



# VI ESTUDIO DEL ESTADO DE LA SEGURIDAD EN LA NUBE

Una iniciativa de:



En colaboración:



## **Copyright**

Todos los derechos reservados. Puede descargar, almacenar, utilizar o imprimir el presente Estudio de Cloud Security Alliance España, Cloud Security Alliance Perú, Cloud Security Alliance Argentina, ISACA-Madrid, Cloud Security Alliance Chile, Cloud Security Alliance Bolivia, Cloud Security Alliance Brasil, Cloud Security Alliance Colombia e ISMS Forum Spain, atendiendo a las siguientes condiciones: (a) el Estudio no puede ser utilizado con fines comerciales; (b) en ningún caso el Estudio puede ser modificado o alterado en ninguna de sus partes; (c) el Estudio no puede ser publicado sin consentimiento; y (d) el copyright no puede ser eliminado del mismo.

# 6º ESTUDIO DEL ESTADO DE LA SEGURIDAD EN LA NUBE

## **Con la participación de los siguientes profesionales y organizaciones:**

### **Coordinadores**

Mariano J. Benito (GMV), CSA-España  
Gerardo Guzman (Banco de Crédito BCP), CSA-Perú  
Luciano Moreira (Vice Presidente), CSA-Argentina  
Erik De Pablo (Director Investigación), ISACA-Madrid  
Abdel Aliaga (Presidente), CSA-Bolivia  
Ricardo Urbina (Presidente), CSA-Chile  
Leonardo Goldim (Presidente); CSA-Brasil  
Isabel Yepes (Evangelista), CSA-Colombia

### **Analistas**

Alfredo Alva (Banco Comercio Perú), CSA-PE  
Josep Bardalló (SVT-Cloud), CSA-ES  
Alberto Bernaldez (Liberty Seguros), CSA-ES  
Walter Cabanillas (Independiente), CSA- PE  
Manuel Caldas (Telefonica), CSA-PE  
Vicente Campayo (Eurocaja Rural), CSA-ES  
Fernando Carrillo (AirOn Group), CSA-PE  
Aldo Carlessi (Atmosfera), CSA-PE  
Concepción Cordón (EMASA), CSA-ES  
Omar Crespo (Mibanco), CSA-PE  
Richard Croce (Gildemeister), CSA-PE  
Carlos Cruzado (tgestiona), CSA-PE  
Antonio Fernandes (FINSAs), CSA-ES  
Juan Garcia Galera (CEMI – Ayto. Málaga), CSA-ES  
Alfonso Gómez (Banco de España), CSA-ES  
Ángel Heredia (Eulen), CSA-ES  
Christian Ibiri (Cloud Legion), CSA-AR  
Julio Peñas (Independiente), CSA-ES  
Susana Rey Baldomir (ISMS Forum), CSA-ES,  
Jorge Antonio Rojas (Independiente), CSA-PE  
Martin Vega (Red Científica Peruana), CSA-PE  
Rafael Vasquez (Banco Crédito Perú), CSA-PE

# ÍNDICE

<b>I. Resumen ejecutivo</b>	<b>6</b>
<b>II. Objetivos y Ámbito del Estudio</b>	<b>8</b>
<b>III. Análisis de Expectativas de los Usuarios de la Nube</b>	<b>10</b>
<b>IV. Requisitos Exigidos por los Usuarios de la Nube</b>	<b>13</b>
<b>V. Valoración por los Usuarios de su Satisfacción con los Servicios en la Nube</b>	<b>17</b>
<b>VI. Evolución Expectativas vs Requisitos vs Resultados</b>	<b>21</b>
<b>VII. Visión sobre Shadow IT</b>	<b>23</b>
<b>VIII. Estado de Concienciación en Seguridad de los Usuarios</b>	<b>28</b>
<b>IX. Evolución de Incidentes de Seguridad en Servicios en Nube</b>	<b>31</b>
<b>X. Resolución de Conflictos entre cliente y usuario de servicios</b>	<b>37</b>
<b>XI. Soporte para IoT en Servicios en la Nube</b>	<b>39</b>
<b>XII. Comentarios particulares para el caso de España, CSA-ES</b>	<b>41</b>
<b>XIII. Ficha Técnica del Estudio</b>	<b>43</b>

# RESUMEN EJECUTIVO

Con la presentación de esta 6ª edición, el Estudio del Estado del Arte de Seguridad en la Nube pone a disposición de las entidades interesadas en la seguridad en la Nube una perspectiva histórica singular para entender los factores que están facilitando o dificultando la evolución de los modelos de computación hacia este escenario, y la evolución de dichos factores.

Así, el estudio ya identifica consistentemente varios factores a lo largo del tiempo: constantes y muy altas expectativas de los clientes sobre la Seguridad que les va a ofrecer la Nube; acompañadas de una exigencia de requisitos de seguridad más que altos, en particular en requisitos técnicos y cada vez más de cumplimiento y privacidad; y que resultan en una satisfacción creciente pero aún insuficiente con la seguridad de los servicios de Nube recibidos.

Otra de las tendencias que el estudio refrenda es que las empresas de menor tamaño se benefician más de la Nube: Se declaran más satisfechas; hacen más eficiente la detección, gestión y respuesta a incidentes; y permiten eliminar problemas de ShadowIT.

Precisamente ShadowIT es aún un asunto candente. El estudio detecta una polarización cada vez más acusada entre organizaciones que tienen una visión neutra o positiva que tolera y hasta fomentan ShadowIT; y organizaciones con una visión negativa y que en consecuencia va poniendo límites a este paradigma dando más peso a sus propios servicios de TI.

Además, esta edición del estudio ha identificado algunos hallazgos novedosos y relevantes. En algunos casos, se trata de nuevas informaciones y visiones sobre puntos ya analizado. Por ejemplo, la concienciación en seguridad en la Nube crece en sus usuarios, tanto a nivel de directivos como de empleados y ya se puede calificar como "Alta". Y se ha identificado que los muchos proveedores de Nube tienen planificado como manejar recursos adicionales para sus clientes que pudieran ser necesarios durante un incidente de seguridad.

En su constante evolución, el 6º estudio se ha fijado por primera vez en IoT y cómo las organizaciones están diseñando y/o soportando estos servicios, y el rol que desempeña la Nube en este esquema. Un rol sin duda destacado, en tanto que mayor parte de las empresas que están desplegando servicios IoT se están apoyando en la Nube, y en particular en Nubes Públicas o en Nubes Privadas.

El Estudio también analiza por primera vez como se facturan servicios de Nube consumidos, y la forma en la que usuarios y proveedores pueden conciliar sus diferencias en el punto, para encontrar que hay tanto mecanismos como voluntad para utilizarlos, de ser preciso.

El 6º Estudio del Estado del Arte de Seguridad en la Nube se ha realizado en 2018 en cooperación entre los capítulos Español, Peruano, Argentino, Chileno, Boliviano, Brasileño y Colombiano de Cloud Security Alliance, y el capítulo de Madrid de ISACA, continúa la serie de estudios realizados en 2013, 2014, 2015, 2016 y 2017. El equipo de analistas que ha preparado desea y confía en que este Estudio y sus contenidos sean de utilidad para sus lectores.



# OBJETIVOS Y ÁMBITOS DE ESTUDIO

El objetivo del presente estudio continúa la serie de estudios sobre el Estado del Arte en la Seguridad de los Servicios en la Nube que vienen desarrollando desde el año 2013, y busca investigar y conocer el Estado del Arte de la adopción de servicios en la Nube, y el papel que juega la seguridad en la adopción de estos servicios. Todo ello, desde el punto de vista de los Usuarios de Servicios en la Nube.

Para ello, este 6º Estudio del Estado del Arte de Seguridad en la Nube trabaja en un triple eje:

- En primer lugar, continúa con varias de las líneas de investigación básicas sostenidas a lo largo de los estudios, que buscan identificar cuáles son las expectativas de los usuarios de los servicios en la Nube, en qué requisitos concretos se traducen estas expectativas, y qué tanto satisfechos están los usuarios con los servicios recibidos de su CSP. También se incluyen aspectos relativos a los servicios más reclamados desde la Nube y los modelos de prestación de servicios desde la Nube preferidos. Por otra parte, en esta edición se discontinúan las investigaciones realizadas sobre certificaciones de seguridad en la Nube, ya sean de las organizaciones o de su personal.
- En segundo lugar, se continúan investigando aspectos relacionado con la prestación de servicios desde la Nube y su seguridad, ya analizados en estudios anteriores. Entre estos aspectos, se incluyen el Shadow IT, la gestión de Incidentes y la concienciación en seguridad de personas y organizaciones sobre el uso de la Nube.
- Por último, el estudio incluye dos nuevos elementos de estudio asociados al uso de la Nube por clientes más maduros. Estos aspectos son el uso de "IoT desde la Nube" y el "brokering y tarificación de los CSP", junto con un seguimiento de temas de importancia para el uso seguro de los servicios en la nube ya abordados en estudios anteriores; expectativas y satisfacción con los servicios.



Este análisis se realiza tanto para la situación existente a la realización del mismo, como desde un punto de vista histórico dado que el Estudio se ha realizado en 2013 , 2014 , 2015 , 2016 y 2017, que incluyeron España (todos los estudios), Perú (desde 2015), Argentina (desde 2016) y Chile, Colombia, Bolivia y Brasil (desde 2017).

El estudio centra su campo de estudio en los mercados hispanohablantes en los países cuyo capítulo local de Cloud Security Alliance ha participado. Y ha contado con analistas de los Capítulos de CSA señalados, junto con el capítulo de ISACA en Madrid.

El Estudio se basa en la información recogida exclusivamente por organizaciones usuarias de estos servicios, sin que se haya contactado con empresas proveedoras de servicios en la Nube (CSP, de Cloud Service Providers).

---

1 En español: (<https://www.ismsforum.es/ficheros/descargas/estudio-del-estado-de-la-seguridad-en-cloud.pdf>). En inglés: (<https://www.ismsforum.es/ficheros/descargas/csa-es-2013cloudsecuritystateoftheart1386576745.pdf>).

2 En inglés: (<http://www.ismsforum.es/ficheros/descargas/csa-en-2014-cloudsecuritystateoftheart20141119.pdf>). En español: (<https://www.ismsforum.es/ficheros/descargas/csa-es-2014-cloudsecuritystateoftheart20141119.pdf>)

3 (<https://www.ismsforum.es/ficheros/descargas/csa-es-pe-2015-estudio-estadodelarte-nube-es.pdf>) y ([https://csacongress.org/wp-content/uploads/2015/11/csa-congress-emea-2015\\_-\\_Spanish-and-Peruvian.pdf](https://csacongress.org/wp-content/uploads/2015/11/csa-congress-emea-2015_-_Spanish-and-Peruvian.pdf))

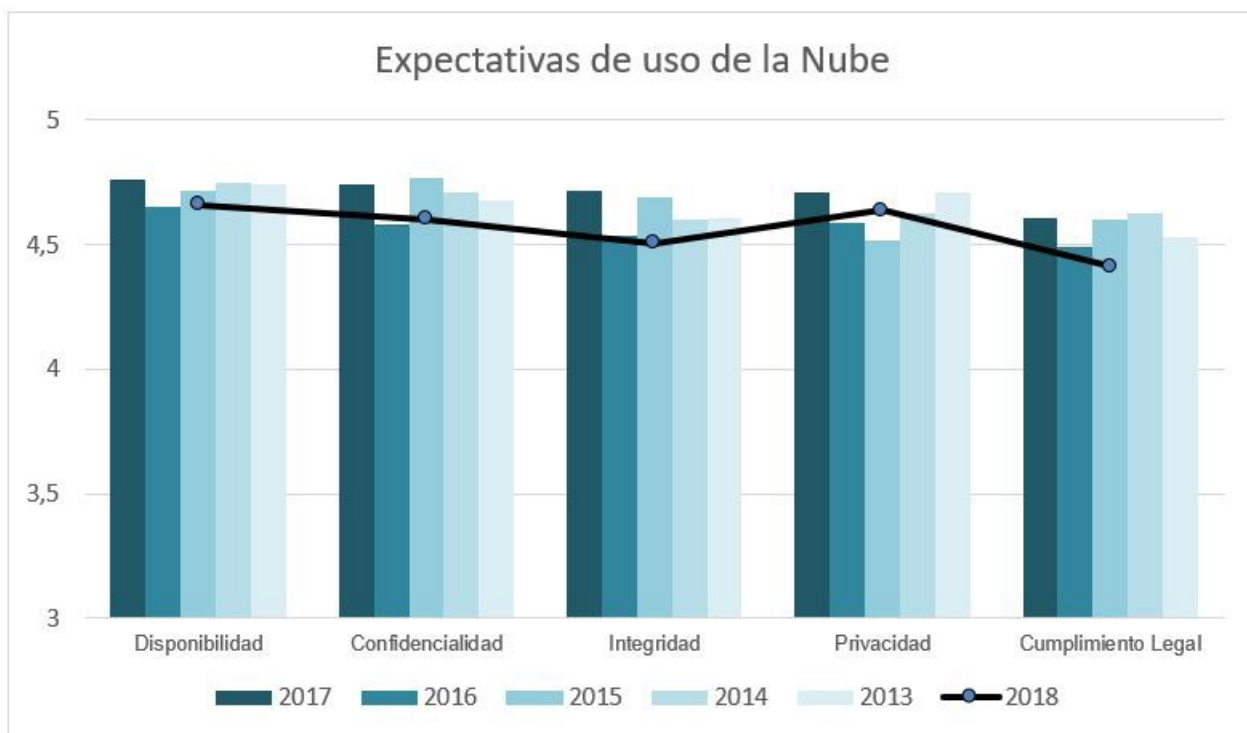
4 (<http://www.ismsforum.es/ficheros/descargas/iv-cloudsecurity-sota-2016-csa-es-pe-ar-isaca-mad.pdf>). En inglés (<https://csacongress.org/wp-content/uploads/2016/11/Mariano-Benito-Cloud-Computing-State-of-the-Art-Analysis.pdf>)

5 (<https://www.ismsforum.es/ficheros/descargas/v-estado-del-arte1511800752.pdf>)

# Análisis de Expectativas de los Usuarios de la Nube

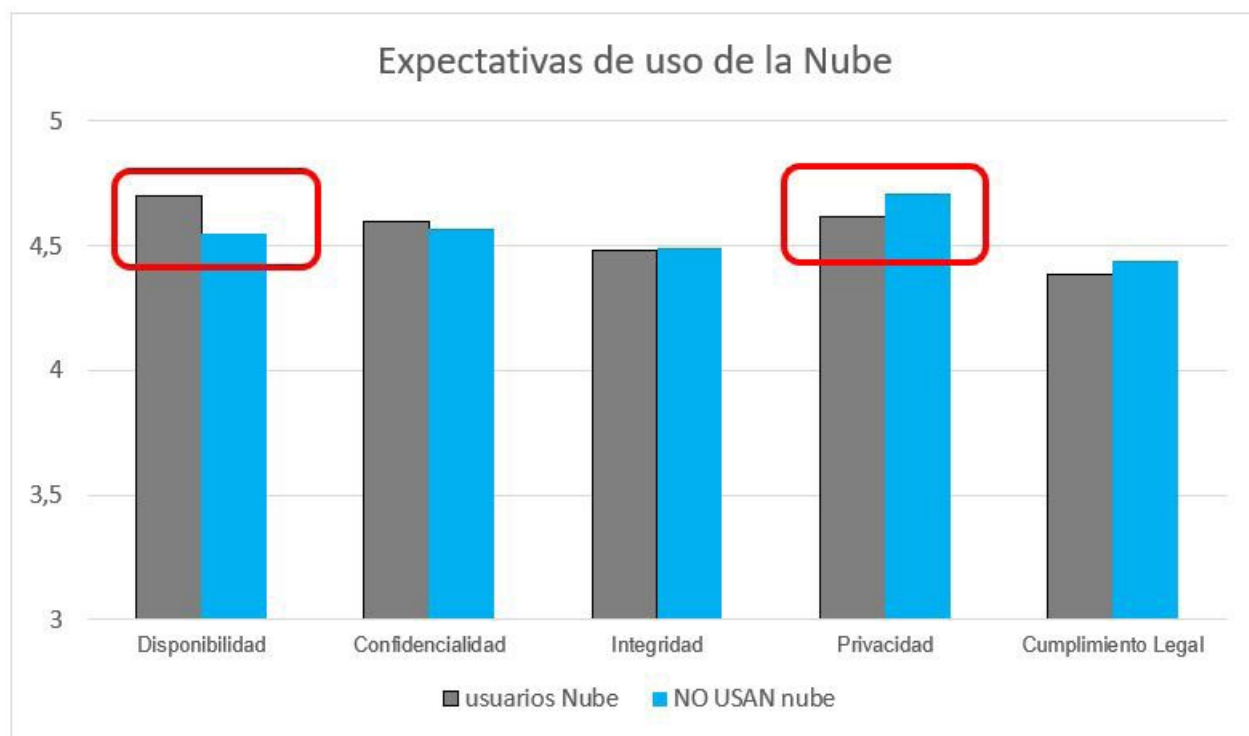
Este bloque del Estudio se centra en analizar qué expectativas generales tienen los usuarios (reales o potenciales) de servicios en la Nube. Estas expectativas no tienen por qué traducirse en requisitos o acciones específicas.

El análisis global del total de datos recopilados muestra un retroceso generalizado en todos los parámetros analizados frente a los valores del estudio de 2017. Sin embargo, el retroceso no es demasiado significativo, ya que se trata de variaciones porcentualmente bajas y a que los resultados identificado siguen correspondiendo con la expectativa de los usuarios de Servicios en la Nube de que estos servicios se presten en condiciones de muy alta confidencialidad, disponibilidad, integridad y disponibilidad, y ligeramente menor de cumplimiento legal por parte de estos servicios. De hecho, solo dos de los valores (integridad y cumplimiento legal) se encuentran en valores mínimos históricos, aunque por muy escaso margen.



Conclusión: Los usuarios siguen teniendo expectativas muy altas respecto de las condiciones de confidencialidad, disponibilidad, integridad, privacidad y cumplimiento legal en las que se prestan los servicios en la Nube

El estudio ha encontrado conclusiones interesantes también cuando analiza las diferencias en expectativas entre los participantes en el estudio que se declaran usuarios de servicios en la Nube frente a los que no se declaran como tales. En particular, las diferencias son apreciables en la valoración del parámetro "Disponibilidad", en el que los usuarios de Nube tienen una mayor exigencia, frente al parámetro "Privacidad", en el que los usuarios de Nube actúan de forma más relajada que los no usuarios. Estos datos apuntan al efecto que tienen las compañías a adoptar los servicios de Nube, que hacen que aquellas compañías que priman la prestación de servicios en todo momento sean más susceptibles de contratar servicios en la Nube para mejor garantizar la continuidad de prestación de los mismos. Por el contrario, las organizaciones que no contratan servicios en la Nube declaran una mayor preocupación por los requisitos de privacidad de estos servicios, y probablemente consideren que los proveedores de servicios en la Nube no satisfacen suficientemente estas expectativas.



Conclusión: los usuarios de servicios en la Nube tienen mayores expectativas respecto de la disponibilidad de los servicios, frente a los NO usuarios de servicios en la Nube, que están más preocupados por las condiciones de privacidad de los servicios.

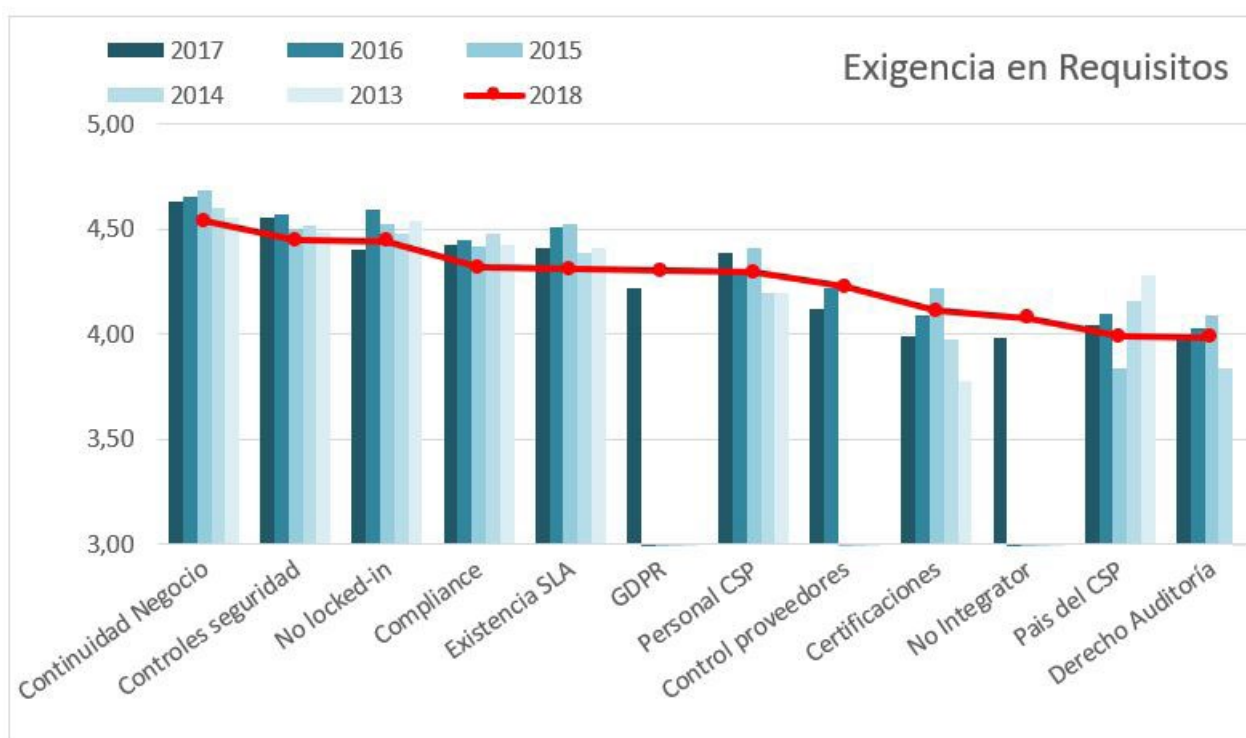
En conclusión, se mantiene la expectativa de muy altas garantías de seguridad en la prestación de servicios en la Nube.

# Requisitos Exigidos por los Usuarios de la Nube

## IV

En la práctica, las organizaciones que desean contratar servicios en la Nube deben ser capaces de trasladar sus expectativas sobre estos servicios a la exigencia de requisitos de servicio concretos. Así y por un lado, los proveedores de servicios en la Nube pueden ofrecer servicios y características de los mismos alineadas con las expectativas de sus usuarios; y por otro lado, los usuarios de servicios pueden efectivamente priorizar sus expectativas declarando algunas de ellas como críticas, y postergando o renunciando a otras características que pudieran ser deseable, pero que resultan complejas o más caras de conseguir. O que simplemente, sería bueno que se tuvieran.

Por ello, el estudio analiza la exigencia efectiva de los usuarios a los proveedores de servicios en la Nube de características concretas de seguridad que deberían estar presentes en los servicios en la Nube que se reciben. O que pudieran recibirse de forma complementaria o no agregada del propio servicio.



En primer lugar, debe resaltarse la estabilidad de los requisitos exigidos a los proveedores de los servicios en la Nube. Los resultados obtenidos en este 6º estudio son cercanos a los obtenidos en años anteriores, tanto en valor como en relevancia entre los mismos. De hecho, el promedio de la valoración de los requisitos apenas varía en este estudio (4,25) frente a los de años anteriores (4,26), es decir, el nivel de exigencia de los clientes a sus proveedores de servicios en la Nube es algo mayor que Alto.

El análisis particularizado de la exigencia de los distintos requisitos ofrece varias conclusiones interesantes.

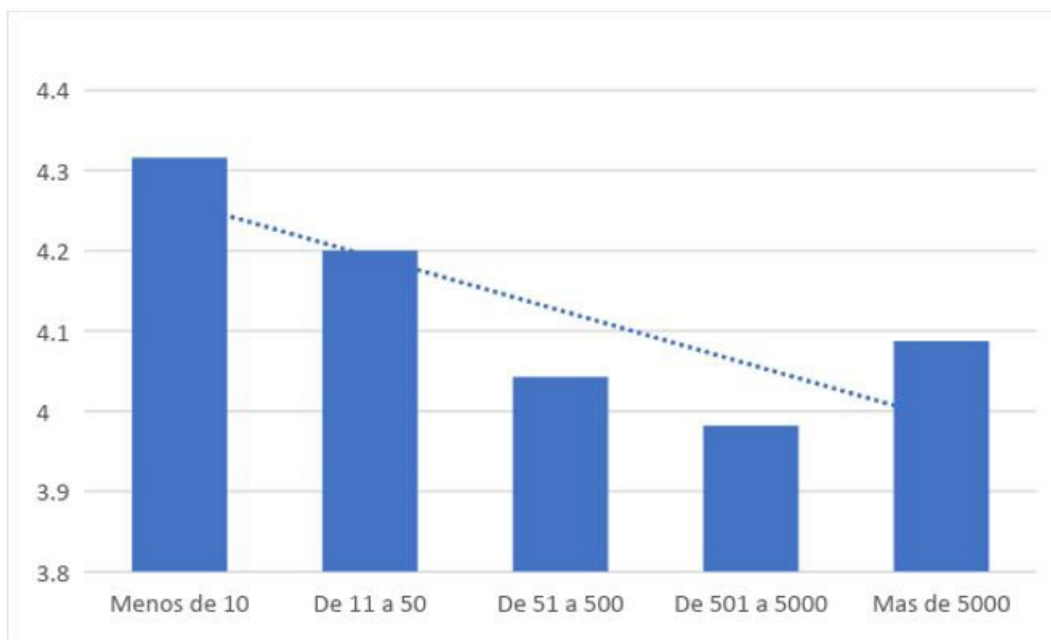
En primer lugar, los requisitos de mayor exigencia siguen siendo fundamentalmente técnicos: Controles de seguridad implantados y garantías de continuidad de negocio por el proveedor de servicios en la Nube. Junto a ellos, los usuarios valoran la libertad de selección de proveedor de servicios en la Nube y rechazan no poder cambiar (efecto locked-in). Mientras, los requisitos de menor exigencia siguen siendo la ubicación del proveedor y el derecho de auditoría sobre el proveedor de servicios en la Nube.

Conclusión: Los requisitos exigidos con más intensidad siguen siendo requisitos con un fuerte componente técnico: continuidad de negocio, controles de seguridad, locked-in.

En segundo lugar, se reducen las diferencias entre la intensidad con que se exigen los diversos requisitos, en tanto que baja el nivel de exigencia para los controles de mayor exigencia que se señalaban en el párrafo anterior, mientras que sube el nivel de exigencia los controles relacionados con otros proveedores externos que participan en el servicio en la Nube, tales como integradores de servicios en la Nube, o los proveedores del proveedor. Un análisis más detallado revela que esta tendencia es similar en todas las geografías y para todos los tamaños de empresas y de sectores. Lo que apunta a que las organizaciones reconocen cada vez con más intensidad que la provisión de servicios en la Nube no es sólo una relación bilateral entre cliente y proveedor de servicios en la Nube, y que hay más actores en la misma que deben ser considerados.

En tercer lugar, al analizar la exigencia de requisitos de certificación en función del tamaño del usuario de servicios en la Nube, se detecta que el cumplimiento de este requisito es más valorado por organizaciones de menor tamaño. Este análisis refuerza el papel de las certificaciones como generadores de confianza y facilitadores del establecimiento de relaciones entre varias organizaciones. Como acabamos de señalar en el punto anterior, este es crecientemente el caso en la provisión de servicios en la Nube.

Nivel de exigencia de certificaciones en la Nube según el tamaño de la organización



Conclusión: se reconoce crecientemente el papel e importancia de los proveedores e intermediarios entre clientes y proveedores servicios en la Nube. Y con más intensidad cuando el cliente es una organización de menor tamaño.

Merece también un análisis la exigencia en cumplimiento de directivas de privacidad, que figuran como requisito "GDPR". Este aspecto era considerado con particular intensidad por el equipo de analistas por la entrada en vigor en 2018 de varias regulaciones en la materia (GDPR en Europa, LPDP en Argentina), muy similares en su orientación y requisitos. Y que, al menos en GDPR, pueden establecer requisitos globales para todos los participantes en la prestación de servicios en la Nube.

El análisis de los resultados obtenidos arroja como primera conclusión una subida en el nivel de exigencia de este requisito, posicionándolo en el escalón de los segundos requisitos más exigidos por el cliente y a la altura del cumplimiento del SLA o el cumplimiento legal en general. Este crecimiento en la exigencia parece razonable, y en particular, el alineamiento del cumplimiento de regulaciones de privacidad con el cumplimiento legal en general.

Sin embargo, este alineamiento en la exigencia en los requisitos no es completo. En particular con la exigencia de los requisitos de "Ubicación geográfica del proveedor" y "Derecho de auditoría del cliente", en tanto que son dos aspectos frecuentemente señalados de obligado cumplimiento en las regulaciones en privacidad. Estos dos requisitos son los que menos exigen los usuarios de servicios en la Nube a sus proveedores, quedando a punto de llegar a nivel Alto. Respecto de la "Ubicación geográfica del proveedor", la exigencia menor puede explicarse por el trabajo sostenido por los proveedores de servicios en la Nube globales para prestar servicios desde un número creciente de áreas geográficas locales, para el aseguramiento del cumplimiento regulatorio global con independencia de la ubicación geográfica desde la que preste el servicio, y por la existencia de proveedores locales o con presencia local en las distintas geografías, que simplifica el cumplimiento ligado a ubicación geográfica. Pero no se ha identificado por este equipo de analistas ninguna explicación plausible para la limitada exigencia sobre el derecho a auditoría.

Por último, el equipo de analistas ha analizado las variaciones en la exigencia del requisito GDPR en función de la ubicación geográfica de los usuarios de servicios en la Nube. No se han encontrado variaciones significativas entre las distintas geografías, tanto en aquellas directamente afectadas por las nuevas regulaciones de privacidad, como en aquellas que no han tenido cambios legislativos en 2018. Este resultado puede ser inicialmente sorprendente, puesto que cabría esperar una relación más directa entre la existencia de regulaciones en la materia con la exigencia del requisito, aspecto ya detectado en la edición de 2017 de este Estudio. Pero en opinión del equipo de analistas, este resultado demuestra que la necesidad de privacidad ya estaba establecida en las organizaciones con anterioridad a estas nuevas regulaciones, y que la publicación de las nuevas regulaciones junto con la incansable repetición en el mercado de mensajes de aseguramiento de su cumplimiento ha terminado de propagar y establecer como materia el requisito de cumplimiento en privacidad. En todas las geografías indistintamente. Aunque (como se señalaba para la exigencia del requisito de derecho de auditoría) aún no se sea plenamente consciente de qué supone este cumplimiento.

Conclusión: la exigencia de cumplimiento en privacidad (GPDR, LPDP, LPVP, LODP y otras) ya está al nivel del cumplimiento legal en otras materias, y en todas las geografías.



# Valoración por los Usuarios de su Satisfacción con los Servicios en la Nube

# V

Frente a ediciones anteriores de este Estudio del Estado del Arte, esta 6ª edición ha realizado un esfuerzo de simplificación de los objetivos analizados respecto de la satisfacción de los clientes de servicios en la Nube, concentrando la evaluación de satisfacción únicamente en cuatro parámetros, frente a los hasta 8 de ediciones anteriores.

Los resultados obtenidos revelan una mejora sustancial en la satisfacción de los usuarios de los servicios. Todos los parámetros analizados llegan a su máximo histórico de la serie, y en el caso concreto de la satisfacción con el cumplimiento legal, podría calificarse de cambio de tendencia. Con esta mejora, y por primera vez en la serie de estudios, la satisfacción de los usuarios con los servicios en la Nube que recibe puede calificarse como "Alta".



# VALORACIÓN POR LOS USUARIOS DE SU SATISFACCIÓN CON LOS SERVICIOS EN LA NUBE

El análisis detallado de los datos de mejora revela una satisfacción generalizada en todos los aspectos analizados. No es una mejora específica de ciertas tipologías de usuarios mientras que otras siguen estando satisfechas a los niveles detectados en ediciones anteriores del estudio: todas ellas suben.

Conclusión: la satisfacción de los usuarios con los servicios en la Nube puede calificarse como "Alta" por primera vez en esta serie de estudios. Siendo una valoración consistentemente "Alta" para todos los tipos de usuarios de la Nube.

Al analizar de forma segmentada la satisfacción por cada tipo de usuario, pueden identificarse algunas tendencias interesantes.

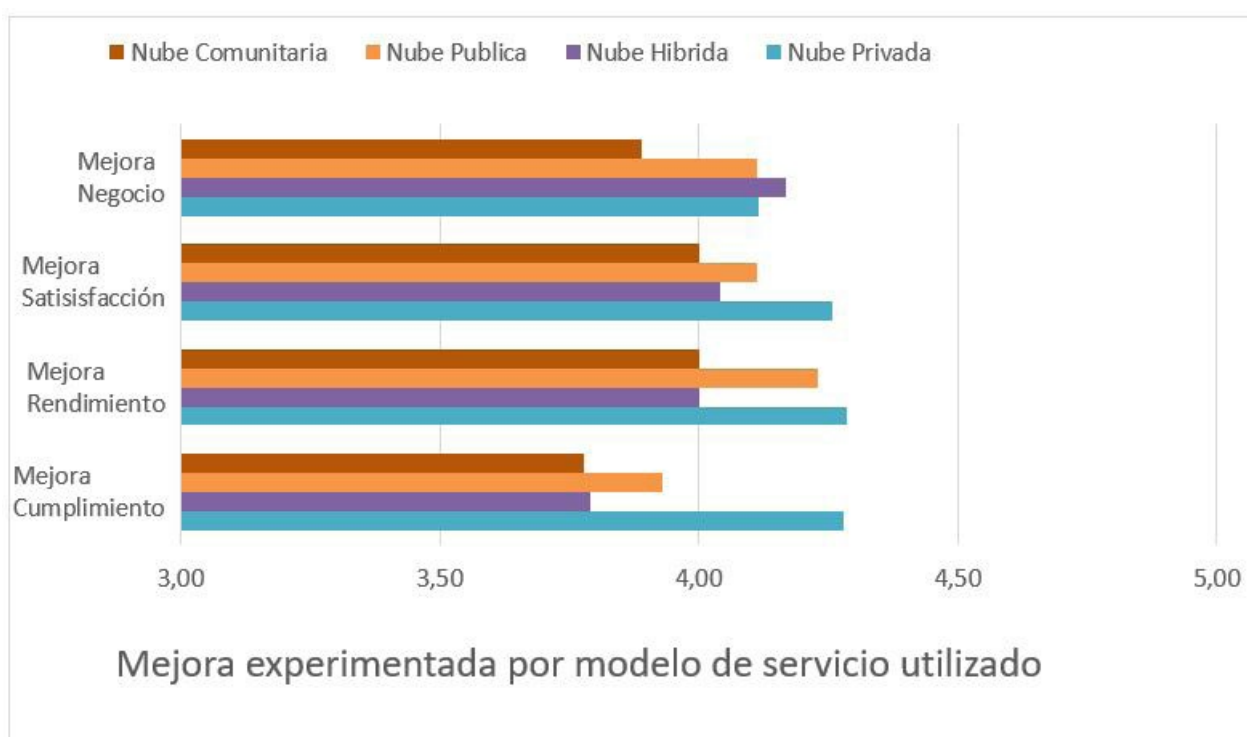
Respecto del tipo de servicios consumidos desde la Nube, cabe destacar que la mejora en cumplimiento legal es consistentemente más baja que en otros campos. Y por otra parte, los usuarios se declaran más satisfechos con los servicios en la Nube más flexible, sobre los que pueden ejercer más acciones de control y configuración (IaaS y PaaS), mientras que su satisfacción con los servicios SaaS es consistentemente más baja. Y por ello no deber ser sorprendente que la satisfacción con el cumplimiento en servicios SaaS sea la más baja de todas ellas.



# VALORACIÓN POR LOS USUARIOS DE SU SATISFACCIÓN CON LOS SERVICIOS EN LA NUBE

Al repetir el análisis frente al modelo de Nube utilizado por los usuarios, los resultados son consistentes: los servicios más flexibles resultan más satisfactorios. En este caso, esto se refleja en una satisfacción ampliamente mayor sobre las nubes privada, siendo la Nube pública pura la segunda mejor opción.

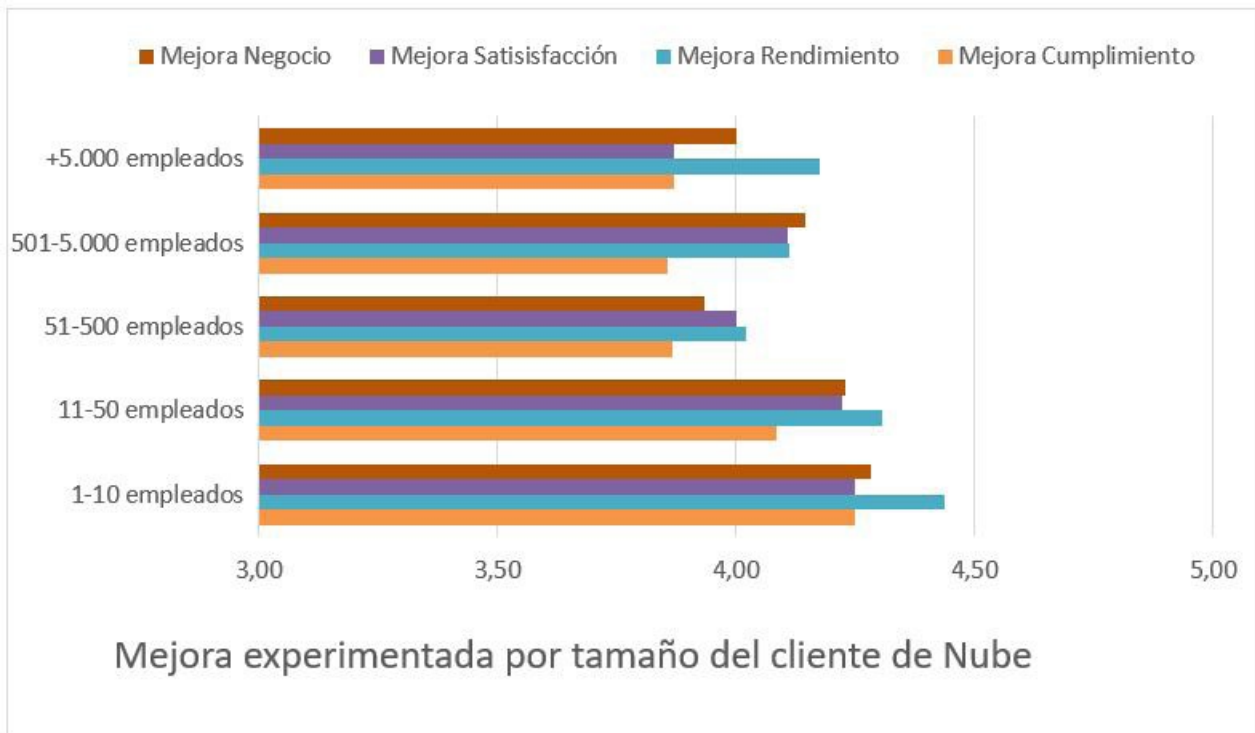
Y también en esta línea, la satisfacción con el cumplimiento legal en la Nube resulta menor, con una excepción muy notable: Los usuarios de Nube privada están muy satisfechos con el nivel de cumplimiento legal que obtienen en sus Nubes Privadas.



Conclusión: los usuarios se declaran más satisfechos con los servicios de Nube estándar y simples de manejar sin sacrificar la capacidad de control y configuración del mismo: IaaS/PaaS y Nube Privada son las opciones más satisfactorias.

Al analizar la satisfacción en función del tamaño de compañía, puede observarse un efecto ya señalado respecto de las expectativas sobre los servicios en la Nube: las organizaciones de menor tamaño se benefician particularmente de los servicios en la Nube, mientras que las organizaciones de tamaño intermedio se declaran como menos satisfechas, y las organizaciones de mayor tamaño están en un punto intermedio de satisfacción.

# VALORACIÓN POR LOS USUARIOS DE SU SATISFACCIÓN CON LOS SERVICIOS EN LA NUBE



Finalmente, en un análisis por ubicación geográfica de los clientes de servicios de Nube, puede apreciarse que la satisfacción de los clientes en España y en Europa es menor que la de los clientes en LATAM. Y en todos los casos, señalando al cumplimiento legal como el área menos satisfactoria de todas las analizadas.

Conclusión: La satisfacción de los clientes con el cumplimiento legal en la Nube mejora, pero aún queda camino de mejora.

Conclusión: Los clientes de menor tamaño y con menores recursos propios perciben mayores beneficios del uso de la Nube.

# Evolución Expectativas vs Requisitos vs Resultados

## VI

La comparación entre las expectativas que tienen los usuarios de los servicios en la Nube, frente a los requisitos que efectivamente solicitan de estos servicios y la satisfacción con los servicios que finalmente reciben comienza a experimentar una esperable convergencia. Fundamentalmente, por la mejora con la satisfacción experimentada. Pero también por la reducción en las expectativas de los clientes.

En este sentido, es necesario continuar con la monitorización de este proceso, para verificar que la convergencia se sigue produciendo, y para asegurar si dicha convergencia se debe a que los proveedores de servicios en la Nube están proporcionando servicios más adaptados a las expectativas y requisitos de sus clientes, o si los clientes asumen el portfolio de servicios en la Nube que se les ofrecen y los utilizan tal cual, resignándose a no poder intervenir en su mejora y adaptación a las necesidades de negocio.

Conclusión: decrece la diferencia entre expectativas y satisfacción de los usuarios de servicios en la Nube. ¿Se han mejorado los servicios, o se han aceptan en su estado actual?

Conclusión: Los servicios en la Nube aún deben seguir mejorando hasta que los usuarios estén satisfechos a la altura de sus expectativas. O al menos a la altura de los requisitos que se exigen.



La perspectiva que tienen los usuarios de la importancia del cumplimiento de regulaciones es alto (4.22 en promedio) sobre todo para entornos SaaS en nube pública (más del 30% para ambos). Esto se corrobora con que el nivel de cumplimiento de seguridad aumenta en la Nube (3.94 en promedio). El número de incidentes no aumenta (2.50 en promedio), la criticidad de estos incidentes no aumenta (1.87 en promedio) así como el coste por incidente (1.87 en promedio). Finalmente, la cantidad de detecciones se percibe en aumento (2.31 en promedio).

Conclusión: los usuarios de la Nube confían y dependen de la seguridad que les brinda el proveedor de la Nube. Porque la mayoría contrata servicios SaaS, así como la mayoría usa Nube pública. Sin embargo, esto refleja que los usuarios de la nube no están muy maduros con respecto a controles que se puedan implementar para escenarios Paas/laas. Los proveedores de la Nube que brindan más de un tipo de tecnología deben compartir con sus clientes los controles que implementan para que los usuarios tengan más controles y los porcentajes de incidentes, criticidad y costos disminuya.

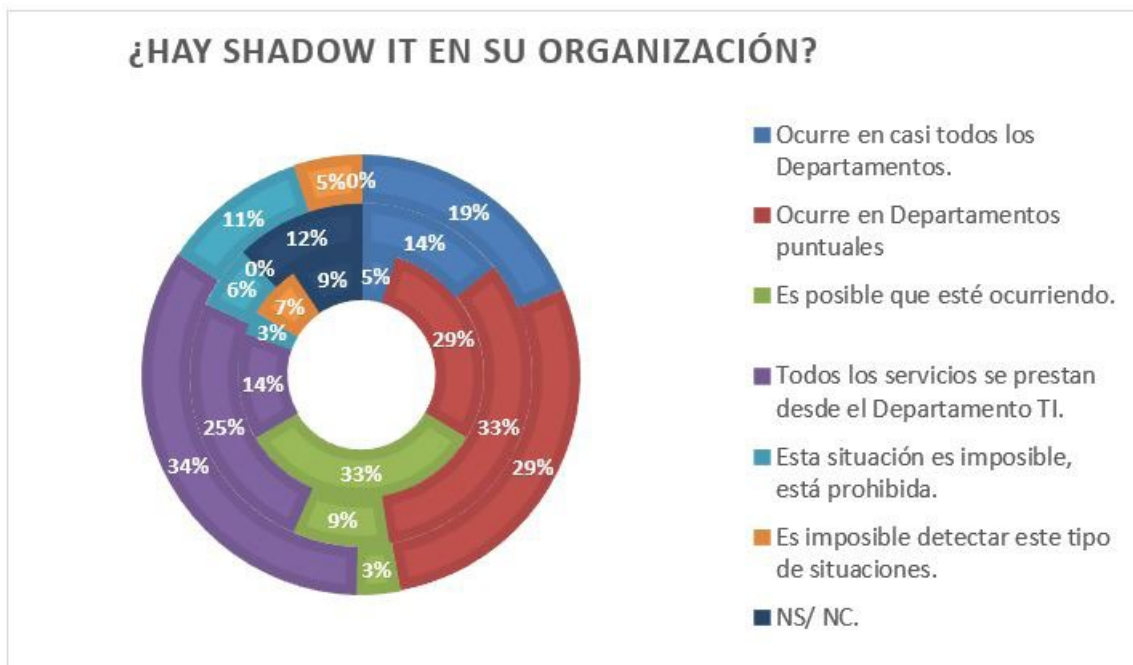
# Visión sobre Shadow IT



El fenómeno de ShadowIT, definido como la capacidad de los departamentos No-IT de una organización de contratar y utilizar servicios en la Nube sin la colaboración del departamento IT, e incluso ocultando deliberadamente, sigue siendo motivo de preocupación para las organizaciones y, por lo tanto, motivo de análisis en el presente estudio.

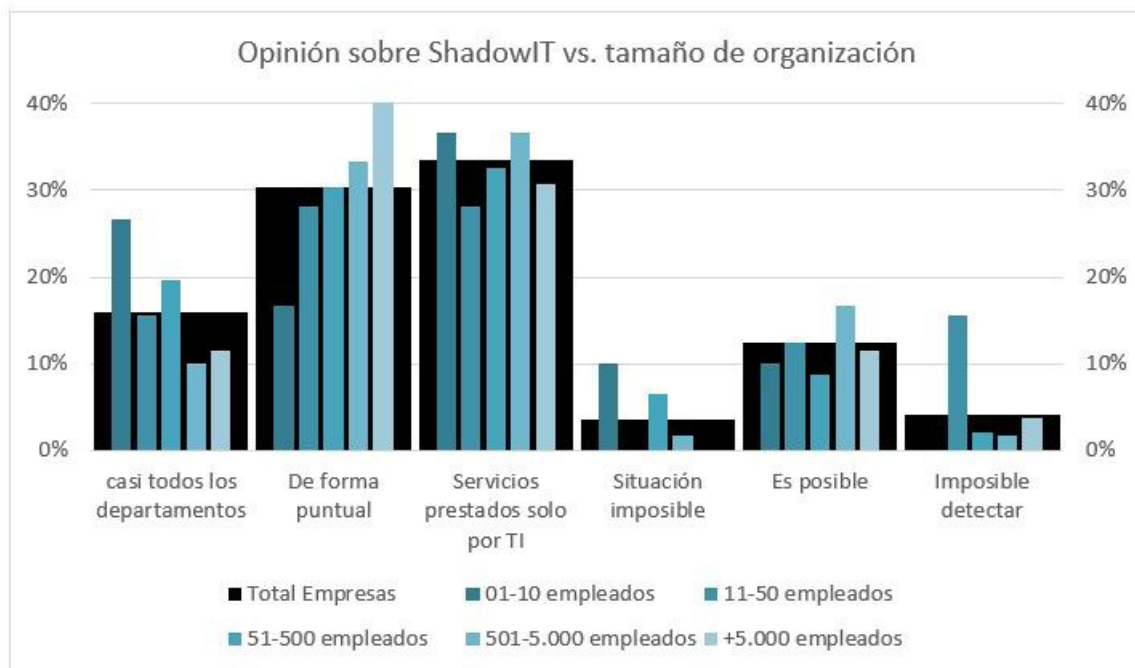
Como en años anteriores, la primera cuestión que debe plantearse es si ShadowIT está ocurriendo efectivamente en las organizaciones y si las organizaciones son conscientes y conocedoras de ello, o no es el caso.

Los datos recopilados en 2018 continúan con la polarización de visiones sobre ocurrencia ShadowIT que se deriva de la mayor permanencia del fenómeno en las organizaciones y su mayor conocimiento. Un 11% de los participantes siguen sin tener información sobre la ocurrencia del fenómeno, a la vez que crecen del 25% al 34% los que señalan que esta tarea ya está en el departamento de TI de las organizaciones, y del 14% al 19% los que creen que es un fenómeno generalizado en todos los departamentos, prácticamente en la misma proporción que varía la opinión de que ShadowIT ocurre en departamentos puntuales (del 33% al 29%). Apuntando posiblemente a que las organizaciones están controlando el fenómeno donde lo han identificado, mientras que en otros casos, la organización no logra controlar el fenómeno y este se extiende a toda la organización.



Buscando entender mejor este fenómeno, se ha analizado como varía la opinión sobre ShadowIT en las organizaciones en función de su tamaño. Los hallazgos son relevantes, en tanto que la opinión sobre la involucración de TI como prestador único de servicios es esencialmente similar en todos los casos y cercano al 34% identificado anteriormente. De la misma forma que es constante en torno al 45% la suma entre los que señalan que ShadowTI es un fenómeno generalizado y los que señalan que es una situación puntual. Pero el peso de estos elementos está claramente condicionado por el tamaño de la organización, de forma que mientras que las empresas de menor tamaño opinan que es un fenómeno común a todos los departamentos, las empresas de mayor tamaño sostienen que es un fenómeno que ocurre de forma puntual. Y esta opinión evoluciona de forma sostenida a medida que la empresa crece. Posiblemente esta opinión se fundamenta en el crecimiento en capacidades de servicio y de control de los servicios de los Departamentos de TI a medida que la empresa gana tamaño y el departamento TI crece en consonancia.



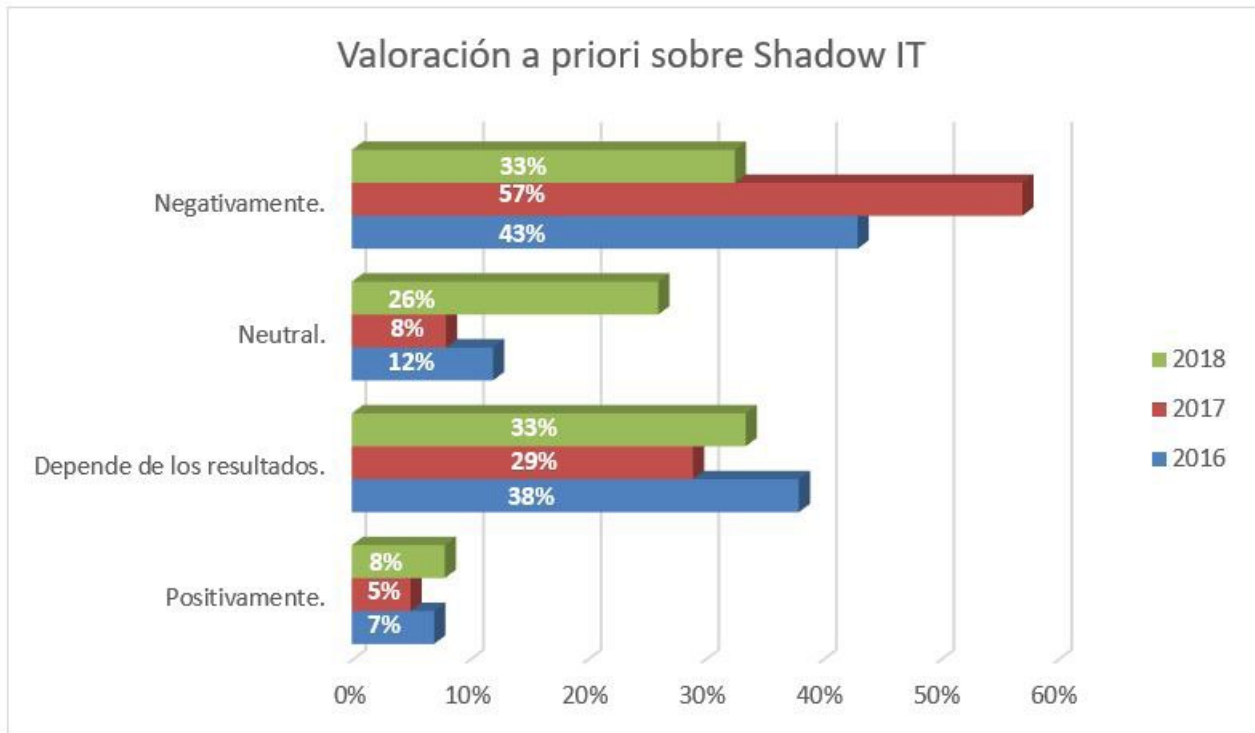


Conclusión: Shadow IT es una realidad mejor conocida por las organizaciones, pero aún no está completamente detectada por los Servicios IT.

Conclusión: La ocurrencia de Shadow IT está asociada a la capacidad de los Departamentos de TI de prestar servicio, es decir, de su tamaño y recursos.

El estudio en esta edición no analiza los factores que provocan ShadowIT, pero sí que investiga la evolución de la visión que se tiene sobre ShadowIT.

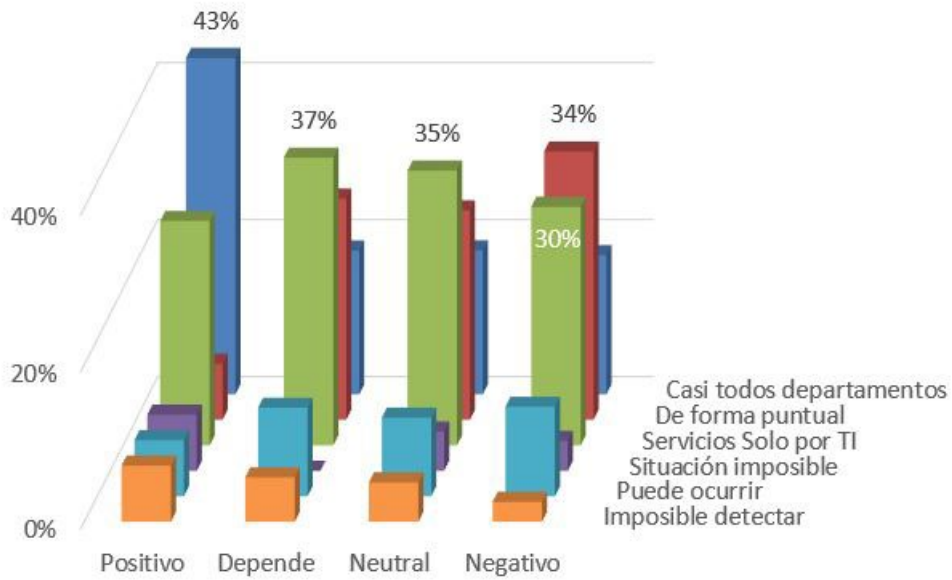
La edición anterior del estudio detectó que las valoraciones negativas de ShadowIT eran cada vez más mayoritarias llegando hasta el 57% de los participantes. En esta edición, esa visión pierde claramente apoyos, dejando en casi igualdad a lo que tienen una visión negativa de ShadowIT frente a los que tienen una visión resultadista que se posiciona sobre el fenómeno en función de los resultados que en cada caso se consigan con la aplicación de ShadowIT. Este empate técnico se produce exclusivamente por el trasvase de muchas opiniones negativas sobre ShadowIT hacia el grupo de opiniones neutrales sobre el fenómeno, que crece en casi la misma proporción que baja el grupo de valoraciones positivas.



El análisis de este cambio aparente en la tendencia detectada en 2017 no ha producido una explicación plausible. En particular, y en comparación con los valores obtenidos por ocurrencia del fenómeno, no se ha podido verificar la existencia de posiciones consistentes. Así, cabría esperar que quien tenga una visión negativa de ShadowIT apoyase mayoritariamente que estas actividades se realizasen desde TI, cuando en realidad señalan con más frecuencia (34%) la opción de que ocurre en departamentos puntuales. Hasta un 18% señala que ocurre en casi todos los Departamentos. Por la misma razón, quienes creen que ShadowIT es positivo no deberían apoyar la opción de que sean una tarea para el Departamento de TI, cuando en realidad el 30% apoya esta opción.

Por lo tanto, el estudio no establece la razón de este cambio en la visión sobre la conveniencia de ShadowIT.

Valoración Shadow IT vs. Opinión sobre Ocurrencia



# VIII

## Estado de Concienciación en Seguridad de los Usuarios

El estudio en 2018 repite el análisis iniciado en 2016 sobre el grado de concienciación de las organizaciones respecto de los servicios prestados desde la Nube.

Este estudio ha detectado una mejora sustancial en el grado de concienciación de las personas usuarias de servicios en la Nube, tanto por parte de sus directivos como por parte de sus empleados. Así, el nivel de concienciación pasa la valoración "suficiente" a la que antes no se llegaba, pudiendo clasificarse como de "Alta Concienciación".



Conclusión: Aumenta la concienciación de las personas, acercándose al grado "Alto" de concienciación.

Analizando estos datos de forma más detallada y con la perspectiva de años anteriores, se aprecia una mejora generalizada de la concienciación en todos los ámbitos, sectores, perfiles profesionales y tipologías de empresa.

Dos son los aspectos más destacables de esta mejora generalizada.

El primer aspecto es la influencia del tamaño de la compañía en el nivel de concienciación general. Este aspecto replica el comportamiento en otros aspectos investigados, en los que las organizaciones de menor tamaño tienen mejores grados de concienciación que organizaciones de mayor tamaño hasta que se llega a las organizaciones de mayor tamaño, en las que se vuelve a mejorar.



El segundo aspecto es las diferencias percibidas en concienciación entre diversos sectores, donde se han identificado en los puestos más bajos de este ranking de concienciación a sectores habitualmente punteros, que llevan trabajando intensamente en seguridad y con servicios en la Nube y que incluso fueron pioneros en su adopción. La posición de estos sectores (Banca, Energía y utilities o sanidad) podría basarse en una mayor autoexigencia en sus niveles de concienciación, si bien la información recopilada durante este estudio no permite asegurar esta conclusión. Máxime, cuando el sector empresarial que se declara más concienciado (aseguradoras) también ha realizado en el pasado un trabajo previo serio y sostenido en seguridad y en adopción de la Nube.



Conclusión: Las organizaciones de menor tamaño están más concienciadas sobre la necesidad de tener servicios seguros en la Nube.

# Evolución de Incidentes de Seguridad en Servicios en Nube

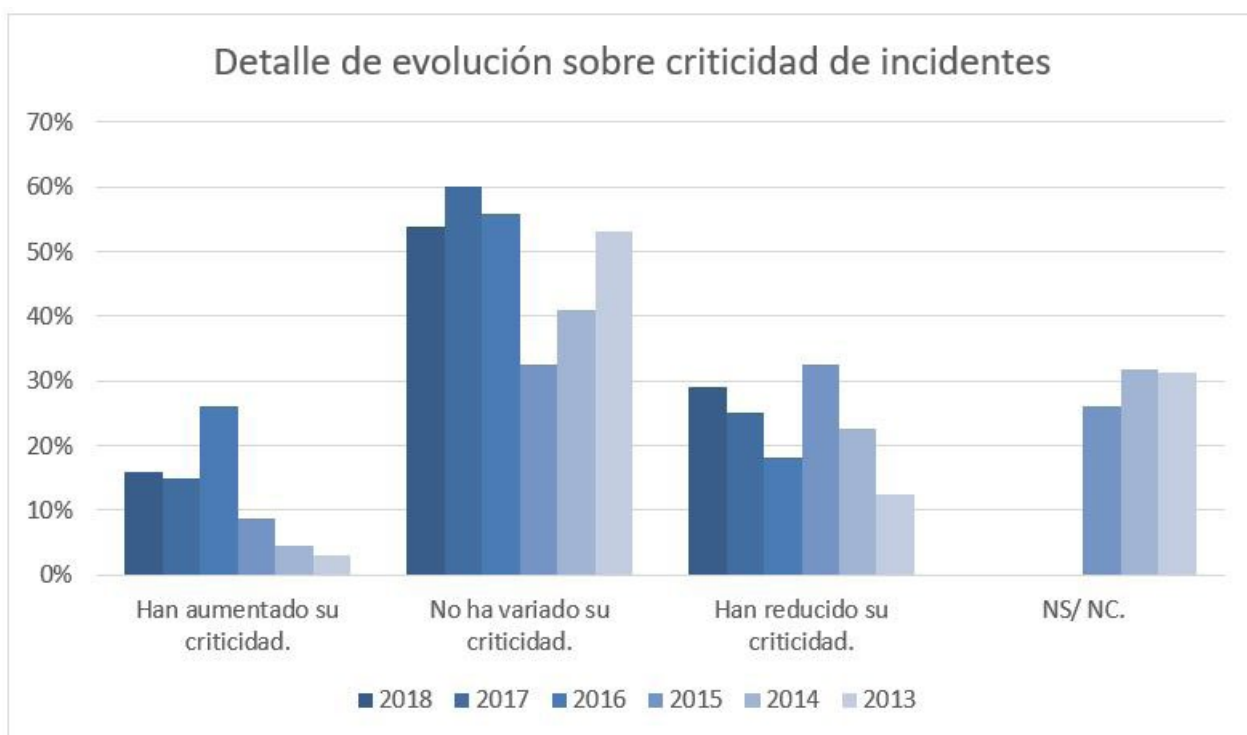
# IX

Este 6º Estudio del Estado del Arte ha incrementado el foco de estudios anteriores en los aspectos relativos a los Incidentes de seguridad. Así, además de investigar aspectos ya trabajados previamente, tales como el número, criticidad o capacidad de detección de incidentes de seguridad o el coste asociado al proceso, se va a investigar la capacidad del proveedor de servicios en la Nube de proporcionar recursos adicionales extraordinarios que pueden ser necesarios únicamente durante la gestión y respuestas a un incidente, tales como consumos adicionales, forense, técnicos especializados en CSIRT u otros.

En primer lugar, al analizar de forma histórica la evolución de la criticidad de los incidentes de seguridad tras la migración a servicios en la Nube podemos observar que esta migración supone una reducción en la criticidad de los incidentes, y en particular, una reducción en el último periodo estudiado. Este fenómeno lo vemos muy asociado a la capacidad de detección y respuesta de los usuarios para incidentes en sus servicios en la Nube.

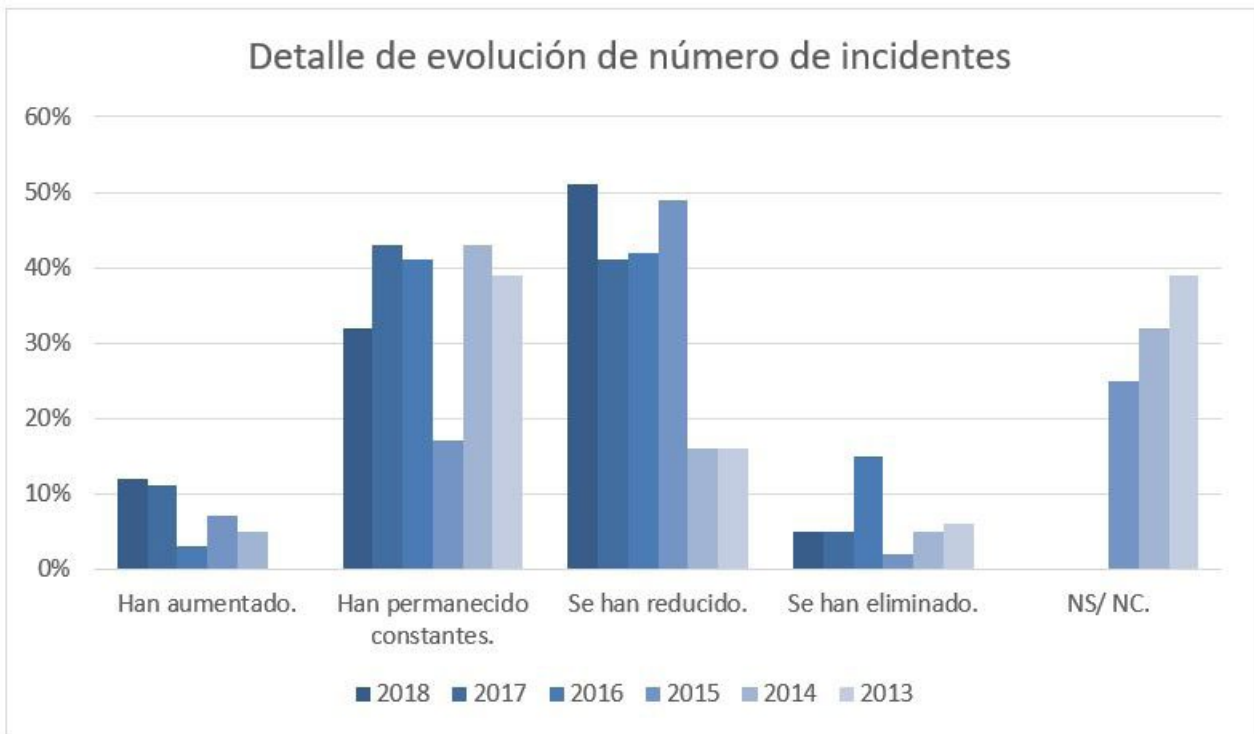
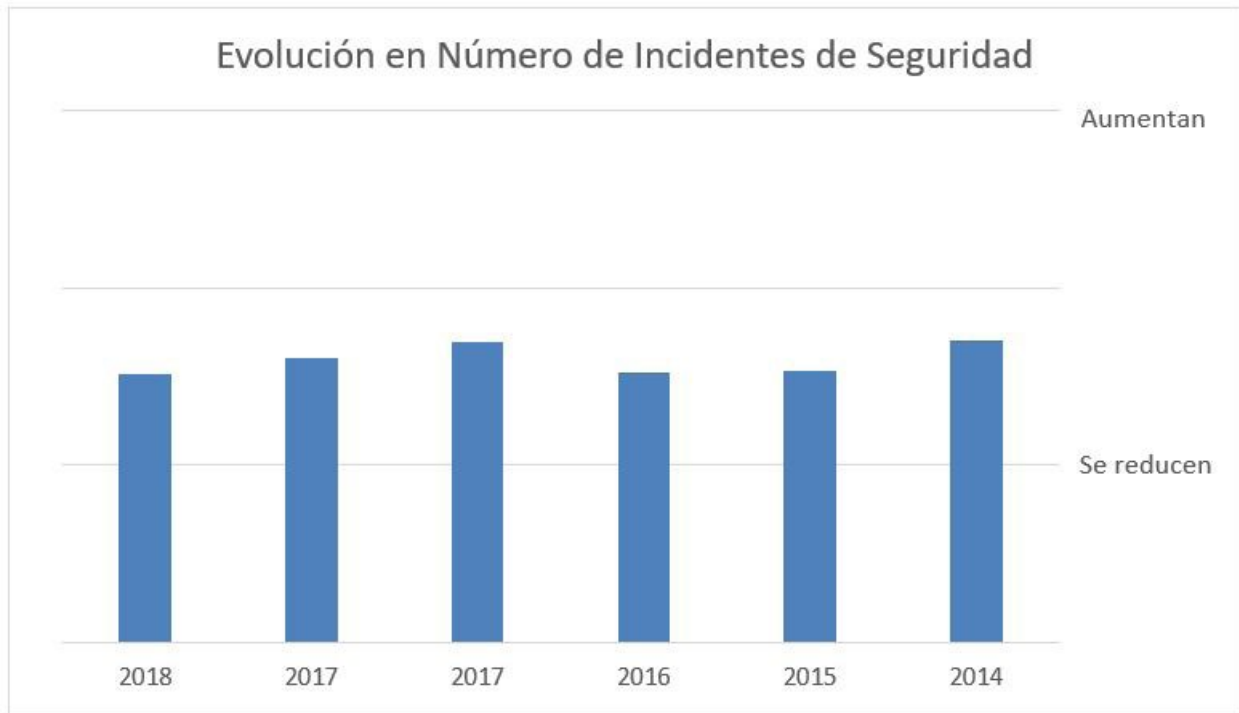


Analizando las opiniones particulares, el escenario frente al detectado en la edición de 2018. Así, tres de cada cinco usuarios opinan que no ha habido cambios en la criticidad de las incidencias detectadas, mientras que la proporción de usuarios que valoran los incidentes como menos críticos (uno de cada cuatro) es mayor que la proporción de usuarios que valoran que son más críticos (uno de cada seis).



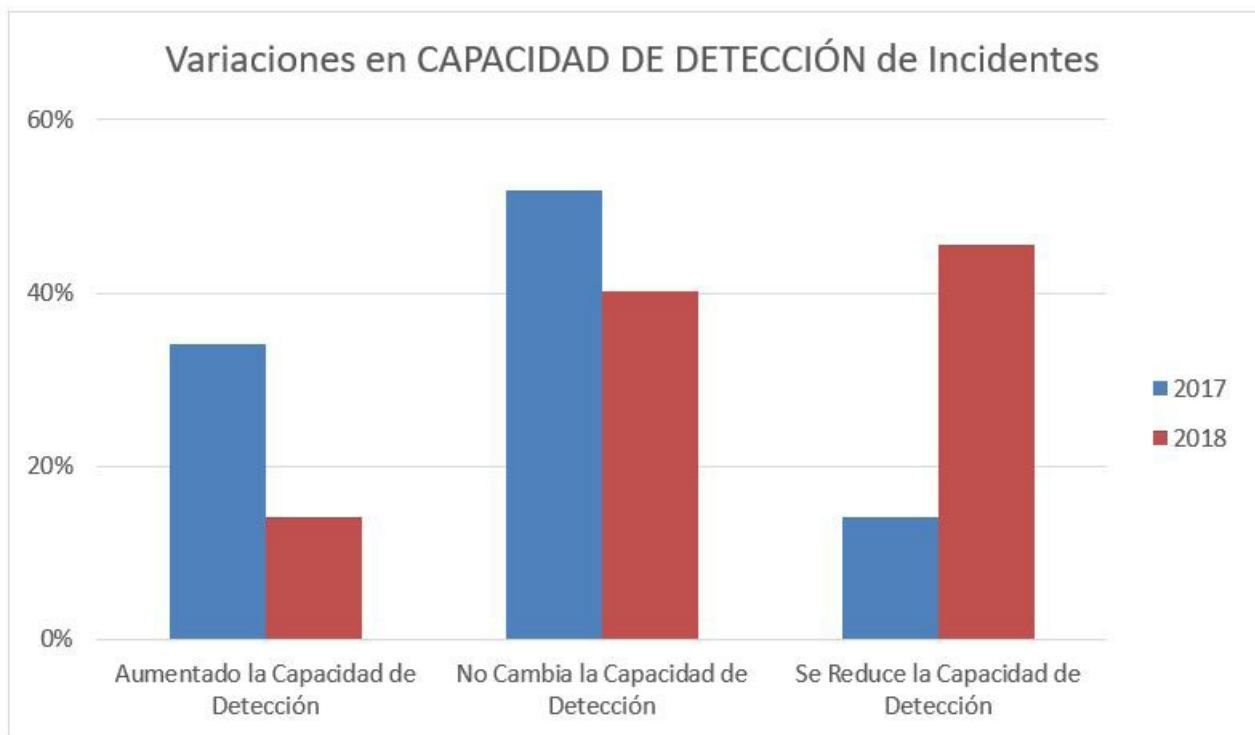
Al analizar el número de incidentes detectados que perciben los usuarios, esta edición del estudio concluye, de nuevo y como en ediciones anteriores, que el uso de servicios en la Nube conlleva en general una reducción del número total de incidentes de seguridad. En esta edición, debe destacarse un claro aumento del número de usuarios que han reducido el número de incidentes de seguridad frente a los que antes señalaban que permanecía constante.



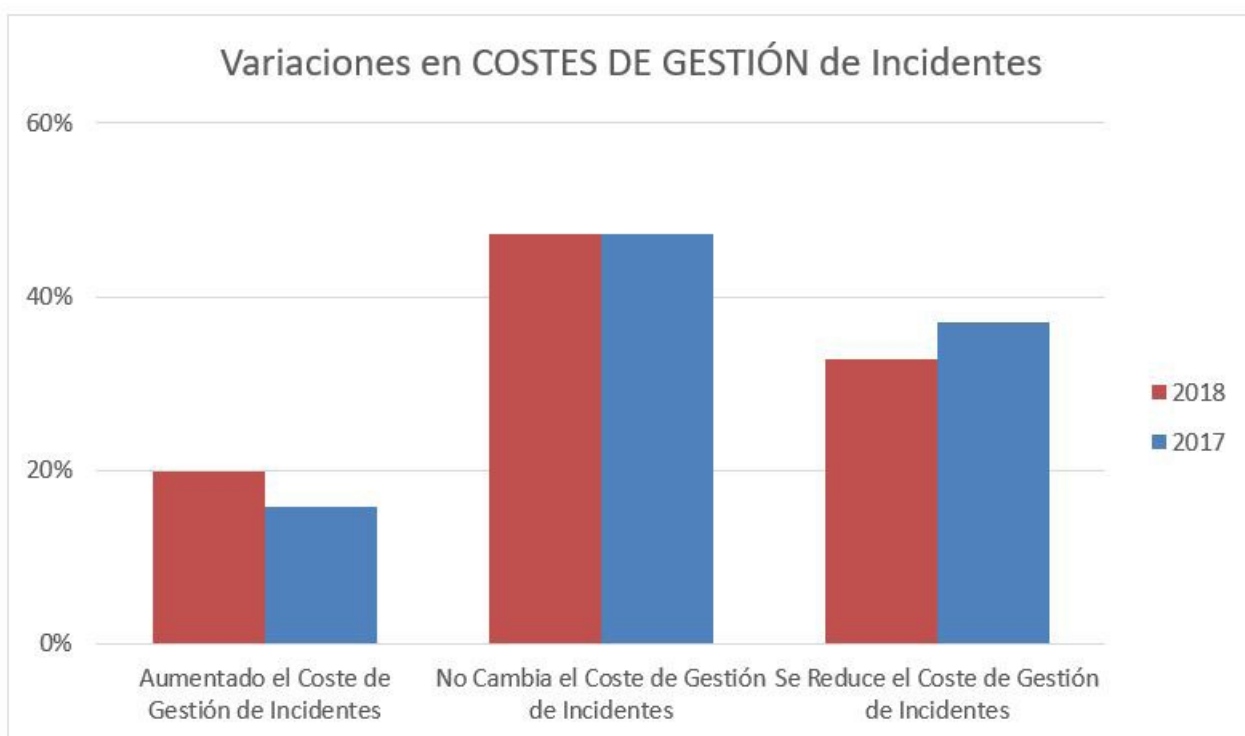


Conclusión: Al migrar a servicios en la Nube, las organizaciones pueden esperar mejoras en sus incidentes, tanto en su número como en su criticidad.

Respecto del Análisis en el número de incidentes de seguridad, los resultados de esta edición del estudio son contradictorios con los de la edición anterior, por lo que no parece adecuado extraer conclusiones sobre estos datos.

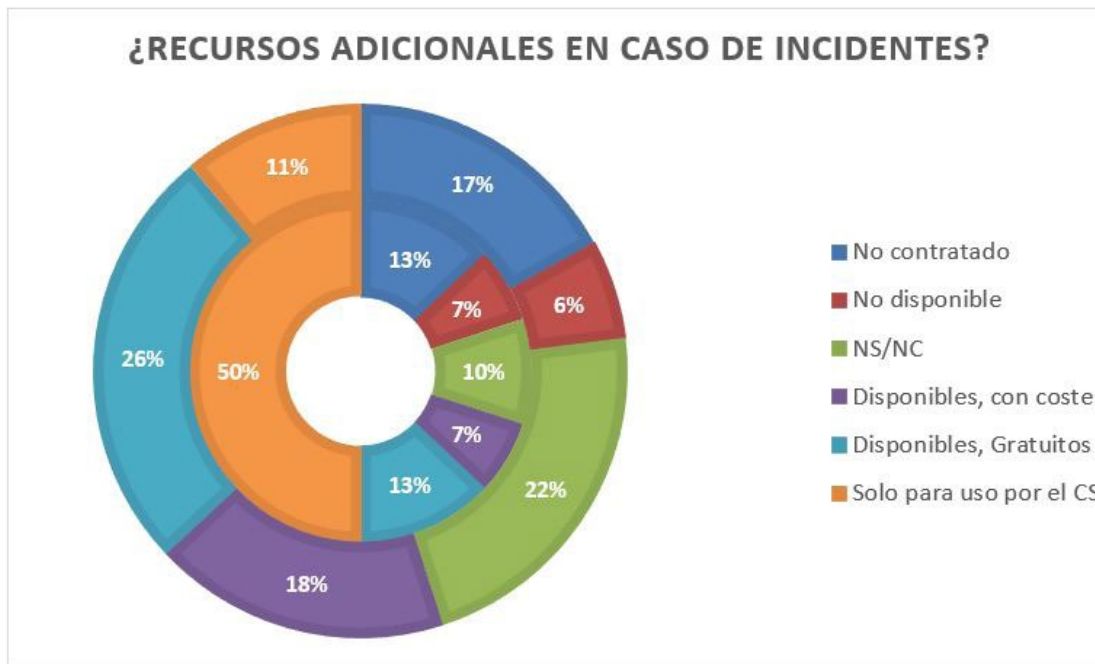


Respecto del análisis de variación de costes en las organizaciones derivados de la gestión de incidentes con el uso de servicios en la Nube, no se detectan variaciones significativas respecto de los resultados de la anterior edición del estudio. Así, la mayoría de los encuestados respondieron que siguen dedicando el mismo volumen de recursos de la organización para la gestión de incidentes antes de utilizar servicios en la Nube, mientras que el 20% de las organizaciones deben dedicar más recursos y el 30% recortan los recursos dedicados a gestión de incidentes de seguridad.

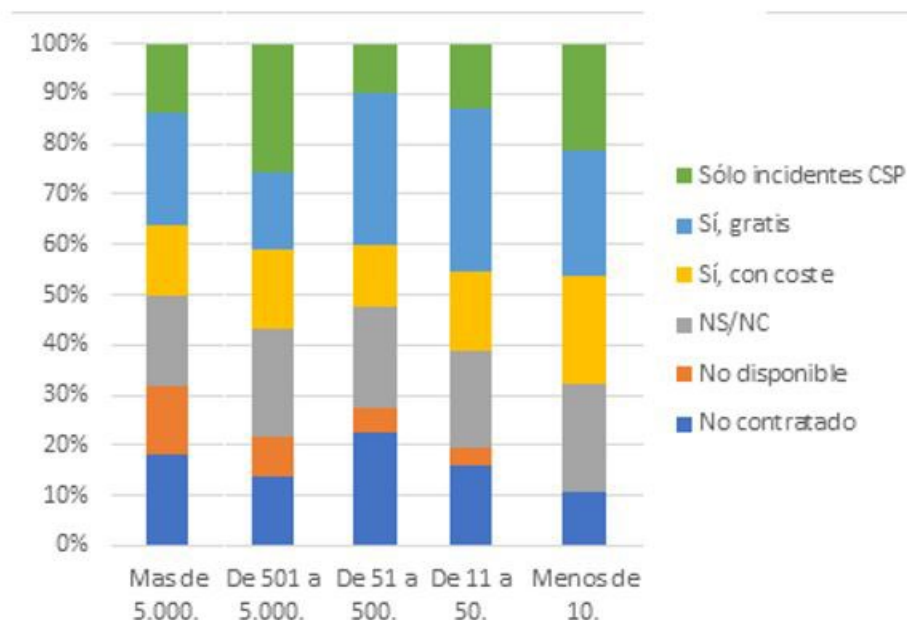


Respecto de la inclusión de recursos adicionales por parte del proveedor de servicios en la Nube para la gestión de incidentes, se presentan por separado los resultados para las empresas ubicadas en España, frente a las de otras geografías. Esta diferencia geográfica resulta destacable, por cuanto el mercado de proveedores de servicios en la Nube tiene un fuerte componente de prestación global de los servicios y por lo tanto, estos recursos adicionales deberían de ofrecerse de forma equivalente en todas las geografías.

No obstante, y hecha esta observación, el estudio ha detectado que en España el 50% de los casos se indica que el Proveedor únicamente gestiona sus incidentes y no los del cliente, frente al 11% que contestan en este sentido en el resto del mundo (eliminando España). Además, se observa que para el resto de los países para los que hay datos los resultados son muy semejantes entre sí, dándose esta divergencia únicamente para España.



Esta divergencia también se observa si hacemos el análisis por tamaño de las empresas, ya que sólo para las empresas de entre 501 a 5000 empleados figura la respuesta de que el proveedor solo gestiona sus propios incidentes como la más destacada, frente al resto de casos. Sin embargo, no se encuentra ninguna razón para esta diferencia.



Conclusión: los CSP tienen contemplada entre sus capacidades la dotación de servicios adicionales para sus usuarios, en caso de incidentes de seguridad del proveedor o de los usuarios.

# Resolución de Conflictos entre cliente y usuario de servicios



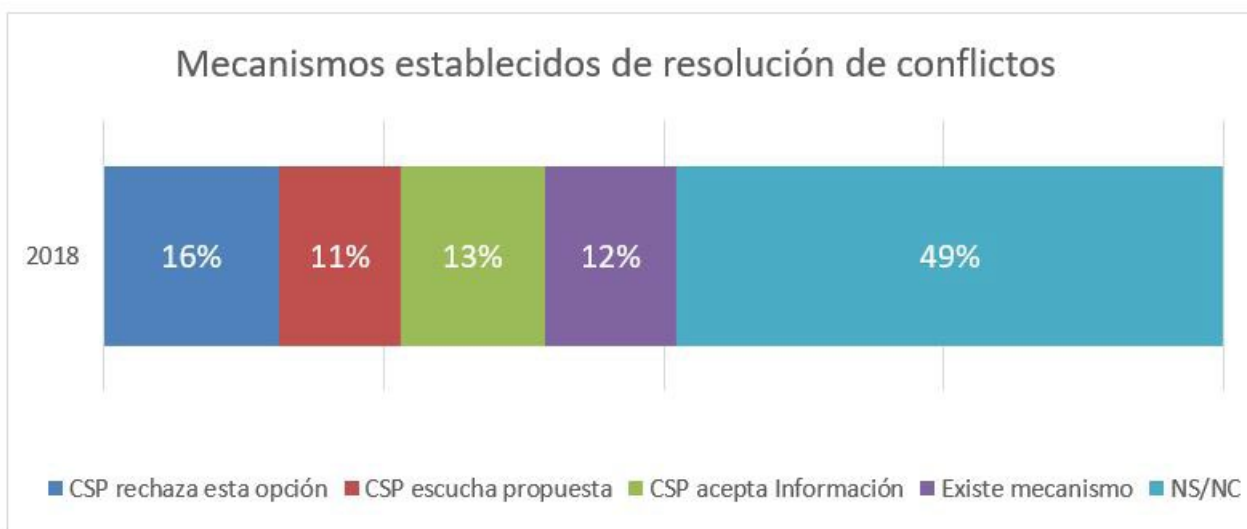
Como novedad en esta 6ª edición del estudio, se ha planteado el análisis de las condiciones y mecanismos diseñados en la prestación de servicios en la Nube cuando existen discrepancias entre el proveedor de servicios y su usuario respecto al tipo y volumen de servicios proporcionados y, consecuentemente, su tarificación. Este interés surge de la propuesta de algunos miembros del equipo de analistas que, conociendo de casos en los que había surgido esta circunstancia, propusieron realizar este análisis para conocer si se trata de una situación más o menos frecuente y para conocer los mecanismos de resolución de la misma que pueden estar disponibles.

El análisis de los resultados para este aspecto se limita a aquellos usuarios que se han declarado usuarios de los servicios en la Nube, puesto que solo esos usuarios pueden haber tenido conflictos con sus proveedores.

En concreto, se ha planteado a los participantes la siguiente pregunta: "¿Admite el CSP la posibilidad de que un tercero resuelva discrepancias en la medición del servicio prestado?"

El análisis de estos usuarios apunta varios aspectos interesantes. En primer lugar, casi de la mitad de los usuarios desconocen si existe tal mecanismo. El desconocimiento se interpreta como síntoma de que este aspecto no les resulta preocupante, pudiéndose deducir que estos usuarios, bien confían en su CSP, bien se encuentran cómodos con el modelo de facturación propuesto por el CSP, bien no se han planteado que este punto pudiera ser motivo de negociación y/o inclusión en los contrato del servicio.

En segundo lugar, un 12% de proveedores de usuarios ya tienen establecido este mecanismo de resolución de conflictos, y un 24% tendrían posibilidad de activarlo aportando información en su caso. Y sólo uno de cada seis usuarios conoce que su proveedor se niega a tener este mecanismo, imponiendo las mediciones de servicio realizadas por el CSP como única fuente válida a efectos de facturación.



Conclusión: Al menos dos de cada cinco usuarios de servicios en la Nube disponen de mecanismos de resolución de conflictos de facturación con su proveedor.

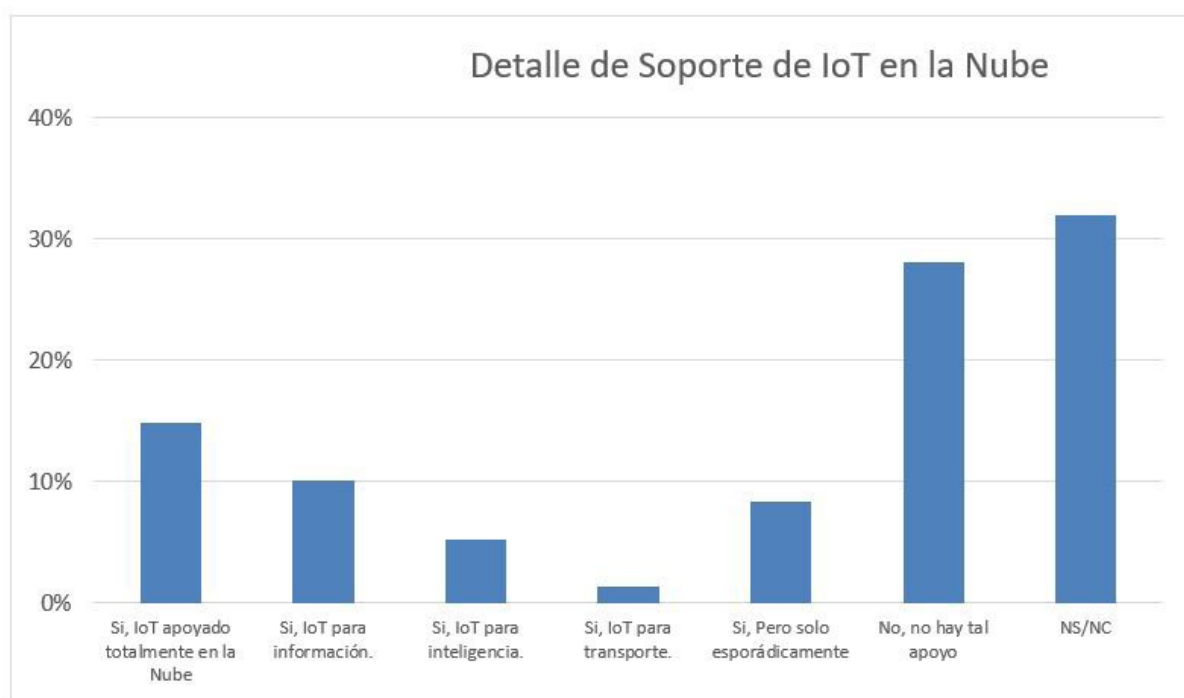
# Soporte para IoT en Servicios en la Nube

# XI

Las tecnologías Internet of Things están ganando creciente uso en las organizaciones, en muchos casos soportadas total o parcialmente en servicios en la Nube. Por ello, y también como novedad en esta 6ª edición del estudio, el equipo de analistas se planteó analizar la relación entre IoT y el papel de la Nube como facilitador del despliegue y operación del servicio IoT por parte de los clientes.

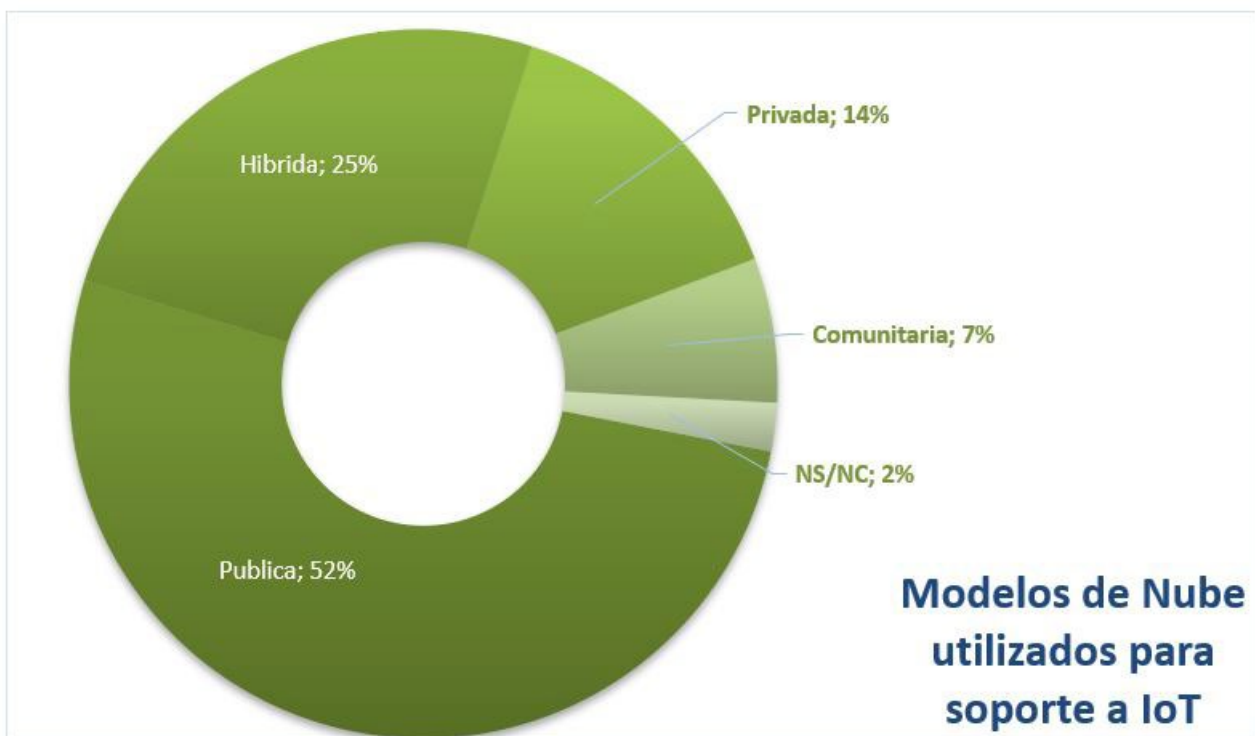
En concreto, se ha planteado a los participantes la siguiente pregunta: "¿Se están soportando servicios IoT sobre servicios en la Nube?"

A esta pregunta, se ha identificado que un 40% de las organizaciones se declaran usuarios de IoT sobre servicios de Nube, en cualquiera de las modalidades que se han planteado. Este porcentaje de usuarios resulta particularmente interesante a la vista de los sectores a los que pertenecen los participantes en el estudio. Y es mayor que el 28% de entidades que declaran que no están usando IoT, y el 32% de entidades que no facilitan información.



Conclusión: 4 de cada 10 organizaciones se declaran ya usuarios de servicios de Nube como soporte a sus programas de IoT.

Resulta también relevante conocer, en aquellos casos en los que se está apoyando IoT sobre la Nube, qué modelos de servicio se están utilizando. Dada la dispersión geográfica inherente en muchos casos a los despliegues IoT, parece probable que IoT se apoye mayoritariamente en servicios de Nube pública, de más facilidad de acceso y/o extensión geográfica, frente a otro tipo de servicios. Y, en efecto, los datos confirman esta posibilidad, dado que el 54% de los usuarios declaran que utilizan IoT sobre Nubes públicas, y un 24% adicional utilizan Nubes híbridas. Datos que refrendan la conjetura inicialmente planteada.



Conclusión: Los usuarios de IoT sobre Nube prefieren servicios de Nube Pública.

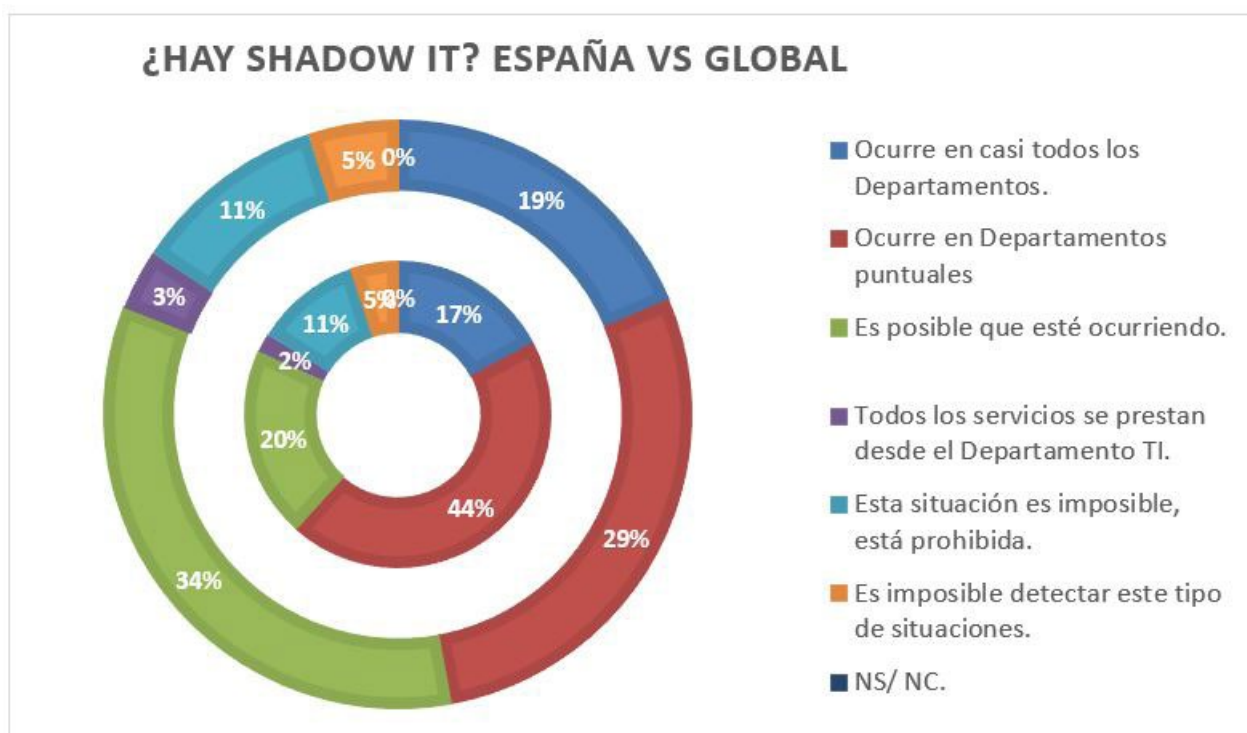


# Comentarios particulares para el caso de España, CSA-ES

# XIII

Además de los hallazgos realizados en el estudio para el total de los países, y de los matices particulares para España que se han señalado a lo largo de este documento, hay algunos elementos adicionales que el equipo de analistas de CSA-ES quisiera incluir, en tanto que son específicos de esta área geográfica.

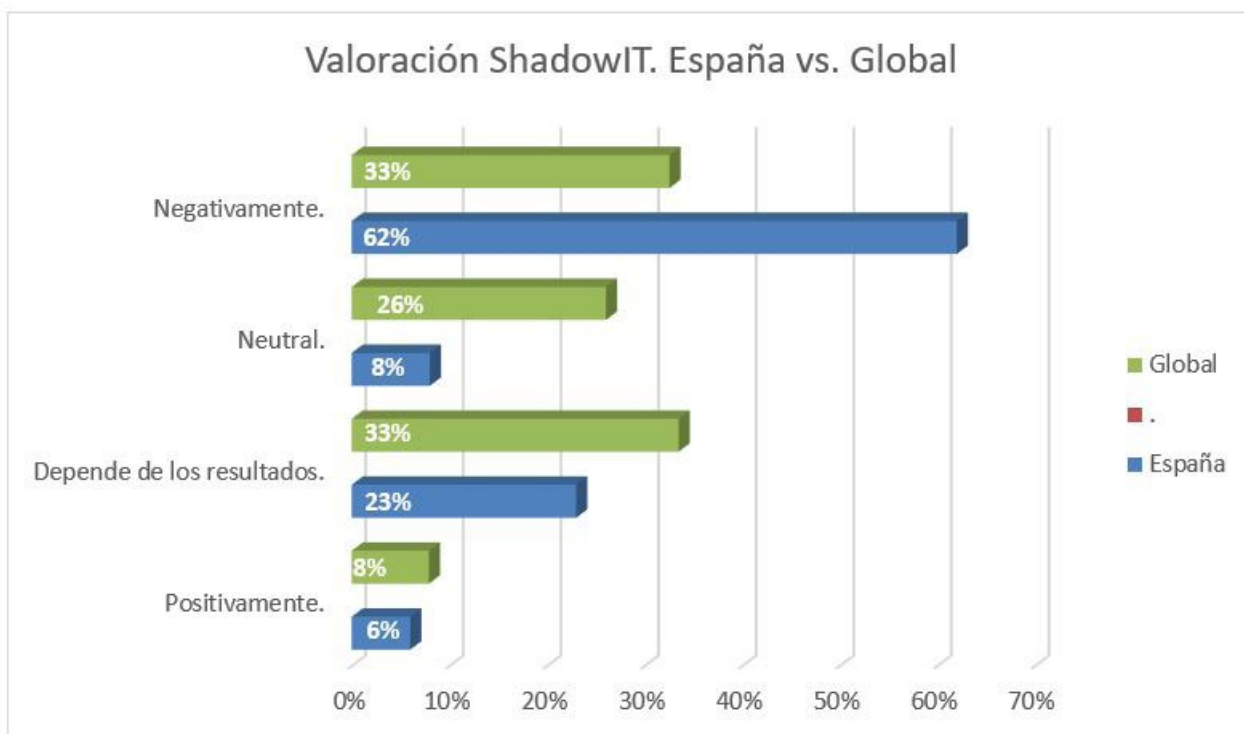
El primer aspecto que se desea destacar es la diferente visión sobre Shadow IT. En particular, en España se señala solo en un 20% de los casos que los servicios se deben prestar desde TI, frente al 34% global. Y en paralelo, un 44% de los usuarios opinan que ShadowIT está ocurriendo en las organizaciones en situaciones puntuales, frente al 29% de opinión global. Esta opinión es particularmente intensa en empresas de más de 500 empleados, que son las que concentran la práctica totalidad de casos que opinan que hay ShadowIT puntualmente.



Y de forma complementaria, la posición de las empresas españolas frente a ShadowIT es radicalmente negativa, abandonando masivamente las posiciones de neutralidad o conveniencia por resultados que se identifican a nivel global, de forma que dos de cada tres empresas se posicionan en contra de ShadowIT.

La combinación de ambos factores apunta a un escenario en el que las empresas españolas consideran que el departamento de TI debería provisionar todos los servicios TI que necesita la organización, pero se considera que esto no ocurre. Pudiera ser por dificultades propias del departamento de TI o porque hay departamentos que oficialmente pueden tomar decisiones autónomas, o porque hay departamento que de facto toman estas decisiones sin más.

La combinación de ambos factores apunta a un escenario en el que las empresas españolas consideran que el departamento de TI debería provisionar todos los servicios TI que necesita la organización, pero se considera que esto no ocurre. Pudiera ser por dificultades propias del departamento de TI o porque hay departamentos que oficialmente pueden tomar decisiones autónomas, o porque hay departamento que de facto toman estas decisiones sin más.



# Ficha Técnica del Estudio

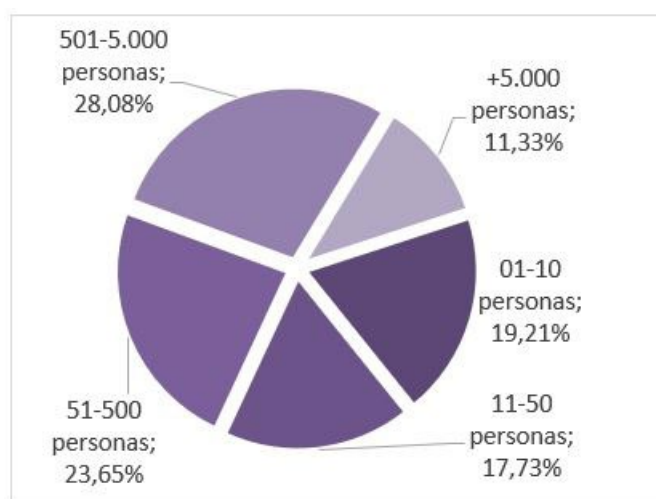
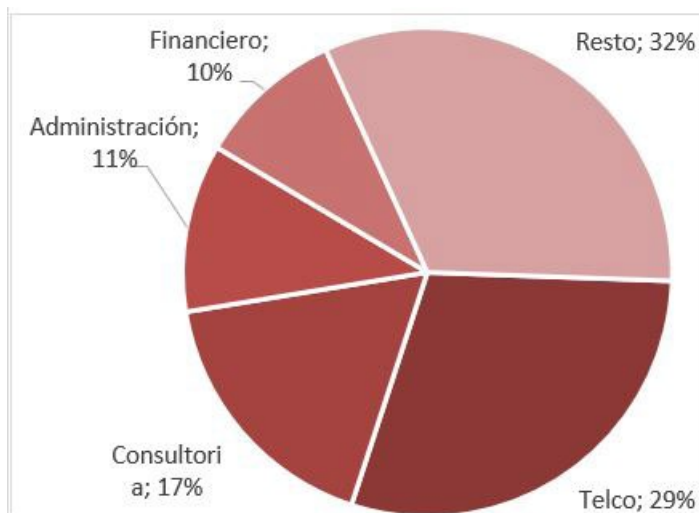
# XIII

Los resultados del análisis y el diseño del estudio ha sido realizado por los profesionales que figuran en la portada del documento, que forman parte de los Capítulos Español, Peruano, Argentino, Chileno, Boliviano, Brasileño y Colombiano de CSA y del Capítulo de Madrid de ISACA, en colaboración con ISMS Forum.

El estudio se ha realizado en base a encuestas recopiladas entre el 10 y el 27 de septiembre de 2017, a través de la plataforma online SurveyMonkey. Se recopilaron un total de 312 respuestas de profesionales y organizaciones.

Con respecto a la distribución de las respuestas por geografía, en la edición 2018 hay que destacar la amplia y equilibrada presencia geográfica de los participantes en el estudio, con representantes en todas las geografías.





En términos de características de las empresas participantes, la mayoría desarrollan su actividad de negocio en el sector de las telecomunicaciones, la consultoría, administración pública o financiero. Siete de cada diez usuarios se declaran usuarios de servicios en la Nube, aunque también hay usuarios que están valorando su incorporación, y otros han dejado sus servicios en la Nube o incluso han descartado su incorporación.

Más información en:



[www.ismsforum.es](http://www.ismsforum.es)