EICDE)

Para orientar las respuestas a esta pregunta se ha tomado como referencia la conceptualización que realizó el INE en la "Encuesta uso TIC en empresas y comercio electrónico 2014-15"[12] que detalla como riesgos la falta de disponibilidad de servicios, la revelación de datos y la destrucción o corrupción de datos.

El 82,8% de las empresas españolas que mantienen una política de seguridad TIC indica contemplar en ella el riesgo de Destrucción o corrupción de datos debido a un ataque o por incidente de seguridad inesperado.

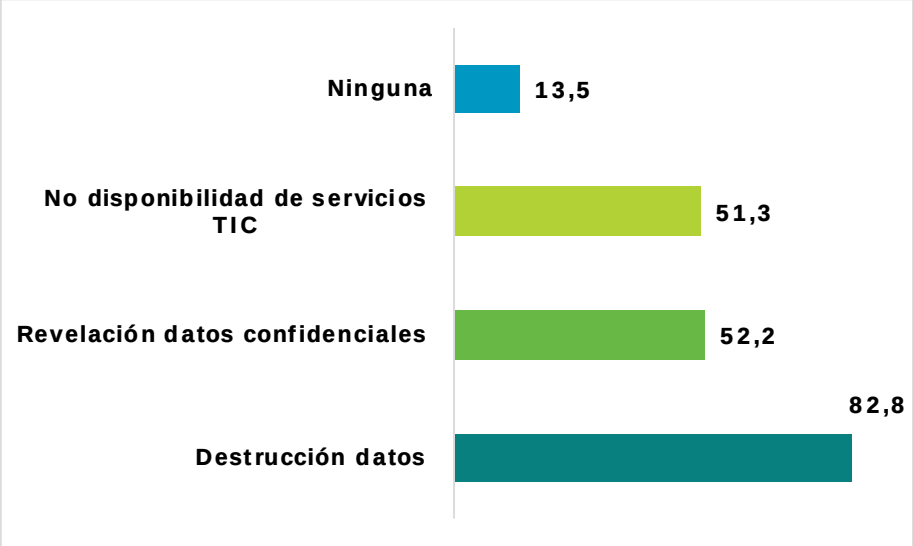
El 52,2% afirma tener definido el riesgo de Revelación de datos confidenciales debido a la intrusión, ataques de *phishing*, *pharming*[13] o por accidente.

El 51,3% indica tener el riesgo definido de Falta de disponibilidad de servicios TIC debido a ataques externos, y un 13,5% de las empresas afirma que no tiene ninguno de estos riesgos definido en su política de seguridad.

[12] "*Encuesta uso TIC en empresas y comercio electrónico*" INE 2015-16. http://www.ine.es/dynt3/inebase/es/index.htm?type=pcaxis&path=/t09/e02/a2015-2016&file=pcaxis&dh=0&capsel=0

[13] Las definiciones de *pharming* y *phising* se encuentran disponibles en el *ANEXO V. DEFINICIONES UTILIZADAS*, así como en el citado *"Glosario de términos de ciberseguridad: una guía de aproximación para el empresario"* INCIBE 2017 (en la página 17).

FIGURA 26: RIESGOS DEFINIDOS EN LA POLÍTICA DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 651 (Empresas que han declarado mantener formalmente una política de seguridad).P6.2

La "ETICce" obtuvo un patrón de respuesta en 2015-16 similar al que se ha recogido en este estudio, aunque algo más alto, el 90,8% de las empresas con una política de seguridad manifestó tener definido en su política de seguridad el riesgo de destrucción o alteración de la información debido a accidentes inesperados o ataques, el 68,3% los problemas de funcionamiento de los servicios TIC debido a ataques externos y el 81,9% la revelación de información confidencial debido a la instrucción, *pharming*, *phising* o por accidente.

En cuanto al análisis de la respuesta obtenida y el tamaño de la empresa, parece que a medida que la empresa es más grande indica tener definidos más riesgos en su política de seguridad TIC.

En el caso de las empresas que han indicado tener definidos los riesgos asociados a la Destrucción o corrupción de datos debido a un ataque o por incidente de seguridad inesperado, las pequeñas, medianas y grandes empresas tienen un comportamiento diferenciado de las microempresas, que lo tienen menos definido.

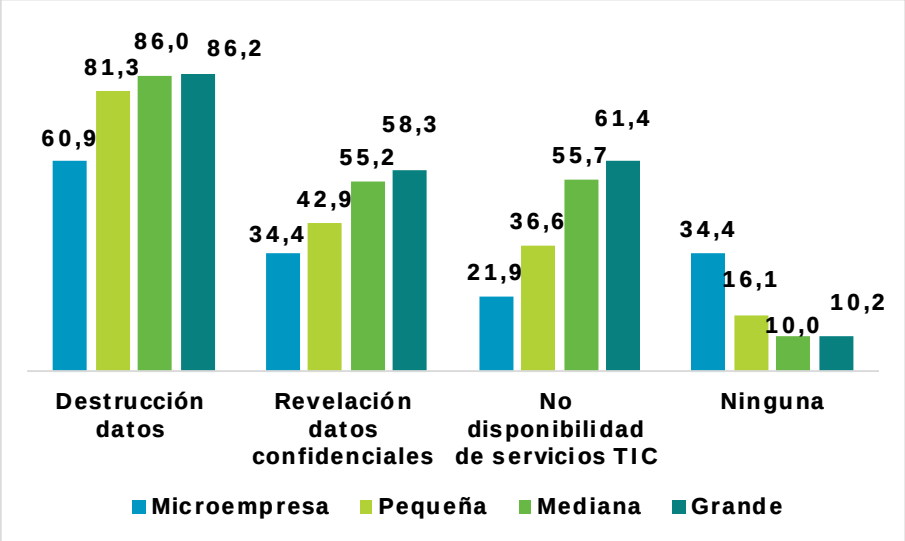
La información es un activo para las empresas: datos de clientes, de facturación, de recursos humanos… Es esencial que, cuando llegue el final de su ciclo de vida y deje de ser útil, se destruya de una manera segura. INCIBE dispone de la guía para el borrado seguro de datos con el objetivo de mitigar este riesgo: https://www.incibe.es/protege-tu-empresa/guias/borrado-seguro-informacion-aproximacion-el-empresario

Las microempresas y las pequeñas empresas tienen definido el riesgo de Revelación de datos confidenciales debido a la intrusión, ataques de *phishing*, *pharming* o por accidente, en un porcentaje menor que las medianas y grandes empresas, lo que tiene relación con que sean las que indican contar en menor medida con información clasificada, por lo que la falta de activos de este tipo supondría menor sensibilidad a la hora de definir riesgos asociados a la revelación de datos confidenciales.

Dentro de la empresa existen bienes intangibles como la cartera de clientes, las tarifas, el conocimiento comercial, la propiedad intelectual o la reputación. Las fugas de información, riesgo al que todas las empresas están expuestos, son una realidad para la que INCIBE ha desarrollado una guía para orientar e informar a los empresarios: https://www.incibe.es/protege-tu-empresa/guias/guia-fuga-informacion

En lo que se refiere al riesgo asociado a la falta de disponibilidad de servicios TIC por ataque externo, ocurre igualmente que las microempresas y pequeñas empresas indican tener definido este riesgo en menor proporción que las medianas y grandes.

FIGURA 27: RIESGOS DEFINIDOS EN LA POLÍTICA DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 64, Pequeña 112, Mediana 221, Grande 254 (Empresas que han declarado mantener formalmente una política de seguridad). P6.2 [14]

El patrón de datos recogido en la "ETICce" 2014-15 ha sido similar al registrado en el presente estudio, ya que también se destacaba como

[14] La categoría "Destrucción de datos" se refiere al riesgo de destrucción o corrupción de datos debido a un ataque o por incidente de seguridad inesperado, la categoría "Revelación datos confidenciales" a revelación de datos confidenciales debido a la intrusión, ataques de *phishing*, *pharming* o por accidente y la categoría "No disponibilidad de servicios TIC" a la falta de disponibilidad de servicios TIC por ataque externo.

riesgo más definido el de destrucción o corrupción de datos, mientras el riesgo de revelación de datos confidenciales y no disponibilidad de servicios TIC se encontraban en segundo y tercer lugar, aunque con algo más de diferencia que en el presente estudio (81,9% y 68,3% para pequeñas, medianas y grandes empresas, y 77,9% y 56,6% para microempresas). No obstante, esta diferencia no es significativa ya que la metodología entre ambos estudios es distinta, la "ETICce" realizó una pregunta dicotómica para cada una de las respuestas y en el presente estudio se realizó una pregunta multirrespuesta.

EL SECTOR QUE MÁS HA DEFINIDO LA REVELACIÓN DE DATOS CONFIDENCIALES EN SU POLÍTICA DE SEGURIDAD ES EL DE ALIMENTACIÓN Y TEXTIL

74,5%

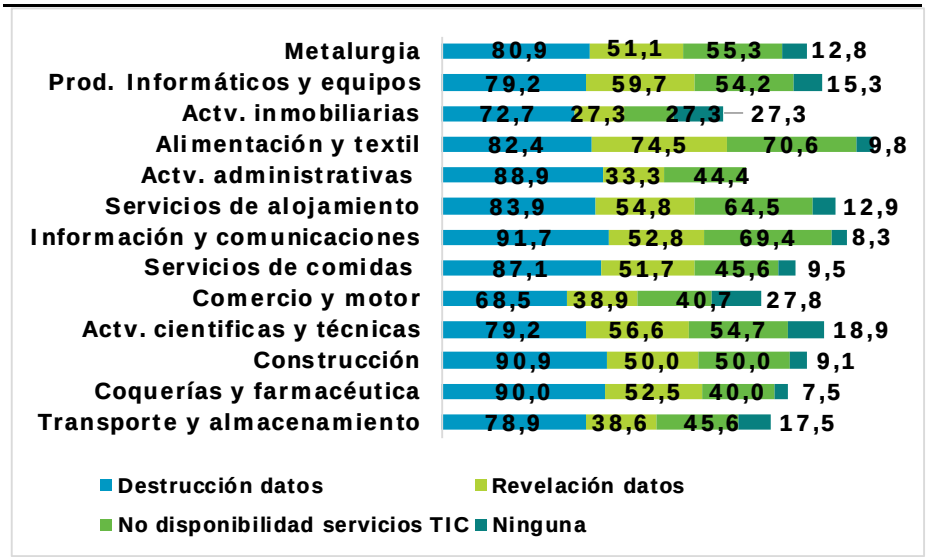
Para terminar con este apartado, el análisis en función de los sectores de actividad muestra un comportamiento bastante similar entre todas las empresas. Destaca, al igual que en otras variables que sea el sector de Información y comunicaciones el que ha definido el riesgo de destrucción o corrupción de datos en mayor medida, 91,7%. De otro lado, son las empresas pertenecientes al sector de Alimentación, textil, madera y papel las que más han indicado tener contemplado el riesgo de revelación de datos confidenciales debido a la intrusión, ataques de *phising*, *pharming* o por accidente (74,5%) y la Falta de disponibilidad de servicios TIC en su política de seguridad (70,6%). Estos sectores también figuran por debajo de la media en lo que se refiere a las empresas que indican que no tienen ninguno de los riesgos evaluados recogidos en su política de seguridad.

EN LO QUE RESPECTA A LA FALTA DE DISPONIBILIDAD DE SERVICIOS TIC EL SECTOR QUE MÁS LO HA DEFINIDO ES EL DE ALIMENTACIÓN Y TEXTIL

70,6%

Entre las empresas que más han indicado no haber definido ninguno de los riesgos anteriores aparecen los sectores de Comercio al por mayor, al por menor y venta y reparación de vehículos de motor con un 27,8% y de Actividades inmobiliarias (27,3%), por lo que su política de seguridad es menos explícita en lo que se refiere a los riesgos que habitualmente se identifican.

FIGURA 28: RIESGOS DEFINIDOS EN LA POLÍTICA DE SEGURIDAD POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 57, Coquerías y farmacéutica 40, Metalurgia 22, Informática y mecánica 53, Construcción 54, Comercio y motor 147, Transporte y almacenamiento 36, Alojamiento 31, Servicios de comidas 9, Información y comunicaciones 51, Actividades inmobiliarias 11, Actividades científicas y técnicas 72, Actividades administrativas 47 (Empresas que han declarado mantener formalmente una política de seguridad). P6.2[15]

[15] La categoría "Destrucción datos" se refiere al riesgo de destrucción o corrupción de datos debido a un ataque o por incidente de seguridad inesperado, la categoría "Revelación datos" a revelación de datos confidenciales debido a la intrusión,

RAZONES PARA IMPLEMENTAR POLÍTICA DE SEGURIDAD

76,5%
MANIFIESTA 4 O MÁS RAZONES PARA IMPLEMENTAR UNA POLÍTICA DE SEGURIDAD

96,2%
INTEGRIDAD DATOS E INFORMACIÓN

73,9%
DISPONIBILIDAD SERVICIOS

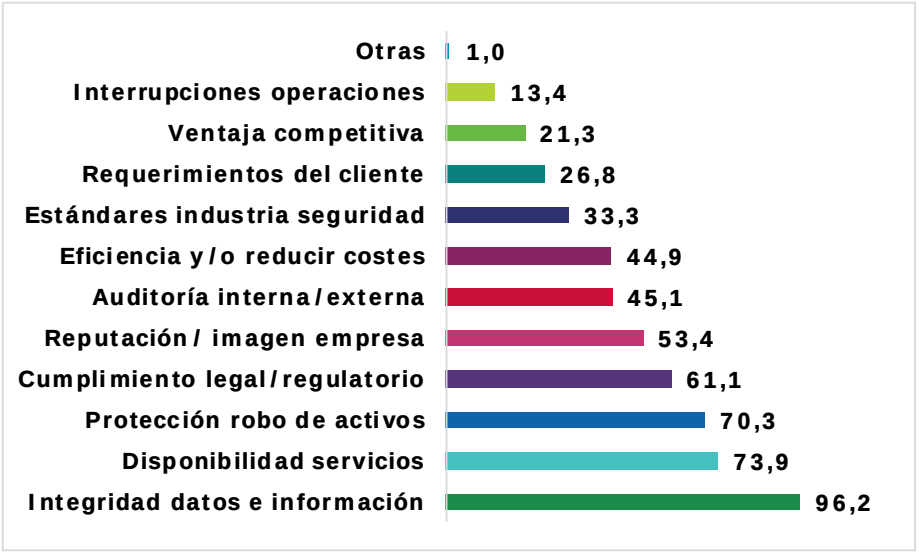
70,3%
PROTECCIÓN ROBO DE ACTIVOS

Razones que llevaron a implementar la política de seguridad

Con objeto de conocer las razones que han llevado a las empresas a implementar las políticas o estrategias de seguridad y continuidad de negocio se han creado 11 categorías de respuesta resultado de integrar 8 de las respuestas del "Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas"[16] de 2012, (garantizar la disponibilidad de las operaciones de negocio/disponibilidad de los servicios en caso de crisis, reputación y protección de la imagen pública de la empresa, ventaja competitiva frente a otros competidores del mercado, requerimientos del cliente, como respuesta a un requerimiento de auditoría interna/externa, cumplimiento de requerimientos regulatorios y legales, alinearse con los principales estándares de la industria de seguridad y anteriores interrupciones en las operaciones de negocio), y añadir las categorías: mejorar la eficiencia y/o reducir costes, la protección contra el robo de activos de la empresa y asegurar la integridad de los datos y la información.

La mayoría de las empresas consultadas, el 76,5%, manifiesta cuatro o más razones que le han llevado a definir e implementar la política de seguridad TIC. La razón más mencionada por las empresas por la que implementan una política de seguridad es la de Asegurar la integridad de los datos y la información con un 96,2% de las respuestas. El segundo motivo para implementar una política de seguridad es Garantizar la disponibilidad de las operaciones de negocio y la disponibilidad de los servicios en caso de crisis, con un 73,9%. Del mismo modo, la Protección contra el robo de activos de la empresa (70,3%) es el tercer motivo más mencionado.

FIGURA 29: RAZONES QUE LLEVARON A IMPLEMENTAR LA POLÍTICA DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 835 (Empresas que han declarado mantener algún tipo de política, certificación, estrategia de continuidad de negocio). P6.3[17]

ataques de *phishing*, *pharming* o por accidente y la categoría "No disponibilidad de servicios TIC" a la falta de disponibilidad de servicios TIC por ataque externo.

[16] "*Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*" INTECO 2012. (Actualmente INCIBE).

[17] Las categorías han sido simplificadas para los gráficos que muestran la tasa de respuesta de esta pregunta: Integridad datos e información: asegurar la integridad de los datos y la información; disponibilidad servicios: garantizar la disponibilidad

Por otro lado, los motivos menos mencionados son Anteriores interrupciones en las operaciones de negocio (13,4%), la Ventaja competitiva frente a otros competidores del mercado (21,3%) y Requerimientos del cliente (26,8%).

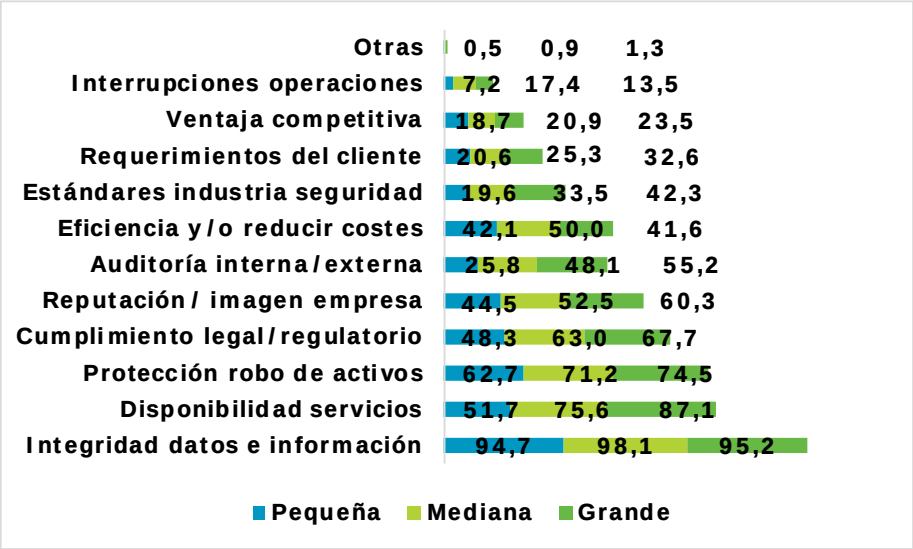
Las razones que expresan las empresas españolas a la hora de implementar una política de seguridad son distintas en función de la respuesta que dieron a las alternativas planteadas relacionadas con la definición de la propia política de seguridad TIC, mantener una certificación ISO 27001 o haber definido una estrategia de continuidad de negocio.

Las respuestas de las empresas que indican estar certificadas por la ISO 27001, muestran que las razones que les ha llevado a implantar la norma se deben a requerimientos del cliente o para obtener una ventaja competitiva frente a otros competidores del mercado en mayor medida que el resto de las empresas, lo que indicaría que la obtención de la ISO 27001 está vinculada con la demanda y el mercado. De esta forma, es posible que si no existiera esta demanda las empresas no optarían por abordar el proceso de certificación.

También se deduce del análisis que las empresas que afirman haber definido una estrategia de continuidad de negocio han indicado, como razón para el desarrollo de este proceso el haber sufrido anteriores interrupciones en las operaciones de negocio, en mayor medida que aquellas que seleccionaron otras respuestas (mantener una política de seguridad o estar certificadas por la ISO 27001), lo que indicaría, a su vez, que la definición de una estrategia de continuidad de negocio constituye una reacción a los problemas que pudieran haber surgido en las empresas.

de las operaciones de negocio/disponibilidad de los servicios en caso de crisis; protección robo de activos: la protección contra el robo de activos de la empresa; cumplimiento legal/regulatorio: cumplimiento de requerimientos regulatorios y legales; reputación/imagen empresa: reputación y protección de la imagen pública de la empresa; auditoría interna/externa: como respuesta a un requerimiento de auditoría interna/externa; eficiencia y/o reducir costes: mejorar la eficiencia y/o reducir costes; estándares industria seguridad: alinearse con los principales estándares de la industria de seguridad; requerimientos del cliente: requerimientos del cliente; ventaja competitiva: ventaja competitiva frente a otros competidores del mercado; interrupciones operaciones: anteriores interrupciones en las operaciones de negocio.

FIGURA 30: RAZONES QUE LLEVARON A IMPLEMENTAR LA POLÍTICA DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Pequeña 209, Mediana 316, Grande 310 (Empresas que han declarado mantener algún tipo de política, certificación, estrategia de continuidad de negocio). P6.3

En lo que a su distribución por tamaño se refiere, existe una correlación entre medianas y grandes empresas y el número de razones por las que implanta una política de seguridad. De manera que las medianas y grandes empresas mencionan más motivos que las pequeñas empresas. [18]

En relación con la distribución sectorial de la respuesta sobre las razones que llevaron a la implementación de políticas de seguridad, se puede apuntar que los sectores que más razones han indicado tener para implementar su política de seguridad son: el de Información y comunicaciones con una media de 6,63 menciones, el de Actividades profesionales, científicas y técnicas con una media de 5,86 menciones y muy próximo a éste el sector de Coquerías, productos farmacéuticos, caucho y plásticos con 5,88 menciones.

Certificación ISO 27001

La norma ISO/IEC 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional por la *International Organization for Standardization*. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el ciclo PDCA - acrónimo de *Plan, Do, Check, Act* (Planificar, Hacer, Verificar, Actuar). La norma constituye la base del proceso de certificación de las organizaciones que han implementado su sistema

[18] El recorrido del cuestionario se acortó en esta pregunta para las microempresas debido a la necesidad de acortar el tiempo medio de respuesta y valorando las características propias de este tamaño de empresa.

de gestión de la seguridad de la información, de acuerdo con sus requerimientos.

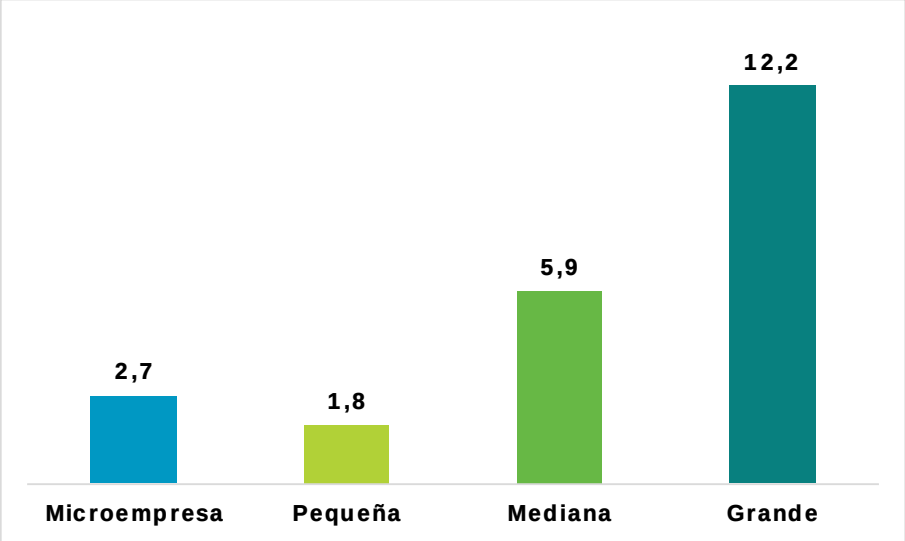
Los datos muestran que solo el 5,7% de las empresas españolas están certificadas en la norma ISO 27001.

CERTIFICACIÓN POR LA ISO 27001

Atendiendo al tamaño de la empresa, las empresas grandes son las que más cuentan con la certificación en la ISO 27001 con un 12,2% y las pequeñas empresas las que menos con un 1,8%.

5,7%
ESTÁN CERTIFICADAS POR LA ISO 27001

FIGURA 31: CERTIFICACIÓN ISO 27001 POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P6

LAS EMPRESAS QUE MÁS HAN MANIFESTADO ESTAR CERTIFICADAS POR LA ISO 27001 PERTENECEN A LOS SECTORES DE

INFORMACIÓN Y COMUNICACIONES
28%

ACTIVIDADES PROFESIONALES, CIENTÍFICAS Y TÉCNICAS
14%

ACTIVIDADES ADMINISTRATIVAS Y AUXILIARES
11,5%

En la encuesta llevada a cabo en el marco del "Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas" 2012[19], se recogía que el 13,3% de las empresas afirmaba estar certificada o en proceso de certificación. También se recogía que un 28,9% desconocía si lo estaba. Estos porcentajes tan elevados no se correspondían con la realidad dado que las empresas confundían la ISO 27001 con la ISO 9001, según la propia información recogida por el estudio.

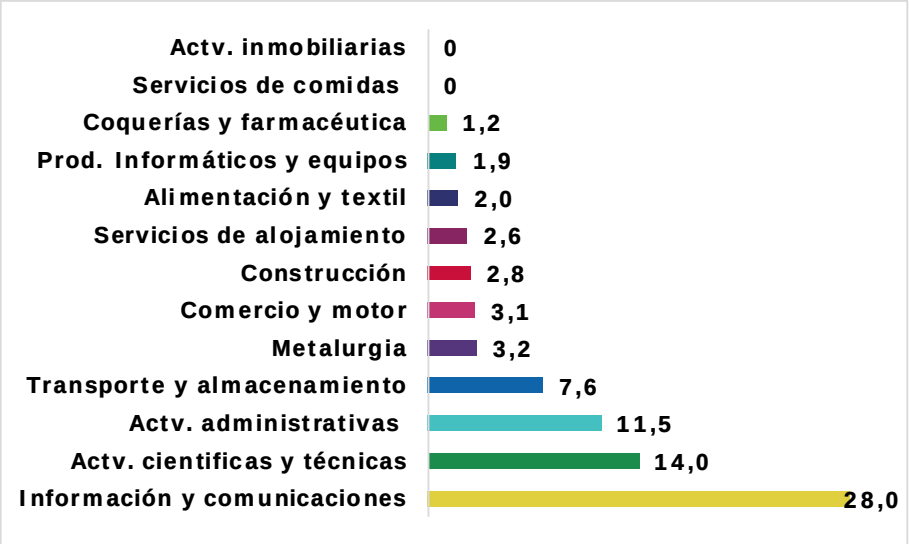
Para apoyar esta tesis se realizó un análisis documental que clarificó que en 2012 solo existían en España 711 empresas certificadas en la ISO 27001, lo que supondría un 0,02% sobre el total de empresas existentes en España.

En el estudio actual se ha conseguido reducir el volumen del sesgo respecto a 2010, aunque sigue existiendo.

En cuanto a la distribución sectorial, destaca muy por encima de las demás el sector de la Información y las comunicaciones con un 28%. También tiene un alto grado de certificación el sector de las Actividades profesionales, científicas y técnicas con un 14% y el de Actividades administrativas y servicios auxiliares con un 11,5%.

[19] "*Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*" INTECO 2012. (Actualmente INCIBE).

FIGURA 32: CERTIFICACIÓN ISO 27001 POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P6

Las empresas que pertenecen al sector de Actividades inmobiliarias, así como las que pertenecen a Servicios de comidas y bebidas manifiestan que no cuentan con una certificación ISO 27001, estos dos sectores también eran los que menos señalaban tener definida una política de seguridad TIC.

Disposición de una estrategia de continuidad de negocio

ESTRATEGIA DE CONTINUIDAD DE NEGOCIO

41% DE LAS EMPRESAS LA HAN DEFINIDO

Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permita a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. La estrategia de continuidad de negocio da respuesta a estos incidentes que ponen en riesgo la actividad de las organizaciones. De esta forma, la estrategia permite garantizar que se puede dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de la imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes de seguridad graves.

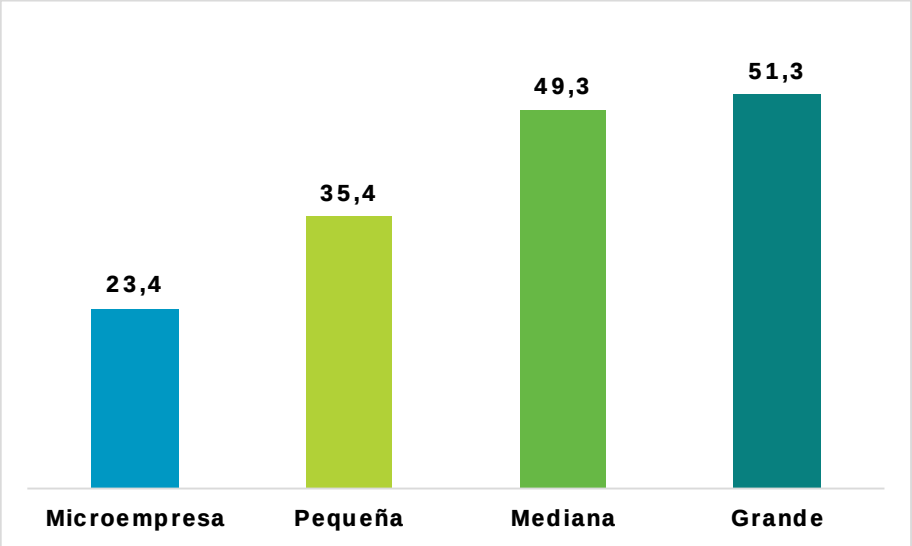
El indicador obtenido es que el 41% de las empresas afirman haber definido una estrategia de continuidad de negocio.

Tal y como ocurría con las empresas que han definido formalmente una política de seguridad TIC, el caso de la estrategia de continuidad de negocio también correlaciona positivamente con el tamaño de la empresa.

La seguridad al 100% no existe. Las empresas deben estar preparadas para protegerse y reaccionar lo antes posible ante incidentes de seguridad que pudieran dañar la capacidad operativa o hacer peligrar la continuidad del negocio. Se ha de ser capaz de dar una respuesta rápida y eficaz ante cualquier contingencia grave. Puesto que se trata de uno de los aspectos críticos para mantener la actividad, dentro de los dosieres de INCIBE existe uno dedicado exclusivamente a los planes de contingencia y continuidad: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

En lo que a su distribución por tamaño se refiere, existe una relación proporcional entre definir una estrategia de continuidad de negocio y el tamaño de una empresa, así las medianas y grandes tienen definida formalmente una política de seguridad en mayor proporción que las microempresas y las pequeñas empresas.

FIGURA 33: EXISTENCIA DE POLITICAS Y ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P6

En 2016 el 36% de las PYME españolas han afirmado haber definido una estrategia de continuidad de negocio. Este indicador fue medido en 2012 en el "Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas"[20]. Los datos no son comparables debido a la diferente categorización de la pregunta, sin embargo, resulta relevante apuntar el crecimiento de empresas

[20] *"Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas"* INTECO 2012. (Actualmente INCIBE).

que afirman tener definida una estrategia de continuidad de negocio en 2016.

TABLA 3: NIVEL DE IMPLANTACIÓN ESTRATEGIA DE CONTINUIDAD DE NEGOCIO EN LA PYME ESPAÑOLA EN 2012 VS. 2010.

Estrategia de continuidad de negocio	2010	2012
Sí, elaborada e implantada	17%	15%
Sí, pero solo la parte tecnológica	22%	16%

Fuente: Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas, INTECO 2012 (Actual INCIBE), Gráfico 30

En lo que a distribución sectorial se refiere destacan unos sobre otros.

Las empresas que más indican tener definida una estrategia de continuidad de negocio pertenecen a los sectores de Información y comunicaciones (58,7%), Coquerías, productos farmacéuticos, caucho y plásticos (55,6) y Transporte y almacenamiento (50,6%). Por el contrario, los sectores que menos indican tener estrategias de continuidad de negocio definidas son el sector de Servicios de comidas y bebidas con un 20,6%, el de Actividades inmobiliarias con un 25,6% y, finalmente, el de la Construcción con un 29,9%.

LOS SECTORES QUE MÁS INDICAN TENER UNA ESTRATEGIA DE NEGOCIO IMPLANTADA SON LOS DE

INFORMACIÓN Y COMUNICACIONES

58,7%

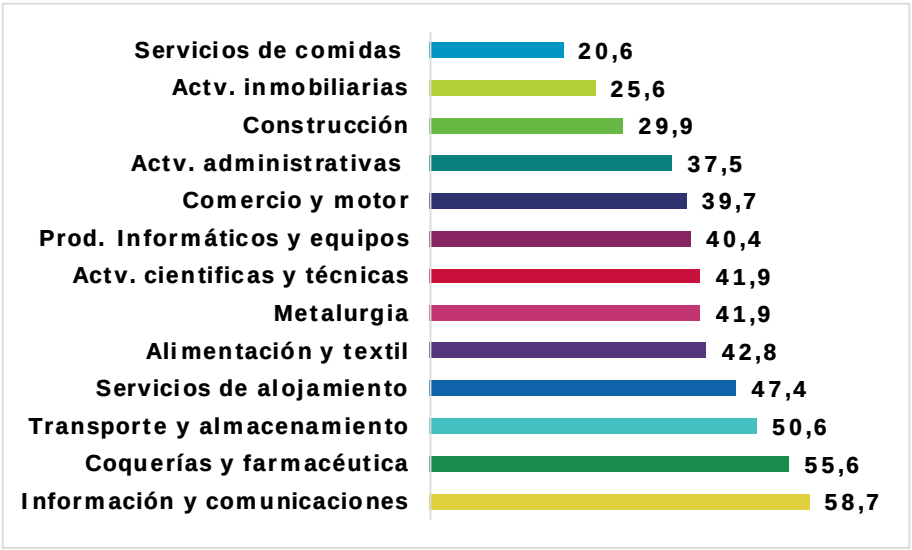
COQUERÍAS Y FARMACÉUTICA

55,6%

TRANSPORTE Y ALMACENAMIENTO

50,6%

FIGURA 34: EXISTENCIA DE POLITICAS Y ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO POR SECTOR. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Alimentación y textil 152, Coquerías y farmacéutica 81, Metalurgia 62, Informática y mecánica 104, Construcción 177, Comercio y motor 353, Transporte y almacenamiento 79, Alojamiento 76, Servicios de comidas 34, Información y comunicaciones 75, Actividades inmobiliarias 39, Actividades científicas y técnicas 129, Actividades administrativas 104.P6

En resumen, las empresas que pertenecen al sector de la Información y Comunicaciones destacan sobre las demás tanto en la definición formal de una política de seguridad TIC, como en la certificación ISO 27001 y en la definición de una estrategia de negocio. Por el contrario, las empresas que pertenecen al sector de Servicios de comidas y bebidas son las que más han contestado que no tienen una política de seguridad definida con un 58,8%, seguidas del sector de la Construcción con un 51,4% y Actividades inmobiliarias con un 51,3%.

5.2 Sistemas y soluciones

Empresas que utilizan sistemas internos de seguridad por tipo (Indicador 37 en EICDE)

SISTEMAS INTERNOS DE SEGURIDAD MÁS EXTENDIDOS

86,9%
AUTENTICACIÓN CON CONTRASEÑA SEGURA

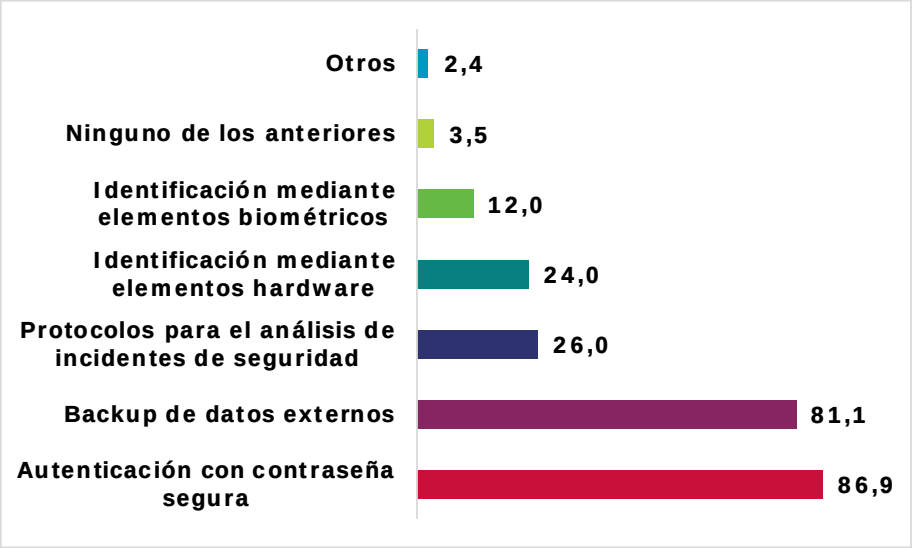
81,1%
BACKUP DE DATOS EXTERNOS

Con el objetivo de obtener el indicador 37 en EICDE se ha solicitado a las empresas que indicaran qué sistemas internos de los que se detallan a continuación tenían implantados en su empresa:

- Autenticación con contraseña segura. El 86,9% de las empresas consultadas ha señalado contar con este sistema interno de seguridad en su empresa. La autenticación con contraseña segura sirve para aportar mayor seguridad a procesos, aplicaciones y sistemas de la empresa.
- Backup de datos externos. El 81,1% de las empresas consultadas ha indicado contar con este sistema interno de seguridad. El backup es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida.
- Protocolos para el análisis de incidentes de seguridad. El 26% de las empresas consultadas ha señalado tener este tipo de protocolo implantado en su empresa.
- Identificación mediante elementos hardware. El 24% de las empresas consultadas afirma contar con este sistema interno de seguridad, asociado a algún elemento físico como una tarjera de identidad.
- Identificación mediante elementos biométricos. El 12% de las empresas indica poseer este sistema de identificación mediante la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo para su autentificación.

Las tecnologías biométricas son un conjunto de métodos que sirven para reconocer de forma automática a personas analizando sus características físicas (iris, huella digital, palma de la mano, rostro,…) o su comportamiento (voz, forma de andar, escritura,...). Aunque el índice de penetración de estos sistemas no es demasiado alto, la tendencia va en aumento. INCIBE ha creado la guía Tecnologías biométricas aplicadas a la ciberseguridad: https://www.incibe.es/protege-tu-empresa/guias/tecnologias-biometricas-aplicadas-ciberseguridad-guia-aproximacion-el

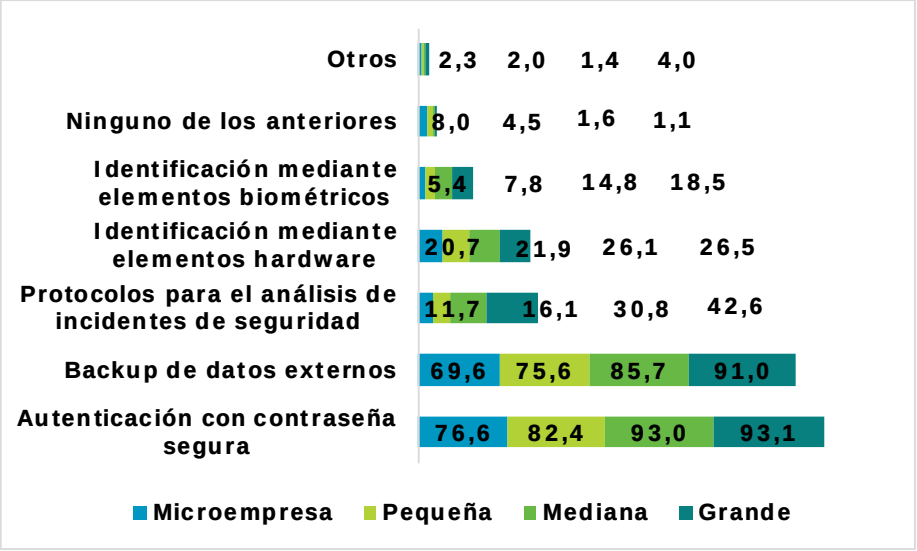
FIGURA 35: SISTEMAS INTERNOS DE SEGURIDAD UTILIZADOS. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501. P7

Respecto a la distribución de la respuesta atendiendo al tamaño de la empresa, se puede observar una relación proporcional de manera que cuanto mayor es su tamaño, más indican las empresas utilizar sistemas internos de seguridad.

FIGURA 36: SISTEMAS INTERNOS DE SEGURIDAD UTILIZADOS POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 299, Pequeña 398, Mediana 426, Grande 378. P7[21]

[21] La categoría identificación mediante elementos hardware corresponde a: identificación de usuario y autenticación mediante elementos hardware, y la categoría identificación mediante elementos biométricos a: identificación de usuario y autenticación mediante elementos biométricos.

El uso del Backup de datos externos fue medido por el "Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas"[22] en 2007, el cual recogía que el 66,5% de las empresas pequeñas y medianas afirmaban contar con este sistema interno de seguridad, mientras que los datos actuales indicarían que el porcentaje de Pymes (microempresas, pequeñas y medianas empresas) que afirma realizar *backups* habría crecido en estos años en 11 puntos porcentuales hasta un 77,8%.

Revisadas las respuestas de las empresas desde la perspectiva de los sectores de actividad se aprecia cierta variabilidad de la respuesta. Existen algunos sectores que están relacionados significativamente, de manera que tienden a utilizar en mayor o menor medida determinados sistemas internos de seguridad.

Por un lado, en el sector de la Construcción se observa una relación proporcional negativa respecto a los sistemas internos de seguridad dado que las empresas que se dedican a esta actividad en general tienden a utilizar menos los distintos sistemas analizados, tales como la Autenticación con contraseña segura, la Identificación de usuario y autenticación mediante elementos hardware y los Protocolos para el análisis de incidentes de seguridad.

Del mismo modo, el sector del Comercio al por mayor, al por menor y venta y reparación de vehículos de motor utiliza menos los Protocolos para el análisis de incidentes de seguridad en comparación con los demás sectores. Igualmente, en el ámbito del sector de Servicios de comidas y bebidas las empresas tampoco utilizan los Protocolos para el análisis de incidentes de seguridad, pero, además, indican utilizar menos el Backup de datos externos que las empresas de otros sectores

De otro lado, existe una relación positiva entre el sector de Información y comunicaciones y los sistemas internos de seguridad ya que sus empresas indican utilizar de forma general más sistemas internos de seguridad y en concreto mencionan con mayor frecuencia la Autenticación por contraseña segura, el Backup de datos externos y los Protocolos para el análisis de incidentes de seguridad. Por su parte, las empresas que se dedican al sector de Actividades profesionales, científicas y técnicas y Actividades administrativas y servicios auxiliares, utilizan en mayor proporción el Backup de datos externos que las empresas de otros sectores, lo que podría tener relación con el uso de información sensible.

Para completar el análisis, se han cruzado los datos sobre el uso de sistemas internos de seguridad con las razones que llevan a una empresa a implementar actuaciones de seguridad, con el objetivo de valorar si son distintos los motivos que llevan a las empresas a utilizar distintos sistemas internos de seguridad.

[22] "*Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*" INTECO 2007. (Actualmente INCIBE).

Los tres sistemas internos de seguridad más utilizados comparten las mismas motivaciones: la protección contra el robo de activos, garantizar la disponibilidad de las operaciones de negocio/servicios en caso de crisis y la ventaja competitiva.

La diferencia se produce entre las empresas que han indicado utilizar Protocolos para el análisis de incidentes de seguridad que han afirmado, además, estar motivadas por el cumplimiento de requerimientos regulatorios/legales y por anteriores interrupciones en las operaciones de negocio.

Productos de seguridad

En este apartado se describe la situación respecto a la tipología de productos de seguridad implantados en las empresas con el fin de conocer el nivel de implantación de soluciones de seguridad y su evolución.

INCIBE a través de su Catálogo, pone a disposición de los usuarios más de 5000 referencias de productos y servicios de ciberseguridad. Además da la oportunidad a aquellas compañías cuya actividad esté centrada en servicios de ciberseguridad, de formar parte del listado: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

PRODUCTOS DE SEGURIDAD

97,8%
PRODUCTOS ANTIVIRUS/ANTI ESPÍA

76,1%
CORTAFUEGOS Y FILTROS DE CONTENIDOS WEB

71,4%
HERRAMIENTAS DE CONTINGENCIA Y CONTINUIDAD

A grandes rasgos, la demanda de soluciones es significativa dado que el 66% de las empresas consultadas afirma utilizar más de cuatro tipos de soluciones.

A continuación, se expone la situación en lo que se refiere al uso de productos de seguridad con respecto a los 11 tipos de productos de seguridad considerados, que son los contemplados por INTECO (actual INCIBE) en su Taxonomía de soluciones de seguridad TIC (2009)[23].

- **Uso de Productos antivirus/anti espía (Indicador número 31 en EICDE).** El 97,8% de las empresas consultadas afirma contar con este tipo de producto entre sus soluciones de seguridad, coincidiendo exactamente con el dato que se registró en 2009.[24]

  Aunque el análisis por tipo de empresa y sector se presenta más adelante, cabe señalar que las grandes empresas y las pertenecientes a los sectores de Coquerías, productos farmacéuticos, caucho y plásticos, así como las de Servicios de alojamiento y Actividades inmobiliarias son las que más manifiestan utilizar productos antivirus/anti espía.

[23] Véase en anexo las definiciones de los distintos productos de seguridad definidos en la *"Taxonomía (v 2.0) de soluciones de seguridad TIC"* INTECO 2009. (Actualmente INCIBE).

[24] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

- Los Cortafuegos, destinados a proteger los sistemas y dispositivos conectados a una red, son el segundo producto de seguridad más utilizado por las empresas consultadas con un 76,1%.
- Le siguen las empresas que cuentan entre sus soluciones con las Herramientas de contingencia y continuidad de negocio 71,4%.
- En cuarto lugar, el 51,9% de las empresas consultadas afirma poseer sistemas de Autenticación y certificación digital destinados al uso y utilización de certificados digitales para aportar mayor seguridad a procesos, aplicaciones y sistemas.
- Las Herramientas anti-fraude destinadas a proteger a los usuarios de ataques que utilizan prácticas denominadas de ingeniería social, ocupan el quinto lugar en el nivel de implantación de soluciones de seguridad con un 51,2% de la respuesta.
- Con una penetración ya inferior a la mitad de empresas, los Sistemas de control de tráfico en la red destinados al control de la actividad de las infraestructuras de comunicaciones de una organización, son implantados por el 39,4% de las empresas.
- El 28,9% de las empresas afirma poseer Herramientas de seguridad en movilidad, cuya misión se basa en proteger las redes inalámbricas y dispositivos móviles o dispositivos en movilidad.
- El 23,9% de las empresas afirma utilizar Máquinas virtuales.
- El 18,9% de las empresas manifiesta utilizar Herramientas criptográficas, destinadas a proteger la confidencialidad de la información tanto en tránsito como almacenada.
- El 16,8% de las empresas consultadas ha indicado utilizar Sistemas de control de contenidos confidenciales, que previenen la difusión, accidental o intencionada, de cualquier tipo de información o datos fuera de una organización.
- Finalmente, el 14,3% de las empresas ha manifestado utilizar Herramientas de auditoría técnica y forense.

FIGURA 37: PRODUCTOS DE SEGURIDAD. RESPUESTA EXPRESADA EN %

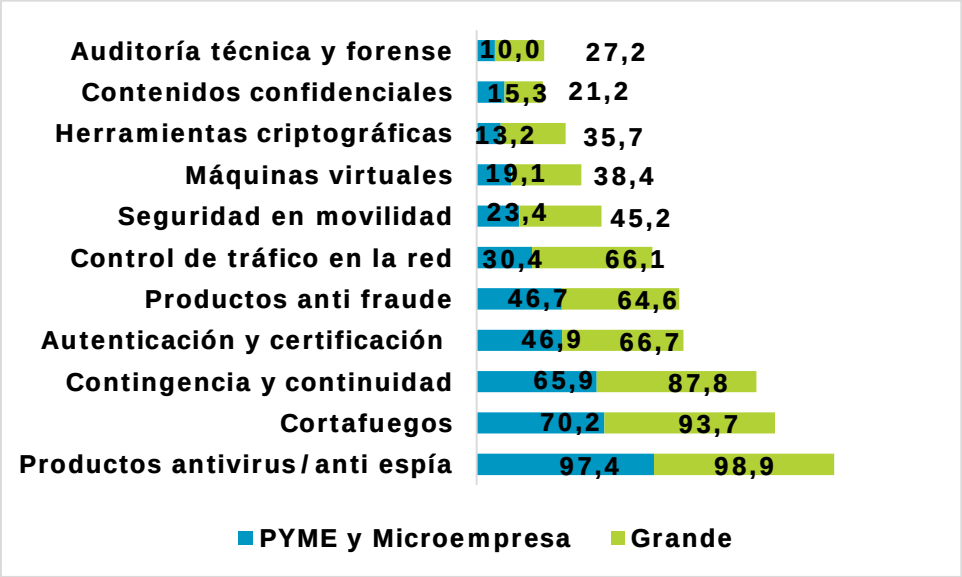
Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501. P8[25]

[25] Las categorías han sido simplificadas para los gráficos que muestran la tasa de respuesta de esta pregunta: Cortafuegos: cortafuegos, filtros de contenidos web,

Respecto a la distribución de la respuesta atendiendo al tamaño de la empresa:

Existe una relación positiva y proporcional entre el tamaño de la empresa y el número de productos de seguridad que han implantado las empresas, de manera que las grandes empresas han manifestado utilizar mayor número de productos que las PYME y microempresas.

FIGURA 38: PRODUCTOS DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base PYME y microempresa 1,123, Grande 378. P8

MEDIDAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES

90%
ACCESO MEDIANTE CÓDIGO PIN

75,2%
CONTRASEÑA DE DESBLOQUEO

46,4%
ACTUALIZACIONES DE SOFTWARE

41,2%
PROGRAMA ANTIVIRUS

En cuanto al análisis de la distribución de respuesta por sectores de actividad, no existen muchas variaciones en función de los productos de seguridad. No obstante, el sector de la Información y las comunicaciones y el de Coquerías, productos farmacéuticos, caucho y plásticos, destacan de manera positiva entre todos los demás dado que las empresas que dedican su actividad a estos sectores manifiestan utilizar un número mayor de productos de seguridad. En el lado contrario encontramos al sector de la Construcción, que destaca negativamente entre todos los sectores.

Medidas de seguridad en dispositivos móviles

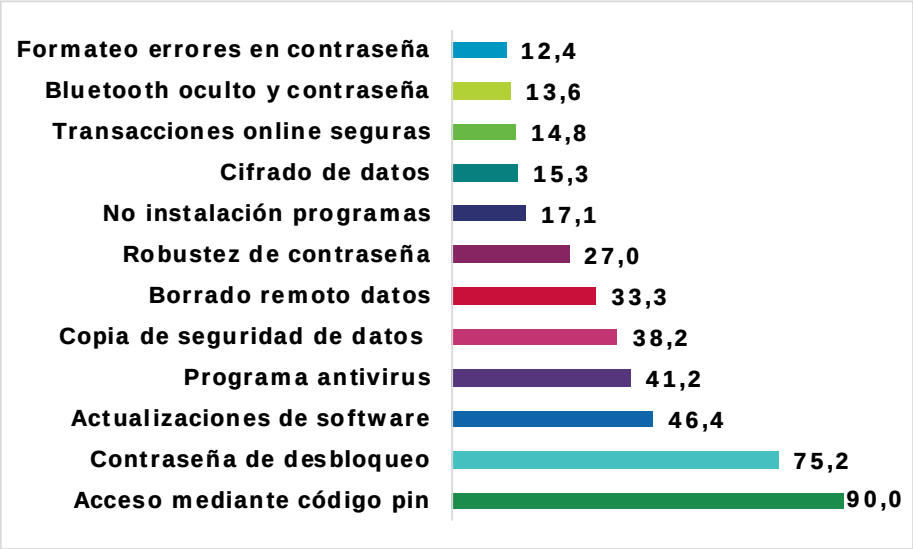
Se ha solicitado a las empresas que indicaran cuáles son las medidas de seguridad que utilizan en sus dispositivos móviles con el objetivo de obtener un indicador asociado. Esta pregunta se ha dirigido solo a las pequeñas, medianas y grandes empresas con la intención de acortar el recorrido del cuestionario entre las microempresas.

IDS, IPS; Contingencia y continuidad: herramientas de contingencia y continuidad (copias de seguridad, recuperación); autenticación y certificación: sistemas de autenticación y certificación digital y otros sistemas de gestión de accesos y control de identidades; control de tráfico en la red: sistemas de control de tráfico en la red; seguridad en movilidad: herramientas de seguridad en movilidad (para móviles, en redes inalámbricas wifi); máquinas virtuales: máquinas virtuales para realizar acciones no fiables (ejecutar ficheros, visitar páginas web).

El resultado obtenido muestra el uso extendido de medidas de seguridad en dispositivos móviles ya que el 72% de las empresas consultadas han mencionado que utilizan tres o más medidas de seguridad en estos dispositivos.

Las medidas de seguridad más mencionadas son el Acceso mediante código, pin, (90%) y la Contraseña de desbloqueo (75,2%). Les siguen las Actualizaciones de software automáticas (46,4%) y los Programas antivirus con un 41,2%.

FIGURA 39: MEDIDAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.064 (Empresas que disponen de dispositivos, portátiles, dispositivos móviles, tabletas. P9[26]

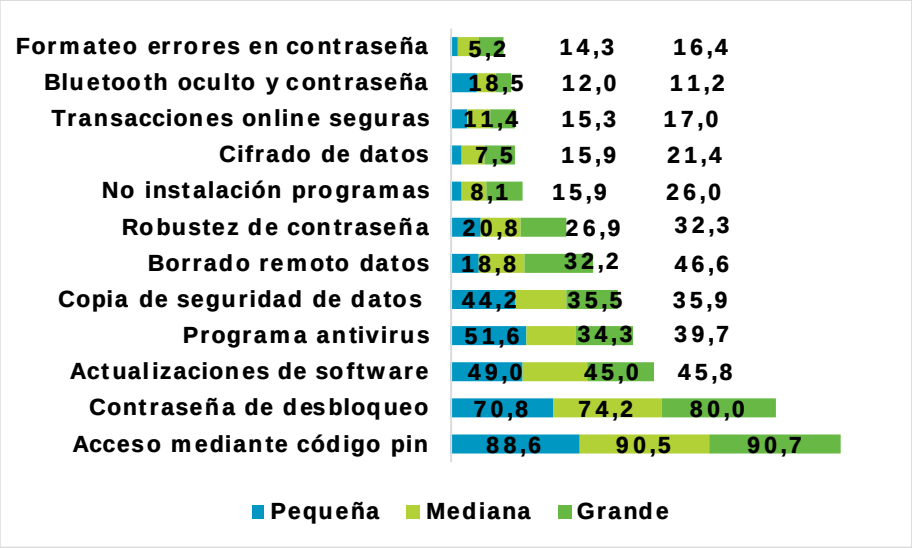
El uso de medidas de seguridad en dispositivos móviles aumenta conforme aumenta el tamaño de la empresa en la mayoría de los casos, así ocurre por ejemplo en el caso del Acceso mediante código pin, la Contraseña de desbloqueo, la Robustez de contraseña o el Borrado remoto de datos.

Muchas empresas manejan información confidencial desde dispositivos móviles como *smartphones*, tabletas, ordenadores portátiles, etc. dejando a sus empleados acceder a la información y recursos de la empresa desde fuera del entorno corporativo. Antes de usar un dispositivo personal en su negocio recomendamos leer detenidamente la Guía dispositivos móviles para uso profesional: https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el

[26] Las categorías han sido simplificadas para los gráficos que muestran la tasa de respuesta de esta pregunta: Actualizaciones de software: actualizaciones de software automáticas; copia de seguridad de datos: copia de seguridad de datos sensibles; borrado remoto datos: borrado remoto de datos en caso de extravío; no instalación de programas: imposibilidad de instalación de programas o aplicaciones; cifrado de datos: cifrado de datos y/o comunicaciones; transacciones online seguras: comprobación de conexiones seguras para transacciones online; formateo errores en contraseña: formateo tras errores en la contraseña.

Sin embargo, hay medidas que se podría decir son más características de las pequeñas empresas que de las medianas y grandes, dado que la frecuencia de la respuesta es mayor entre estas empresas proporcionalmente que entre las medianas y grandes. Así ocurre en el caso de las Actualizaciones automáticas de software, los Programas antivirus o la Copia de seguridad de datos.

FIGURA 40: MEDIDAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Pequeña 308, Mediana 391, Grande 365. P9

SERVICIOS ESPECIALIZADOS DE SEGURIDAD

72,2%
SERVICIOS DE CUMPLIMIENTO DE LA LEGISLACIÓN

51,8%
SERVICIOS DE FORMACIÓN

36,6%
SERVICIOS DE PLANIFICACIÓN E IMPLANTACIÓN DE INFRAESTRUCTURAS

Respecto a la distribución sectorial de la respuesta sobre las medidas de seguridad en dispositivos móviles, se pueden resaltar dos sectores en los que las empresas han manifestado utilizar un mayor número de medidas de seguridad; estos son: Coquerías productos farmacéuticos, caucho y plástico y el sector de la Metalurgia y fabricación de productos metálicos, con una media de cinco menciones cada uno.

Servicios especializados de seguridad

Para conocer la demanda de servicios especializados de seguridad se ha utilizado de nuevo la taxonomía de 2009 referida con anterioridad[27], que define 9 tipos de servicios especializados de seguridad.

- Los Servicios de cumplimiento de la legislación (LOPD) son los que más han manifestado las empresas consultadas utilizar con un 72,2% de las respuestas. Estos servicios ayudan a las empresas a cumplir con la legislación vigente en esta materia.
- El 51,8% de las empresas consultadas ha indicado que su negocio utiliza Servicios de formación. Estos servicios permiten a las empresas mejorar la preparación de sus empleados para lidiar con situaciones propensas a desencadenar un incidente de seguridad y aportan, por tanto, valor añadido a la empresa.

[27] *"Taxonomía (v 2.0) de soluciones de seguridad TIC"* INTECO 2009. (Actualmente INCIBE).

- Los Servicios de planificación e implantación de estructuras son utilizados por el 36,6% de las empresas consultadas.
- Los Servicios de contingencia y continuidad del negocio son utilizados por el 36,2% de las empresas consultadas.
- Un 32,8% de las empresas han mencionado recurrir a la Externalización de servicios de seguridad.
- Los Servicios de auditoría técnica son utilizados por el 30% de las empresas consultadas.
- El 28,9% de las empresas han manifestado utilizar servicios de Implantación y certificación de normativa.
- Un 27,9% de las empresas consultadas ha indicado utilizar servicios de Gestión de incidentes.
- Finalmente, el servicio que menos han señalado las empresas consultadas es el de Certificación y acreditación de políticas de seguridad, planes de seguridad y gestión de riesgos con un 27,7%.

FIGURA 41: SERVICIOS ESPECIALIZADOS DE SEGURIDAD. RESPUESTA EXPRESADA EN %

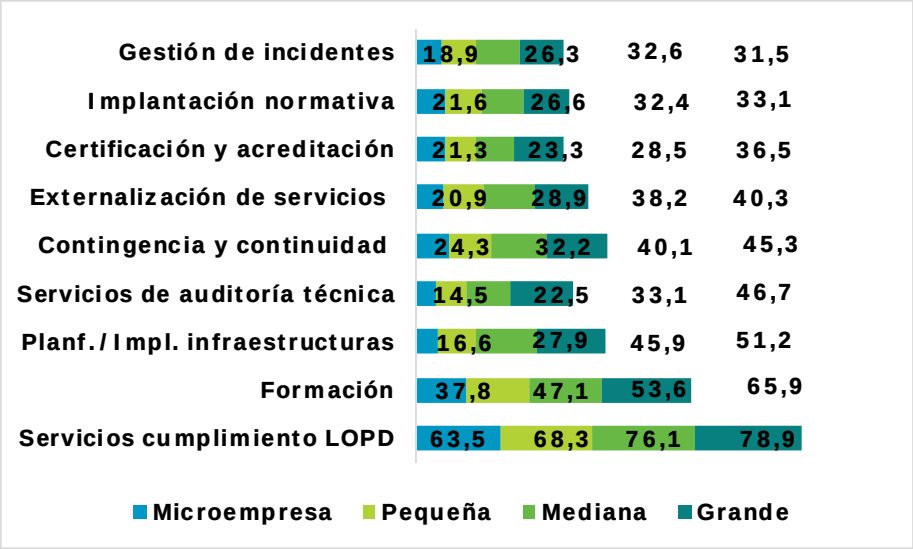
Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.476. P13

Al igual que ocurría con los productos de seguridad, el uso de los servicios especializados está relacionado proporcionalmente con el tamaño de la empresa, de manera que cuando aumenta el tamaño de la empresa también aumenta el número de tipos de servicios de seguridad que utiliza.

Cabe destacar que el servicio especializado que representa una variación mayor según el tamaño de las empresas a que responde es el de Planificación e implantación de infraestructuras con un 26,3%,

por lo que parece ser más característico de medianas y grandes empresas que de pequeñas y microempresas.[28]

FIGURA 42: SERVICIOS ESPECIALIZADOS DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 296, Pequeña 391, Mediana 414, Grande 375. P13[29]

No existe un patrón claro en la distribución de la respuesta de los servicios especializados de seguridad utilizados según el sector de actividad al que pertenezcan. Llama la atención que las empresas pertenecientes al sector de Información y comunicaciones manifiesten en menor proporción que las demás empresas (un 61,3% frente a una media de 72,2%) utilizar Servicios de cumplimiento de la legislación (LOPD). Esto podría indicar que las empresas del sector de Información y comunicaciones son más propensas a ofrecer este servicio, que a demandarlo.

Seguridad en las conexiones inalámbricas

SEGURIDAD EN LAS CONEXIONES INALÁMBRICAS

77,3%

PROTEGE LA RED WIFI UTILIZANDO EL PROTOCOLO WPA, WPA2

Se ha requerido información sobre los protocolos de seguridad utilizados en las conexiones inalámbricas. Para generar este indicador se ha mejorado la referencia de la clasificación del estudio de 2009[30] puesto que se ha distinguido entre los protocolos WPA y los protocolos WEP. La pregunta solo se ha dirigido a pequeñas, medianas y grandes

[28] Para calcular estos porcentajes se han sumado de un lado el resultado de microempresas y pequeñas y de otro el de medianas y grandes, para calcular después la variación entre ambos grupos.

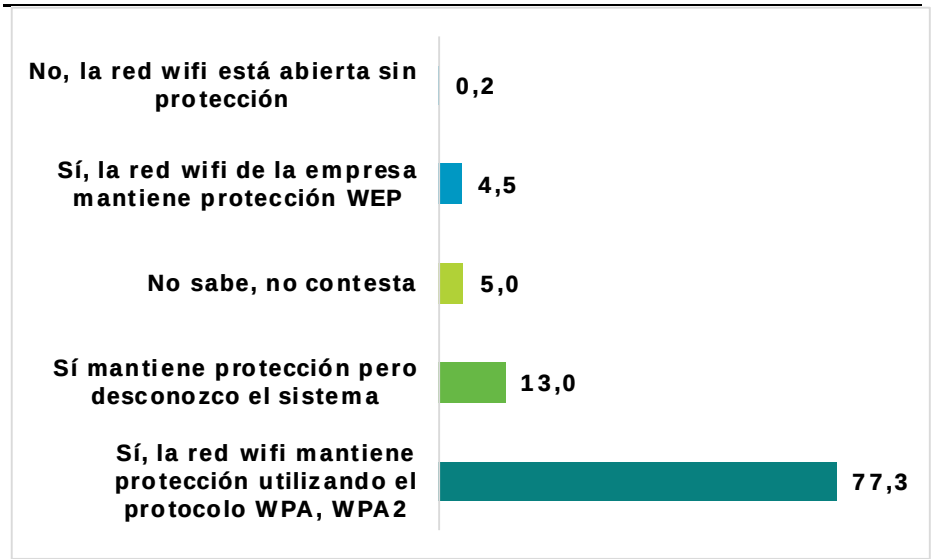
[29] Las categorías han sido simplificadas para los gráficos que muestran la tasa de respuesta de esta pregunta: Servicios cumplimiento LOPD: servicios de cumplimiento de la legislación (LOPD); Planf. /Impl. infraestructuras: planificación e implantación de infraestructuras; Contingencia y continuidad: servicios de contingencia y continuidad; externalización de servicios: externalización de servicios de seguridad: seguridad gestionada, *outsourcing*; certificación y acreditación: certificación y acreditación de políticas de seguridad, planes de seguridad, gestión de riesgos; implantación normativa: implantación y certificación de normativa.

[30] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

empresas con la intención de recortar el recorrido del cuestionario de las microempresas.

El resultado es bastante positivo ya que el 77,3% de las empresas consultadas ha manifestado que su red wifi mantiene protección utilizando WPA, WPA2. Tan sólo el 4,5% de las empresas consultadas todavía afirma contar con protección WEP y un residual 0,2% de las empresas tienen la red wifi abierta sin protección.

FIGURA 43: SEGURIDAD EN LAS CONEXIONES INALÁMBRICAS. RESPUESTA EXPRESADA EN %



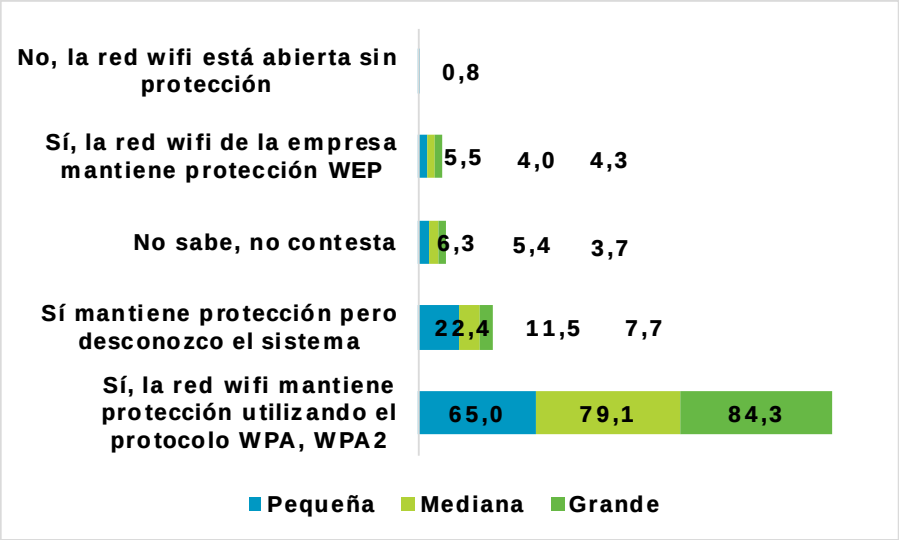
Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016.Base 977 (Empresas que han señalado que disponen de equipos y redes de comunicaciones). P10

No obstante, hay un porcentaje de empresas que desconocen cuál es la protección de seguridad de sus redes inalámbricas. De hecho, un 13% asegura que mantiene protección, pero desconoce el sistema y un 5% lo desconoce o prefiere no contestar.

El uso de dispositivos móviles y conexiones inalámbricas en el ámbito corporativo facilita y promueve el acceso a la información y a los recursos de la organización desde distintos lugares y situaciones como por ejemplo: comerciales, trabajo de campo, flotas de distribución, etc. Puesto que se trata de uno de los servicios más usados en pymes, INCIBE, consciente de los riesgos de esta tecnología, cuenta con un dosier específico para conocer los aspectos más importantes de Protección en movilidad y conexiones inalámbricas: https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-movilidad-conexiones-inalambricas

Si bien los datos no son comparables en toda su amplitud dado que el universo de empresas al que iba dirigido era diferente, el estudio de 2009, indicaba que un 81,8% de las empresas (micro y pequeñas empresas) manifestaron mantener protección wifi utilizando alguno de los dos protocolos mencionado (WEP/WPA), porcentaje idéntico al actual (para el conjunto de las empresas) si sumamos las dos respuestas.

FIGURA 44: SEGURIDAD EN LAS CONEXIONES INALÁMBRICAS POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Pequeña 254, Mediana 373, Grande 350. P10

Existe una relación proporcional entre el tamaño de la empresa y la seguridad en sus conexiones inalámbricas. De manera que las grandes y medianas empresas utilizan el protocolo WPA o WPA2 en mayor proporción significativamente que las pequeñas. Lo que concuerda con el nivel de desconocimiento del tipo de protección de la red wifi, ya que es inversamente proporcional al tamaño de las empresas, esto es, cuanto menor es el tamaño de la empresa mayor es el desconocimiento sobre el tipo de protección de su red wifi.

El análisis por sectores indica que todos mantienen un buen nivel de protección, las empresas que más afirman estar protegidas mediante el protocolo WPA y WPA2 son las pertenecientes al sector de Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor con un 89,3%, lo que resulta lógico debido a que desarrolla gran parte de su actividad en el ámbito informático. En el lado contrario encontramos el sector de Servicios de alojamiento, cuyas empresas declaran estar protegidas mediante este protocolo solo en un 64,2%.

5.3 Necesidades sobre las soluciones de seguridad

Valoración de las características de los productos de seguridad

Con el objetivo de obtener indicadores relacionados con la valoración de los productos de seguridad y sus características, se ha solicitado a las empresas que valoren siete características en una escala que va desde “Muy valorado” hasta “Nada valorado”. Los aspectos más valorados se pueden identificar como requisitos que deben mantener las soluciones para ser consideradas como adecuadas por parte de las empresas.

VALORACIÓN CARACTERÍSTICAS PRODUCTOS DE SEGURIDAD

93,5%

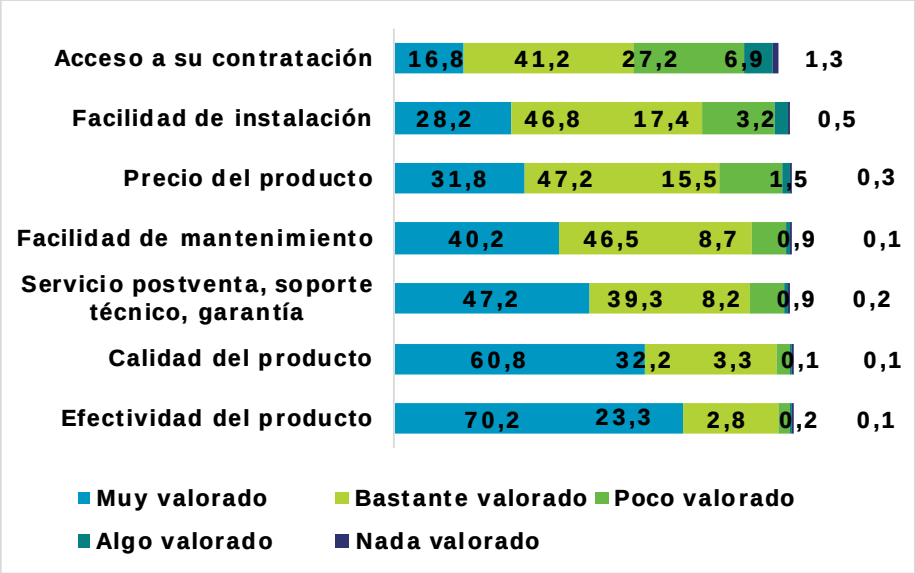
VALORAN POSITIVAMENTE LA EFECTIVIDAD DEL PRODUCTO

93%

VALORAN POSITIVAMENTE LA CALIDAD DEL PRODUCTO

La definición de estas características se ha llevado a cabo tras combinar la clasificación realizada en el "Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas" 2007[31] y en el "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas" 2009[32], a la que se le ha añadido una consideración adicional sobre el precio del producto.

FIGURA 45: VALORACIÓN DE LAS CARACTERÍSTICAS DE LOS PRODUCTOS DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1. 494. P12

Las empresas valoran positivamente todas las características de los productos de seguridad sobre las que se les ha pedido opinión, sin embargo, hay dos características que destacan sobre todas las demás, que son la Efectividad y la Calidad. De este modo, un 93,5% y un 93% de las empresas, respectivamente, consideran la Efectividad y la Calidad como elementos muy valorados o bastante valorados.[33]

Las características que menos valoran las empresas consultadas en los productos de seguridad son el Acceso a su contratación y la Facilidad de instalación. Por otro lado, resulta llamativo que aspectos como el Servicio postventa, soporte técnico y garantía o la Facilidad de mantenimiento resulten más valorados que el Precio del producto.

En este sentido, cabe destacar que el precio no es un factor determinante en la decisión de asumir un producto específico de seguridad, lo que permite concluir que se prima el valor que aporta al negocio por encima del coste de la solución.

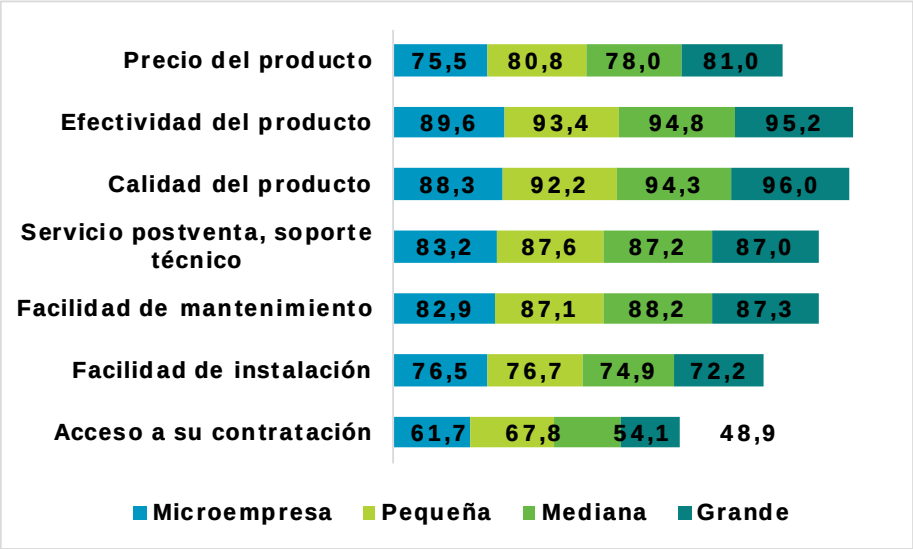
[31] "*Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*" INTECO 2007. (Actualmente INCIBE).

[32] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

[33] En la explicación ofrecida la categoría "Valorado", recoge el extremo de "Muy valorado" y "Bastante valorado" y la categoría de "No valorado", recoge el extremo "Nada valorado" y "Algo valorado". De esta forma se pretende eliminar la categoría intermedia de "Poco valorado" y aproximarnos mejor a la valoración positiva o negativa de la empresa de la característica específica.

Analizada la respuesta según el tamaño se puede apreciar como la distribución de las respuestas no es muy diferente. No obstante, se pueden identificar características de productos más valoradas entre microempresas y pequeñas empresas de un lado, y medianas y grandes de otro.

FIGURA 46: VALORACIÓN POSITIVA DE LAS CARACTERÍSTICAS DE PRODUCTOS DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 298, Pequeña 395, Mediana 423, Grande 378. P12

De este modo, vista la distribución de las respuestas cabe indicar que para las microempresas y pequeñas empresas el Acceso a la contratación y la Facilidad de instalación, son aspectos proporcionalmente más relevantes que otros, estando su respuesta por encima de la referida por las empresas medianas y grandes.

Las empresas de menor tamaño valoran más la accesibilidad del producto, probablemente por la falta de tiempo o de personal especializado para abordar las cuestiones relativas a la seguridad. Lo que podría indicar que buscan soluciones fáciles de gestionar.

Por otro lado, las medianas y grandes empresas valoran proporcionalmente más el servicio postventa y la garantía, así como la calidad y efectividad del producto.

El "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas" realizado en 2009 recogía la valoración de las PYME de las características de la oferta de productos y servicios de seguridad. Si bien es cierto que los datos no son comparables debido al uso distinto de la escala de valoración[34], resulta interesante señalar que el orden de los aspectos más valorados fue en su momento muy

[34] El estudio de INTECO (actualmente INCIBE) utilizó una escala de cuatro ítems: Lo valoro mucho, lo valoro poco, no lo valoro en absoluto y no sabe.

similar a los recogidos en el análisis actual. De este modo se valoró en primer lugar la calidad y efectividad del producto con un 66,6%, el servicio postventa se valoró en segundo lugar con un 62,1%, y la facilidad de instalación en tercer lugar con un 44,4%. Todo ello viene a indicar que el comportamiento de la demanda es similar al de entonces y podría seguir criterios bastante estables.

VALORACIÓN NECESIDAD DE LOS SERVICIOS ESPECIALIZADOS DE SEGURIDAD

Valoración de la necesidad de los servicios especializados de seguridad

Se ha solicitado a las empresas que valoren la importancia que los distintos servicios especializados de seguridad tienen para su negocio con el objetivo de obtener un indicador sobre la necesidad de servicios especializados de seguridad.

El servicio especializado más importante para las empresas españolas es el Servicio de cumplimiento de la legislación (LOPD) ya que un 78,7% lo considera necesario. En segundo lugar, un 74,4% de las empresas españolas considera necesarios los Servicios de formación, mientras un 72,3% considera la necesidad de Servicios de contingencia y continuidad de negocio. Por otra parte, la categoría especializada de seguridad que se considera más prescindible es la Externalización de servicios con un 37,5%.[35]

EL SERVICIO MÁS VALORADO COMO NECESARIO ES EL DE CUMPLIMIENTO DE LA LEGISLACIÓN (LOPD)

78,7%

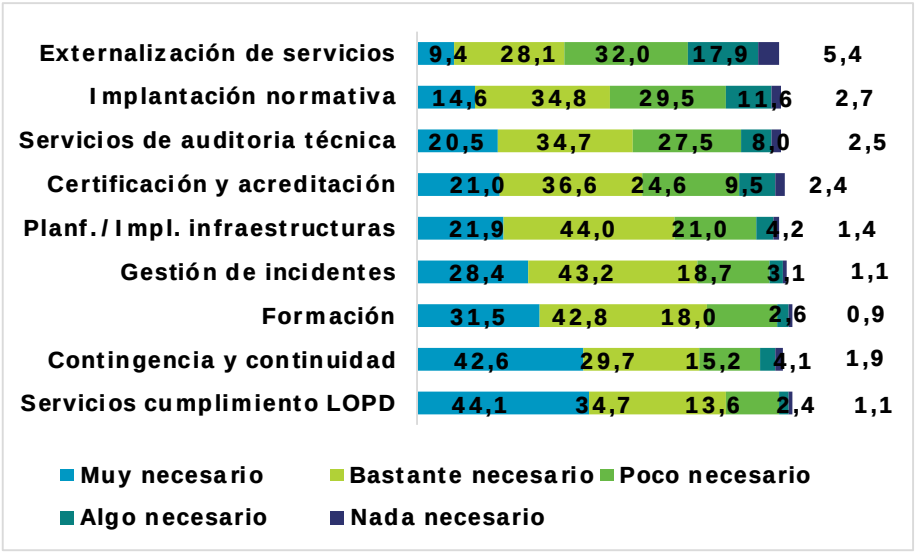
74,4%

CONSIDERA LOS SERVICIOS DE FORMACIÓN COMO NECESARIOS

72,3%

CONSIDERA LOS SERVICIOS DE CONTINGENCIA Y CONTINUIDAD DE NEGOCIO COMO NECESARIOS

FIGURA 47: VALORACIÓN NECESIDAD DE LOS SERVICIOS ESPECIALIZADOS. RESPUESTA EXPRESADA EN %

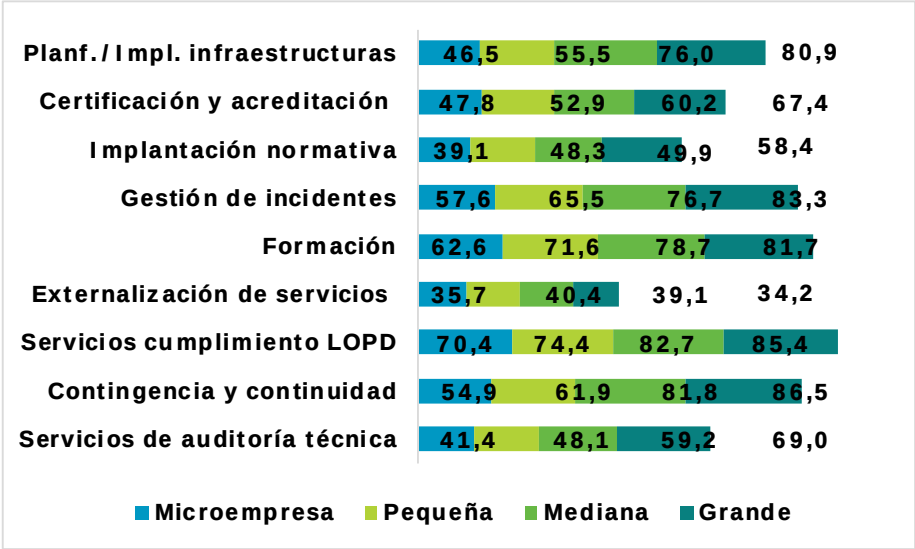


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.482. P13

Respecto a la existencia de alguna relación determinante entre considerar necesario un servicio y el tamaño de la empresa, cabe indicar que es directamente proporcional al tamaño para todos los servicios especializados, menos en el caso de la Externalización de servicios, donde las respuestas no guardan una relación proporcional.

[35] Para conocer los servicios especializados que se consideran más necesarios se ha creado la categoría "Necesario", que integra el extremo de "Muy necesario" y "Bastante necesario"; y la categoría "Prescindible", que recoge el extremo "Nada necesario" y "Algo necesaria". De esta forma se pretende eliminar la categoría intermedia "Poco necesario" y aproximarnos mejor a la necesidad de la empresa.

FIGURA 48: VALORACIÓN DE LA NECESIDAD DE LOS SERVICIOS ESPECIALIZADOS SEGÚN TAMAÑO. RESPUESTA EXPRESADA EN % (MUY NECESARIO + BASTANTE NECESARIO)



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 297, Pequeña 391, Mediana 417 y Grande 377. P13

Al igual que en el caso de los productos, el "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas" en 2009 recogió la valoración de las PYME de los servicios especializados de seguridad. Si bien los datos no son comparables debido al uso distinto de la escala de valoración[36], cabe destacar, sobre el servicio de asesoramiento especializado para el cumplimiento de la LOPD que ha crecido el número de empresas que los consideran muy necesario o bastante necesario. Todo ello viene a confirmar que el cumplimiento de la LOPD ha pasado a ser una prioridad para muchas empresas españolas.

Como se ha señalado anteriormente, INCIBE a través de su Catálogo, pone a disposición de los usuarios más de 5000 referencias de productos y servicios de ciberseguridad. Además da la oportunidad a aquellas compañías cuya actividad esté centrada en servicios de ciberseguridad, de formar parte del listado: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

[36] Este estudio de INTECO (actualmente INCIBE) utilizó una escala de cuatro ítems: Muy necesario, necesario, poco necesario y no sabe.

5.4 Barreras a la implementación de medidas y soluciones de seguridad

Barreras para la implementación de medidas de seguridad (Indicador 30 EICDE)

Para terminar con el capítulo de herramientas y medidas de seguridad resulta relevante conocer de qué factores depende la demanda y las limitaciones que se encuentran las empresas a la hora de implantar medidas de seguridad.

Las "Barreras para la implementación de medidas de seguridad" es el indicador 30 en EICDE y se han definido a partir de la clasificación utilizada por el "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas" 2009.

Los datos reflejan cierta disparidad de criterios a la hora de percibir barreras a la implementación de medidas y soluciones de seguridad. De las empresas que perciben barreras el 62,2% ha realizado tan solo una mención, el 24,7% percibe dos barreras para no implementar medidas de seguridad y el restante 14% tres motivos o más.

Cabe resaltar, también, que un alto porcentaje de empresas declara no percibir ninguna barrera a la implementación de medidas de seguridad (36,7%).

El motivo que más peso tiene para las empresas españolas a la hora de dejar de utilizar medidas de seguridad es el precio del producto, un 36,1% considera que los productos son caros y no tienen el presupuesto suficiente para adquirirlos. Esto parece una contradicción con respecto a que el precio no era una característica valorada por las empresas, aunque es posible que sean compatibles las respuestas en la medida que sea un condicionante para algunas empresas y no para todas. En cualquier caso, esto supone un reto para las empresas proveedoras de productos de seguridad, ya que estos habrán de adaptarse a las necesidades de las empresas.

De otro lado, el 28,8% de las empresas afirma no tener tiempo para abordar el proceso que supone implementar medidas de seguridad, y un 25,4% indica tener falta de personal cualificado para encargarse de soluciones de seguridad.

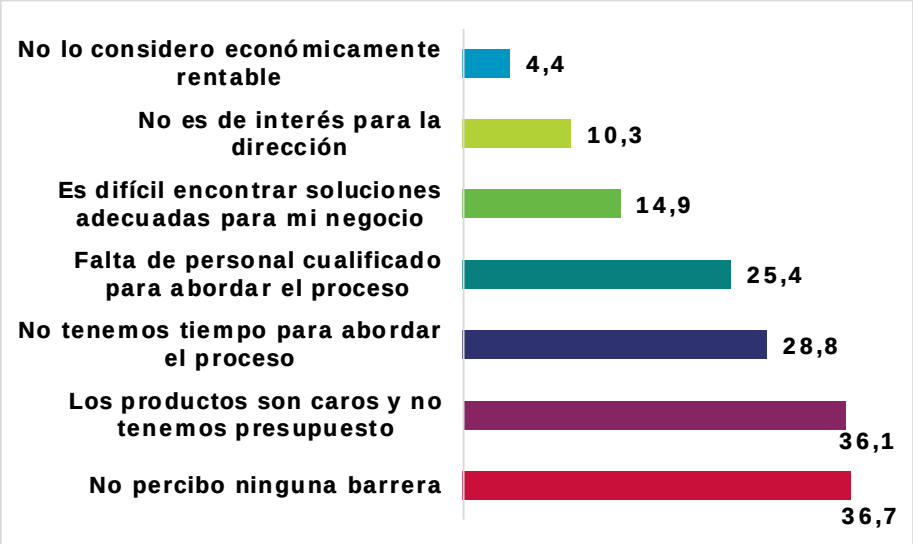
BARRERAS A LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

36,1%
LOS PRODUCTOS SON CAROS Y NO TENEMOS PRESUPUESTO

28,8%
NO TENEMOS TIEMPO PARA ABORDAR EL PROCESO

25,4%
FALTA DE PERSONAL CUALIFICADO PARA ABORDAR EL PROCESO

FIGURA 49: BARRERAS A LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD. RESPUESTA EXPRESADA EN %

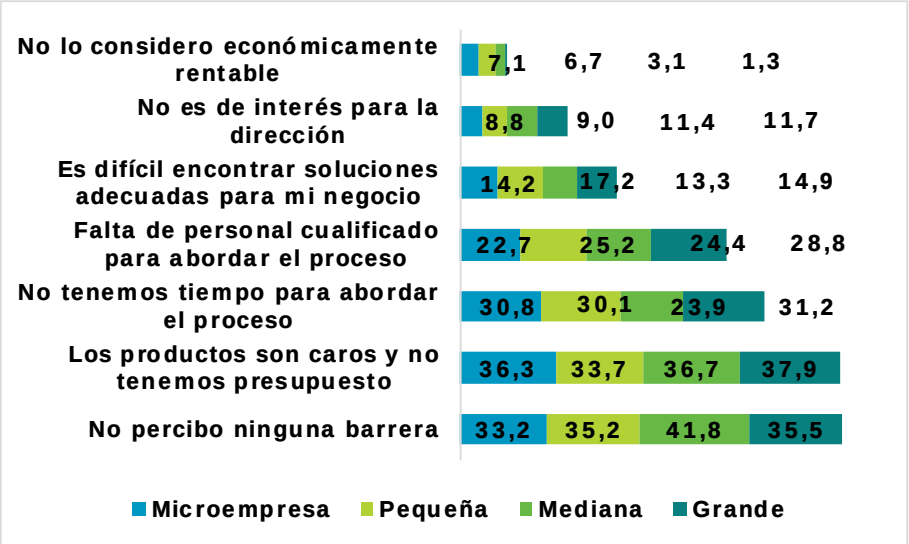


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.473. P14

De manera residual encontramos las empresas que consideran que es difícil encontrar soluciones adecuadas para su negocio (14,9%) y aquellas que afirman que no es de interés para la dirección (10,3%). Tan sólo un 4,4% indica que no lo considera económicamente rentable.

En cuanto a la distribución por tamaño de empresa, no parece existir ningún patrón específico de respuesta manteniendo una distribución bastante homogénea con algunas diferencias poco significativas.

FIGURA 50: BARRERAS A LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 295, Pequeña 389, Mediana 414, Grande 375. P14

Las empresas pequeñas, medianas y grandes perciben en mayor proporción que no existen barreras a la implementación de medidas de seguridad que las microempresas (33,2%), aunque la diferencia con las pequeñas (35,2%) y grandes (35,5%) empresas es de apenas dos puntos porcentuales, lo que no parece relevante. Son las medianas empresas las que no perciben barreras en mayor medida (41,8%).

Por otro lado, resulta llamativo que la falta de tiempo sea percibida como una barrera a la implementación de medidas de seguridad, de forma similar por parte de las microempresas (30,8%), pequeñas (30,1%) y grandes (31,2%) empresas, siendo las medianas otra vez las que tienen un comportamiento diferenciado (23,9%).

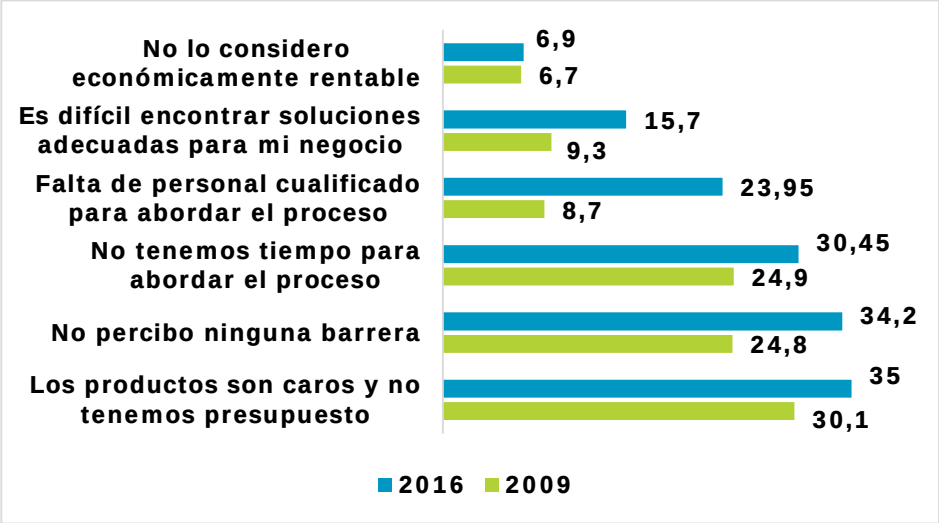
Finalmente, resulta llamativo que sean las grandes empresas las que observen la falta de personal cualificado como una barrera, frente a las microempresas, lo que sin duda tiene que ver con la mayor conciencia que pueden tener las grandes empresas sobre la complejidad que supone abordar la seguridad y las capacidades que debe mantener el personal dedicado a ello en un ámbito complejo como son este tipo de organizaciones.

Si se observa la evolución de las barreras a la implementación tomando como referencia el Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas de 2009, se verifica que los motivos para no implantar medidas de seguridad

relacionados con el precio y la falta de tiempo han crecido, pero sobre todo la falta de personal cualificado es el motivo que muestra un mayor crecimiento habiendo pasado de suponer el 8,7% de las pequeñas empresas y microempresas al 24%.

De otro lado, para este universo concreto también han aumentado las empresas que no perciben ninguna barrera del 24,8% al 34,2%.

FIGURA 51: EVOLUCIÓN BARRERAS A LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD 2009-2016 (PEQUEÑAS EMPRESAS Y MICROEMPRESAS). RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 295 y Pequeña 389. P14 y Estudio de INTECO (actual INCIBE) sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas 2009. Gráfico 8.[37]

El análisis de la distribución de la percepción de las empresas sobre las barreras a la implementación según el sector de actividad al que se dediquen no ha mostrado diferencias significativas.

Barreras a la implementación percibidas para los productos de seguridad

Tras conocer cuáles son los productos de seguridad que predominan entre las empresas españolas, resulta interesante conocer cuáles son los motivos que llevan a las empresas a no implantarlos en su negocio. Para ello se ha elaborado la siguiente tabla en la que se muestra la relación entre las barreras que perciben las empresas y los productos de seguridad que utilizan. La base de cálculo en cada caso está constituida por el número de empresas que declaran no utilizar cada producto.

[37] Para la elaboración del gráfico de evolución de las barreras a la implementación se ha eliminado la categoría "No es de interés para la dirección" por no ser comparable con el estudio de INTECO (actual INCIBE).

TABLA 4: MOTIVOS PARA NO UTILIZAR PRODUCTOS DE SEGURIDAD.

Herramientas y medidas de seguridad	No es adecuado para mi negocio	Falta de personal cualificado	Precio	Falta de tiempo	No resulta interesante	No es rentable
Productos anti fraude	15,9%	24,9%	36,6%	30,3%	12%	5,6%
Productos antivirus o anti espía	12,5%	15,6%	34,4%	28,1%	9,4%	3,1%
Herramientas de auditoría técnica y forense	14,4%	24,4%	35,8%	29,1%	10,3%	4,7%
Sistemas de autenticación y certificación digital y otros sistemas de gestión	12,6%	23,6%	36,6%	31,6%	12%	5,5%
Herramientas de contingencia y continuidad	13,9%	22,8%	34,9%	27,6%	11,1%	7,2%
Sistemas de control de contenidos confidenciales	13,6%	25,2%	37,6%	30,1%	11,3%	4,7%
Sistemas de control de tráfico en la red	15,3%	25,3%	35,9%	29,5%	10,2%	5,6%
Cortafuegos, filtros de contenidos web, IDS, IPS	12,6%	23,7%	33,7%	28,9%	12,9%	7,4%
Sistemas de herramientas criptográficas	14,6	25,5%	37,4%	29,9%	11,3%	5%
Herramientas de seguridad en movilidad	13,9%	25,4%	36,9%	30,1%	10,9%	5,2%
Máquinas virtuales para realizar acciones no fiables	14,3%	24,9%	35,9%	28,5%	10,4%	4,9%

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.473. Cruce P8 y P14.

Entre las empresas que han manifestado no utilizar Sistemas de control de contenidos confidenciales destaca la influencia del precio en su decisión con un 37,6%.

La falta de tiempo para abordar el proceso afecta algo más a las empresas que han indicado no implementar Sistemas de autenticación y certificación digital y otros sistemas de gestión (31,6%) y los Productos antifraude (30,3%).

Por otro lado, las empresas que no han implantado Sistemas de herramientas criptográficas han manifestado no hacerlo por su precio (37,4%) y por la falta de personal cualificado (25,5%).

Algunos de los productos de seguridad más habituales en las empresas han sido considerados como no interesantes, como son los Cortafuegos, filtros de contenidos web (12,9%), los Productos antifraude (12%) y los Sistemas de autenticación y certificación digital y otros sistemas de gestión (12%).

Barreras a la implementación percibidas para los sistemas internos de seguridad

Se ha realizado el mismo cruce sobre las barreras en función de los sistemas internos de seguridad, con el objetivo de comprobar cuáles son los motivos declarados por las empresas que predominan entre las empresas que no implantan sistemas de seguridad.

El precio (39,9%) y la falta de tiempo para abordar el proceso (35,2%) destacan como principales barreras para la implementación de sistemas de Autenticación con contraseña segura.

De otro lado, la falta de personal cualificado es el motivo más extendido entre las empresas que no han implantado sistemas de Identificación de usuario y autenticación mediante elementos hardware (25,3%) y mediante elementos biométricos (25,1%).

TABLA 5: MOTIVOS PARA NO UTILIZAR SISTEMAS INTERNOS DE SEGURIDAD

Sistemas internos de seguridad	No es adecuado para mi negocio	Falta de personal cualificado	Precio	Falta de tiempo	No resulta interesante	No es rentable
Autenticación con contraseña segura	11,4%	23,3%	39,9%	35,2%	13%	8,8%
Backup de datos externos	10,2%	23%	36,1%	24,8%	12,8%	7,7%
Identificación de usuario y autenticación mediante elementos biométricos	14,3%	25,1%	36,2%	29,2%	9,9%	4,8%
Identificación de usuario y autenticación mediante elementos hardware	13,8%	25,3%	38,4%	30,5%	10,8%	4,4%
Protocolos para el análisis de incidentes de seguridad	13,7%	24,9%	37,4%	31,4%	11,3%	4,7%

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.473. Cruce P7 y P14.

Barreras a la implementación percibidas para los servicios especializados de seguridad

Con los servicios especializados de seguridad ocurre lo mismo que con los productos y sistemas internos, destacan los motivos de precio, falta de tiempo y personal cualificado, y entre los servicios que más barreras de implementación presentan se puede destacar la importancia del precio para implementar Servicios de contingencia y continuidad (39,5%) y la falta de tiempo para abordar el proceso de implantar servicios de Formación (31,9%) y servicios de Implantación y certificación de normativa (31,9%).

Las empresas que declaran no utilizar los servicios de Certificación y acreditación de políticas de seguridad lo hacen principalmente por falta de personal con un 26,8%.

TABLA 6: MOTIVOS PARA NO UTILIZAR SERVICIOS ESPECIALIZADOS DE SEGURIDAD

Servicios especializados	No es adecuado para mi negocio	Falta de personal cualificado	Precio	Falta de tiempo	No resulta interesante	No es rentable
Servicios de auditoría técnica	14%	24,9%	37,2%	32,1%	11,2%	5,1%
Servicios de contingencia y continuidad	12,3%	25,4%	39,5%	31,7%	12,4%	6,1%
Servicios de cumplimiento de la legislación LOPD	12,7%	24,7%	34%	32,5%	13,7%	6,4%
Externalización de servicios	13,6%	24,5%	37,2%	30,3%	11,8%	5%
Formación	12,8%	24,8%	37,5%	31,9%	12,4%	5,4%
Gestión de incidentes	14,6%	25,9%	38,3%	30,5%	11,4%	5%
Implantación y certificación de normativa	13,6%	26,6%	37,6%	31,9%	11,5%	4,6%
Certificación y acreditación de políticas de seguridad	13,8%	26,8%	37,8%	32%	11,7%	5,4%
Planificación e implantación de infraestructuras	14,1%	26,4%	37,4%	30,7%	10,7%	5,6%

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.473. Cruce P7 y P13B.

6 INCIDENTES DE SEGURIDAD

6.1 Incidentes de seguridad y consecuencias

Descrito el uso de sistemas y soluciones de seguridad en las empresas españolas, en este apartado se presentan los datos sobre cuáles son los incidentes de seguridad que ocurren con mayor frecuencia en las empresas y en qué medida afectan a sus activos tecnológicos y de información.

INCIBE cuenta con un servicio que trata de resolver los incidentes en ciberseguridad que afectan a las empresas. Para utilizarlo, simplemente hay que enviar un correo a incidencias@certsi.es explicando el problema. El equipo del CERTSI de INCIBE se pondrá en contacto con usted para ofrecerle ayuda y recomendaciones

Grado de conocimiento de las incidencias de seguridad (Indicador 35 en EICDE)

CONOCIMIENTO DE LAS INCIDENCIAS DE SEGURIDAD

94,8%

DE LAS EMPRESAS

HA DECLARADO CONOCER LAS CONSECUENCIAS DE **MÁS DE 4 CONTINGENCIAS**

La primera observación destacable se refiere a valorar si las empresas conocen las consecuencias de los incidentes de seguridad que pueden ocurrir (Indicador 35 en EICDE).

Sobre este particular se puede concluir que las empresas españolas están bastante concienciadas de cuáles son los incidentes de seguridad y las consecuencias negativas que se pueden derivar de ellos, ya que el 94,8% ha declarado conocer las consecuencias de más de cuatro contingencias. A continuación, se exponen las categorías de respuesta que se dieron a elegir entre las empresas consultadas:

- La infección por programas informáticos que pueden infectar a otros ficheros/programas mediante la modificación del mismo (Virus), son los incidentes más conocidos por las empresas consultadas. Un 96,7% de las empresas responde que conoce las consecuencias negativas que se derivan de este incidente.

En la actualidad la amenaza más temida por las empresas son los ataques de *ransomware*. Por ello INCIBE dispone por un lado del Servicio Antiransomware: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware para tratar de solucionar los problemas de este riesgo y además cuenta con una guía https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario para conocer más en detalle este tipo de malware y cómo hacerle frente

- Un 94,6% de las empresas ha manifestado conocer el Correo basura y sus consecuencias. Este tipo de correo hace referencia a los mensajes no solicitados, no deseados o con remitente no conocido.

GRADO DE CONOCIMIENTO DE LAS INCIDENCIAS DE SEGURIDAD

EL VIRUS ES LA CONTINGENCIA MÁS CONOCIDA ENTRE LOS INCIDENTES DE CIBERSEGURIDAD

96,7%

LE SIGUE EL CORREO BASURA

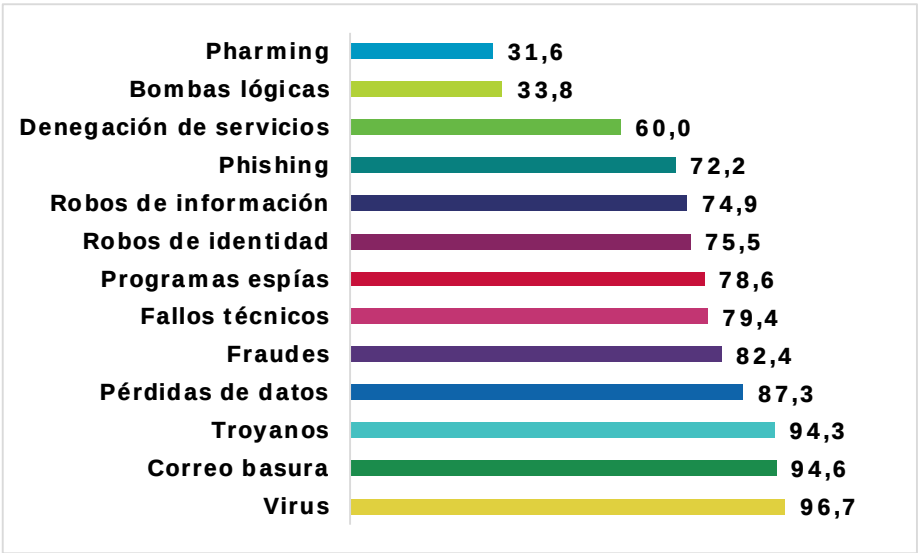
94,6%

TROYANOS

94,3%

- Un 94,3% de las empresas consultadas conocen que los Troyanos presentan un nivel de peligrosidad alto.
- El 87,3% de las empresas consultadas ha manifestado conocer las consecuencias que tiene la Pérdida de datos en su negocio.
- El 82,4% afirma conocer las consecuencias negativas que pueden tener los Fraudes en el funcionamiento de su empresa.
- El 79,4% de las empresas consultadas ha señalado conocer las consecuencias negativas que pueden derivarse de los Fallos técnicos.
- El 78,6% de las empresas consultadas manifiesta conocer la existencia y consecuencias de Programas espías.
- El 75,5% de las empresas ha reconocido que los Robos de identidad tienen consecuencias negativas en su empresa.
- El 74,9% afirma conocer también las consecuencias negativas que tienen los Robos de información como incidente de seguridad.
- Un 72,2% de las empresas consultadas ha manifestado conocer los problemas que se derivan del *Phishing* como incidente de seguridad.
- El 60% de las empresas ha reconocido las consecuencias negativas de la Denegación de servicios para el funcionamiento de su empresa.
- En último lugar, las empresas han reconocido las consecuencias negativas que se derivan de las Bombas lógicas (33,8%) y el *Pharming* (31,6%).

FIGURA 52: PERCEPCIÓN CONSECUENCIAS NEGATIVAS QUE PUEDAN DERIVARSE DE INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %

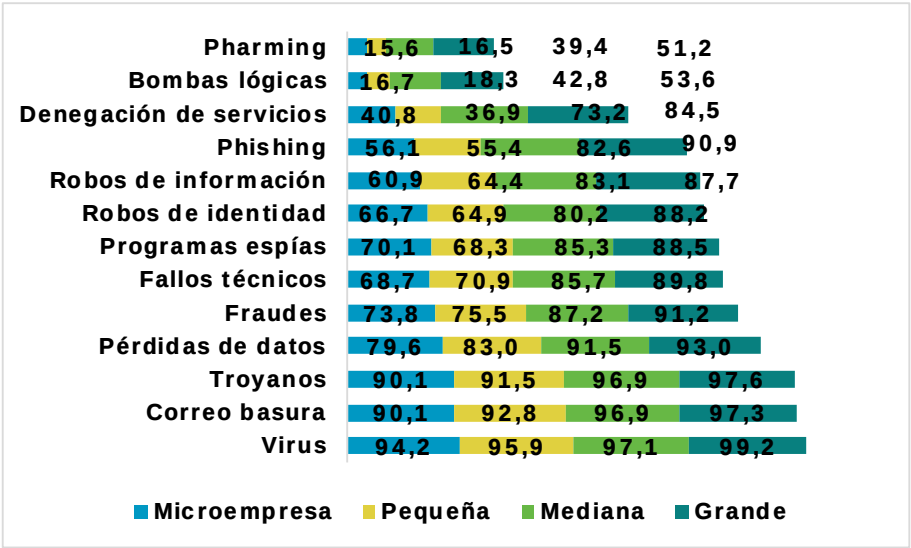


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.469. P15

Las medianas y grandes empresas tienen mayor conocimiento sobre las consecuencias negativas que tienen los incidentes de seguridad para su negocio que las microempresas y pequeñas empresas.

Cuanto mayor es la empresa mayor grado de conocimiento muestra de las consecuencias que las incidencias de seguridad tienen para su negocio.

FIGURA 53: PERCEPCIÓN CONSECUENCIAS NEGATIVAS QUE PUEDAN DERIVARSE DE INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 294, Pequeña 388, Mediana 414, Grande 373. P15

INCIDENTES DE SEGURIDAD SUFRIDOS DURANTE EL ÚLTIMO AÑO

30%

DE LAS EMPRESAS CONSULTADAS NO HA SUFRIDO NINGÚN INCIDENTE DE SEGURIDAD DURANTE EL ÚLTIMO AÑO

EL INCIDENTE DE SEGURIDAD MÁS SUFRIDO ES LA AFECTACIÓN POR CÓDIGO DAÑINO

46,5%

Respecto a la distribución sectorial, destacan las empresas que se dedican al sector de Coquerías, productos farmacéuticos, caucho y plástico ya que han manifestado conocer en mayor proporción las consecuencias de los incidentes de ciberseguridad que las demás empresas.

Incidentes de seguridad sufridos (Indicador 32 en EICDE)

Un incidente de ciberseguridad es un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones de la organización y de amenazar la seguridad de la información.

Los ataques dirigidos a empresas son cada vez más comunes. Así la información sobre clientes, proveedores o usuarios que poseen las organizaciones constituye un activo de gran valor que los atacantes pueden convertir en lucro económico o daño *reputacional* a la compañía afectada.

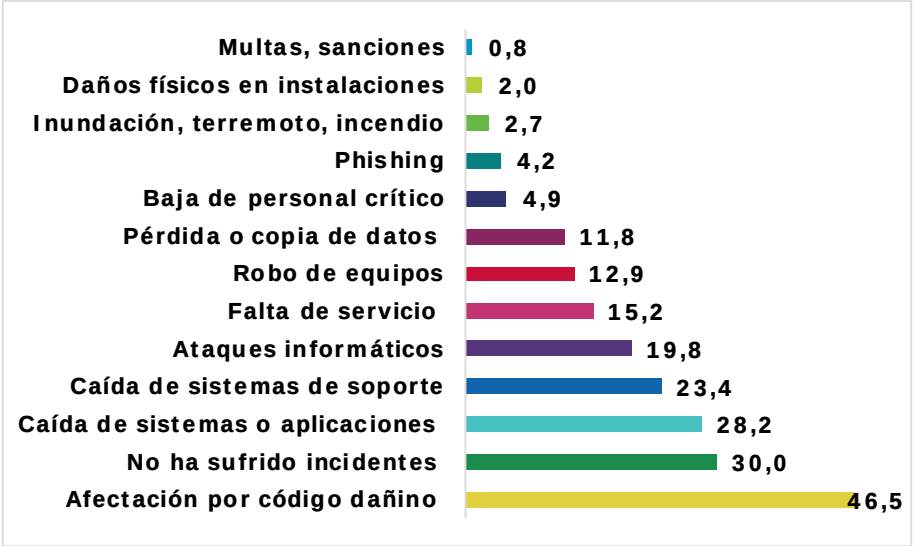
Con el objetivo de conocer los incidentes de seguridad que las empresas consultadas manifiestan haber sufrido durante el último año y obtener así el indicador 32 en EICDE, se ha solicitado a las

empresas que señalasen uno o más incidentes sufridos a partir de la clasificación establecida en estudios previos y la creada por el Centro Criptológico Nacional[38].

Frente a los ataques dirigidos, desde INCIBE se quiere concienciar para hacer frente también a este tipo de riesgos. Algunas referencias que pueden consultarse acerca de esa amenaza son:
- El fraude del CEO:
https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo
- Pretenden "hackear" su empresa:
https://www.incibe.es/protege-tu-empresa/avisos-seguridad/oleada-correos-fraudulentos-amenazan-hackear-tu-empresa

Los datos reflejan que la mayoría de las empresas ha sufrido algún tipo de incidente de seguridad a lo largo del último año. Tan solo el 30% de las empresas españolas manifiesta que no ha sufrido ningún incidente de seguridad durante dicho período. El 52,2% de las empresas indica que ha sufrido tan solo un incidente de seguridad y el restante dos o más incidentes.

FIGURA 54: INCIDENTES DE SEGURIDAD SUFRIDOS DURANTE EL ÚLTIMO AÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.467. P16

El incidente de seguridad más común entre las empresas consultadas es la Afectación por código dañino (46,5%). La caída de los sistemas o de las aplicaciones y la caída de sistemas de soporte también se encuentran entre los incidentes más comunes, con un 28,2% y un 23,4% respectivamente.

[38] "*Esquema nacional de seguridad gestión de incidentes*" 2016. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Muchos de los incidentes que se producen en las empresas tienen un componente de interacción por parte de algún empleado de la misma, normalmente sin su conocimiento. Para estudiar el nivel de riesgo de una empresa en base a la concienciación de sus usuarios, INCIBE cuenta con el Kit de Concienciación.
https://www.incibe.es/protege-tu-empresa/kit-concienciacion
Este kit cuenta con un manual de implantación y los recursos necesarios para elevar el nivel de concienciación en ciberseguridad de su organización.

El estudio de 2012[39] de pequeñas y medianas empresas reflejaba una situación muy distinta en lo que a incidentes de seguridad se refiere. En dicho estudio casi un 74% de las empresas declaraba no haber sufrido incidentes de seguridad, lo que representa 44 puntos porcentuales más de empresas con respecto a lo indicado en esta encuesta de 2016.

El estudio de 2012 justificó este porcentaje por una falta de concienciación elevada de lo que representan los incidentes y sus consecuencias, ya que en opinión de los expertos existe un amplio porcentaje de incidentes de seguridad que pasan desapercibidos. A lo que, además, hay que añadir la distinta forma de preguntar por los incidentes sufridos. El estudio de 2012 realizó una pregunta dicotómica, "Empresas que afirman haber sufrido algún incidente de seguridad", sin especificar el tipo de incidentes. Es posible que al preguntar por cada uno de los incidentes que pueden producirse, como se hace en la presente encuesta, se haya fomentado la respuesta de las empresas, que se hayan podido ver reconocidas en algún incidente.

En cualquier caso, las respuestas en esta encuesta de 2016 mostrarían cómo ha evolucionado la capacidad de las empresas de identificar la ocurrencia de los distintos incidentes, lo que indicaría en consecuencia una capacidad mayor de respuesta.

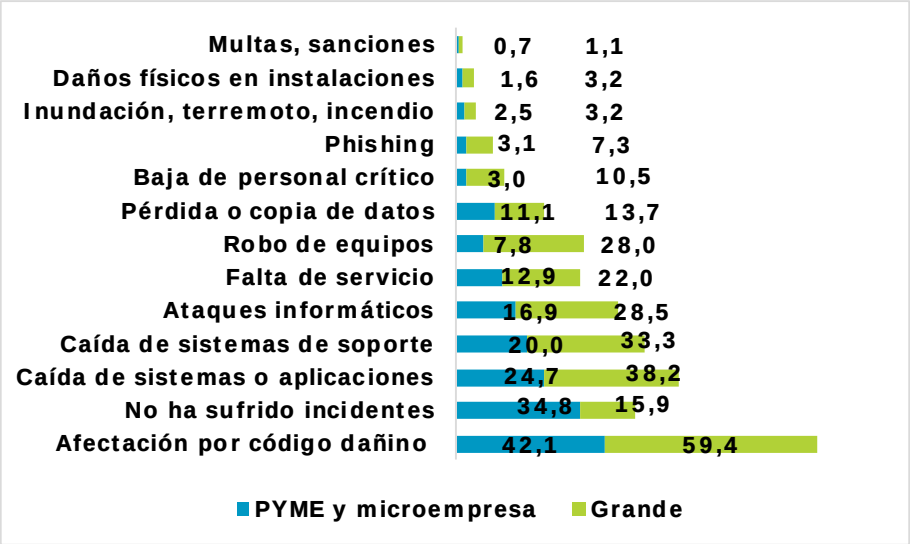
Siguiendo la línea de los resultados obtenidos, resulta positivo que las empresas declaren sufrir más incidentes de seguridad, ya que implica una evolución en la concienciación acerca de los riesgos a los que están expuestas.

Tras analizar la distribución por tamaño de empresa de la respuesta sobre haber sufrido incidentes de seguridad, se observa que existe una relación proporcional entre la frecuencia de incidentes de seguridad y el tamaño, de manera que cuanto mayor son las empresas más incidentes de seguridad manifiestan sufrir. Las PYME y microempresas manifiestan en menor proporción que las grandes

[39] "*Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*" INTECO 2012. (Actualmente INCIBE).

sufrir incidentes, lo que también podría indicar que las grandes empresas son más conscientes de los incidentes que sufre su empresa, dado que, por lo general, cuentan con departamentos de informática y monitorizan dichos procesos.

FIGURA 55: INCIDENTES DE SEGURIDAD SUFRIDOS DURANTE EL ÚLTIMO AÑO SEGÚN TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base PYME y microempresas 1.095 y Grande 372. P16

CARACTERIZACIÓN DE LA EMPRESA E INCIDENTES DE SEGURIDAD

82,5% DE LAS EMPRESAS CONSULTADAS QUE GESTIONA INSTALACIONES E INFRAESTRUCTURAS DE SISTEMAS HA SUFRIDO INCIDENTES DE SEGURIDAD

80,3%

DE LAS EMPRESAS QUE GESTIONA INFORMACIÓN CLASIFICADA, SENSIBLE O CONFIDENCIAL HA SUFRIDO INCIDENTES DE SEGURIDAD

No existen grandes diferencias entre sectores de actividad a los que pertenecen las empresas y los incidentes que han manifestado haber sufrido durante el último año.

En cualquier caso, las empresas que pertenecen al sector de la Información y las comunicaciones, el sector de Actividades profesionales, científicas y técnicas y el sector de Actividades administrativas y auxiliares son las que han manifestado haber sufrido mayor variedad de incidentes.

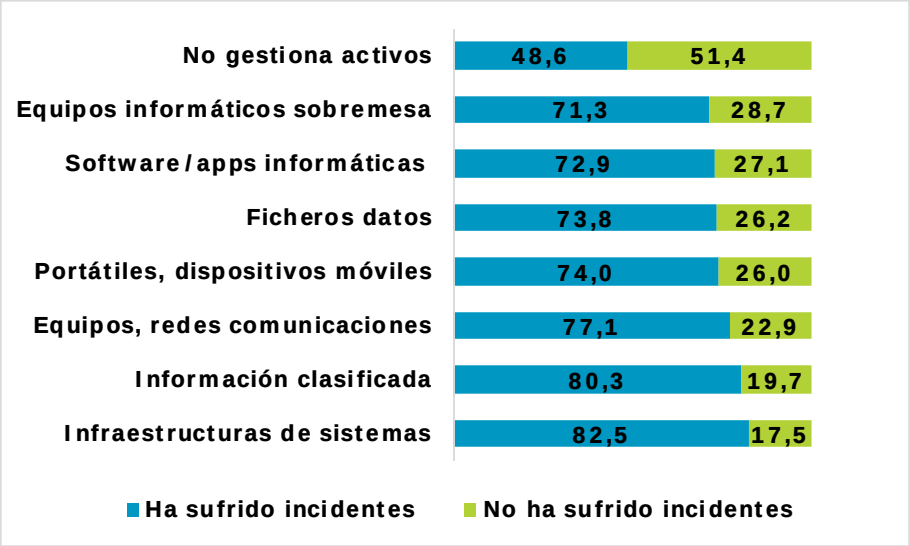
De otro lado, las empresas que pertenecen al sector de las Actividades inmobiliarias son las que más han manifestado haber sufrido un menor número de incidentes de los indicados.

Caracterización de la empresa e incidentes de seguridad

Se ha procedido a cruzar los incidentes de seguridad que empresas han declarado sufrir y el número de activos tecnológicos y de información que manifestaron utilizar con el objetivo de establecer alguna relación entre los activos y los incidentes.

El número de activos tecnológicos y de información que gestionan las empresas y el número de incidencias que registran están proporcionalmente relacionados, cuanto más activos gestiona una empresa más probabilidades hay de que pueda tener algún tipo de incidente ya sea relacionada con la pérdida o robo de información o con fallos tecnológicos, lo que supone la necesidad de una adecuada gestión de los activos.

FIGURA 56: INCIDENTES DE SEGURIDAD SUFRIDOS SEGÚN ACTIVOS TECNOLÓGICOS. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.467. Cruce P1 y P16

Existe por tanto una correlación significativa entre gestionar un gran número de activos tecnológicos y sufrir más incidentes de seguridad. Las Instalaciones e infraestructuras de sistemas es el activo que más incidentes sufre con un 82,5%. Del mismo modo, el 80% de las empresas que gestionan Información clasificada, sensible o confidencial sufre incidentes de seguridad.

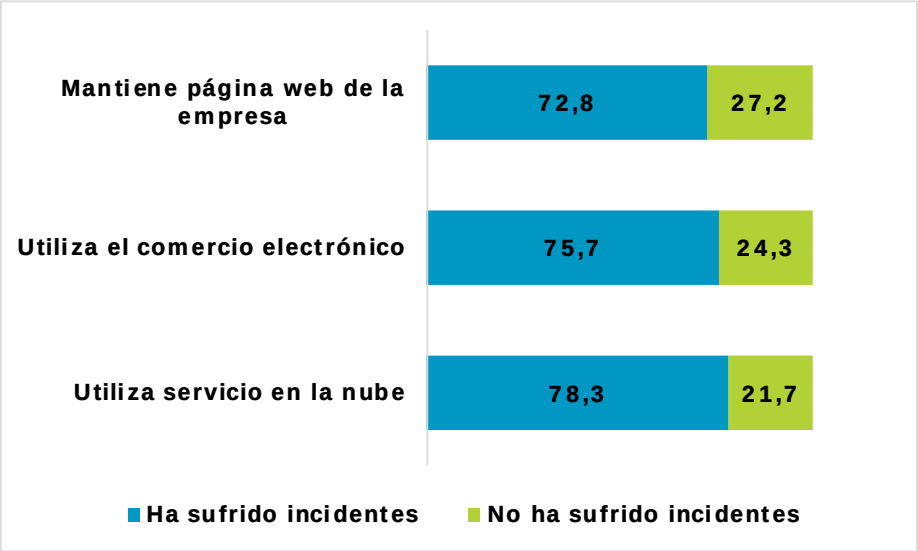
Los activos que según las empresas sufren proporcionalmente menos incidentes de seguridad, son los dos más extendidos en las empresas consultadas. De este modo, un 28,7%de las empresas que mantienen este tipo de activos, en concreto los equipos informáticos de sobremesa, manifiesta que no han sufrido incidentes de seguridad. Del mismo modo, un 27,1% de las empresas que indica que mantienen Software y aplicaciones informáticas indica que no ha sufrido incidentes. Se debe entender, en cualquier caso, que la relación establecida se refiere a la frecuencia relativa de los incidentes vinculada a la frecuencia con que se menciona mantener los activos específicos, lo que no significa que sean los incidentes más o menos frecuentes en términos absolutos.

Por otro lado, se ha procedido a analizar la relación entre las empresas que han sufrido algún incidente de seguridad durante el último año y aquellas que declaraban utilizar alguno tipo de servicio electrónico o realizar algún tipo de transacción electrónica.

Respecto a los servicios o transacciones electrónicas existe una relación positiva y proporcional, de manera que crecen los incidentes de seguridad entre las empresas que declaran utilizar o realizar un mayor número de servicios o transacciones –página web, comercio electrónico o servicios en la nube–.

78,3% DE LAS EMPRESAS QUE UTILIZAN SERVICIO EN LA NUBE SUFREN INCIDENTES DE SEGURIDAD

FIGURA 57: INCIDENTES DE SEGURIDAD SUFRIDOS SEGÚN SERVICIOS ELECTRÓNICOS QUE UTLIZAN. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.467. Cruce P4 y P16[40]

No existen grandes diferencias entre los distintos servicios electrónicos que utilizan las empresas y los incidentes de seguridad que sufren, si bien las empresas que utilizan servicios en la nube sufren más incidentes de seguridad (78,3%) que las que indican realizar operaciones de comercio electrónico (75,7%) o las que mantienen página web de la empresa (72,8%).

Cabe concluir que cuantos más activos tecnológicos y de información gestione una empresa y más presencia en Internet haya desarrollado mediante el uso de servicios o la realización de transacciones electrónicas, la empresa indica que aborda más riesgos e incidentes de seguridad. La creciente declaración sobre el uso de activos y servicios electrónicos parece indicar que las empresas se exponen a crecientes problemas de seguridad, por lo que en un entorno como el actual, la seguridad TIC de la empresa se convierte en un elemento esencial para la estabilidad del negocio de las empresas.

Políticas de seguridad e incidentes sufridos

Se ha procedido también a analizar la relación entre las respuestas sobre incidentes de seguridad que han manifestado sufrir las empresas y la existencia de una política de seguridad.

[40] La categoría utiliza servicio en la nube se ha creado a partir de la agrupación de las respuestas referidas a las categorías: tiene contratados a terceros servicios en la nube de alojamiento de correo electrónico y/o página web, contrata servicios en la nube de alojamiento, de acceso de datos y contenidos de información en remoto y contrata aplicaciones de software como servicio en la nube. La categoría utiliza el comercio electrónico reúne las categorías ha realizado compras por comercio electrónico y ha realizado ventas por comercio electrónico.

La existencia de una política de seguridad no supone que se declare que se sufren menos incidentes de seguridad, más bien al contrario, dado que existe una relación proporcional entre la implantación de políticas de seguridad y el número de incidentes que sufren las empresas.

Las empresas que tienen definida una política de seguridad también sufren más incidentes de seguridad, lo que probablemente tiene que ver con la existencia de registros específicos que permiten su gestión, una mayor capacidad de aminorar sus consecuencias y una mayor consciencia de ocurrencia concreta de los incidentes.

Se puede concluir que la existencia de una política de seguridad no disminuye necesariamente la existencia de incidentes, sino que permite una adecuada gestión de los mismos, aminorando su impacto.

POLÍTICAS DE SEGURIDAD E INCIDENTES SUFRIDOS

EL INCIDENTE DE SEGURIDAD MÁS SUFRIDO ENTRE LAS EMPRESAS QUE HAN DEFINIDO UNA POLÍTICA DE SEGURIDAD ES EL ROBO DE EQUIPOS

86,8%

EL SEGUNDO INCIDENTE MÁS COMÚN ES LA BAJA DE PERSONAL CRÍTICO

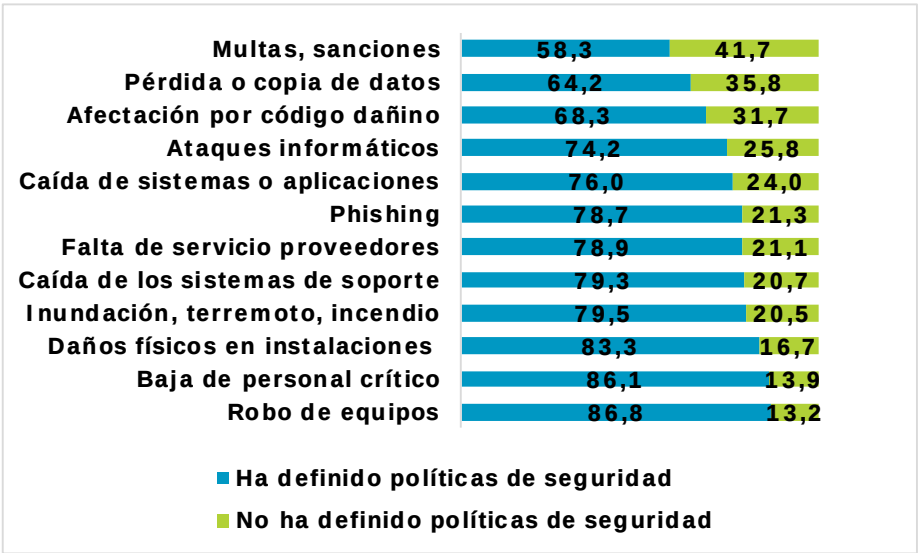
86,1%

EN TERCER LUGAR, ENCONTRAMOS LOS DAÑOS FÍSICOS EN INSTALACIONES

83,3%

Resulta relevante destacar además que los incidentes de seguridad que predominan entre las empresas que han definido una política de seguridad son diferentes a los incidentes de seguridad más comunes entre el resto de las empresas.

FIGURA 58: INCIDENTES DE SEGURIDAD SUFRIDOS Y EMPRESAS QUE HAN DEFINIDO POLÍTICAS DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501. Cruce P6 y P16

Como se puede observar, los incidentes de seguridad más sufridos por las empresas que tienen definida una política de seguridad están relacionados con daños físicos o falta de personal.

Por otra parte, la Afectación por código dañino es uno de los incidentes que menos se producen entre las empresas que han definido una política de seguridad, ya que pasa de ser el incidente de seguridad más padecido por el total de empresas consultadas a ser uno de los que menos afectan a aquellas que han declarado haber definido una política de seguridad.

Todo ello, muestra la relevancia de adoptar políticas de seguridad en la medida que permiten mejorar la gestión de los incidentes reduciendo su impacto y controlar en mayor medida la ocurrencia de determinados tipos de incidentes.

Productos de seguridad e incidentes sufridos

También se ha procedido a analizar la relación entre los distintos productos de seguridad utilizados y los incidentes de seguridad sufridos con el objetivo de identificar si disminuyen los incidentes con el uso de productos concretos.

TABLA 7: INCIDENTES SUFRIDOS SEGÚN PRODUCTOS SEGURIDAD

Incidentes de seguridad	Productos anti-fraude	Productos anti-virus	Herramientas de auditoría técnica	Sistemas autenticación y certificación	Herramientas contingencia y continuidad	Control contenidos confidenciales	Control de tráfico en la red	Cortafuegos	Sistemas de herramientas criptográficas	Herramientas de seguridad en movilidad	Máquinas virtuales
Ataques informáticos	24,4%	20,1%	32,2%	22,4%	22,2%	28,9%	28,5%	22,8%	29,2%	27,7%	30,3%
Afectación por código dañino	52,2%	47%	51,7%	48,7%	51%	45%	53,8%	51,6%	56,6%	51,2%	57,2%
Robo de equipos	17,1%	13,1%	23,7%	17,1%	16,1%	20,9%	22,4%	16%	25,3%	20,9%	19,5%
Pérdida o copia de datos e información	12,6%	11,9%	15,2%	13,3%	12,9%	14,1%	13%	12,4%	13,9%	13,3%	13,9%
Caída de los sistemas o aplicaciones de la empresa	32,1%	28,4%	44,5%	35,4%	32,6%	36,9%	38,3%	32,3%	39,5%	36%	39,7%
Caída de los sistemas de soporte	29,7%	23,8%	38,9%	28,6%	28,7%	28,1%	35,4%	27,9%	36,7%	31,4%	37,4%
Daños físicos	2,7%	2%	4,7%	2,6%	2,4%	4,8%	3,4%	2,2%	4,3%	3,3%	2%
Phising	5,7%	4,1%	12,3%	5,6%	5,3%	6,4%	6,2%	4,9%	8,5%	5,8%	4,8%
Baja personal crítico	6,5%	4,9%	11,8%	7,6%	6,2%	9,2%	8,9%	6,3%	7,8%	7,4%	9,9%
Falta de servicio proveedores	18,1%	15,4%	19,9%	18,8%	17,1%	20,5%	21,4%	17,6%	22,8%	18,4%	20,4%
Inundación, terremoto	3,7%	2,7%	2,8%	3,4%	3%	4,4%	3,2%	3%	5,3%	4,7%	3,7%
Multas, sanciones	0,5%	0,8%	0,9%	0,8%	0,8%	1,6%	0,7%	0,8%	1,1%	0,9%	0,8%

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.501. Cruce P8 y P16

En general la frecuencia con que las empresas mencionan haber sufrido los incidentes de seguridad más relevantes (Afectación por código dañino, la Caída de sistemas o aplicaciones y/o la Caída de sistemas de soporte) es similar independientemente de los productos de seguridad implantados. En la tabla anterior se indica en qué tipo de soluciones de seguridad se manifiestan en mayor medida cada uno de los incidentes.

Se muestra, por ejemplo, en términos relativos, que las empresas que utilizan Máquinas virtuales para realizar acciones no fiables son las que más padecen la Afectación por código dañino con un 57,2% y las que más han declarado haber tenido Ataques informáticos durante el último año (30,2%).

Las empresas que cuentan entre sus soluciones con Herramientas de auditoría técnica y forense son las que mencionan más incidentes de seguridad. De este modo, son las que más indican que han padecido la Caída de sistemas de soporte con un 38,9%, Pérdida o copia de datos con un 15,2%, Abuso de privilegios y/o usos inadecuados por suplantación de identidad (*phishing*) con un 12,3%, lo que puede estar relacionado con la capacidad que generan las herramientas mencionadas de detectar la ocurrencia de incidentes de seguridad.

Como se viene señalando en este informe, INCIBE a través de su Catálogo, pone a disposición de los usuarios más de 5000 referencias de productos y servicios de ciberseguridad. Además da la oportunidad a aquellas compañías cuya actividad esté centrada en servicios de ciberseguridad, de formar parte del listado: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

Consecuencias derivadas de los incidentes de seguridad (Indicador 33 en EICDE)

Con el objetivo de medir las consecuencias de los incidentes de seguridad, se ha solicitado a las empresas que indicaron haber sufrido algún incidente que identificaran las consecuencias que generó en su negocio.

A continuación, se detalla la clasificación de las consecuencias derivadas de los incidentes de seguridad utilizada, para lo que se ha tomado como referencia del "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas" 2009[41].

- Pérdida de tiempo de trabajo (horas)
- Problemas de conexión/redes
- Caída de los ordenadores
- Daños en los equipos (hardware)
- Pérdida de confianza en los medios electrónicos
- Daños en la imagen/reputación de su negocio
- Fraude con prejuicio económico

[41] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

CONSECUENCIAS INDICENTES DE SEGURIDAD

61,6%

DE LAS EMPRESAS CONSULTADAS, LA PÉRDIDA DE TIEMPO DE TRABAJO FUE UNA DE LAS CONSECUENCIAS DE LOS INDICENTES DE SEGURIDAD SUFRIDOS

LOS PROBLEMAS DE CONEXIÓN O DE REDES SON LA SEGUNDA CONSECUENCIA MÁS NOMBRADA

31,2%

SEGUIDA DE LA PÉRDIDA DE ARCHIVOS Y DATOS

30,6%

- Pérdida de archivos, datos
- Multas, sanciones
- Otros

En opinión de las empresas que han declarado haber sufrido algún incidente de seguridad, la consecuencia más relevante a la que se enfrentan es la Pérdida de tiempo de trabajo (horas) con un 61,6% de las respuestas.

FIGURA 59: CONSECUENCIAS DERIVADAS DE LOS INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.027 (Empresas que han sufrido incidentes de seguridad en el último año). P16.1

En segundo lugar, las consecuencias más mencionadas por las empresas están asociadas a los Problemas de conexión y redes con un 31,2%, seguido muy de cerca de la Pérdida de archivos y datos con un 30,6%.

Relativamente alto puede considerarse que el 23% de las empresas encuestadas afirme que los incidentes de seguridad no tuvieron consecuencia alguna, lo que puede suponer que no se conocen realmente las posibles consecuencias que se han derivado, o que dichos incidentes no fueron significativos.

Respecto a la distribución por tamaño de empresa de las consecuencias de los incidentes de seguridad no existe una relación significativa y proporcional. Sin embargo, sí se puede concluir que se han identificado consecuencias más características de unos tamaños de empresa que de otros.

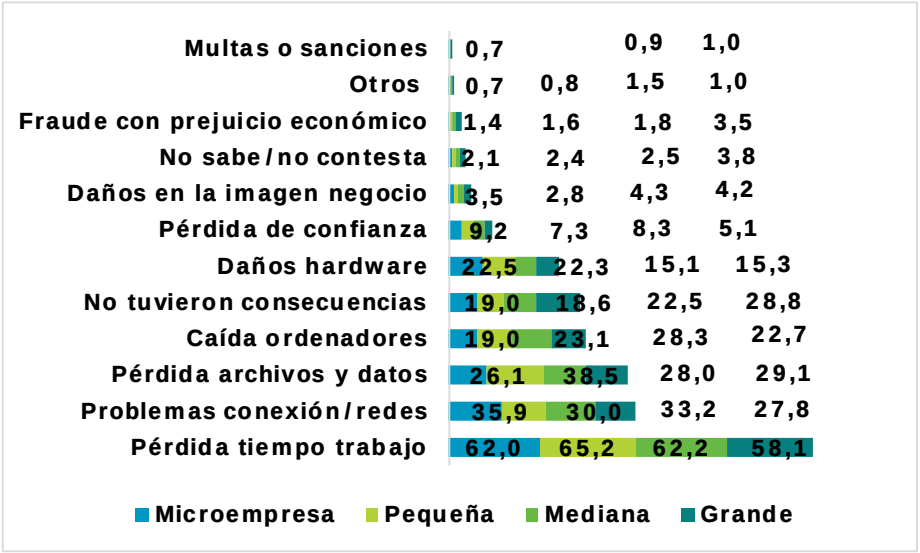
La pequeña empresa tiende a referir consecuencias físicas derivadas de sus incidencias de seguridad, como los Daños en los equipos (hardware) con un 22,3% o lógicas como la Pérdida de archivos y datos con un 38,5%.

Las medianas empresas son más proclives significativamente a sufrir una interrupción en los procesos de trabajo derivada de la Caída de los ordenadores con un 28,3%.

Las grandes empresas mencionan que sufren un menor número de consecuencias negativas derivadas de incidentes de seguridad.

De esta forma, el hecho de que las grandes empresas sufran mayor número de incidentes de seguridad y, por el contrario, denoten menores consecuencias, refuerza la idea de que su mayor preparación ante los incidentes minimiza las consecuencias negativas que estos tienen para su negocio.

FIGURA 60: CONSECUENCIAS DERIVADAS DE LOS INCIDENTES DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 142, Pequeña 247, Mediana 325 y Grande 313. P16.1

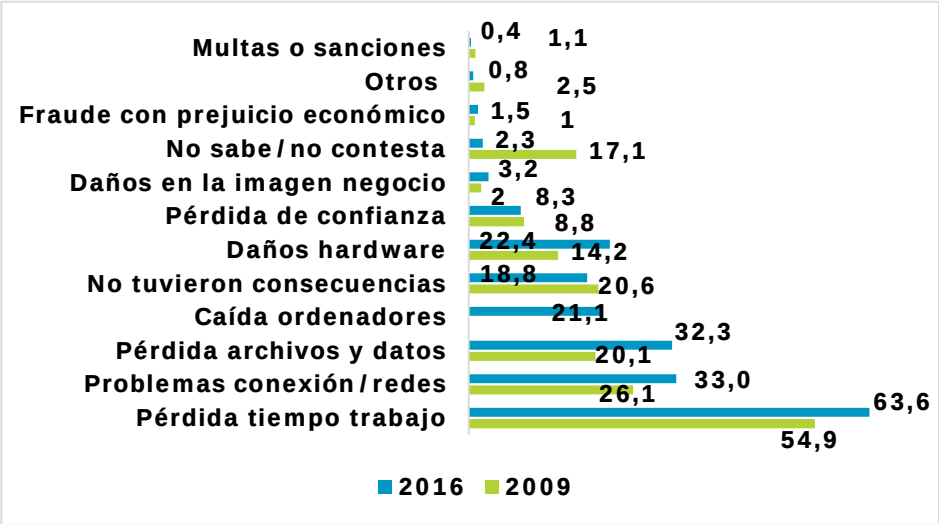
El estudio realizado en 2009[42] sobre la seguridad y la e-confianza en las pequeñas y microempresas, apuntaba las mismas consecuencias principales que se han recogido en esta ocasión.

La ocurrencia asociada a la mayoría de las consecuencias negativas derivadas de los incidentes de seguridad ha aumentado en 2016 respecto a 2009, exceptuando la Pérdida de confianza en los medios electrónicos, así como las Multas o sanciones, que han disminuido muy levemente.

Cabe destacar, no obstante, que se ha reducido considerablemente el número de las que no saben o no contestan en lo que se refiere a las consecuencias negativas que han producido los incidentes de seguridad sufridos en su empresa, pasando de representar el 17,1% de las microempresas y pequeñas empresas en 2009 a tan solo el 2,3% en 2016. Esto supone un elemento positivo ya que indica que han desarrollado mayor capacidad para entender y afrontar las consecuencias de los incidentes de seguridad.

[42] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

FIGURA 61: EVOLUCIÓN DE LAS CONSECUENCIAS DERIVADAS DE LOS INCIDENTES DE SEGURIDAD 2009-2016. RESPUESTA EXPRESADA EN % (PEQUEÑA EMPRESA Y MICROEMPRESA)



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa y Pequeña empresa 697. P16.1; y Estudio INTECO (actual INCIBE) sobre la seguridad y la e-confianza en las pequeñas y medianas empresas 2009. Base 1.708. Gráfico 46.

Respecto a las consecuencias que más proliferan según los sectores de actividad de las empresas españolas, se puede señalar que las empresas pertenecientes al sector de Actividades profesionales, científicas y técnicas tienden a señalar menos consecuencias que las demás (con un 34,7%).

Los Servicios de comidas y bebidas son el sector que más ha indicado que los incidentes de seguridad han supuesto una pérdida de tiempo de trabajo con un 73,7%. Respecto a los Problemas de conexión/redes son más comunes para las empresas del sector de Servicios de alojamiento con un 40,4%. La pérdida de archivos y datos ha sido más pronunciada entre las empresas del sector de Actividades administrativas y servicios auxiliares con un 40%.

Por último, la Caída de ordenadores está relacionada significativamente con el sector de Coquerías, productos farmacéuticos, caucho y plásticos en un 37%.

Como se ha señalado anteriormente INCIBE cuenta con un servicio de Itinerarios Interactivos por sectores. La ciberseguridad abarca campos muy heterogéneos y los riesgos que pueden afectar a las empresas también lo pueden ser en base a las características de los diferentes sectores. Podrá conocer con más detalle cuáles son las amenazas que podrían afectarle más directamente, consultando de forma amena los Itinerarios Interactivos Sectoriales de Ciberseguridad de INCIBE: https://itinerarios.incibe.es/

Incidentes de seguridad y consecuencias percibidas

Existen ciertas correlaciones significativas entre algunos incidentes de seguridad y las consecuencias que se derivan de ellos.

La Afectación por código dañino es el incidente más extendido entre las empresas consultadas y lo relacionan con la Pérdida de tiempo de trabajo (65%) y la Pérdida de archivos y datos (37,1%). De manera que las empresas que han declarado haber sufrido Afectación por código dañino tienden a relacionarlo en mayor medida con la Pérdida de tiempo de trabajo y la Pérdida de archivos y datos que las demás.

TABLA 8: CONSECUENCIAS DE LOS INCIDENTES DE SEGURIDAD DECLARADOS.

Consecuencias	Ataques informáticos	Afectación por código dañino	Robo de equipos	Pérdida/copia de datos	Caída de sistemas/alicaciones	Caída de sistemas de soporte	Daños físicos en instalaciones	Phishing	Baja de personal	Falta de servicio	Inundación, terremoto	Multas, sanciones
No se derivó ninguna consecuencia	23,4%	22%	25,4%	12,7%	19,9%	20,4%	16,7%	16,4%	22,2%	18,8%	15,4%	8,3%
Fraude con prejuicio económico	3,4%	2,1%	1,6%	4%	1,9%	1,7%	6,7%	9,8%	5,6%	2,2%	5,1%	-
Multas o sanciones	0,3%	0,7%	2,1%	3,5%	1,2%	1,2%	6,7%	3,3%	1,4%	0,9%	5,1%	25%
Daños en la imagen del negocio	7,9%	3,4%	5,8%	9,2%	5,1%	5,5%	13,3%	8,2%	6,9%	6,7%	5,1%	-
Pérdida de confianza en los medios electrónicos	9,6%	7,6%	6,9%	15%	8,2%	9%	13,3%	11,5%	12,5%	11,7%	7,7%	-
Daños en equipos	17,5%	18,3%	24,9%	30,6%	20,1%	22,2%	60%	29,5%	20,8%	18,4%	56,4%	33,3 %
Pérdida de archivos/datos	37,5%	37,1%	32,3%	63,6%	31,7%	25,4%	20%	32,8%	30,6%	28,7%	17,9%	41,7 %
Problemas de conexión/red	29,9%	27,1%	33,9%	35,8%	48,4%	51%	60%	41%	44,4%	48%	51,3%	41,7 %
Pérdida tiempo de trabajo	64,9%	65%	61,4%	72,3%	70,2%	70,3%	80%	72,1%	68,1%	70%	59%	41,7 %
Caída de los ordenadores	28,9%	23,6%	28,6%	30,1%	37,5%	36,4%	46,7%	44,3%	34,7%	35,9%	46,2%	41,7 %

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.027 (Empresas que han sufrido incidentes de seguridad en el último año). Cruce P16 y P16.1

Las empresas que han manifestado haber sufrido una Caída de los sistemas o aplicaciones han indicado haber tenido consecuencias similares asociados a la Pérdida de tiempo de trabajo (70,2%), Problemas de conexión/redes (48,4%) y Caída de los ordenadores (37,5%).

Las empresas que han afirmado haber sufrido Caída de los sistemas de soporte indican además un mayor número de consecuencias tales como Pérdida de tiempo (70,3%), Problemas de conexión/redes (51%), Caída de los ordenadores (36,4%), Daños en los equipos (hardware) (22,2%) y Daños en la imagen/reputación de su negocio (5%).

Las pocas empresas que han indicado haber padecido falta de servicio por parte de proveedores lo han relacionado con las consecuencias de Pérdida de tiempo de trabajo (70%), Problemas de conexión/redes (48%), Caída de los ordenadores (35,9%), Pérdida de confianza en los medios electrónicos (11,7%) y Daños en la imagen/reputación de un negocio (6,7%).

6.2 Impacto y repercusión de los incidentes de seguridad

Impactos de los incidentes de seguridad (Indicador 34 en EICDE)

Analizadas las consecuencias que han tenido los incidentes de seguridad, se ha preguntado a las empresas por el impacto que han sufrido con el objetivo de medir el indicador 34 en EICDE.

El impacto de los incidentes de seguridad está muy focalizado ya que el 87% de las empresas ha mencionado tan solo una opción. De este modo, los resultados son casi unánimes ya que el 94,7% apuntan a un Impacto operativo, en alusión a la paralización de las actividades, pérdida de tiempo, o realización de tareas extraordinarias.

IMPACTO DE LOS INCIDENTES DE SEGURIDAD

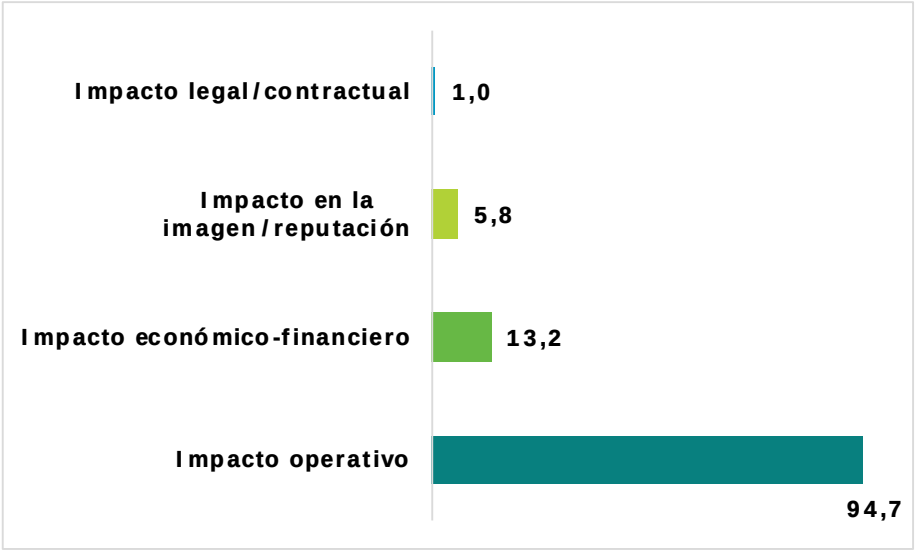
94,7%

DE LAS EMPRESAS HA SUFRIDO UN IMPACTO OPERATIVO COMO CONSECUENCIA DE LOS INCIDENTES DE SEGURIDAD

13,2%

HA SUFRIDO UN IMPACTO ECONÓMICO-FINANCIERO

FIGURA 62: IMPACTO DE LOS INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.026 (Empresas que han sufrido incidentes de seguridad en el último año). P16.2

Esta respuesta es congruente con las principales consecuencias que se apuntaron derivadas de los incidentes de seguridad (Pérdida de tiempo de trabajo 61,6%, Problemas de conexión/redes 31,2% y Pérdida de archivos y datos 39,6%).

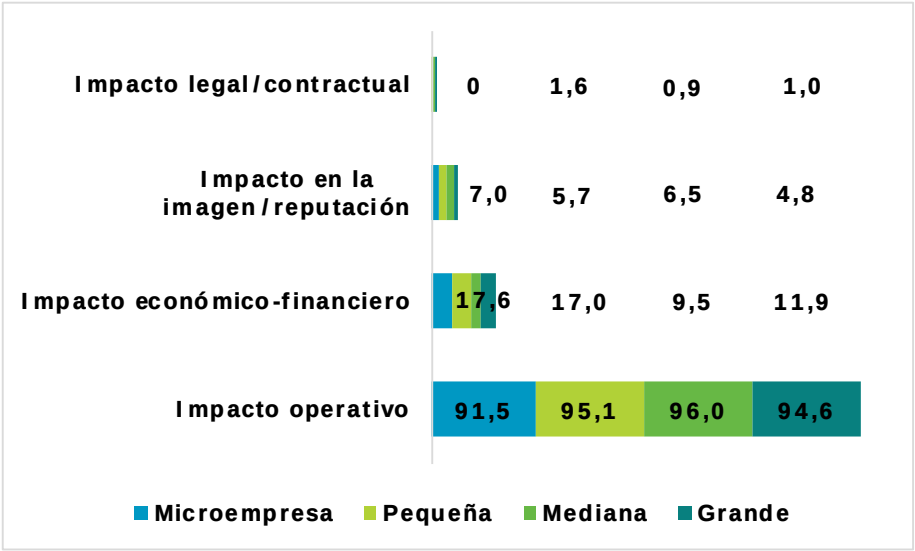
Se muestra mucho menos relevante la respuesta sobre el Impacto económico-financiero con un 13,2%, referido a las pérdidas económicas derivadas de los incidentes. Todo ello refleja que las empresas españolas no tienen por costumbre evaluar el impacto económico de los incidentes de seguridad, así como la necesidad de generar procesos que permitan medir ese impacto económico.

De este modo, parecería lógico entender que el impacto operativo asociado a la perdida de horas de trabajo, genera pérdidas de productividad y en consecuencia deriva en un impacto económico, aunque no se reconozca su existencia por parte de las empresas.[43]

La gestión de riesgos es clave para realizar una adecuada gestión de la seguridad de la información. Sin duda debe convertirse en un proceso estratégico aplicado en la estructura de la empresa con una sólida conexión con los procesos de decisión y la estrategia. Para evitar el impacto de un incidente, antes es recomendable realizar una gestión de riesgos adecuada. INCIBE pone a disposición de todos los empresarios una guía con las pautas básicas: https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario

El tipo de impacto que han tenido los incidentes de seguridad en la empresa y su tamaño no guarda relación. El impacto operativo, afecta en un porcentaje muy similar a todos los tamaños de empresa, aunque se puede resaltar el 91,5% de las microempresas afirman que los incidentes han ocasionado un impacto operativo frente al 96% de las empresas medianas. Destaca además que el impacto económico financiero ha sido mencionado con mayor frecuencia entre las microempresas y pequeñas empresas (17,6% y 17%) que entre las medianas y grandes.

FIGURA 63: IMPACTO DE LOS INCIDENTES DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 142, Pequeña 247, Mediana 325 y Grande 312. P16.2

[43] Es posible que en futuros análisis sea conveniente cuantificar las horas de trabajo perdidas, con el fin de asociar el impacto operativo a las consecuencias económicas que se puedan derivar.

Desde una perspectiva sectorial las empresas que pertenecen al sector de Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor son las que indican un mayor Impacto económico-financiero con un 17,8%.

Las empresas que pertenecen al sector de Servicios de alojamiento son las que más han indicado haber tenido un Impacto operativo con un 98,1%.

Respecto al Impacto en la imagen/reputación de la empresa se ha producido en mayor proporción en el sector de Actividades administrativas y servicios auxiliares con un 10% y el Impacto legal/contractual con un 5,3% se ha producido más en el sector de Servicios de comidas y bebidas.

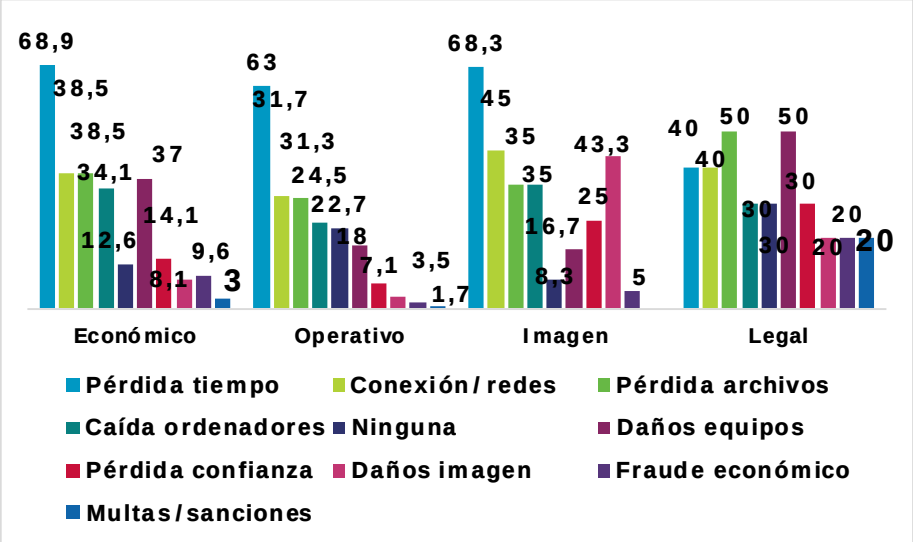
Relación entre la percepción de consecuencias negativas de los incidentes y su impacto en las empresas

Para terminar con el apartado del impacto de los incidentes de seguridad que han percibido las empresas, resulta interesante comprobar qué tipo de consecuencias derivadas de los incidentes han relacionado las empresas con cada uno de los tipos de impacto definidos.

Los problemas de conexión/redes han tenido en mayor proporción un impacto en la imagen/reputación de la empresa con un 45%. La pérdida de archivos y datos ha tenido un impacto en las empresas bastante repartido, aunque destaca el impacto económico-financiero sobre los demás con un 38,5%.

El 22,7% de las empresas cuyos incidentes han tenido un impacto operativo en su negocio, asumen sin embargo que de los incidentes de seguridad que sufrieron no se derivó ninguna consecuencia negativa.

FIGURA 64: CRUCE IMPACTO DE LOS INCIDENTES DE SEGURIDAD POR CONSECUENICAS DERIVADAS. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.177 (Empresas que han sufrido incidentes de seguridad en el último año). Cruce P16.1 y P16.2

REPERCUSIÓN ECONÓMICA DE LOS INCIDENTES DE SEGURIDAD

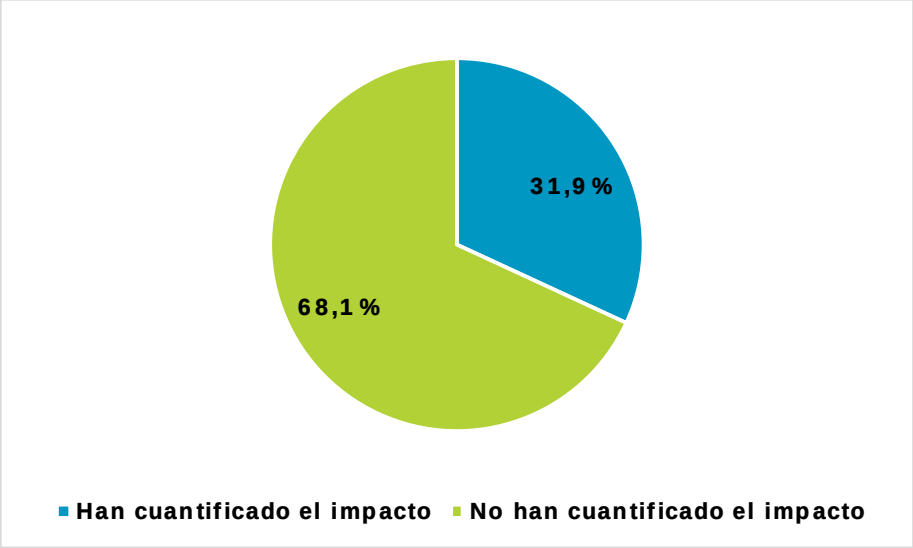
31,9%

DE LAS EMPRESAS QUE IDENTIFICAN IMPACTO ECONOMICO LO HAN CUANTIFICADO

Repercusión económica de los incidentes de seguridad (Indicador 34 en EICDE)

Tan solo el 32% de las empresas manifestaron haber cuantificado el impacto económico que los incidentes tuvieron en su empresa, lo que parece indicar que se requiere una mayor concienciación sobre la necesidad de cuantificar el impacto económico de los incidentes de seguridad.

FIGURA 65: REPERCUSIÓN ECONÓMICA DE LOS INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %

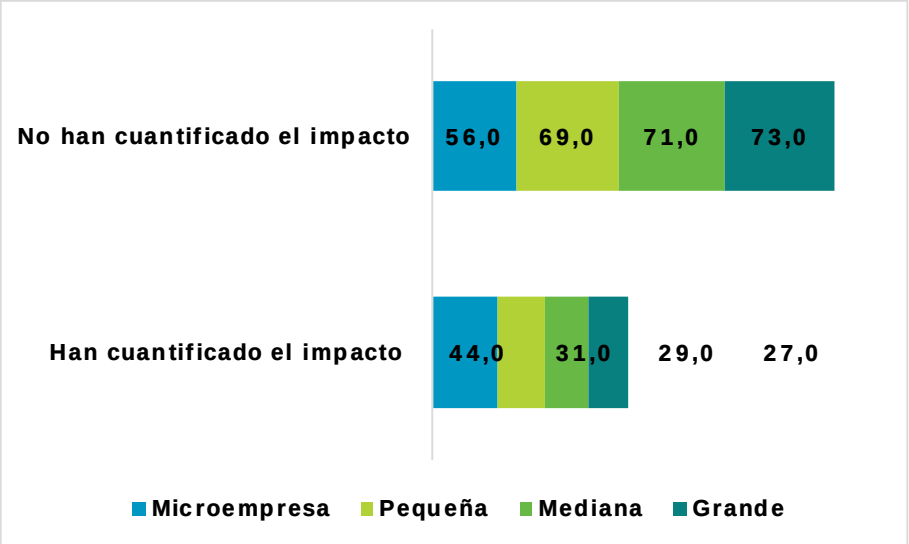


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 135 (Empresas que han indicado que los incidentes sufridos han tenido un impacto económico). P16.3

Respecto a la distribución por tamaño de las empresas y la repercusión económica de los incidentes de seguridad, existe una relación inversamente proporcional, de manera que las microempresas son las que cuantifican los daños económicos en un mayor porcentaje, 44%, seguidas de las pequeñas empresas con un 31%, medianas empresas 29% y, finalmente, grandes empresas 27%.

En lo que a sectores de actividad se refiere no existe una relación clara, en parte debido a la baja respuesta que ha tenido esta pregunta. Sin embargo, se puede destacar las empresas que más han cuantificado el impacto que los incidentes de seguridad han tenido en su negocio, que pertenecen al sector de Servicios de comidas y bebidas con un 66,7% y al sector de Actividades administrativas y servicios auxiliares con un 62,5%.

FIGURA 66: REPERCUSIÓN ECONÓMICA DE LOS INCIDENTES DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 25, Pequeña 42, Mediana 31, Grande 37. P16.3

VOLUMEN PÉRDIDAS ECONÓMICAS

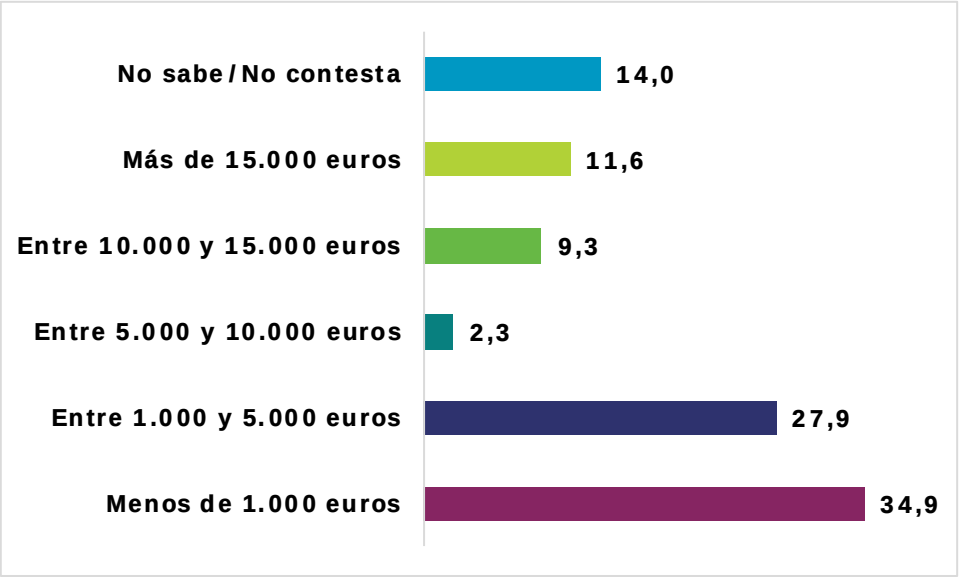
34,9% HA CUANTIFICADO SU PÉRDIDA EN MENOS DE 1.000 EUROS

27,9% HA CUANTIFICADO SU PÉRDIDA ENTRE 1.000 Y 5.000 EUROS

Volumen de las pérdidas económicas derivadas de incidentes de seguridad

Con el objetivo de obtener un indicador sobre la distribución de las pérdidas económicas derivadas de los incidentes de seguridad, se ha solicitado a las empresas que sufrieron un impacto económico que lo cuantificaran entre los rangos que se exponen en el siguiente gráfico.

FIGURA 67: PERJUICIO ECONÓMICO DERIVADO DE LOS INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 43 (Empresas que han cuantificado el impacto económico de los incidentes sufridos). P16.4

El grueso de las empresas ha cuantificado el perjuicio económico ocasionado por los incidentes en menos de 5.000 euros ya que el 62,8% cifra sus pérdidas entre menos de 1.000 euros y 5.000 euros.

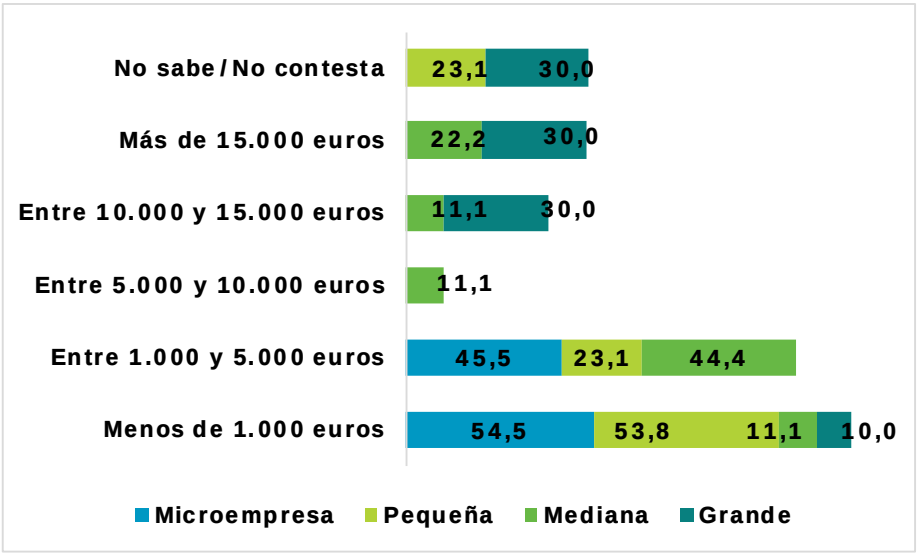
El 20,9% de las empresas cuantifica sus pérdidas económicas entre 10.000 y más de 15.000 euros y tan solo el 2,3% sitúa la cifra entre 5.000 y 10.000 euros. Por otra parte, destaca que el 14% de las empresas no conozca la cuantía económica que han generado los incidentes de seguridad en su negocio.

¿Merece la pena realizar un análisis de lo que ocurriría en su negocio en caso de sufrir un incidente de seguridad grave? Puede que se haya preguntado muchas veces está cuestión. La respuesta es sencilla, si le preocupa que su negocio continúe funcionando y no desaparezca o se paralice durante un largo periodo de tiempo, entonces sí merece la pena llevar a cabo un análisis de impacto. Más información en el siguiente enlace: https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-realizar-analisis-impacto-negocio

Respecto a la distribución por tamaño del perjuicio económico, la tasa de respuesta a esta pregunta es demasiado baja como para realizar conclusiones exentas de un error asumible. No obstante, tal y como se desprende del gráfico, las microempresas y pequeñas empresas concentran su cuantía económica por debajo de los 5.000 euros, las empresas medianas se reparten entre todos los rangos y las grandes empresas concentran sus pérdidas económicas entre 10.000 y 15.000 euros y más de 15.000 euros.

La baja tasa de respuesta para esta pregunta puede tener que ver con que las empresas no están interesadas en referir datos económicos relacionados con su actividad, aunque solo sea a efectos de uso estadístico de los mismos.

FIGURA 68: PERJUICIO ECONÓMICO DERIVADO DE LOS INCIDENTES DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 11, Pequeña 13, Mediana 9, Grande 10. P16.4

Distribución de las pérdidas económicas según los incidentes de seguridad sufridos durante el último año

Para terminar el análisis del impacto económico que han tenido los incidentes sufridos por las empresas en su negocio, se ha procedido a cruzar el perjuicio económico con los incidentes sufridos en el último año de manera que se ofrezca una visión general entre incidentes y perjuicio económico. Tal y como sucedía en el anterior apartado, la baja tasa de respuesta relacionada con la distribución de las pérdidas económicas dificulta un análisis estadísticamente fiable, no obstante, se han podido identificar algunas cuestiones.

El 73,3% de las empresas que han cuantificado sus daños en menos de 1.000 euros ha sufrido Afectación por código dañino. Respecto a las empresas que cifran sus pérdidas entre 1.000 y 5.000 euros, han distribuido su respuesta entre Afectación por código dañino 58,3% y Caída de los sistemas o aplicaciones 50%.

Tan sólo una empresa ha contestado que los incidentes de seguridad sufridos han tenido un perjuicio económico entre 5.000 y 10.000 euros y ha sido como consecuencia de una Caída de los sistemas o aplicaciones de la empresa. Respecto a las empresas que han afirmado haber sufrido un perjuicio económico entre 10.000 y 15.000 euros lo han atribuido esencialmente debido a Ataques informáticos, Robo de equipos y pérdida o copia de datos e información (75%).

TABLA 9: PERJUICIO ECONÓMICO DERIVADO DE LOS INCIDENTES DE SEGURIDAD

Incidentes	Menos de 1.000 euros	Entre 1.000 y 5.000 euros	Entre 5.000 y 10.000 euros	Entre 10.000 y 15.000 euros	Más de 15.000 euros	No lo sé
Ataques informáticos	20%	41,7%	-	75%	20%	50%
Afectación por código dañino	73,3%	58,3%	-	25%	40%	66,7%
Robo de equipos	13,3%	33,3%	-	75%	40%	33,3%
Pérdida o copia de datos e información	20%	41,7%	-	75%	20%	-
Caída de los sistemas o aplicaciones	20%	50%	100%	50%	60%	33,3%
Caída de los sistemas de soporte	13,3%	16,7%	-	25%	60%	-
Daños físicos	6,7%	-	-	25%	-	-
Phishing	-	-	-	25%	20%	16,7%
Baja personal crítico	6,7%	-	-	-	40%	-
Falta de servicio proveedores	20%	16,7%	-	25%	20%	33,3%
Inundación, terremoto	6,7%	8,3%	-	25%	20%	33,3%
Multas, sanciones	6,7%	8,3%	-	-	-	-

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 43. Cruce P16.4 y P16

El perjuicio económico de más de 15.000 euros ha sido motivado en mayor medida por incidentes relacionados con la Caída de los sistemas o aplicaciones de la empresa y con la Caída de los sistemas de soporte (60%). Para finalizar, resaltar que el 40% de las empresas que han tenido un perjuicio económico de más de 15.000 euros ha mencionado como causa el incidente de Baja de personal crítico.

6.3 Respuesta a los incidentes de ciberseguridad y cambio de hábitos

RESPUESTA A LOS INCIDENTES DE SEGURIDAD

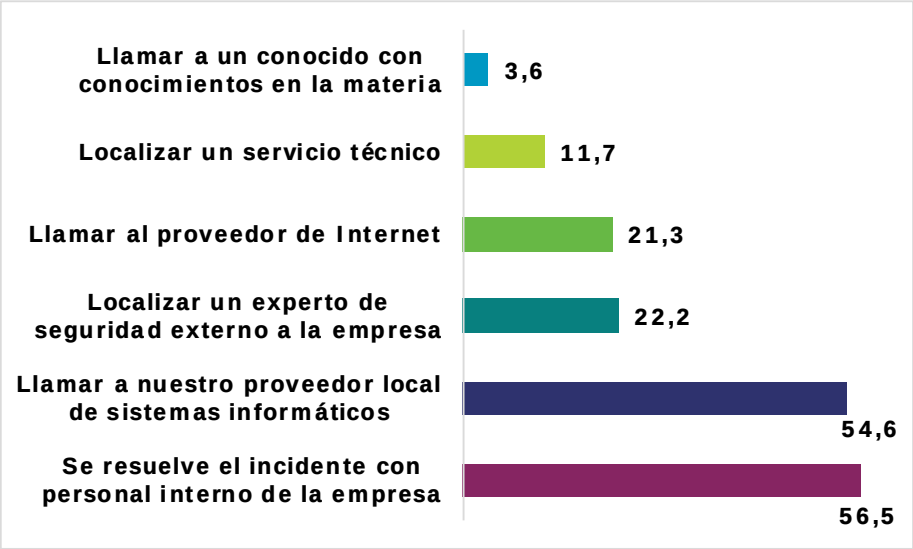
56,5%
HA RESUELTO LA INCIDENCIA A TRAVÉS DE PERSONAL INTERNO DE LA EMPRESA

54,6% HA LLAMADO A SU PROVEEDOR LOCAL DE SISTEMAS INFORMÁTICOS PARA RESOLVER LA INCIDENCIA

Respuesta a los incidentes de seguridad

Resulta relevante analizar la respuesta que dan las empresas para resolver esos incidentes. Para ello, se ha solicitado a las empresas que elijan entre los 6 tipos de respuesta que se reparten fundamentalmente entre Resolver la incidencia con personal interno de la empresa 56,5% y Llamar al proveedor local de servicios informáticos 54,6%.

FIGURA 69: RESPUESTA A LOS INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.466. P19

Un 22,2% de las empresas consultadas ha recurrido a localizar un experto de seguridad externo a la empresa en el momento que ha sufrido un incidente, un 11,7% ha recurrido a localizar un servicio técnico y un 3,6% ha recurrido a un conocido con conocimientos.

Todo ello significa que aproximadamente un 35,5% de las empresas, en algún momento de alguna manera ha improvisado a la hora de resolver los incidentes de seguridad que le han ocurrido, buscando soluciones espontáneas de carácter coyuntural.

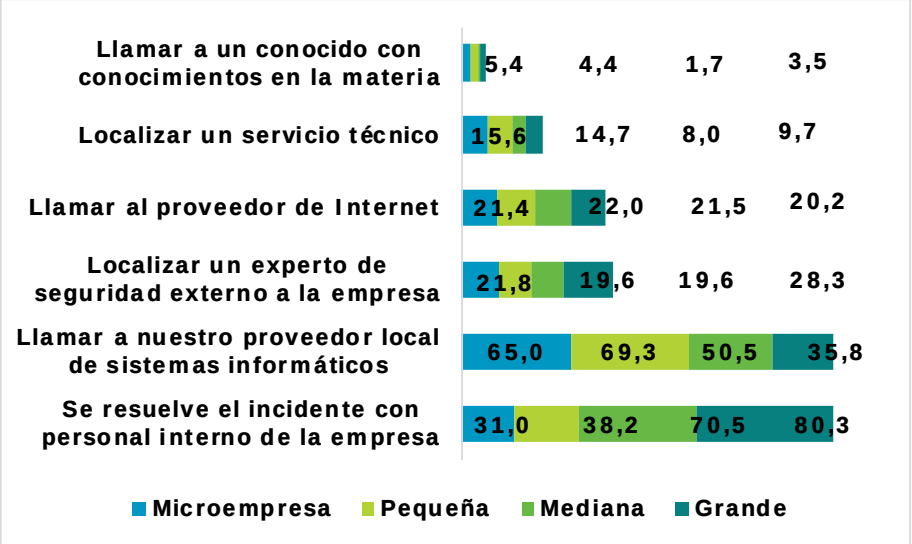
El resto de las respuestas denotan una mayor preparación de las empresas al recurrir a los proveedores de servicios habituales, sea el proveedor de internet (21,3%) o el proveedor TIC habitual (54,6%), o a resolver el incidente mediante el personal interno (55,5%) de la empresa.

Respecto a la distribución por tamaño, el comportamiento de las empresas es distinto. Son las empresas de mayor tamaño las que resuelven los incidentes con personal interno. Las grandes y medianas empresas los resuelven de manera interna en un 80,3% y un 70,5% respectivamente, mientras las pequeñas y microempresas lo hacen en menor medida (38,2% y un 31% respectivamente).

Por el contrario, a la hora de llamar a su proveedor local de sistemas informáticos la relación es inversa. Las microempresas y pequeñas

empresas tienden a llamar más a su proveedor local, en un 65% y un 69,3% mientras las medianas lo hacen en un 50,5% y las grandes en un 35,8%.

FIGURA 70: RESPUESTA A LOS INCIDENTES DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 294, Pequeña 387, Mediana 414, Grande 371. P19

El "Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas"[44] realizado en 2012, mostraba que las respuestas más frecuentes fueron recurrir a personal de la empresa con un 48,5% y recurrir a un servicio técnico profesional externo con el 33,5%.

Respecto a la respuesta que han dado las empresas a los incidentes de seguridad según el sector de actividad al que pertenecen, destaca que el 85,3% de las empresas del sector de Información y comunicaciones resuelve los incidentes con personal interno de la empresa, lo que tiene que ver con la naturaleza de su actividad.

Entre las que responden llamando a su proveedor local de sistemas informáticos destacan las empresas del sector de Servicios de alojamiento con un 72% y Transportes y almacenamiento 68,8%.

Entre los sectores más propensos a buscar una solución improvisada figuran las del sector de Actividades administrativas y servicios auxiliares, dado que un 28,4% indican que localizan a un experto de seguridad.

Igualmente, el 16% de las empresas que localizan un servicio técnico pertenecen al sector Servicios de alojamiento, y entre las empresas que llaman a un conocido con conocimientos en la materia destaca el sector Servicios de comidas y bebidas con un 8,8%.

[44] "*Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*" INTECO 2012. (Actualmente INCIBE).

CAMBIO DE HÁBITOS COMO CONSECUENCIA DE INCIDENTES DE SEGURIDAD

58,2%
DE LAS EMPRESAS HA ESTABLECIDO PROTOCOLOS DE SEGURIDAD MÁS ESTRICTOS TRAS SUFRIR UN INCIDENTE DE SEGURIDAD

40,9% HA INSTALADO NUEVAS HERRAMIENTAS Y ACTUALIZADO PROGRAMAS

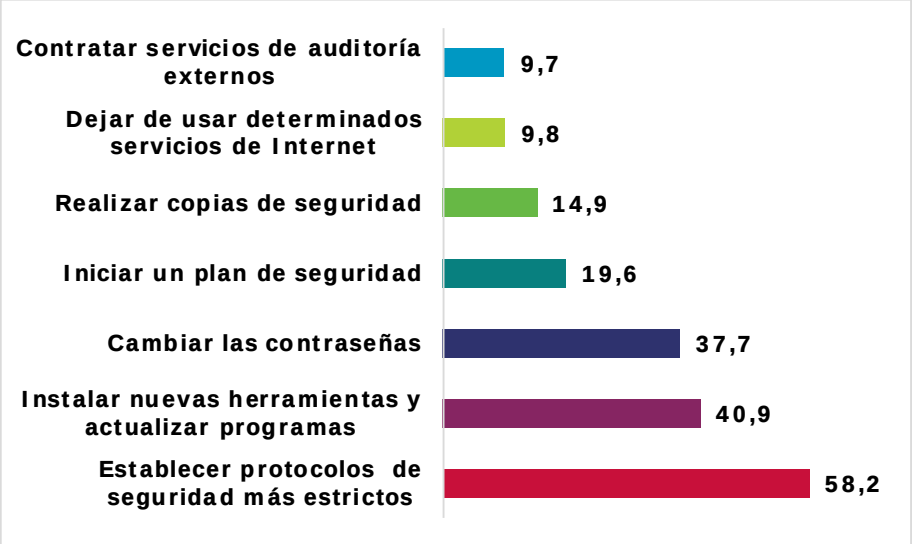
37,7% HA CAMBIADO SUS CONTRASEÑAS

Cambio de hábitos como consecuencia de incidentes de seguridad

Con objeto de conocer si los incidentes de seguridad afectan al comportamiento de las empresas y sus hábitos de seguridad, se ha solicitado a las empresas que identificasen los cambios de hábitos que se han producido tras un incidente de seguridad, atendiendo a la clasificación de respuestas utilizada en el estudio de 2009[45].

Ante un incidente de seguridad las empresas responden estableciendo protocolos de seguridad más estrictos en un 58,2% de los casos; instalando nuevas herramientas y actualizando programas en un 40,9% y cambiando las contraseñas en un 37,7%.

FIGURA 71: CAMBIO DE HÁBITOS TRAS SUFRIR INCIDENTES DE SEGURIDAD. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.023 (Empresas que han sufrido incidentes de seguridad en el último año). P20

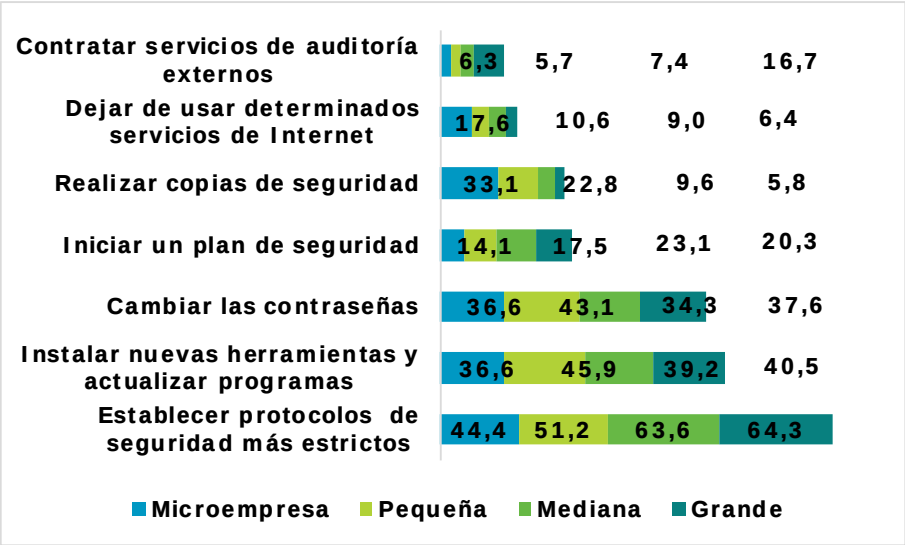
La distribución de la respuesta según tamaño muestra que los cambios de hábitos que se producen son diferentes en función de esta variable.

Las empresas que han manifestado dejar de usar determinados servicios de Internet y haber comenzado a realizar copias de seguridad pertenecen en mayor proporción a microempresas y pequeñas empresas.

Por el contrario, son las medianas y grandes empresas las que indican en mayor medida que establecen protocolos y procedimientos de seguridad más estrictos, o bien contratan servicios de auditoría externos.

[45] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

FIGURA 72: CAMBIO DE HÁBITOS TRAS SUFRIR INCIDENTES DE SEGURIDAD POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 142, Pequeña 246, Mediana 324 y Grande 311. P20

Las empresas pertenecientes al sector de Información y comunicaciones son las que más manifiestan de manera significativa haber establecido protocolos y procedimientos de seguridad más estrictos tras haber sufrido un incidente de seguridad, con el 70,3% de las respuestas de este sector.

Las empresas que pertenecen al sector de Servicios de alojamiento con un 29,4% y al sector de la Construcción con un 24,1% son las que más han afirmado de manera significativa haber comenzado a realizar copias de seguridad tras un incidente de seguridad en su negocio.

Los datos aportados por el "Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas"[46] en 2009 no son comparables debido a diferencias metodológicas, no obstante, cabe señalar que el estudio recogió que el 42,9% de las microempresas y pequeñas empresas habían instalado o actualizado programas y/o herramientas, un 30,9% no había realizado ningún cambio de hábitos y un 24,6% comenzó a realizar copias de seguridad a raíz de haber sufrido un incidente de seguridad.

Los empleados son los encargados de gestionar, procesar, almacenar, modificar, transmitir y eliminar la información en una empresa. Son el engranaje principal para el buen funcionamiento, pero ¿conocen los riesgos en materia de seguridad? Para evaluar la conciencia en ciberseguridad de la empresa, puede usar el anteriormente mencionado Kit de Concienciación de INCIBE: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[46] "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO 2009. (Actualmente INCIBE).

7 PRIVACIDAD Y TENDENCIAS

7.1 Políticas de privacidad

SERVICIOS DISPONIBLES EN PÁGINA WEB

62,7%

DE LAS EMPRESAS HA MANIFESTADO QUE SU PÁGINA WEB CUENTA CON UNA DECLARACIÓN DE POLÍTICA DE INTIMIDAD, SALVAGUARDA DE LA PRIVACIDAD O CERTIFICACIÓN

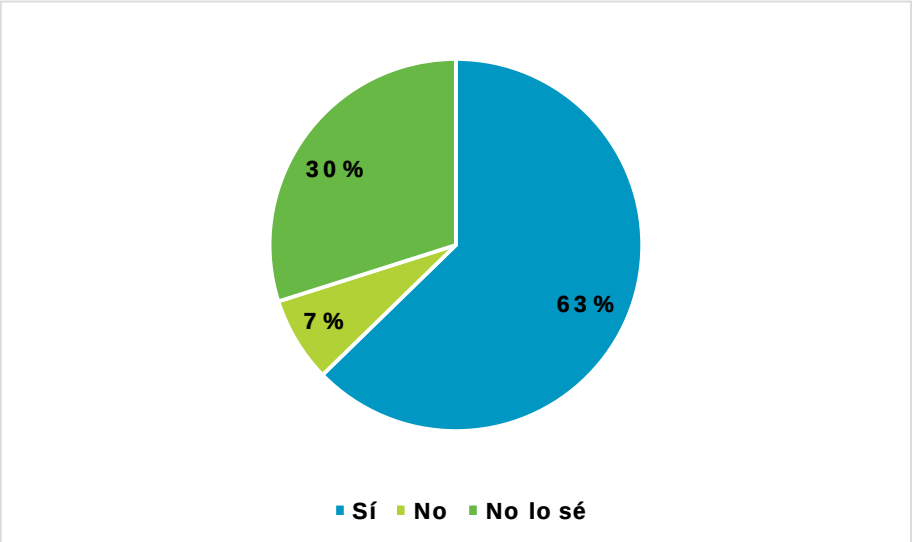
Servicios disponibles en página web: declaración de intimidad o certificación relacionada con la seguridad (Indicador 40 en EICDE)

Con el objetivo de conocer si las empresas cumplen con la normativa o certifican su página web y medir el indicador 40 en EICDE, se ha solicitado a las empresas que mencionaron poseer página web que señalaran si su empresa mantiene una declaración de política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web.

El resultado ha sido que el 62,7% de las empresas consultadas ha manifestado contar con una declaración de política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web.

Cabe destacar que entre las empresas con página web, en un alto porcentaje (30%) se desconoce si su página cumple con la normativa o está certificada. Lo que muestra que existe recorrido en lo que se refiere a mejorar esta situación orientando procesos que permitan impulsar la adecuación de las empresas a estos requisitos.

FIGURA 73: DECLARACIÓN POLÍTICA DE INTIMIDAD, SALVAGUARDA DE PRIVACIDAD O CERTIFICACIÓN RELACIONADA CON LA SEGURIDAD DEL SITIO WEB. RESPUESTA EXPRESADA EN %

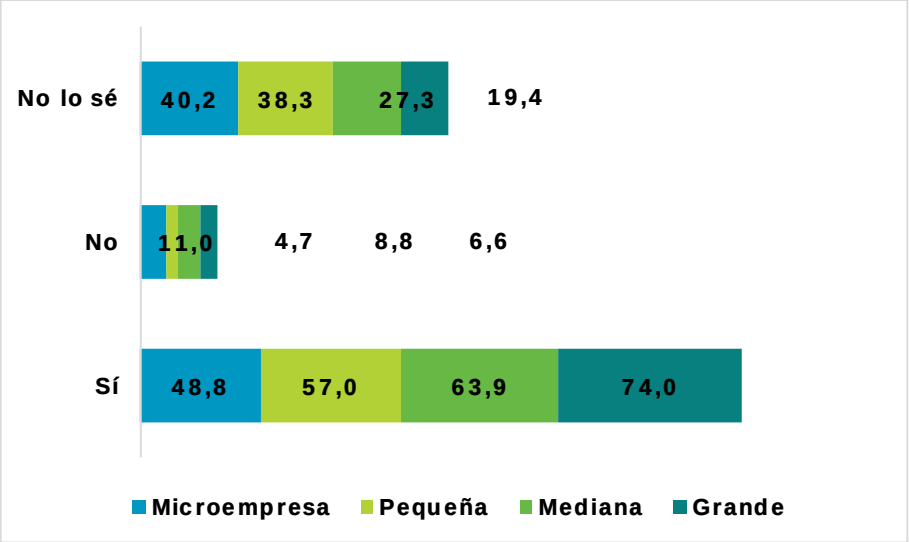


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.064 (Empresas que han indicado que mantienen página web). P21

Respecto a la distribución de la respuesta atendiendo al tamaño de la empresa se encuentra una relación significativa.

Existe una relación proporcional entre las empresas que manifiestan contar con una declaración política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web y el tamaño de la empresa, de manera que cuanto mayor es la empresa, crece la afirmación de cumplir con la normativa o certificación web.

FIGURA 74: DECLARACIÓN POLÍTICA DE INTIMIDAD, SALVAGUARDA DE PRIVACIDAD O CERTIFICACIÓN RELACIONADA CON LA SEGURIDAD DEL SITIO WEB POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 164, Pequeña 277, Mediana 319 y Grande 304. P21

Cabe destacar que un porcentaje alto de microempresas no sabe cuál es la situación de su página web (40,2%), lo que indica el desconocimiento que mantiene este tipo de empresas sobre la realidad de su situación, o bien que dan menos importancia al cumplimiento efectivo de los requerimientos.

El dato registrado por la "ETICce"[47] en las encuestas de 2014-15 y 2015-16 es para las pequeñas, medianas y grandes empresas 68,4 en 2015 y 69,2% en 2016, y para las microempresas en 2016, 56,4%.

En cuanto a la distribución según el sector de actividad al que pertenecen, las empresas que indican en mayor proporción cumplir con la normativa o mantener la certificación relacionada pertenecen al sector de Actividades inmobiliarias con un 70,6% y al sector de Información y comunicaciones con un 70%.

[47] "*Encuesta sobre el uso de las tecnologías de la información y las comunicaciones y del comercio electrónico en las empresas*" INE 2014-15 http://www.ine.es/dynt3/inebase/es/index.htm?type=pcaxis&path=/t09/e02/a2014-2015&file=pcaxis&dh=0&capsel=0

CONOCIMIENTO Y ADECUACIÓN A LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

88,1%

DE LAS EMPRESAS HA MANIFESTADO CONOCIMIENTO SOBRE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

81,9%

DE LAS EMPRESAS HA MANIFESTADO CONOCER SU SUJECIÓN A DICHA NORMATIVA EN CASO DE DISPONER DE FICHEROS DE DATOS PERSONALES

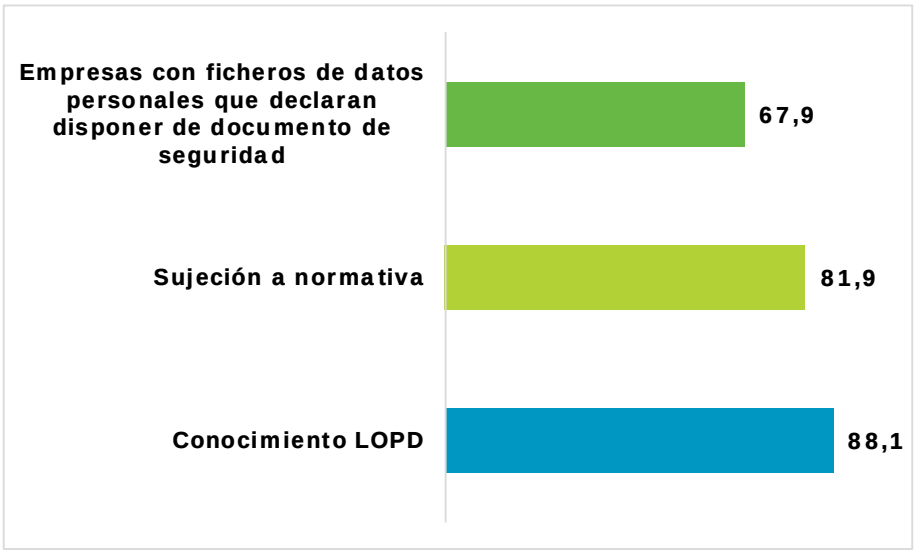
67,9% DE LAS EMPRESAS CON FICHEROS DE DATOS PERSONALES DECLARAN DISPONER DE DOCUMENTO DE SEGURIDAD

Conocimiento de la Ley Orgánica de Protección de Datos (Indicador 42 en EICDE), Sujeción a la normativa y empresas con ficheros de datos personales que declaran disponer de documento de seguridad (Indicador 41 en EICDE)

Con el objetivo de medir los indicadores 42 "Conocimiento de la LOPD", 41 "Empresas con ficheros de datos que declaran disponer de documento de seguridad" y un tercero asociado a las empresas que están sujetas a la normativa, se ha solicitado a las empresas que indiquen cuál es su situación respecto a estas cuestiones.

El 60,7% de las empresas consultadas han indicado las tres opciones, lo que indica que un alto porcentaje de empresas conoce la LOPD, conoce la sujeción a la normativa y disponen de documento de seguridad para sus ficheros de datos personales.

FIGURA 75: CONOCIMIENTO Y ADECUACIÓN A LA NORMATIVA SOBRE PROTECCIÓN DE DATOS. RESPUESTA EXPRESADA EN %



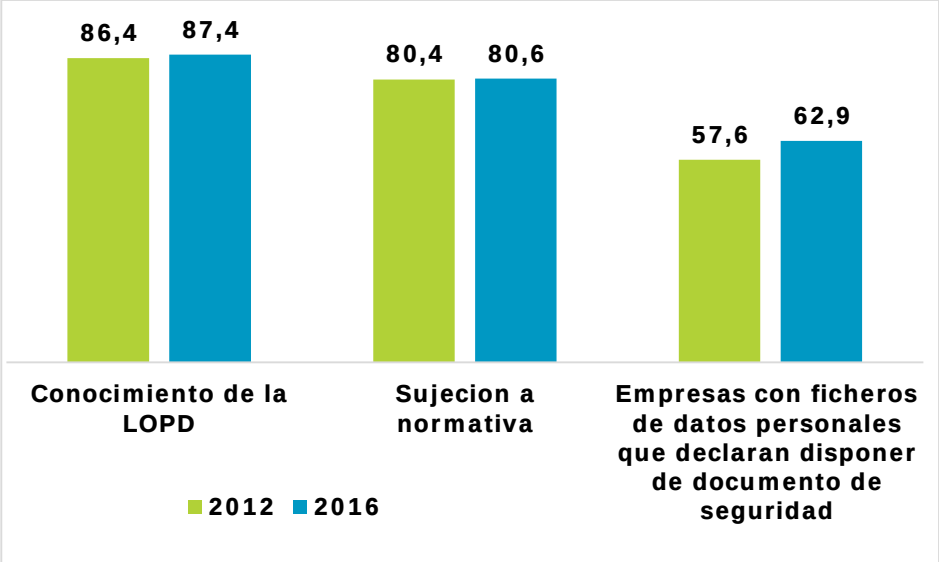
Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.462. P22

Concretamente, el 88,1% de las empresas consultadas ha indicado que su empresa conoce la Ley Orgánica de Protección de Datos, el 81,9% de las empresas consultadas afirma que su empresa conoce que está sujeta a dicha normativa en caso de disponer de ficheros de datos personales de cualquier tipo y el 67,9% de las empresas ha manifestado que dispone de un documento de seguridad donde se recogen las medidas técnicas y organizativas que rigen la actuación del personal con acceso a los sistemas de información.

En cuanto al porcentaje de empresas que afirman conocer la Ley Orgánica de Protección de Datos ha aumentado ligeramente desde 2012, como se puede apreciar en el siguiente gráfico comparativo con los datos del "Estudio sobre la protección de datos en las empresas españolas"[48] realizado en 2012, estudio referido específicamente al conjunto de PYME y Microempresas, esto es Pequeñas empresas (10 a 49 empleados), Medianas (50 a 249) y Microempresas (0 a 9), es decir con un tamaño de 0 a 249 trabajadores.

[48] "*Estudio sobre la protección de datos en las empresas españolas*" INTECO 2012. (Actualmente INCIBE).

FIGURA 76: EVOLUCIÓN DE LAS EMPRESAS QUE MANIFIESTAN CONOCER LA LOPD, ESTAR SUJETAS A LA NORMATIVA Y DISPONER DE DOCUMENTO DE SEGURIDAD PARA SUS FICHEROS DE DATOS PERSONALES (2012-2016). RESPUESTA EXPRESADA EN % PARA PYME Y MICROEMPRESA

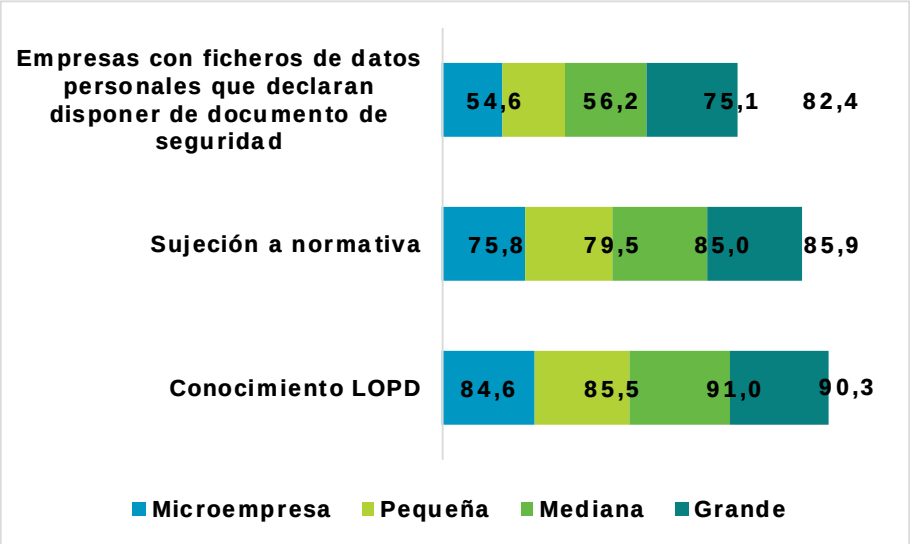


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base PYME y Microempresa 1.092. P22 y Estudio INTECO (actualmente INCIBE) sobre la protección de datos en las empresas españolas 2012. Base 1.109. Gráfico 1, 2 y 3.

Las empresas, en este caso pymes y microempresas, que declaran conocer que están sujetas a la normativa en caso de disponer de ficheros de datos personales de cualquier tipo se mantiene estable, por otro lado, se observa un crecimiento notable de estas empresas con ficheros personales que declaran disponer de documento de seguridad, pasando de representar el 57,6% en 2012 al 62,9% de las PYME y Microempresas consultadas en 2016.

Según su tamaño se ha observado una relación proporcional y positiva de manera que las medianas y grandes empresas han manifestado en mayor proporción que conocen la ley y su adecuación a la normativa sobre protección de datos, que las pequeñas y microempresas.

FIGURA 77: CONOCIMIENTO Y ADECUACIÓN A LA NORMATIVA SOBRE PROTECCIÓN DE DATOS POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 293, Pequeña 386, Mediana 413 y Grande 370. P22

La distribución según el sector de actividad no presenta grandes variaciones, aunque cabe destacar que las empresas que pertenecen al sector de Información y comunicaciones son las que más han señalado conocer la normativa a la que está sujeta la empresa en caso de disponer de datos personales (86,7%) y disponer de un documento de seguridad que recoja las medidas técnicas y organizativas que rigen la actuación del personal con acceso a los sistemas de información (81,3%).

Deber de información (Indicador Nº43 en EICDE), garantía de derechos ARCO y solicitud de consentimiento

Previo análisis de la distribución de respuesta se van a exponer brevemente los indicadores del cumplimiento de la LOPD que se han medido:

DEBER DE INFORMACIÓN, GARANTÍA DE DERECHOS ARCO Y SOLICITUD DE CONSENTIEMIENTO

93,6%

DE LAS EMPRESAS MANIFIESTAN INFORMAR SOBRE LA EXISTENCIA DE FICHEROS PERSONALES

- Deber de información: el art.5 de la LOPD regula el deber de información al afectado, previo tratamiento de sus datos de carácter personal. Así, contempla que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de los siguientes aspectos:
  - De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
  - Del carácter obligatorio o facultativo de su respuesta.
  - De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - De la posibilidad de ejercitar los derechos ARCO.
  - De la identidad y dirección del responsable del tratamiento o de su representante.

- Garantía de derechos ARCO: la LOPD reconoce los derechos de los titulares de los datos a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales (arts. 15-17 LOPD). Los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) son detallados en la RDLOPD, que establece que deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos ARCO (art. 24.2 RDLOPD).
- Solicitud de consentimiento: el art. 6 de la LOPD establece la normativa para recabar el consentimiento de los afectados en el tratamiento de sus datos de carácter personal.

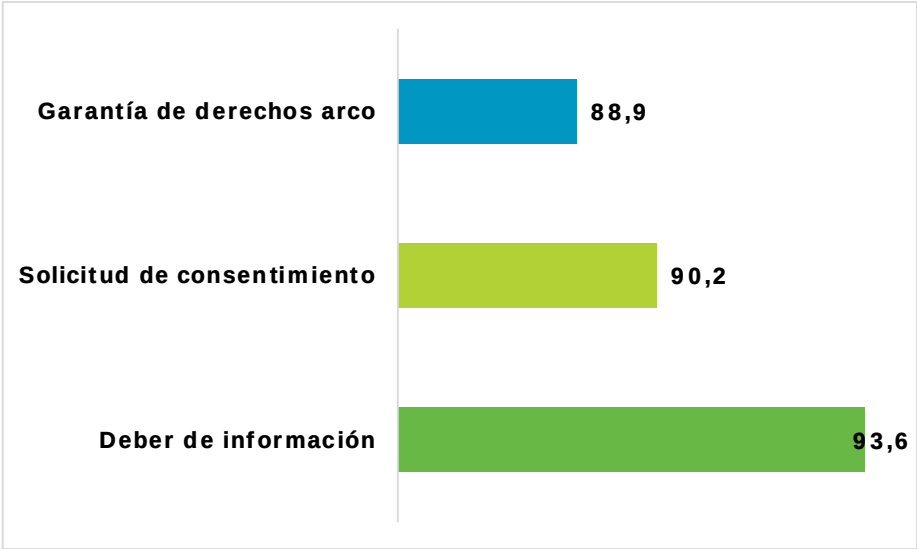
El 93,6% de las empresas consultadas manifiestan informar sobre la existencia de ficheros de datos personales.

El 90,2% de las empresas consultadas requiere el consentimiento expreso para el tratamiento de los datos personales. El porcentaje de empresas PYME y Microempresas que requieren el consentimiento expreso para el tratamiento de los datos personales ha aumentado respecto al registrado en 2012 por INTECO (actual INCIBE), pasando de un 75,9% a un 85,9% de las PYME y Microempresas consultadas en 2016.

Finalmente, el 88,9% mantiene un procedimiento para facilitar y garantizar el derecho de acceso, rectificación, cancelación y oposición sobre los datos personales. El porcentaje de empresas PYME y Microempresas que manifestaron en 2012 garantizar el cumplimiento de derechos ARCO fue sensiblemente inferior al que se ha obtenido este año (51% en 2012, 88,2% 2016).

El hecho de que haya aun aproximadamente entre un 10% y un 12% de empresas de este tamaño que no cumple con las obligaciones derivadas de la LOPD, muestra que hay recorrido en lo que se refiere a la necesidad de sensibilizar a las empresas sobre su cumplimiento.

FIGURA 78: DEBER DE INFORMACIÓN, GARANTÍA DE DERECHOS ARCO Y SOLICITUD DE CONSENTIMIENTO. RESPUESTA EXPRESADA EN %

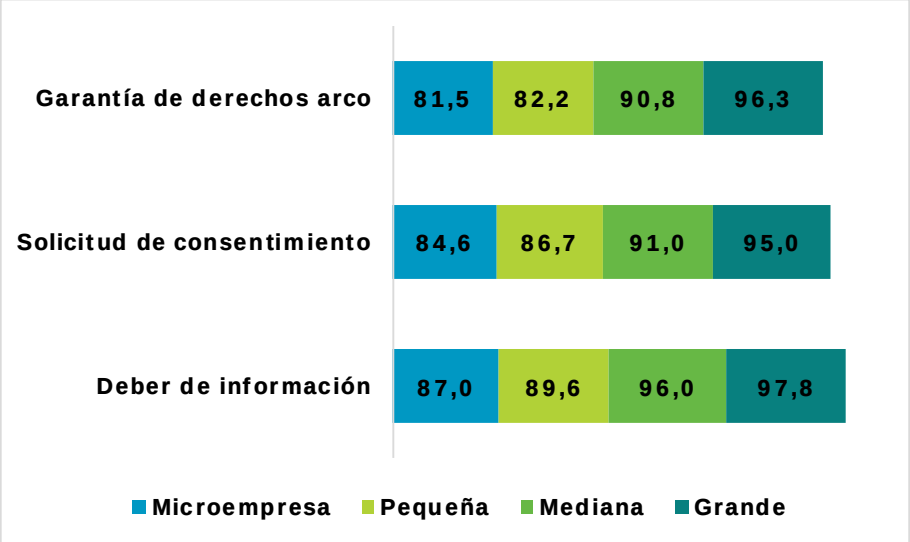


Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.099 (Empresas que han indicado que mantienen ficheros de datos personales). P23

La labor de sensibilización referida con anterioridad parece que debe incidir fundamentalmente en las microempresas y las pequeñas y medianas empresas.

Al igual que en otros casos el análisis de la distribución de respuesta sobre el conocimiento y cumplimento de las obligaciones derivadas de la norma por tamaño de empresa indica que cuanto mayor es la empresa mayor es la proporción de empresas que manifiestan cumplir sus obligaciones.

FIGURA 79: DEBER DE INFORMACIÓN, GARANTÍA DE DERECHOS ARCO Y SOLICITUD DE CONSENTIMIENTO POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Microempresa 162, Pequeña 270, Mediana 346 y Grande 321. P22

En cuanto al análisis de la distribución de respuesta por sectores de actividad, todas las empresas consultadas que pertenecen al sector Servicios de comidas y bebidas informan sobre la existencia de ficheros de datos personales.

Las empresas que pertenecen al sector de Información y comunicación son las que más requieren el consentimiento expreso para el tratamiento de los datos personales (98,2%), como viene siendo habitual por la afinidad de su actividad son las más sensibilizadas con la materia.

Para terminar, las empresas que pertenecen al sector de Actividades administrativas y servicios auxiliares también manifiestan requerir el consentimiento expreso para el tratamiento de datos personales, así como el procedimiento para facilitar y garantizar el derecho de acceso, rectificación, cancelación y oposición sobre datos personales en mayor proporción que las demás (96,4%).

7.2 Tendencias tecnológicas en la privacidad y la seguridad

TENDENCIAS TECNOLÓGICAS EN LA PRIVACIDAD Y LA SEGURIDAD

Con el objetivo de obtener nuevos indicadores sobre la percepción del impacto de tendencias tecnológicas en la privacidad y seguridad de los datos y la información corporativa, se ha solicitado a las pequeñas, medianas y grandes empresas que valoren su grado de acuerdo en una escala de cinco categorías, desde "Totalmente de acuerdo" a "Totalmente en desacuerdo", con una serie de afirmaciones que se analizan a continuación:[49]

73,2%

DE LAS EMPRESAS MANIFIESTAN QUE EL USO DE DISPOSITIVOS PERSONALES PARA EL ACCESO A DATOS E INFORMACIÓN CORPORATIVOS SUPONE UN RIESGO QUE INTENTAN EVITAR

- Se ha pretendido valorar la tendencia creciente en las relaciones laborales a orientar las tareas a la consecución de objetivos, más que a la presencia física en una oficina o centro de trabajo, por lo que se ha detectado que en el ámbito laboral se utilizan cada vez más los dispositivos personales, lo que supone un creciente riesgo ya que pueden encontrarse más expuestos a ciberamenazas.

  Así lo confirma un 73,2% de las empresas que ha manifestado que el uso de dispositivos personales para el acceso a datos e información corporativos supone un riesgo que intentamos evitar.

  En este mismo sentido, se ha identificado una tendencia a trabajar desde Internet que se ha contrastado con la percepción de las empresas de que la movilidad y el acceso remoto a los sistemas y datos corporativos desde múltiples dispositivos está incrementando la vulnerabilidad de sus activos y hace más compleja la gestión de la seguridad.

Ante el creciente manejo de información confidencial desde dispositivos móviles en el acceso de los empleados a información y recursos desde fuera del entorno corporativo, INCIBE como se ha señalado anteriormente, recomienda antes de usar un dispositivo personal en su negocio, leer detenidamente la Guía dispositivos móviles personales para uso profesional (BYOD): https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el

67,4% DE LAS EMPRESAS OPINA QUE LA MOVILIDAD Y EL ACCESO REMOTO A LOS SISTEMAS Y DATOS CORPORATIVOS DESDE MÚLTIPLES DISPOSITIVOS ESTÁ INCREMENTANDO LA VULNERABILIDAD DE SUS ACTIVOS Y HACE MÁS COMPLEJA LA GESTIÓN DE LA SEGURIDAD

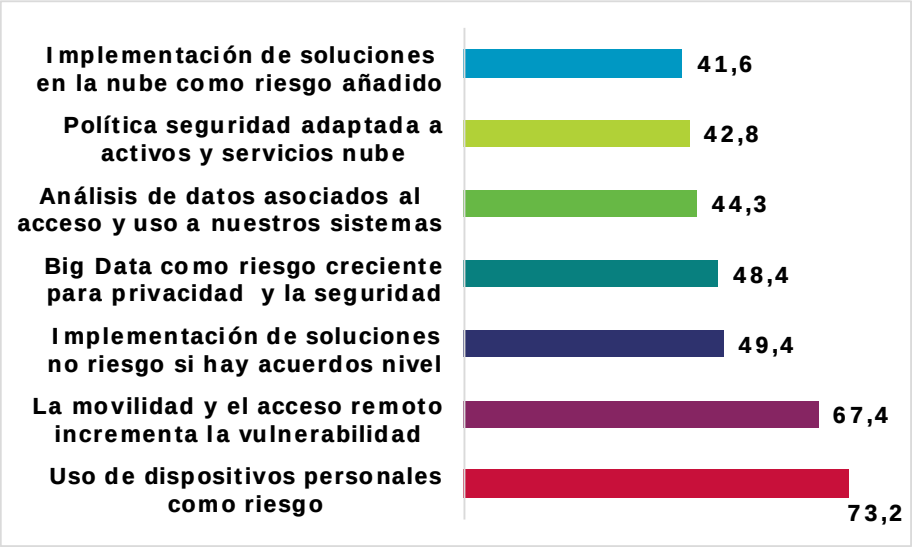
- Respecto a la irrupción del Big Data en el mundo empresarial, el 48,4% de las empresas consultadas considera que el análisis de macro datos y el uso masivo de datos representa un riesgo creciente para la privacidad de las personas y la seguridad de la información corporativa.
- En lo que respecta a los servicios en la nube, las empresas han manifestado en un porcentaje muy similar recurrir a A.N.S (acuerdos de nivel de servicio) con proveedores y adaptar su propia política de seguridad para controlar la privacidad y la seguridad de los activos de información y servicios que mantienen en la nube. No obstante, un 41,6% de las empresas consultadas

[49] Para simplificar el análisis se han agrupado las categorías en "De acuerdo" (agrupa las respuestas de "Totalmente de acuerdo" y "Bastante de acuerdo") y "En desacuerdo" ("Bastante en desacuerdo" y "Totalmente en desacuerdo"). Tanto en el análisis como en las gráficas se hará referencia a la categoría "De acuerdo".

todavía considera que la implementación de soluciones en la nube es un riesgo añadido para la privacidad y la seguridad de los activos de información.

- Por último, cabe resaltar positivamente que un porcentaje elevado de empresas mantienen una estrategia de análisis de datos asociados al acceso y uso a sus sistemas de información, que les ayuda a mejorar su seguridad y conocer sus vulnerabilidades (44,3%).

FIGURA 80: EMPRESAS QUE INDICAN ESTAR DE ACUERDO CON TENDENCIAS TECNOLÓGICAS EN LA PRIVACIDAD Y SEGURIDAD DE DATOS. RESPUESTA EXPRESADA EN %



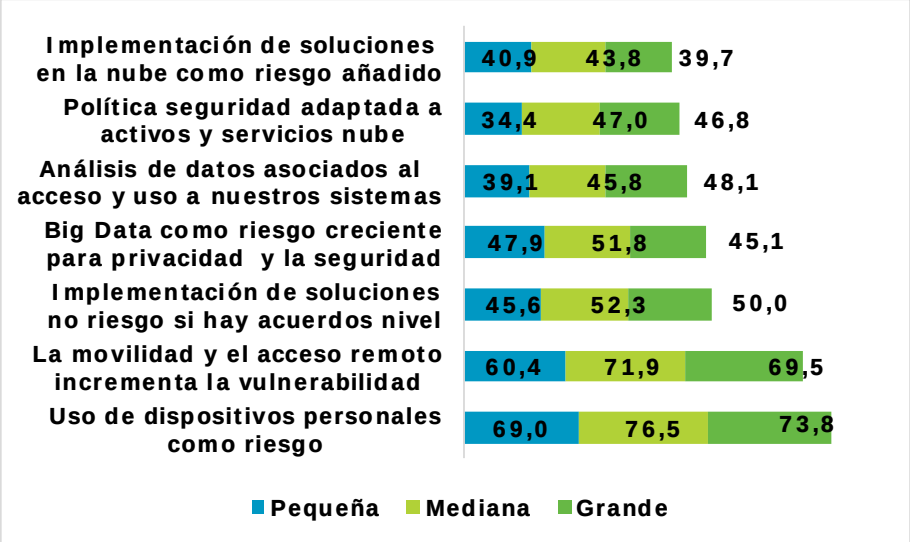
Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base 1.167. P24

Para un porcentaje bastante alto de las empresas consultadas el uso de dispositivos personales para el acceso a datos e información, y la movilidad y el acceso remoto a sus sistemas y datos suponen un riesgo.

Esto representa un reto para la seguridad TIC ya que la tendencia al uso de dispositivos personales para trabajar y el acceso remoto a los sistemas y datos desde otros lugares pueden exponer a la empresa a sufrir incidentes de seguridad imprevistos.

No existe una relación significativa entre las tendencias tecnológicas en la privacidad y la seguridad y el tamaño de la empresa, según la distribución de respuesta no existen grandes variaciones.

FIGURA 81: EMPRESAS QUE INDICAN ESTAR DE ACUERDO CON TENDENCIAS TECNOLÓGICAS EN LA PRIVACIDAD Y SEGURIDAD DE DATOS POR TAMAÑO. RESPUESTA EXPRESADA EN %



Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016. Base Pequeña 384, Mediana 413 y Grande 370. P22

En cuanto a la distribución de la respuesta de las empresas según el sector de actividad al que se dediquen, cabe destacar el comportamiento de dos sectores.

Las empresas que pertenecen al sector de Actividades administrativas y servicios auxiliares opinan en mayor medida que las demás, que el uso de dispositivos personales para el acceso a datos e información corporativa supone un riesgo para su negocio con un 83,9%.

Por otro lado, las empresas que pertenecen al sector de Información y comunicaciones son las que han manifestado en mayor proporción y de manera significativa (57,6%) estar adaptando su política de seguridad para el control de la privacidad y la seguridad de los activos de información y servicios que mantienen en la nube. Esto concuerda con la caracterización previa que se hizo del uso de servicios en la nube por sector, ya que las empresas del sector de Información y comunicaciones eran de las que más manifestaban utilizar tanto servicios de alojamiento, como servicios de almacenamiento y aplicaciones de software como servicio en la nube.

Además, las empresas del sector de Información y comunicaciones son las que más manifiestan (57,6%) mantener una estrategia de análisis de datos asociados al acceso y uso a sus sistemas de información.

ANEXO I. METODOLOGÍA

El estudio se ha desarrollado en tres fases.

- La primera fase se ha correspondido con el análisis de fuentes documentales. De este modo, se han revisado informes y datos provistos por un conjunto de organismos y entidades públicas y privadas que desarrollan procesos de investigación sobre la seguridad en las empresas.
- La segunda fase ha constituido la elaboración de un modelo estadístico fiable y la ejecución del trabajo de campo orientado a la obtención de los indicadores del esquema para la confianza digital.
- La tercera fase ha constituido la elaboración del informe final.

Análisis de fuentes documentales

La relación de fuentes documentales utilizadas para el desarrollo de este estudio se puede consultar en Anexo II.

El análisis permitió conocer el proceso que ha generado el "Esquema de indicadores para la confianza digital".

Igualmente, permitió verificar aquellos indicadores integrados en el esquema que habían sido abordados por estudios precedentes relacionados con la materia[50], estableciendo las relaciones específicas entre los indicadores generados por los estudios precedentes y los del esquema. Una vez establecida la relación, se conoció la definición específica de cada indicador y se procedió a su posible homogeneización, con el fin de generar indicadores que pudieran ser comparables desde el punto de vista temporal. Esta homogeneización no ha sido posible en todos los casos.

Definido cada uno de los indicadores y la existencia de valores previos, se procedió a definir las preguntas específicas de la encuesta que ha servido de base para la realización del trabajo de campo, cuyo contenido y alcance se incluye en anexo.

Modelo estadístico y trabajo de campo

El universo objeto de estudio ha sido las empresas españolas inscritas en el Registro Mercantil relacionadas con un conjunto de CNAE seleccionados. A diferencia del universo de la Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones y del Comercio Electrónico en las Empresas realizada por el Instituto Nacional de Estadística, en esta encuesta del ONTSI no se incluyen en la investigación las empresas constituidas por autónomos.

La selección de los CNAE se ha realizado para que coincidan con los utilizados por el Instituto Nacional de Estadística en la encuesta mencionada, con el fin de conseguir la mayor comparabilidad posible entre los datos obtenidos por ambas encuestas[51].

El universo de empresas al que se ha dirigido la encuesta se ha obtenido a través del Sistema de Análisis de Balances Ibéricos (SABI), que permite obtener los datos del Registro Mercantil, seleccionando todas las empresas activas de los CNAE investigados, independientemente de su tamaño, quedando el universo constituido por 584.503 empresas.

En un universo tan grande como el definido hubiera bastado con realizar 384 encuestas para lograr significatividad estadística para un nivel de confianza del 95% y un error muestral del 5%.

Sin embargo, dado que la población se distribuye fundamentalmente en empresas con menos de 50 trabajadores (suponen el 98% del total de empresas), las medianas y grandes

[50] Particularmente los indicadores de los diversos estudios realizados por INTECO, actual Instituto Nacional de Ciberseguridad (INCIBE), así como por el Instituto Nacional de Estadística (INE) y Eurostat.

[51] Debe entenderse, no obstante, que los datos obtenidos no son plenamente comparables entre sí, por dos razones. De un lado porque la forma de preguntar no es necesariamente la misma en las dos encuestas. De otro porque el universo utilizado en la encuesta es diferente, fundamentándose este estudio en las empresas inscritas en el Registro Mercantil y el del INE en el Directorio Central de Empresas (DIRCE).

empresas apenas tendrían representación, por lo que se perdería capacidad de inferencia para estos grupos. De otro lado, hay sectores de actividad que apenas tienen población, como el de Reparación de ordenadores y equipos de comunicación (CNAE 95.1) o el de Suministro de agua, actividades de saneamiento, gestión de residuos y contaminación (CNAE 36-99), que no llegan siquiera al 1% de la población total.

Buscando la representatividad total del universo, se ha elaborado un modelo con mayor significatividad estadística y, sobre todo, mayor capacidad de inferencia a la población global.

Este modelo clasifica el universo total de empresas en cuatro poblaciones atendiendo a su tamaño: microempresas (menos de 10 empleados), pequeñas empresas (de 10 a 49 empleados), medianas empresas (de 50 a 249 empleados) y grandes empresas (más de 250 empleados), siguiendo la clasificación del Registro Mercantil.

Se entiende que estos grupos de empresas son lo suficientemente heterogéneos entre sí y homogéneos dentro de cada uno, para ser tratados como poblaciones distintas. Esta clasificación ha permitido mayor capacidad de comparación de los comportamientos de las empresas en materia de seguridad de la información atendiendo a su tamaño. Además, permitirá inferir los resultados al conjunto de empresas españolas.

Finalmente, con el objeto de recoger información acerca de los sectores de actividad y analizar su comportamiento en el ámbito de cada una de las poblaciones, se han segmentado en 17 estratos que responden a todos los sectores de actividad, conforme a la clasificación del CNAE 2009.

Así, el modelo desarrollado ha determinado la realización de **1.501 encuestas para un nivel de confianza del 95% y un error muestral del +-3%**, distribuidas por población de la siguiente manera:

- Microempresas. Esta población es estadísticamente grande, lo que ha permitido utilizar la fórmula de obtención de la muestra para poblaciones infinitas. Así, se ha determinado que para un nivel de confianza del 95% y la asunción de un error muestral del 6% la muestra obtenida para lograr significatividad estadística, esto es, capacidad de inferencia, es de 299 empresas, que se han distribuido proporcionalmente entre los distintos CNAE.[52]
- La población de pequeñas empresas es, igualmente, estadísticamente grande, por lo que se ha calculado la muestra de igual forma que la población de microempresas. Para un nivel de confianza del 95% y un error muestral del 5% se ha obtenido una respuesta de 398 empresas estadísticamente significativa, distribuidas proporcionalmente por sectores de actividad.
- La población de medianas empresas ya no cumple con la condición estadística para ser considerada población infinita, siendo población finita. Por ello se ha procedido a calcular la muestra para un nivel de confianza del 95% y un error muestral del 5%, obteniéndose una respuesta estadísticamente significativa de 426 empresas, repartidas proporcionalmente entre los grupos de CNAE seleccionados.
- Por último, la población de grandes empresas tampoco cumple con la condición de población infinita, por lo que se ha calculado de la misma forma que la población de medianas empresas, estableciéndose que para un nivel de confianza del 95% y la asunción de un error muestral del 5% la muestra necesaria para lograr significatividad estadística era de 378 empresas, distribuidas proporcionalmente entre los distintos CNAE.

[52] Para esta población han faltado 91 encuestas para llegar a las 390 que establecía la muestra teórica planteada en el informe metodológico, aumentando en una décima el error muestral esperado, de 5% al 6%. Durante todo el trabajo de campo ha existido una dificultad ligada a la naturaleza de esta población, debido a que se tratan de empresas de menos de 10 empleados que apenas cuentan con soporte o personal informático propios con lo que se dificulta su participación en el estudio, que se ha intentado mitigar contactando un número proporcionalmente mayor de empresas hasta llegar a 2.432.

TABLA 10: DISTRIBUCIÓN DE LA MUESTRA POR POBLACIONES

Tamaño empresa	Muestra	Error muestral
Microempresas	299	6%
Pequeñas empresas	398	5%
Medianas empresas	426	5%
Grandes empresas	378	5%
Total empresas	**1.501**	**3%**

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016

Dado que la calidad de los datos de las empresas, obtenidos del Registro Mercantil no es óptima, y que buena parte de los registros carecen de datos completos de contacto, se procedió a depurar la base de datos obtenida, proceso que se ha orientado, también, a incrementar la tasa de respuesta.

En este proceso de depuración se corroboraron o corrigieron los datos de las empresas y se obtuvo su correo electrónico. De este modo, en la medida que el instrumento de consulta ha sido la encuesta web solo se ha requerido información a las empresas que mantenían acceso a Internet.

Con el fin de obtener las 1.501 respuestas referidas con anterioridad se ha requerido la respuesta a un total de **9.506 empresas.**

La elaboración de la base de datos depurada se ha llevado a cabo mediante una distribución proporcional según el tamaño de las empresas y los sectores de actividad, sin embargo tras estudiar la evolución del trabajo de campo y las particularidades de cada uno de los estratos se han reforzado los requerimientos de información allí donde se ha considerado necesario, de manera que se han incluido en el proceso un número superior de microempresas y de empresas de algunos de los sectores de actividad. En algunos sectores de actividad en el ámbito de las empresas grandes se ha llegado prácticamente a agotar el censo, es decir, se ha contactado con casi la totalidad de las empresas.

A continuación, se muestra la distribución de la respuesta por sector de actividad, así como los errores muestrales asumidos para cada uno de los estratos:

TABLA 11: DISTRIBUCIÓN DE LA MUESTRA POR SECTOR DE ACTIVIDAD

Sector de actividad	Muestra	Error muestral
Alimentación, textil, madera y papel	152	8%
Coquerías, productos farmacéuticos, caucho y plásticos	81	11%
Metalurgia y fabricación de productos metálicos	62	12%
Productos informáticos, material y equipo eléctrico, maquinaria y equipo mecánico vehículos de motor	104	10%
Construcción	177	7%
Comercio al por mayor y al por menor y venta y reparación de vehículos de motor	353	5%
Transporte y almacenamiento	79	11%
Servicios de alojamiento	76	11%
Servicios de comidas y bebidas	34	17%
Información y comunicaciones	75	11%

Actividades inmobiliarias	39	16%
Actividades profesionales, científicas y técnicas	129	9%
Actividades administrativas y servicios auxiliares	104	10%
Otros sectores	36	16%

Fuente: Encuesta ONTSI sobre confianza digital en las empresas 2016[53]

Explotación de datos

En primer lugar, se ha realizado un análisis descriptivo de todas las variables recogidas en el cuestionario.

En segundo lugar, con objeto de aportar valor y refutar hipótesis previas se ha llevado a cabo un análisis bivariado entre las variables consideradas "dependientes" y las "explicativas", a través de una prueba de significatividad "*Chi – cuadrado*".

Como resultado se han obtenido valores para los indicadores propuestos en el *Desk Research* previo y su correspondiente informe metodológico, sin embargo, cabe mencionar que se ha considerado oportuno eliminar un indicador del análisis, dado que un error metodológico no ha permitido medirlo correctamente. Este indicador es el de "compras por comercio electrónico", cuya cifra obtenida ha sido muy superior a la esperada, dado que al preguntar a las empresas si realizan comercio electrónico no se han excluido determinadas prácticas no consideradas comercio electrónico (como los mensajes o correos electrónicos escritos de forma manual), lo que sin duda habrá de tenerse en cuenta a la hora de realizar futuros estudios.

Ficha técnica de la encuesta

- Universo identificado: todas las empresas españolas activas según el Registro Mercantil con acceso a Internet.
- Perfil del encuestado respondiente: el responsable TIC, o en su defecto el representante legal o administrador de la empresa.
- Ámbito geográfico: todo el territorio nacional.
- Técnica de recogida de información: cuestionario web, con soporte telefónico.
- Duración de la encuesta: tiempo estimado de 30 minutos.
- Periodo de trabajo de campo: del 29 de agosto al 23 de diciembre de 2016.
- Diseño muestral: Muestreo aleatorio estratificado por tamaño de empresa y sector de actividad, con afijación proporcional.
- Tamaño muestral: 1.501
- Margen de error: ± 3% para datos globales, nivel de confianza del 95% (p=q=0,5).

El cuestionario para las microempresas ha sido reducido en 3 preguntas tal como se indica en anexo.

[53] La Categoría Otros sectores agrupa los siguientes sectores: Energía eléctrica, gas, vapor y aire acondicionado; Suministro de agua, actividades de saneamiento y gestión de residuos; Agencias de viajes, operadores turísticos y servicios de reservas y Reparación de ordenadores y equipos de comunicación. Se ha decidido eliminar estos sectores del análisis porque contaban con un error superior al 17%, lo que desvirtuaba su fiabilidad estadística.

ANEXO II. FUENTES DOCUMENTALES

En este apartado se incluyen las referencias de los principales documentos que se han utilizado en el desarrollo de este informe.

- La "*Agenda Digital para España*" de 2013. En la agenda se establece la política del Gobierno de España para desarrollar la economía y la sociedad digital durante el período 2013 -2015, y constituye "marco de referencia para establecer una hoja de ruta en materia de Tecnología de la Información y las Comunicaciones (TIC) y de administración electrónica; establecer la estrategia de España para alcanzar los objetivos de la Agenda Digital para Europa; maximizar el impacto de las políticas púbicas en TIC para mejorar la productividad y la competitividad; y transformar y modernizar la economía y sociedad española mediante un uso eficaz e intensivo de las TIC por la ciudadanía, empresas y Administraciones". el marco en la cual se recogen entre otras las prioridades relacionadas con la confianza digital en el "Plan de confianza en el ámbito digital".
- El "*Plan de confianza en el ámbito digital*". Este es uno de los siete planes que integraron originalmente la Agenda Digital para España en junio de 2013. El Plan hace suyo el mandato conjunto de la Agenda Digital para España, de la Estrategia Europea de Ciberseguridad y de la Estrategia de Seguridad Nacional para avanzar en los objetivos conjuntos de construir un clima de confianza que contribuya al desarrollo de la economía y la sociedad digital, disponer de un ciberespacio abierto, seguro y protegido, garantizar un uso seguro de las redes y los sistemas de información, y responder a los compromisos internacionales en materia de ciberseguridad.
- "*Propuesta de indicadores para el esquema para la confianza digital*" de 30 de abril de 2014. Documento interno del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), Área de Indicadores (Red.es).
- El "*Nuevo esquema de indicadores para la Confianza Digital*" de 28 de octubre de 2014. Documento interno del Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información, Área de Indicadores (Red.es).
- "*Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*" INTECO*****, 2008, trabajo de campo realizado en marzo de 2007. Dos indicadores del esquema, relacionados con la confianza digital en empresas, el 34 y 35, se replican de este estudio, ambos en el grupo de incidentes sobre ciberseguridad.
- "*Estudio sobre la seguridad y la e-confianza en las pequeñas y microempresas españolas*" INTECO*****; 2009 (trabajo de campo Febrero 2009- Junio 2009). Cuatro de los indicadores que componen el nuevo esquema, relacionados con la confianza digital en empresas, proceden de este estudio: dos de ellos relativos a herramientas y medidas de seguridad: el número 30 (Barreras para la implementación de medidas de seguridad) y el 31 (Utilización del antivirus). Uno relativo a incidentes de ciberseguridad (33. Consecuencias derivadas de los incidentes de seguridad), y uno más asociado a la preparación de empresas (39. Estado de actualización del sistema operativo y de las herramientas de seguridad).
- "*Estudio sobre el estado de la PYME española ante los riesgos y la implantación de Planes de Continuidad de Negocio*" INTECO*****, 2010 (trabajo de campo Febrero 2010- Junio 2010) y "*Estudio sobre seguridad de la información y continuidad de negocio en las empresas españolas*" INTECO*****, 2012 (trabajo de campo: parte A, seguridad de la información y e-confianza, diciembre 2011 - enero 2012; parte B, continuidad de negocio, enero-febrero 2012). Un indicador del esquema, relacionado con la confianza digital en empresas, el 32 procede de este estudio en el subgrupo de incidentes sobre ciberseguridad.

- "*Estudio sobre la protección de datos en las empresas españolas*" INTECO* 2008 y 2012. En ambos casos tres indicadores (41, 42 y 43) del nuevo esquema, relacionados con la confianza digital en empresas pequeñas y medianas (Pyme), proceden de este estudio, todos en el grupo de privacidad, subgrupo de protección de datos personales.
- "*Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones y del Comercio electrónico en las Empresas*" Instituto Nacional de Estadística (INE). Dos de los indicadores del esquema relacionados con la preparación de las empresas se pueden obtener de esta encuesta anual, el 36: empresas que han definido formalmente una política de seguridad TIC, y el 38: riesgos que se incluyen en la política de seguridad. También se puede obtener el 40: servicios disponibles en la página web: declaración de política de intimidad o certificación relacionada con la seguridad del sitio web. Finalmente, los seis indicadores relativos a las transacciones electrónicas de las empresas los números 44 a 47 ambos inclusive están vinculados a esta encuesta.
- Taxonomía v 2.0 de soluciones de seguridad TIC. Centro Demostrador de Tecnologías de Seguridad (CDTS) – INTECO* 2009. Esta taxonomía es una clasificación de las soluciones de seguridad integrando productos y servicios, que se ha utilizado en el desarrollo de la metodología. Taxonomía de soluciones de seguridad TIC – INCIBE 2015
- CCN-STIC-817 v1.0 Criterios comunes para la Gestión de Incidentes de Seguridad en el ENS. Centro Criptológico Nacional. 2012. Esta metodología desarrolla una clasificación de los incidentes de seguridad y su definición que ha sido utilizada en el desarrollo de la metodología propuesta.

* INCIBE era anteriormente INTECO.

ANEXO III. CUESTIONARIO WEB

Nº	Ámbito	Pregunta	Población a la que se dirige
1	Caracterización de la empresa	¿Qué tipo de **activos tecnológicos y de información** gestiona actualmente su empresa? *(Señale todas aquellas respuestas que considere oportunas).* a) **Ficheros de datos personales**. b) Información clasificada, sensible o confidencial. c) Software o aplicaciones informáticas. d) Equipos informáticos de sobremesa. e) Portátiles, dispositivos móviles y tabletas. f) Equipos y redes de comunicaciones. g) Instalaciones e infraestructuras de sistemas (**CPD**). h) Otros *(indique cuales*).	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta.*
2	Caracterización de la empresa	¿Su empresa utiliza Internet como usuario y proveedor de determinados servicios electrónicos, nos podría indicar que tipo de servicios electrónicos o transacciones realiza de las que se exponen a continuación? *(Señale todas aquellas respuestas que considere oportunas).* a) Mantiene una **página web** de la empresa. b) Utiliza servicios de banca electrónica. c) Utiliza la **firma digital** en alguna comunicación de la empresa. d) Utiliza la **firma digital** para relacionarse con la Administración Pública. e) Utiliza la **firma digital** para relacionarse con sus clientes y proveedores. f) Ha realizado compras por comercio electrónico. g) Ha realizado ventas por comercio electrónico. h) Tiene contratados a terceros **servicios en la nube** de alojamiento de correo electrónico y/o página web. i) Contrata **servicios en la nube** de almacenamiento, de acceso a datos y contenidos de información, en remoto. j) Contrata aplicaciones de **software como servicio en la nube** (software de gestión y/o contabilidad-**ERP**, gestión de clientes-**CRM**, etc.). k) Otros (*indicar cuáles*)	Microempresas, pequeñas, medianas y grandes. *A todas las empresas* *Multirespuesta.*
3	Caracterización de la empresa	¿En qué medida la **seguridad de la información** constituye una prioridad para su negocio? *(Por favor, Señale una única respuesta)* a) No constituye una prioridad. b) Constituye una prioridad menor. c) Tiene una elevada prioridad. d) Es una de las máximas prioridades de la	Microempresas, pequeñas, medianas y grandes. *A todas las empresas* *Única respuesta.*

		empresa.	
3.1	Caracterización de la empresa	Podría indicarnos si alguna vez la **Seguridad TIC** o la protección de datos le ha limitado a la hora de realizar transacciones electrónicas (*Responda sí o no a las siguientes afirmaciones)* a) La seguridad Tic ha limitado a la empresa a la hora de realizar ventas en Internet. b) La protección de datos nos ha limitado a la hora de realizar ventas en Internet. c) La seguridad TIC ha limitado a la empresa a la hora de realizar compras por Internet. d) La protección de datos personales ha limitado a la empresa a la hora de realizar compras por internet.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas* *Obliga a contestar si o no a cada alternativa*
4	Caracterización de la empresa	¿Podría indicarnos si o no a las afirmaciones siguientes relacionadas con el tipo de personal que de soporte informático en materia de seguridad TIC? *(Señale las respuestas que estime necesarias que sean compatibles)* a) Mantenemos personal dedicado. especializado en seguridad TIC. b) El personal interno que nos da soporte informático en general se ocupa también de la seguridad. c) Nos da soporte una empresa externa especializada en materia de seguridad con continuidad. d) Solicitamos soporte de forma reactiva cuando surge una necesidad. e) No hemos tenido necesidad de soporte especializado.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas* *Multirespuesta.*
5	Caracterización de la empresa	¿Podría indicarnos si en su empresa los **sistemas operativos** y **herramientas de seguridad** están actualizadas? *(Señale la respuesta que más se aproxime a la realidad de su empresa)* a) Sí están actualizados. b) No están actualizadas. c) No sabe/ no contesta.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Única respuesta.*
6	Herramientas y medidas de seguridad utilizadas	Para identificar si su empresa mantiene o ha definido formalmente algún tipo de política o estrategia de seguridad podría indicarnos si han realizado las siguientes acciones y si para ello ha requerido **asesoramiento externo**. *(Señale todas aquellas respuestas que considere pertinentes)* a) Tenemos definida formalmente una **política de seguridad TIC**. b) Estamos certificados en la **ISO 27001** que define el **Sistema de Gestión de la Seguridad de la información** de la empresa. c) Hemos definido una **estrategia de continuidad de negocio**. d) No hemos realizado ninguna de las actuaciones anteriores.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta y dicotómica asociada a cada respuesta positiva*

6.1	Herramientas y medidas de seguridad utilizadas	¿Cuándo fue definida o se hizo la última revisión de la **política de seguridad TIC**? (*Señale la respuesta que se adecue a la realidad de su empresa).* a) Dentro de los últimos 12 meses. b) Hace más de 12 meses y menos de 24 meses. c) Hace más de 24 meses.	Microempresas, pequeñas, medianas y grandes. (*Sólo a empresas que han declarado mantener formalmente una política de seguridad, respuesta A en pregunta anterior*) *Única respuesta*.
6.2	Herramientas y medidas de seguridad utilizadas	¿Están los siguientes **riesgos** definidos en su **política de seguridad TIC**? *(Señale todas aquellas respuestas que considere pertinentes).* a) Destrucción o corrupción de datos debido a un ataque o por un **incidente de seguridad** inesperado. b) Revelación de datos confidenciales debido a la intrusión, ataques de **phishing**, **pharming** o por accidente. c) Falta de disponibilidad de servicios TIC debido a ataques externos (p.e.: ataque de denegación de servicio **DDoS**).	Microempresas, pequeñas, medianas y grandes. (*Sólo a empresas que han declarado mantener formalmente una política de seguridad respuesta A) en pregunta anterior*). *Multirespuesta.*
6.3	Herramientas y medidas de seguridad utilizadas	¿Cuáles son las razones que le han llevado o le van a llevar a implementar las actuaciones de seguridad TIC referidas con anterioridad? *(Señale tantas respuestas como estime pertinentes)* a) Mejorar la eficiencia y/o reducir costes. b) Asegurar la integridad de los datos y la información. c) La protección contra el robo de los activos de la empresa. d) Garantizar la disponibilidad de las operaciones de negocio/ disponibilidad de los servicios en caso de crisis. e) Reputación y protección de la imagen pública de la empresa. f) Ventaja competitiva frente a otros competidores del mercado. g) Requerimientos del cliente. h) Como respuesta a un requerimiento de auditoría interna/externa. i) Cumplimiento de requerimientos regulatorios/legales. j) Alinearse con los principales estándares de la industria de seguridad. k) Anteriores interrupciones en las operaciones de Negocio. l) Otras razones u objetivos *(especificar cuáles).*	Pequeñas, medianas y grandes. *Solo a las empresas de dichas poblaciones que declaran mantener algún tipo de política, certificación, estrategia de continuidad de negocio* *Multirespuesta.*
7	Herramientas y medidas de seguridad utilizadas	¿Señale a continuación por favor qué tipo de sistemas internos de seguridad utiliza de los indicados a continuación? *(*Señale *todas aquellas respuestas que considere pertinentes)* a) Autenticación con **contraseña segura** b) **Backup** de datos externos c) Identificación de usuario y autenticación mediante **elementos biométricos**	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta.*

		d) Identificación de usuario y autenticación mediante **elementos hardware** e) Protocolos para el análisis de **incidentes de seguridad** f) Otras (*especifique cuáles)*	
8	Herramientas y medidas de seguridad utilizadas	¿Con el fin de conocer las soluciones y tipología de herramientas de seguridad que utilizan las empresas españolas, indíquenos cuáles de las siguientes herramientas ha implantado en su empresa? (*Seleccione todas las herramientas que haya implantado*). a) **Productos anti fraude** (anti **phishing** y/o anti **spam**). b) **Productos antivirus** o anti espía (anti **malaware**). c) **Herramientas de auditoría técnica y forense**. d) **Sistemas autenticación** y certificación digital y otros **sistemas de gestión de accesos** y control de identidades. e) **Herramientas de contingencia y continuidad** (copias de seguridad, recuperación). f) **Sistemas de control de contenidos confidenciales**. g) **Sistemas de control de tráfico en la red**. h) **Cortafuegos**, filtros de contenidos web, IDS, IPS. i) **Sistemas de herramientas criptográficas** (cifrado de datos, encriptación de mensajería). j) **Herramientas de seguridad en movilidad** (para dispositivos móviles, en **redes inalámbricas Wifi**). k) Otros *(especificar cuáles*).	Microempresas, pequeñas, medianas y grandes. *A todas las empresas. Multirespuesta.*
9	Herramientas y medidas de seguridad utilizadas	¿Con respecto a los dispositivos móviles que mantiene su empresa podría indicarnos cuáles de las siguientes medidas de seguridad son utilizadas en dichos dispositivos? (*Señale todas aquellas respuestas que considere oportunas).* a) Acceso mediante **código pin** (contraseña) b) Contraseña de desbloqueo c) **Copia de seguridad** de datos sensibles d) **Bluetooth** oculto y con contraseña e) Actualización de software automáticas f) Programa **antivirus** **g) Robustez de contraseña** h) **Formateo** tras errores en la contraseña i) Imposibilidad de instalación de programas o aplicaciones j) Borrado remoto de datos en caso de extravío k) Cifrado de datos y/o comunicaciones	Pequeñas, medianas y grandes. *Solo a las empresas que en la pregunta 1 han señalado que disponen de dispositivos, portátiles, dispositivos móviles, tabletas (respuesta e). Multirespuesta.*
10	Herramientas y medidas de seguridad utilizadas	¿Indíquenos, por favor si la **red wifi** de su empresa mantiene protección y el tipo de protección utilizada? *(Señale la respuesta que más se aproxime a la realidad de su empresa)*	Pequeñas, medianas y grandes. *Solo a las empresas que en la pregunta 1 han*

		a) Sí, la **red wifi** mantiene protección utilizando el **protocolo WPA, WPA2**. b) Sí, la **red wifi** de la empresa mantiene **protección WEP**. c) Si, mediante **ocultación del punto de red**. d) Si, mediante el **filtrado de direcciones MAC**. e) Sí mantiene protección, pero desconozco el sistema. f) No, la **red wifi** está abierta sin protección. g) No sabe	*señalado que disponen de redes de comunicaciones (respuesta f).* *Única respuesta.*
12	Herramientas y medidas de seguridad	De las características de los productos de seguridad enunciadas a continuación cuáles son las que valora más. (*Indique para cada característica el grado de valoración que atribuye a cada característica a la hora de adoptar una solución, siendo 1 muy valorado, 2 bastante valorado, 3 algo valorado, 4 poco valorado, 5 nada valorado)* a) Acceso a su contratación. b) Facilidad de instalación. c) Facilidad de mantenimiento. d) Servicio postventa, soporte técnico, garantía. e) Calidad del producto. f) Efectividad del producto. g) El precio del producto. h) Otras (*Especificar cuáles*)	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta.*
13	Herramientas y medidas de seguridad	Ahora le queremos preguntar por los servicios especializados de seguridad. Podría indicarnos si ha contratado alguno de ellos, y si los considera necesarios. *Valórelos estimando una escala de 1 a 5 siendo 1 muy necesario, bastante necesario, algo necesario, poco necesario, no es necesario.* a) **Servicios de auditoría técnica**: servicios de detección de intrusiones, pruebas (auditoría técnica), test de intrusión. **b) Servicios de contingencia y continuidad del negocio.** **c) Servicios de cumplimiento de la legislación (LOPD)** d) Externalización de servicios de seguridad: **seguridad gestionada**, **outsourcing**. e) Formación. f) Gestión de incidentes. g) Implantación y certificación de normativa: h) Certificación y acreditación, de **políticas de seguridad**, **Planes de seguridad**, gestión de riesgos i) Planificación e implantación de infraestructuras Dicotómica Si/no, más la valoración de cada	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta.*

		solución.	
14	Herramientas y medidas de seguridad	Para terminar con este apartado de herramientas y medidas de seguridad ¿Percibe alguna barrera a la implementación de las medidas y soluciones de seguridad adecuadas a los objetivos de su empresa? *(Seleccione todas las respuestas que considere oportunas*) *a)* Es difícil encontrar soluciones adecuadas para mi negocio. *b)* Falta de personal cualificado para abordar el proceso. *c)* Los productos son caros y no tenemos presupuesto. *d)* No tenemos tiempo para abordar el proceso *e)* No es de interés para la dirección. *f)* No lo considero económicamente rentable. *g)* No percibo ninguna barrera.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta.*
15	Incidentes sobre ciberseguridad	¿Podría indicarnos si antes de iniciar este cuestionario conocía las consecuencias negativas que puedan derivarse de los incidentes de seguridad siguientes? (*Señale todos aquellos incidentes cuyas consecuencias conocía)* *a)* Bombas lógicas. *b)* Correo basura. *c)* Denegación de servicios. *d)* Fallos técnicos. *e)* Fraudes. *f)* Pérdidas de datos. *g)* Pharming. *h)* Phishing. *i)* Programas espías. *j)* Robos de identidad. *k)* Robos de información. *l)* Troyanos. *m)* Virus.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas.* *Multirespuesta.*
16	Incidentes sobre ciberseguridad	¿Podría indicarnos qué tipo de incidentes de seguridad ha sufrido durante el último año? *(Señale todas aquellas respuestas que respondan a la realidad de su empresa.)* *a)* **Ataques informáticos**. *b)* **Afectación por código dañino** (por ejemplo, por un virus). *c)* Robo de equipos. *d)* Pérdida o copia de datos e información. *e)* Caída de los sistemas o aplicaciones de la empresa. *f)* Caída de los sistemas de soporte (climatización, líneas y dispositivos de comunicación, etc.). *g)* Daños físicos en instalaciones o equipos derivados de cambios físicos no autorizados. *h)* **Abuso de privilegios** y/o usos **inadecuados por suplantación de identidad** (phishing). *i)* Baja de personal crítico.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas* *Multirespuesta*

		j) Falta de servicio por parte de proveedores. *k)* Inundación, terremoto, incendio. *l)* Multas, sanciones. *m)* Otros *(especificar cuáles).* *n)* La compañía no ha sufrido incidentes de seguridad en el periodo mencionado.	
16.1	Incidentes sobre ciberseguridad	¿Más concretamente podría decirnos si de los incidentes de seguridad ocurridos se ha derivado alguna de las consecuencias siguientes*? (Señale todas aquellas respuestas que considere pertinentes.)* *a)* De los incidentes ocurridos no se derivó ninguna situación de importancia. *b)* Fraude con prejuicio económico. *c)* Multas o sanciones. *d)* Daños en la imagen/reputación de su negocio. *e)* Pérdida de confianza en los medios electrónicos. *f)* Daños en los equipos (**hardware**). *g)* Pérdida de archivos y datos. *h)* Problemas de conexión/redes. *i)* Pérdida de tiempo de trabajo. *j)* Caída de los ordenadores. *k)* Otros (*especificar cuáles*). *l)* No sabe /no contesta.	Microempresas, pequeñas, medianas y grandes. *Solo a empresas que indican en la pregunta anterior que han sufrido incidentes de seguridad en el último año.* *Multirespuesta.*
16.2	Incidentes de ciberseguridad	Podría indicarnos el tipo de impacto que han tenido en su empresa los incidentes sufridos el pasado año. (Seleccione aquellas respuestas que considere oportunas.) • Impacto económico-financiero*. (Referido a las pérdidas económicas derivadas de los incidentes de seguridad).* • Impacto operativo. (*En alusión a la paralización de las actividades, pérdida de tiempo, realización de tareas extraordinarias, como consecuencia de dichos acontecimientos)*. • Impacto en la imagen/reputación. (*En referencia a la pérdida de confianza de los clientes, imagen de marca que una empresa puede padecer como consecuencia de un incidente de seguridad).* • Impacto legal/contractual. *(En caso de haber sido señalada como infractora de requerimientos legales o acuerdos contractuales con terceros - clientes, socios, accionistas, etc*.).	Microempresas, pequeñas, medianas y grandes. *Solo a empresas que indican en la pregunta anterior que han sufrido incidentes de seguridad en el último año.* *Multirespuesta.*
16.3	Incidentes sobre ciberseguridad	¿Dado que en la pregunta anterior nos indica que los incidentes sufridos han tenido un impacto económico podría indicarnos si ha cuantificado este impacto económico? *a)* Si *b)* No	Microempresas, pequeñas, medianas y grandes. *Solo a empresas que indican en la pregunta anterior que han sufrido impacto económico respuesta (a)*

16.4	Incidentes de ciberseguridad	Podría indicarnos el perjuicio económico que han supuesto esos incidentes: *a)* Menos de 1000 euros *b)* Entre 1000 y 5000 euros *c)* Entre 5000 y 10000 euros *d)* Entre 10000 y 15000 euros *e)* Más de 15000 euros	Microempresas, pequeñas, medianas y grandes. *Solo a las empresas que indican que han indicado si en pregunta anterior a).*
18	Incidentes de ciberseguridad	¿Independientemente de que se hayan producido incidentes de seguridad en el último año podría indicarnos según su percepción cuáles son las causas de los incidentes de seguridad? (*Señale todas aquellas respuestas que considere aplican en su caso).* *a)* La falta de herramientas adecuadas para prevenir los incidentes. *b)* La falta de actualización de los sistemas *c)* La configuración inadecuada de los sistemas. *d)* La carencia de una cultura de seguridad en la organización. *e)* El personal no sigue las normas de seguridad. *f)* El desconocimiento de los incidentes de seguridad y sus consecuencias. *g)* La falta de presupuesto para aplicar las soluciones oportunas. *h)* La falta de asesoramiento adecuado. *i)* Otras (especifique cuáles).	Microempresas, pequeñas, medianas y grandes. *A todas las empresas. Multirespuesta.*
19	Incidentes de ciberseguridad	¿Qué respuesta ha dado o daría su empresa a los incidentes que le han ocurrido en el pasado, o que le pudieran ocurrir en el futuro? *(Señale todas aquellas respuestas que considere aplican en su caso. A todas las empresas independientemente de que hayan sufrido o no incidentes de seguridad).* *a)* Llamar a nuestro proveedor local de sistemas informáticos *b)* Localizar un experto de seguridad externo a la empresa *c)* Llamar a un conocido con conocimientos en la materia *d)* Localizar un servicio técnico *e)* Se resuelve el incidente con personal interno de la empresa *f)* Llamar al proveedor de Internet *g)* Otros *(especificar cuáles)*	Microempresas, pequeñas, medianas y grandes. *A todas las empresas. Multirespuesta.*
20	Incidentes de ciberseguridad	¿Podría indicarnos si al sufrir algún incidente de seguridad en su empresa se ha producido alguna de las actuaciones o cambio de hábitos siguientes? *(Señale todas aquellas respuestas que considere aplican en su caso. A todas las empresas que han indicado que han sufrido incidentes de seguridad).* *a)* Hemos dejado de usar determinados servicios de Internet. *b)* Hemos establecido protocolos y procedimientos de seguridad más estrictos. *c)* Hemos iniciado un **plan de seguridad**.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas Multirespuesta.*

		d) Hemos cambiado las contraseñas. *e)* Hemos comenzado a realizar copias de seguridad *f)* Hemos instalado nuevas herramientas y actualizado nuestros programas *g)* Hemos contratado servicios de auditoría externos. *h)* Otros *(especificar cuáles)*	
21	Privacidad	¿Podría indicarnos si su empresa mantiene en su página web una declaración de política de intimidad, salvaguarda de privacidad o certificación relacionada con la seguridad del sitio web (Indique si o no) *a)* Si *b)* No *c)* No sabe	Microempresas, pequeñas, medianas y grandes. *Sólo a empresas que indican que mantienen página web en la pregunta 2 respuesta a)* *Pregunta dicotómica.*
22	Privacidad	En lo que a política de privacidad se refiere, ¿Podría indicarnos con cuáles de estas afirmaciones se identifica su empresa? *(Señale todas aquellas respuestas con las que se identifique su empresa).* *a)* Mi empresa conoce la **Ley Orgánica de Protección de Datos** *b)* Mi empresa conoce que está sujeta a dicha normativa en caso de disponer **de ficheros de datos personales** de cualquier tipo (personal, clientes y proveedores, etc.) *c)* Mi empresa dispone de un **documento de seguridad** que recoge las medidas técnicas y organizativas que rigen la actuación del personal con acceso a los sistemas de información.	Microempresas, pequeñas, medianas y grandes. *A todas las empresas*. *Multirespuesta.*
23	Privacidad	En caso de mantener ficheros de datos personales, indíquenos si su empresa: *(Responda sí o no a cada afirmación siguiente).* *a)* Informa sobre la existencia **de ficheros de datos personales.** *b)* Requiere el **consentimiento expreso para el tratamiento** de los datos personales. *c)* Mantiene un procedimiento para facilitar y garantizar el **derecho de acceso, rectificación, cancelación y oposición sobre los datos personales**.	Microempresas, pequeñas, medianas y grandes. *Sólo a las empresas que han indicado en la pregunta 1 que mantienen ficheros de datos personales* *(Obliga a contestar si/no a cada una de las opciones)*
24	Tendencias	Para terminar ¿Podría indicarnos su grado de acuerdo o desacuerdo con las siguientes afirmaciones sobre el impacto en la seguridad y la privacidad de las tendencias tecnológicas actuales? (*siendo 1 totalmente de acuerdo, 2 bastante de acuerdo, 3 algo de acuerdo, 4 bastante en desacuerdo, 5 totalmente en desacuerdo*) *a)* El uso de dispositivos personales para el acceso a datos e información corporativos supone un **riesgo** que intentamos evitar. *b)* La movilidad y el acceso remoto a los sistemas y datos corporativos desde múltiples dispositivos está incrementando la **vulnerabilidad** de nuestros activos y hace	Pequeñas, medianas y Grandes empresas. *A todas las empresas*

		más compleja la gestión de la seguridad. *c)* La implementación de **soluciones en la nube** es un riesgo añadido para la privacidad y la seguridad de los **activos de información**. *d)* La implementación de **soluciones en la nube** no es un riesgo añadido si establecen acuerdos de nivel de servicio con proveedores. *e)* Estamos adaptando nuestra **política de seguridad** para el control de la privacidad y la seguridad de los **activos de información** y servicios que mantenemos en la nube. *f)* El análisis de **macro datos** y el uso masivo de datos representa un riesgo creciente para la privacidad de las personas y la seguridad de la información corporativa. *g)* Mantenemos una estrategia de análisis de datos asociados al acceso y uso a nuestros sistemas de información, que nos ayuda a mejorar nuestra seguridad y conocer nuestras **vulnerabilidades**.	

ANEXO IV. RELACIÓN EICDE-CUESTIONARIO

A continuación, a modo de resumen se recoge la relación entre el Esquema de Indicadores de Confianza Digital en España en empresas y las preguntas del cuestionario de donde se originarán dichos indicadores.

Nº	Nombre indicador	Pregunta
Herramientas y medidas de seguridad		
30	Barreras a la implementación de medidas de seguridad	14
31.1	Nivel de utilización de antivirus declarado	8
31.2	Nivel de utilización del antivirus, presencia real	No se puede obtener mediante encuesta.
Incidentes sobre ciberseguridad		
32	Incidentes de seguridad	16
33	Consecuencias derivadas de los incidentes de seguridad	16.1
34	Repercusión económica de los incidentes de seguridad	16.2, 16.3
35	Grado de conocimiento de los incidentes de seguridad	15
Preparación de las empresas		
36	Empresas que han definido formalmente una política de seguridad	6, 6.1
37	Empresas que utilizaban sistemas internos de seguridad por tipo	7
38	Riesgos que incluyen en la política de seguridad TIC	6.2
39.1	Estado de la actualización del sistema operativo y de las herramientas de seguridad (auditado) real	No se puede obtener mediante encuesta
39.2	Estado de la actualización del sistema operativo y de las herramientas de seguridad declarado	5
Privacidad de las empresas		
40	Utilidades de páginas web por parte de las empresas, declaración de política de seguridad o certificación relacionada con la seguridad del sitio web	21
41	Empresas con ficheros con datos personales que declaran disponer de documento de seguridad	1, 22
42	Conocimiento de la LOPD	22
43	Deber de información	23
Transacciones electrónicas		

44	Empresas que han realizado compras por Internet	2
45	Empresas que han realizado ventas por Internet	2
46	Empresas que utilizaron firma digital por motivo	2
47	Porcentaje de empresas en los que problemas de seguridad TIC o protección de datos limitó u obstaculizó realizar ventas a través de Internet	3.1

ANEXO V. DEFINICIONES UTILIZADAS

Seguridad TIC: La seguridad TIC integra aquellas medidas, controles y procedimientos aplicados a los sistemas TIC (Tecnologías de la Información y las Comunicaciones), para asegurar la integridad, autenticidad, disponibilidad y confidencialidad de datos y sistemas de información.

Activos tecnológicos o de información: Un activo en el ámbito de la seguridad de la información, se refiere a cualquier información, sistema relacionado con su tratamiento, o soporte que tenga valor para la organización. Son activos de información desde los dispositivos electrónicos de distinta naturaleza que contienen datos e información, hasta las personas que gestionan dicha información, así como los propios datos e información que genera la empresa en su actividad diaria. Desde el punto de vista de la seguridad, en una empresa, todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario. La tipificación de los activos es de interés como un criterio de identificación de vulnerabilidades y amenazas potenciales, así como para establecer las salvaguardas apropiadas a la naturaleza de cada tipo de activo.

CPD: El acrónimo se corresponde a Centro de Procesamiento de Datos. Un CPD está constituido por un conjunto de recursos necesarios para el procesamiento de información de una empresa, dando soporte al acceso a los servicios y contenidos de información de la organización.

Ficheros de datos personales: Son un tipo de activo que requiere especial protección. La Ley Orgánica 15/1999 de Protección de Datos Personales, define un fichero de datos personales en el artículo 3.b), como "conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". Los ficheros de datos de carácter personal se encuentran sometidos a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos (RGPD).

Página WEB: Fuente de información adaptada para la World Wide Web (WWW) y accesible mediante un navegador de Internet. Esta Información se presenta generalmente en formato HTML y puede contener hiperenlaces a otras páginas web, constituyendo la red enlazada de la World Wide Web. La existencia de una página web en una empresa permite deducir que puede sufrir determinadas amenazas derivadas de su presencia en la World Wide Web.

Firma digital: Información cifrada que identifica al autor de un documento electrónico y autentifica su identidad. Al igual que las firmas manuales, es única y específica de un usuario y o un ordenador. El uso de la firma digital en una empresa indica el grado de madurez de la organización en lo que se refiere al uso de documentos electrónicos como alternativa al papel.

Servicios en la nube*:* Denominación derivada del inglés Cloud Computing. El Cloud Computing, o los servicios en la nube se refiere a los servicios TIC que son usados a través de Internet para tener acceso a software, capacidad de computación, capacidad de almacenamiento, etc. Dichos servicios tienen las siguientes características: son entregados o están disponibles en servidores proveedores de los mismos; pueden aumentar o disminuir fácilmente; y pueden ser utilizados según la necesidad del usuario sin necesidad de interacción con el proveedor del servicio.

Software como servicio en la nube: Derivada de la expresión inglesa Software as a Service (SaaS). Se refiere a un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente. La empresa proveedora TIC se ocupa del servicio de mantenimiento, de la operación diaria y del soporte del software usado por el cliente. Regularmente el software puede ser consultado en cualquier ordenador, se encuentre presente en la empresa o no. Se deduce que la información, el procesamiento, los insumos, y los resultados de la lógica de negocio del software, están hospedados en la compañía de TIC.

ERP: Una solución ERP, del inglés Enterprise Resource Planning, es lo que se conoce en España como software de gestión integrada, y se define como un grupo de módulos conectados a una única base de datos. Es un paquete de software que permite administrar

todos los procesos operativos de una empresa, integrando varias funciones de gestión en un único sistema (compras, ventas, contabilidad, gestión, producción, etc.)

CRM: Del ingles Customer Relationship Management. Es un software para la administración de la relación con los clientes. Puede comprender varias funcionalidades orientadas a la gestión de las oportunidades de negocio, las ventas, los clientes de la empresa, campañas de marketing, etc. así como otras de carácter informacional asociadas al análisis de datos y generación de indicadores sobre la evolución de la relación con clientes, entre otros aspectos.

Seguridad de la información: La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Se puede definir como el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. El concepto integra la seguridad informática, pero es más amplio, dado que los riesgos asociados a la información van más allá del medio informático, dado que pueden estar vinculados a las personas, o a otros soportes tradicionales.

Sistemas operativos: Un sistema operativo es un programa o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes. La mayoría de aparatos electrónicos que utilizan microprocesadores para funcionar, llevan incorporado un sistema operativo (teléfonos móviles, reproductores de DVD, ordenadores, radios, enrutadores, etc.). La actualización del sistema operativo permite disminuir la vulnerabilidad de los dispositivos electrónicos.

Herramientas de seguridad: Las herramientas de seguridad son el conjunto de productos concretos que se utilizan e implementan con el fin de minimizar las vulnerabilidades y amenazas que puedan sufrir los activos tecnológicos y de información (por ej: un antivirus, cortafuegos, filtros de contenidos, etc.). Las soluciones de seguridad integran dos tips de soluciones que son los productos de seguridad TIC y de otro los servicios de seguridad TIC. Las herramientas se asimilan a los productos, aunque también pueden ser utilizadas a la hora de prestar un determinado servicio.

Asesoramiento externo: Se entiende por asesoramiento externo el que haya podido recibir de una empresa o una persona externa a su organización con el fin de desarrollar alguna de las actuaciones propuestas. Generalmente, el asesoramiento externo estará relacionado con un contrato de prestación de servicios.

Política de seguridad TIC: La política de seguridad TIC de una organización constituye el marco de referencia que permite la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad asociados al uso de las TIC y la información de la organización. La política de seguridad TIC queda constituida por tanto como el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro, o acceso no autorizado. Generalmente se instrumenta a través de un plan de seguridad, o plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Igualmente, la política de seguridad se expresa en un documento que denota el compromiso de la dirección de la empresa con la seguridad de la información.

ISO 27001: la norma ISO/IEC 27001 es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el ciclo PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). La norma constituye la base del proceso de certificación de las organizaciones que han implementado su sistema de gestión de la seguridad de la información, de acuerdo con sus requerimientos.

Sistema de Gestión de la Seguridad de la Información: El Sistema de Gestión de Seguridad de la Información (SGSI) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que

constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Estrategia de Continuidad de Negocio: Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permita a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. La estrategia de continuidad de negocio da respuesta a estos incidentes que ponen en riesgo la actividad de las organizaciones. De esta forma, la estrategia permite garantizar que se puede dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de nuestra imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes de seguridad graves.

Análisis de riesgos: Se entiende el análisis de riesgos como el estudio que se realiza con el fin de identificar los activos críticos de los sistemas de información que dan soporte a los procesos de negocio de nuestra organización y las amenazas que puede comprometer su disponibilidad, integridad o confidencialidad. El análisis de riesgos es relevante dado que una vez identificados permite la gestión de esos riesgos, lo que supone establecer qué nivel de riesgo es asumible y cuál no. Ello permitirá definir un plan de tratamiento de riesgos que recoja qué acciones se van a realizar para controlar estos riesgos identificados durante el análisis.

Incidente de Seguridad: Un incidente de seguridad es un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones de la organización y de amenazar la seguridad de la información. Un evento de seguridad que implica una violación de seguridad. En otras palabras, un evento de seguridad en el cual la política de seguridad del sistema es desobedecida o violada.

Phishing: Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Pharming: Supone la suplantación de una página web. Consiste en la explotación de una vulnerabilidad, que permite a un atacante redirigir un nombre de dominio web, a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio, por ejemplo, el de un banco, que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio y no a la verdadera página, con las consecuencias que puede derivar para su seguridad.

Denegación de servicio DDos: la denegación de servicios DDos es un tipo de ataque intencionado. El intento exitoso de un ataque DoS/DDoS (Denegación de Servicio Distribuida) para afectar un servicio o sistema se puede conseguir a través del uso de vulnerabilidades presentes en la infraestructura o, más comúnmente, mediante el envío masivo de grandes cantidades de tráfico y/o peticiones. El resultado es que el sistema no es capaz de responder a las peticiones de servicio de los usuarios legítimos. Un caso muy típico es el de conectar repetidamente muchos ordenadores a una página web hasta saturarla y hacer que los usuarios de la página no puedan acceder a la misma.

Contraseña segura o robusta: Las contraseñas ofrecen la primera línea de defensa contra el acceso no autorizado a un equipo. Cuanto más segura sea la contraseña, más protegido estará el equipo contra hackers y software malintencionado. Una contraseña segura tiene ocho caracteres como mínimo; no contiene el nombre de usuario, el nombre real o el nombre de la empresa; no contiene una palabra completa y es significativamente diferente de otras contraseñas anteriores. Además, está compuesta por caracteres de cada una de las siguientes cuatro categorías: letras mayúsculas, letras minúsculas, números y símbolos del teclado.

Backup o copia de seguridad: Una copia de seguridad o de respaldo, también llamado "backup" (su nombre en inglés) es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos tales como: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica permitiendo su traslado a ubicaciones distintas de la de los datos originales.

Identificación mediante elementos biométricos: Es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autentificación, es decir, para verificar su identidad. Las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas, que se utilizan en procesos de identificación, aunque también se emplean otros elementos como la firma, el paso, o la propia voz que integran elementos físicos y de comportamiento.

Elementos hardware: La palabra hardware se refiere a todas las partes físicas de un sistema informático sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado. Por el contrario, el soporte lógico es intangible y se denomina software. En el ámbito de los procesos de identificación el uso de hardware estaría asociado a algún elemento físico como una tarjeta de identidad.

Productos anti fraude: Las herramientas anti-fraude están destinadas a proteger a los usuarios de ataques que utilizan prácticas denominadas de ingeniería social. Uno de los objetivos de la ingeniería social es conseguir, mediante engaños, datos de los usuarios (contraseñas, cuentas de correo…) para realizar con ellos actividades fraudulentas en internet. Estos ataques consisten, entre otros, en el robo de información personal y de datos bancarios y la suplantación de identidad, utilizando para ello técnicas como intentos de fraude bancario (phishing), redirección de páginas web (pharming), correo electrónico no deseado (spam) o malware diseñado al efecto.

Productos antivirus: Son herramientas destinadas a la protección de sistemas informáticos: servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, etc., frente a todo tipo de software malicioso que pueda afectarles (virus, troyanos, gusanos, spyware, etc.). El software malicioso o malware es una amenaza que utiliza múltiples técnicas y vías de entrada: páginas web, correo electrónico, mensajería instantánea, redes P2P, dispositivos de almacenamiento externos (memorias USB, discos duros externos, CDs, DVDs…), redes P2P, etc. y puertos abiertos en nuestro ordenador. Entre otras, estas vías, son utilizadas por el malware para infectar a los sistemas informáticos y propagarse por ellos, afectando de distintas formas al uso para el que están destinados (impidiendo acciones, vigilando usos, ralentizando sistemas, ejecutando acciones no permitidas…). Las herramientas anti-malware son de uso generalizado y las más antiguas que existen.

Herramientas de auditoría técnica y forense: Son herramientas destinadas a la realización de auditorías de sistemas, aplicaciones y datos, para determinar posibles fallos de seguridad o brechas que pudieran ser fuente de un incidente de seguridad y, por tanto, de un riesgo para los activos de una organización. Por tanto, de forma general, son herramientas de prevención. En esta categoría se incluyen las herramientas de auditoría forense que, a diferencia de las anteriores, están orientadas a determinar qué ocurrió y cómo se ocasionó un incidente de seguridad, una vez que éste ya ha tenido lugar. Por tanto, son herramientas de análisis posteriores a un incidente.

Sistemas de autenticación y certificación digital: Son productos destinados al uso y utilización de certificados digitales para aportar mayor seguridad a procesos, aplicaciones y sistemas. Estos productos permiten utilizar los certificados digitales en multitud de escenarios y situaciones diferentes. Por ejemplo, en la firma de documentos o en la autenticación en sistemas e instalaciones. Los certificados digitales se usan conjuntamente con las tarjetas inteligentes “smart cards”, en las cuales se pueden almacenar certificados digitales, y con dispositivos lectores de este tipo de tarjetas. El DNI electrónico, o DNIe, es un ejemplo de tarjeta inteligente que incluye certificados digitales para autenticación y firma.

Sistemas de gestión de accesos y control de identidades: Son productos destinados a dotar a las empresas y organizaciones de mecanismos que permitan: gestionar usuarios y sus datos de identificación; asociar roles, perfiles y políticas de seguridad; y controlar el acceso a los recursos. Suelen estar integrados con mecanismos de autenticación (véase "autenticación y certificación digital") que posibilitan el control del acceso lógico de los usuarios en los sistemas informáticos.

Herramientas de contingencia y continuidad: Son herramientas cuyo objetivo es facilitar el proceso de implantar planes de contingencia y continuidad en las organizaciones en todas sus fases. Por tanto, son herramientas que facilitan y posibilitan la gestión de los planes de contingencia y continuidad, desde su concepción y diseño hasta su implementación, pasando por su seguimiento, mejora continua y gestión de los incidentes que se puedan dar y que pondrán a prueba dichos planes. Entre estas herramientas, las de recuperación de sistemas, tras un incidente que afecta a la disponibilidad de la infraestructura TIC y las herramientas de copias de seguridad, son fundamentales para la implantación de planes de contingencia y continuidad en las organizaciones. La externalización se ha convertido en un elemento fundamental de este tipo de herramientas, como son las soluciones de copia de seguridad remota. Por otra parte, la virtualización está cobrando importancia a la hora la de conseguir reducir lo máximo posible los tiempos de despliegue y puesta en marcha de infraestructuras de respaldo, con el objetivo de reducir los tiempos de interrupción de la actividad.

Sistemas de control de contenidos confidenciales: Son herramientas que previenen la difusión, accidental o intencionada, de cualquier tipo de información o datos fuera de una organización. Evitan la fuga de información a través de correo electrónico, mensajería instantánea, transferencia de fi cheros mediante FTP, redes P2P, chats, blogs o mediante dispositivos externos de almacenamiento, como es el caso de las memorias USB. Actúan monitorizando todo tipo canales de comunicación, desde y hacia el exterior de la organización, evitando la fuga de información e implementando políticas de uso de información sensible. Se incluyen en estas herramientas aquellos sistemas que gestionan el ciclo de vida de información, controlando el uso autorizado de documentos electrónicos y facilitando la destrucción de los mismos cuando estén en desuso.

Sistemas de control de tráfico en la red: Son herramientas destinadas al control de la actividad de las infraestructuras de comunicaciones de una organización con distintos objetivos: cumplimiento de políticas de seguridad de la organización, seguridad perimetral y disponibilidad y uso adecuado de los recursos. Permiten controlar el tráfico generado y recibido mediante el empleo de sondas o sistemas que recolectan información en tiempo real de los elementos de la red, realizando también un análisis de los datos recogidos para detectar situaciones que están fuera de los parámetros normales de operación. Se realiza así un control sobre el uso del ancho de banda, los usuarios, el tipo de tráfico y del rendimiento en general. Son herramientas centradas en proteger la disponibilidad de las infraestructuras de comunicaciones de las organizaciones.

Cortafuegos: Son productos destinados a proteger los sistemas y dispositivos conectados a una red. Son herramientas que permiten establecer un perímetro de seguridad y garantizar las comunicaciones seguras para evitar accesos no autorizados y ataques provenientes de redes externas y de internet. Esta categoría agrupa a productos que aseguran que las comunicaciones hacia y desde la red, corporativa o doméstica, cumplen las políticas de seguridad establecidas. Para ello rastrean y controlan las comunicaciones, bloqueando el tráfico, detectando comportamientos anómalos y ataques y evitando intrusiones no autorizadas. También se integran en esta categoría las herramientas que permiten extender la red corporativa a entornos distantes (sedes remotas, oficinas) creando enlaces de comunicación seguros.

Sistemas de herramientas criptográficas: Son herramientas destinadas a proteger la confidencialidad de la información tanto en tránsito como almacenada. Permiten el cifrado y descifrado de la información mediante técnicas criptográficas, lo que impide un uso indebido de la misma por personas no autorizadas y permite el intercambio de la información de forma segura a través de medios o sistemas de comunicación inseguros, por ejemplo, a través de correo electrónico o transferencia de ficheros. Así mismo, no sólo protege la confidencialidad de la información, sino que además incorpora mecanismos para detectar modificaciones, cambios o manipulaciones durante su envío o almacenamiento. Por tanto, son herramientas que también protegen la integridad de la información.

Herramientas de seguridad en movilidad: Son herramientas destinadas a la protección de redes inalámbricas y dispositivos móviles o de dispositivos en movilidad (portátiles, PDA's, teléfonos inteligentes, etc.) de forma que se minimicen o reduzcan los incidentes de seguridad. Un ejemplo es la protección de los datos en caso de sustracción o la pérdida de dispositivos. Así mismo, son herramientas que protegen no solo a los dispositivos en movilidad, sino que además proporcionan protección y seguridad a aquellos dispositivos e infraestructuras a las cuales se conectan dichos dispositivos, proporcionando mecanismos de acceso y autenticación robustos, que posibilitan el uso de redes de comunicaciones desde cualquier localización o situación de forma segura. Algunas de estas herramientas disponen además de hardware adicional de autenticación, como lectores biométricos de huella digital, lectores de tarjeta, etc.

Redes Inalámbricas wifi: El término red inalámbrica (en inglés: wireless network) se utiliza para designar la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. La transmisión y la recepción se realizan a través de puertos. Una de sus principales ventajas es notable en los costos, ya que se elimina el cableado ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

Código Pin: El PIN, de las siglas en inglés, *Personal Identification Number* es un número de identificación personal utilizado en ciertos sistemas como el teléfono móvil o el cajero automático para identificarse y obtener acceso al sistema. El PIN es un tipo de contraseña. Sólo la persona beneficiaria del servicio conoce el PIN que le da acceso al mismo; esa es su finalidad. El PIN tiene que ser suficientemente seguro evitar la intrusión no autorizada al servicio que protege.

Bluetooth: Bluetooth es una especificación industrial para redes inalámbricas de área personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia. Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.

Formateado de disco: El formateado de disco es un conjunto de operaciones informáticas, independientes entre sí, físicas o lógicas, que permiten restablecer un disco duro, una memoria USB, una partición del disco duro o de la memoria USB o cualquier otro dispositivo de almacenamiento de datos a su estado original, u óptimo para ser reutilizado o reescrito con nueva información. Esta operación puede borrar, aunque no de forma definitiva, los datos contenidos en él.

Protocolo WPA y WPA2: Wi-Fi Protected Access, llamado también WPA (en español «Acceso Wi-Fi protegido») es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. Una vez finalizado el nuevo estándar 802.11ie se crea el WPA2 basado en este. De este modo, WPA2 es la versión certificada del estándar.

Protección WEP: WEP, es el acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. A partir de 2001, varias debilidades serias fueron identificadas por analistas criptográficos. Como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. Unos meses más tarde el IEEE creó la nueva corrección de seguridad 802.11i para neutralizar los problemas. Hacia 2003, la Wi-Fi Alliance anunció que WEP había sido reemplazado por Wi-Fi Protected Access (WPA). Finalmente en 2004, con la ratificación del estándar completo 802.11i (conocido como WPA2), el IEEE declaró que tanto WEP-40 como WEP-104 fueron revocados por presentar fallos en su propósito de ofrecer seguridad.

Servicios de auditoría técnica: Son servicios destinados a la realización de auditorías de seguridad de carácter técnico que permiten analizar y establecer el nivel real de seguridad de las distintas infraestructuras de soporte de la información y las comunicaciones en las

organizaciones. La información obtenida de estas auditorías es muy valiosa, pues permite detectar todo tipo de vulnerabilidades y posibles brechas en la seguridad de la organización. Con dicha información la organización está en una posición privilegiada para tomar decisiones desde el punto de vista de la seguridad y establecer los planes y acciones destinados a mejorar su nivel de seguridad. Además de los servicios de auditoría destinados a prevención, estableciendo los niveles reales de la infraestructura TIC de una organización, también se incluyen en esta categoría aquellos servicios destinados a la realización de auditorías posteriores a un evento o incidente de seguridad, para establecer las causas y las consecuencias reales del mismo. Por otro lado, también se incluyen en esta categoría de servicios los destinados a la actualización sistemática y automatizada de sistemas y aplicaciones, dirigida a la aplicación sistemática de parches y medidas para eliminar vulnerabilidades y fallos de seguridad.

Servicios de contingencia y continuidad de negocio: Son servicios destinados a la realización de acciones y gestiones encaminadas a la recuperación de la actividad del negocio en casos en que se produzcan incidentes de seguridad que afecten a la información y las tecnologías que los soportan, así como la continuidad de los mismos. Estos servicios persiguen reducir las consecuencias de un incidente de seguridad, incluso aquellos que ocasionen la interrupción de la actividad de la empresa con la consiguiente reducción de la incidencia en el negocio. Estos servicios facilitan la elaboración y aplicación de "Planes de contingencia y continuidad de Negocio" que permiten diseñar y activar alternativas en caso de incidentes a través de estrategias de recuperación y políticas de respaldo, de los distintos activos y recursos de la organización mediante la elaboración de procedimientos, identificación de activos, diseño de acciones y gestión de la información necesarios para realizar acciones de recuperación en respuesta a desastres de seguridad.

Servicios de cumplimiento de legislación: Son servicios que ayudan a las empresas a cumplir con la legislación vigente en materia de seguridad tecnológica o de seguridad de la información, como son la Ley Orgánica de Protección de Datos (LOPD), la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSICE), la Ley de Propiedad Intelectual (LPI) y otras. Mediante estos servicios se ofrece apoyo y guía a las organizaciones desde el diseño a la auditoría, pasando por la implantación de las medidas de tipo jurídico, técnico y organizativo que garantizan el cumplimiento de la legislación.

Externalización de servicios: seguridad gestionada, outsourcing: Son servicios que permiten a las empresas externalizar procesos, infraestructuras y personal de seguridad, de forma que sea una empresa especializada la que se encargue de dicha actividad de forma local o remota. La externalización de servicios de seguridad consiste en la subcontratación de actividades propias de seguridad o actividades que garantizan la seguridad de la información en las empresas. Normalmente la empresa descarga la responsabilidad de los servicios de seguridad a una empresa especializada la cual se encarga de garantizar la seguridad mediante contrato, y reportando a través de informes, logs (registros de actividad de los equipos) o paneles de monitorización y seguimiento.

Ataque informático, dirigido y/o modificación de sitios Web (Defacement): Se considera un ataque dirigido a aquel donde los individuos o la organización víctima están intencionadamente elegidos. Este tipo de ataques pueden incluir otras clases y tipos de ataques (spam con código dañino, Defacements, DoS, etc), pero dada su criticidad, deben considerarse como un tipo independiente si en la fase de clasificación se tienen indicios claros de que son dirigidos. La modificación de sitios web, también denominada en inglés defacement, consite en la explotación de vulnerabilidades con éxito en los sistemas de alojamiento (servidor web) o en las aplicaciones que permiten a un atacante modificar contenidos y páginas web. Estos ataques pueden involucrar la inserción de enlaces a sitios maliciosos y/o añadir contenidos que contienen el mensaje delatacante (políticos, difamatorios, etc).

Afectación por código dañino o malicioso: La afectación por código dañino puede ser un virus, gusano, caballo de troya, rootkit, script, etc. que infecta exitosamente a un sistema o conjunto de sistemas y en donde han fallado las medidas de detección y/o contención establecidas.

Abuso de privilegios y/o usos inadecuados: Esta tipología de incidentes se puede derivar de tres situaciones. En primer lugar, cuando un miembro de la propia organización realiza una violación del uso adecuado de los sistemas y redes de la organización. También se producen por infracciones de derechos de autor o piratería cuando se produce la copia o el uso indebido o no autorizado de material publicado, patentado o en general protegido por derechos de propiedad intelectual. Además, se puede producir el uso indebido de la marca cuando se hace uso de elementos identificativos (logos, imágenes, etc.) en cualquier intento fraudulento para adquirir información sensible, como usuarios, contraseñas o cualquier otra información personal que permitan al atacante hacerse pasar por la organización legítima víctima del incidente. Entrarían en esta categoría ataques de phishing en que la organización es la víctima en tanto que es su imagen la que se está siendo empleada para engañar a los usuarios. No se corresponderían a esta categoría ataques en que el usuario recibe mensajes de phishing de otras organizaciones (por ejemplo, bancos o redes sociales).

Ley Orgánica de Protección de Datos: El pilar de la legislación española sobre protección de datos es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). En virtud de esta ley y de la normativa que la desarrolla (principalmente, reglamento de desarrollo de la LOPD, aprobado por el RD 1720/2007, de 21 de diciembre), se imponen toda una serie de obligaciones tendentes a garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Las obligaciones previstas en la normativa sobre protección de datos recaen sobre las personas físicas o jurídicas, de naturaleza pública o privada, que efectivamente decidan sobre la finalidad, contenido y uso del tratamiento de datos personales. Las empresas, en su calidad de responsables de tratamiento, están incluidas en el ámbito de aplicación de la ley.

Documento de seguridad: El art. 88 del RDLOPD establece la necesidad de disponer de un documento de seguridad que recoja las medidas técnicas y organizativas que rijan la actuación del personal con acceso a los sistemas de información. Los apartados 3 y 4 detallan los aspectos que se deben contemplar en el documento de seguridad que, en cualquier caso, es un documento interno de la organización, que debe mantenerse actualizado en todo momento, y ser revisado siempre que se produzcan cambios relevantes. El documento de seguridad es exigible con independencia del soporte de los ficheros (automatizados y no automatizados) y para cualquier nivel de seguridad (aunque para los ficheros de nivel medio y alto el documento debe cumplir requisitos adicionales, previstos en el art. 88.4 RDLOPD).

Requerimiento de información sobre la existencia de datos personales: El art. 5 de la LOPD regula el deber de información al afectado, previo al tratamiento de sus datos de carácter personal. Así, contempla que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de los siguientes aspectos:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición (ARCO)
- De la identidad y dirección del responsable del tratamiento o de su representante.

En cumplimiento de esta obligación, los responsables de ficheros deben incluir una cláusula informativa en el propio impreso de captación de datos, en formularios de Internet, mediante carteles informativos, mediante una alocución telefónica, etc.

Requerimiento de consentimiento expreso para el tratamiento de datos personales: El art. 6 de la LOPD establece la normativa para recabar el consentimiento de los afectados en el tratamiento de sus datos de carácter personal: “el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa”. ¿Qué se debe entender por consentimiento del interesado? El art. 3 h) es claro en su definición: “toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le

conciernen". Por tanto, el consentimiento debe cumplir estos cuatro requisitos para ser considerado válido. Cuando el tratamiento en cuestión afecta a datos especialmente protegidos, el consentimiento debe ser expreso y, en ciertos casos, por escrito.

Derecho de acceso rectificación, cancelación y oposición sobre datos personales: La LOPD reconoce los derechos de los titulares de los datos a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales (arts. 15-17 LOPD). Los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) son detallados en el RDLOPD, que establece que deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos ARCO (art. 24.2 RDLOPD). Las empresas que traten derechos personales, por tanto, deberán atender las solicitudes de acceso, rectificación, cancelación y oposición de los titulares de los datos, de manera gratuita, y dentro de los plazos previstos legalmente.

- Derecho de acceso: el interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
- Derecho de rectificación: derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales, en el caso de que éstos sean inexactos o incompletos.
- Derecho de cancelación: ofrece al interesado la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.
- Derecho de oposición: el interesado puede oponerse, mediante su simple solicitud, a que sus datos sean tratados con fines de publicidad y de prospección comercial.

Vulnerabilidades: Se denominan vulnerabilidades a los errores de software. Son defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. También se aplica a los activos tecnológicos y de información en general de forma que representan los elementos de estos activos que mantienen problemas de seguridad.

Macro datos o datos masivos: Del inglés big data, es un concepto que hace referencia al almacenamiento de grandes cantidades de datos y a los procedimientos usados para encontrar patrones repetitivos dentro de esos datos. El fenómeno del Big Data también es llamado datos a gran escala, y supone la reutilización de dichos datos obtenidos desde distintas fuentes en procesos que pueden tener fines de investigación social, o de carácter comercial.

INDICE DE GRÁFICOS

INDICE DE TABLAS