V ESTUDIO DEL ESTADO DEL ARTE DE LA SEGURIDAD EN LA NUBE

Una iniciativa de:

En colaboración :

2017

Con la participación de los siguientes profesionales y organizaciones:

COORDINADORES:

Mariano J. Benito (GMV), CSA-España

Aldo Carlessi (ATMOSPHERA), CSA-Perú

Luciano Moreira (Vice Presidente), CSA-Argentina

Erik De Pablo (Director Investigación), ISACA-Madrid

Abdel Aliaga (Presidente), CSA-Bolivia

Freddy Grey (Evangelista), CSA-Chile

Leonardo Goldim (Presidente); CSA-Brasil

Juan Carlos Álvarez Mesa (Presidente), CSA-Colombia

ANALISTAS:

Mª Teresa Avelino (Independiente), ISACA-Madrid

Julio Balderrama (Independiente), CSA-AR

Josep Bardallo (SVT Cloud), CSA-ES

Alberto Bernaldez (Liberty Seguros), CSA-ES

Manuel Caldas (Independiente), CSA-PE

Concepción Cordón (EMASA), CSA-ES

Juan Garcia Galera (CEMI – Ayto. Málaga), CSA-ES

Alfonso Gómez (Banco de España), CSA-ES

Jordi Guijarro (CSUC), CSA-ES

Javier Mora Lavín (Independiente), ISACA-Madrid

Rafael Navajo (GMV), CSA-ES

Julio Peñas (Independiente), CSA-ES

Susana Rey Baldomir (ISMS Forum), CSA-ES,

Alejandro del Río (EY), CSA-ES

Juan Bautista Roa (Analista), CSA-CL

Jorge Antonio Rojas (Independiente), CSA-PE

Eduardo R. Ringach (Independiente), ISACA-Madrid

Leonardo Rosso (Presidente), CSA-AR

Xavi Vila (Grupo Caja de Ingenieros), CSA-ES

Contenido

RESUMEN EJECUTIVO

El V Estudio del Estado del Arte de Seguridad en la Nube confirma muchas de las tendencias en la materia identificadas en las ediciones anteriores, dibujando un escenario estable de las condiciones de seguridad en que se prestan y se consumen los servicios en la Nube, y las consecuencias e impactos que el cambio a estos servicios supone para sus usuarios.

Así, el estudio identifica como los clientes continúan un año más sin sentirse satisfechos con los servicios de la Nube que reciben. Estos servicios siguen estando por debajo del nivel de exigencia que han requerido, y también por debajo de las expectativas en seguridad que tenían, expectativas que están en máximos históricos. El estudio identifica también que las organizaciones cuya actividad está más cercana de la tecnología son las que más satisfechas se encuentran, y a la vez resultan ser las que tienen expectativas más moderadas.

La cercana entrada en vigor del Reglamento General de Protección de Datos (GDPR) se ve reflejada en los resultados del presente Estudio, provocando que suban a la máxima exigencia los requisitos en privacidad de las organizaciones presentes en las geografías en las que GDPR entra en vigor.

ShadowIT sigue siendo un aspecto de interés del estudio, si bien las organizaciones han evolucionado desde el anterior estudio hacia una posición de mayor conocimiento y menor permisividad o tolerancia hacia el fenómeno, que impulsa a los Departamentos de TI a mejorar la calidad de sus servicios hasta igualar los percibidos por los usuarios de ShadowIT.

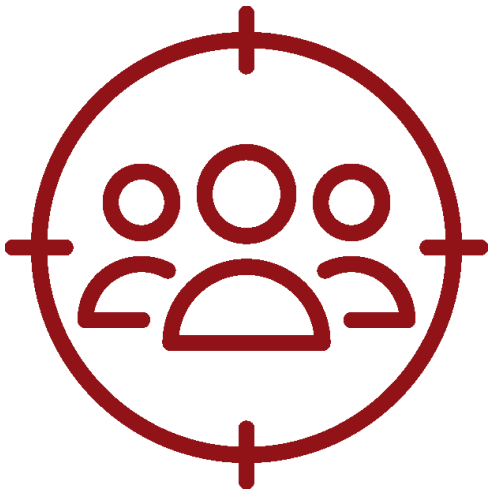
La concienciación y la falta de información precisa sobre las implicaciones en seguridad del uso de Servicios en la Nube sigue siendo una asignatura pendiente. Las Organizaciones se ven aún como insuficientemente concienciadas sobre los riesgos de seguridad en estos Servicios.

La evolución del impacto de los incidentes de seguridad apuntaba en la anterior edición del estudio en una no deseable tendencia hacia la no efectividad, tendencia que se corrige. El V estudio señala que el uso de servicios en la Nube supone un número de incidentes y un impacto similar o inferior, con una mayor capacidad en la detección de incidentes y una dotación de recursos inferior. El estudio revela también que la información sobre la Nube es abundante, está disponible y se consulta frecuentemente. Así como que los esquemas en vigor evaluados para la certificación de profesionales y organizaciones siguen aportando el mismo valor al mercado.

El V Estudio del Estado del Arte de Seguridad en Cloud Computing, realizado en 2017 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 y 2016.

OBJETIVOS Y ÁMBITOS DE ESTUDIO

El objetivo del presente estudio es explorar y conocer el estado del arte de la adopción de la Computación en la Nube, y el papel que juega la seguridad en la adopción de esta tecnología, desde la perspectiva de los usuarios. Para ello, el estudio identifica las expectativas en seguridad que tienen los usuarios en los servicios en la Nube y cómo se aplican esas expectativas en las organizaciones, la satisfacción de las mismas con el modelo de servicios y los servicios recibidos, la disponibilidad de información y certificaciones a su alcance en la adopción de estos servicios, los modelos y servicios más demandados y otros resultados obtenidos por la adopción de servicios en la Nube. Este análisis se realiza tanto para la situación existente a la realización del mismo, como desde un punto de vista histórico.



El estudio centra su campo de estudio en los mercados español y latinoamericano en aquellos países cuyo capítulo local de Cloud Security Alliance ha participado, ampliando el alcance a otros mercados en la medida en que las empresas participantes en el mismo han facilitado información sobre ellos. 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).

En base a todo ello, el presente estudio combina varios ejes de análisis de los datos recopilados de las empresas participantes:

- Conclusiones generales del estudio, sobre la base del TOTAL de los DATOS.

- Visión histórica de evolución de los indicadores de los estudios anteriores de 2013[1] , 2014 [2], 2015 [3] y 2016 [4], que incluyeron España (todos los estudios), Perú (desde 2015) y Argentina (desde 2016).

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).

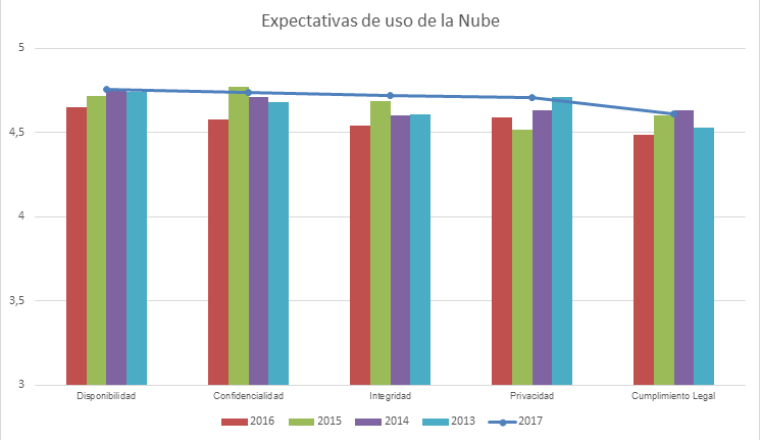
2. En inglés: (http://www.ismsforum.es/ficheros/descargas/csa-en-2014-cloudsecuritystateoftheart20141119.pdf). **En español:** https://www.ismsforum.es/ficheros/descargas/csa-es-2014-cloudsecuritystateoftheart20141119.pdf

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

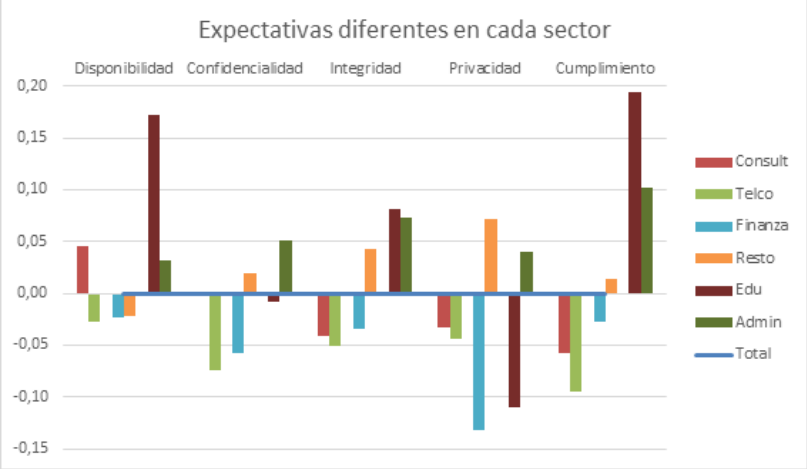
4. http://www.ismsforum.es/ficheros/descargas/iv-cloudsecurity-sota-2016-csa-es-pe-ar-isaca-mad.pdf. **En inglés** https://csacongress.org/wp-content/uploads/2016/11/Mariano-Benito-Cloud-Computing-State-of-the-Art-Analysis.pdf

ANALISÍS DE EXPECTATÍVAS DE USUARIOS DE LA NUBE

Se revierte la ligera tendencia a la baja en todos los objetivos analizados que se estaba detectando en los anteriores estudios, alcanzándose los valores máximos de todos los años analizados. Estos valores corresponden 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.



Las expectativas de los usuarios de los servicios en el Nube están en máximos históricos



Esta visión es compartida por todos los participantes en el estudio. Existen escasas diferencias basadas en el tamaño, puesto o sector de los participantes de la encuesta. Si bien el nivel de expectativa es menor en los usuarios más intensivos de los servicios en la Nube, de forma que la expectativa se reduce a medida que las organizaciones utilizan un número creciente de estos Servicios; y con una mayor exigencia en las expectativas en cumplimiento legal en los participantes europeos.

Se ha realizado también un análisis sectorial centrado en los sectores para los que existe un número de respuestas suficiente. Este análisis señala que, las expectativas son menos elevadas en los sectores más cercanos a la tecnología (consultoría, telecomunicaciones), frente a los sectores de educación o administración, que tienen sistemáticamente expectativas mayores.

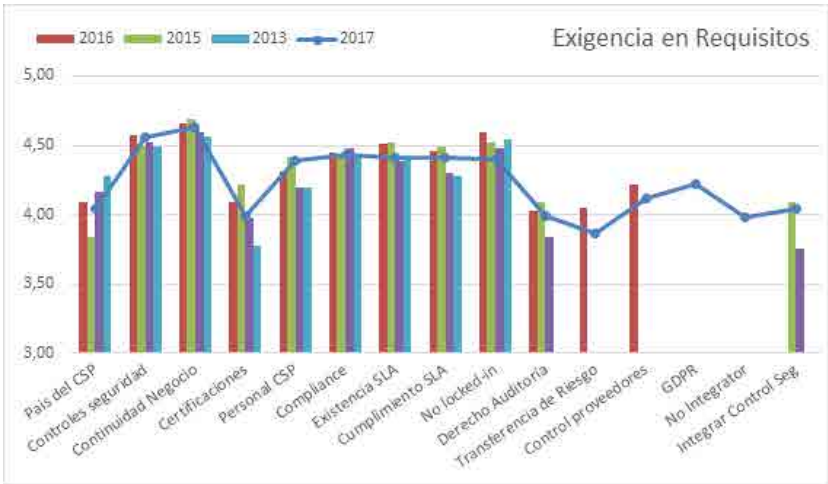
En conclusión, la expectativa de servicios en la Nube de muy altas garantías de seguridad viene manteniéndose a lo largo de todos los años estudiados. El estudio apunta también a que los usuarios tienen cada vez mayores expectativas y más confianza en la Nube. Por ello crecen sus expectativas sobre las condiciones de seguridad en la que se prestan los servicios, en todas las dimensiones de seguridad. También se detecta la influencia de los marcos legales vigentes en cada país en la expectativa de cumplimiento legal, mayor en aquellos sectores sujetos al cumplimiento de regulaciones específicas. Por último, los proveedores de servicios en la Nube deberían considerar las expectativas menores sobre estos servicios que tienen los sectores más cercanos a la tecnología y de los clientes concretos que ya están trabajando con servicios en la Nube.

Las expectativas de los usuarios son más elevadas en los sectores menos tecnológicos

REQUISITOS EXIGIDOS POR LOS USUARIOS

El estudio detecta una disminución leve pero generalizada en los requisitos exigidos a los CSP. El nivel de exigencia sigue siendo alto, pero algo menos que el año pasado.

Los requisitos de mayor exigencia siguen siendo de tipo técnicos (controles de seguridad del CSP y requisitos de continuidad de negocio), mientras que los de menor exigencia no llegan a un nivel de exigencia alto en el requisito, y corresponde con la transferencia de riesgo entre cliente y CSP, la conveniencia de contratación directa de los servicios o a través de un intermediario, el derecho de auditoria o las certificaciones de seguridad obtenidas por el CSP. El único requisito que aumenta en su exigencia es el control sobre los privilegios de acceso del personal del CSP para acceder a los sistemas o a la información, volviendo a los niveles de 2015. Por otra parte, también destaca la reducción en la exigencia en los requisitos de portabilidad (servicio, datos), quedando al casi muy alto nivel de exigencia que tiene el cumplimiento legal o los Acuerdos de Nivel de Servicio.



La exigencia de los usuarios en casi todos los requisitos analizados se valora como de nivel alto y solo algunos casos lo son a un nivel ligeramente menor. Esta situación se mantiene desde los estudios anteriores. De hecho, una revisión histórica de todos los posibles nuevos requisitos analizados en sucesivos estudios demuestra que no se han identificado nuevos requisitos de alta importancia, lo que indica que los requisitos que se están analizando son efectivamente los más relevantes. También se mantiene la relevancia relativa entre los requisitos: así la continuidad de negocio, los controles de seguridad del proveedor, la posibilidad de migración de datos, el cumplimiento legal, la relevancia de los SLAs y su cumplimiento, y las medidas de seguridad sobre el personal del proveedor aparecen de forma recurrente como los requisitos más importantes.

Los requisitos exigidos con más intensidad siguen siendo los relativos a continuidad de negocio, controles de seguridad, locked-in y cumplimiento legal y de los SLAs.

No se observan grandes diferencias en la exigencia de requisitos según la tecnología de Nube utilizada o el tamaño de la organización por facturación o por número de empleados de las organizaciones, diferencia que si se aprecia en la ubicación geográfica del CSP, que los sectores de Administración pública (4,21) y financieros (4,08) valoran con mayor exigencia.

La próxima entrada en vigor el 25 de mayo de 2018 del Reglamento General de Protección de Datos 2016/679 (GDPR) está siendo uno de los temas que más atención despierta en el mercado. El estudio ha abordado específicamente este interés en GDPR, detectando varios aspectos de interés.

• Los usuarios que utilizan todas las tecnologías de Nube (IaaS+PaaS+SaaS) son los que más importancia dan a este requisito (4,30 sobre 5), seguido de los que utilizan SaaS y PaaS (4,23). Los usuarios que utilizan sólo IaaS son los que menos importancia le otorgan (4,11 sobre 5)

• El requisito de cumplimiento de GDPR es mayor en los sectores de administración pública (4,54 de media) , seguido de los sectores servicios (4,37) y financiero (4.22)

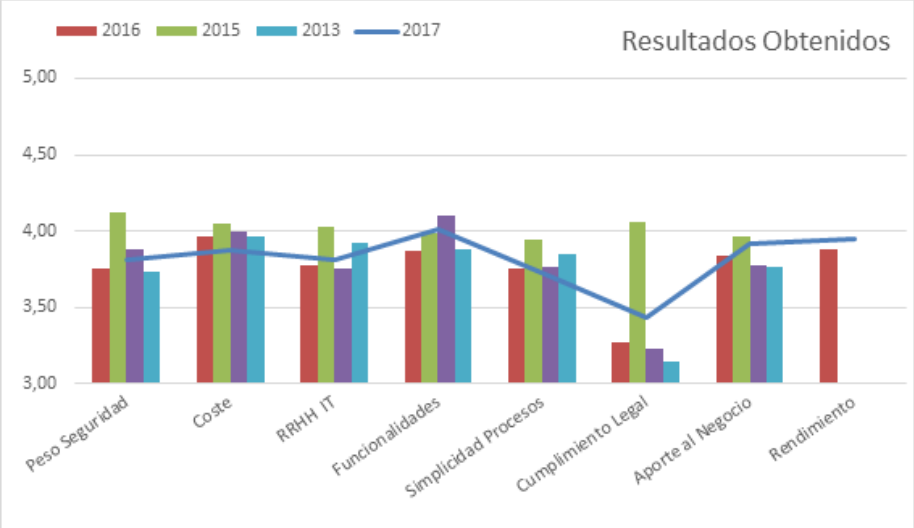
• En un análisis por geografías, el interés por este requisito es más elevado en los países en los que GDPR es parte de su regulación local (España, que lo valora con 4,56 puntos sobre 5), al nivel de los requisitos más exigentes en general. El valor medio en el resto de geografías se reduce significativamente (3,96 sobre 5), al nivel de los requisitos menos exigentes. Una diferencia originada claramente por la incorporación directa de GDPR a la legislación local y la difusión inmediata de esta legislación.

	GDPR
total	4,22
ES	4,56
resto	3,96

La exigencia de requisitos de privacidad en Europa sube al máximo nivel por la prevista entrada en vigor de GDPR

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

El estudio no ha identificado cambios de relevancia en las tendencias previamente identificadas en anteriores estudios respecto de la satisfacción de los usuarios de servicios en la Nube con los servicios que efectivamente reciben.



El estudio sí identifica una mayor satisfacción de los participantes con los servicios en la Nube recibidos respecto de la declarada en 2016. En particular, la satisfacción es menor con el coste de los servicios y es comparable a los resultados del año 2016 respecto de la simplicidad de los procesos. En una comparación histórica, y excluyendo los datos de 2015, la satisfacción en 2017 con los servicios recibidos está en los valores máximos de la serie en todos los casos.

Es destacable en todo caso que la satisfacción de los usuarios con respecto del cumplimiento legal sigue siendo significativamente menor. Si bien la satisfacción declarada en este año aumenta claramente frente a la declarada en años anteriores, sigue siendo claramente menor que en el resto de los parámetros. En este punto, el estudio concluye que las garantías ofrecidas por los CSP para asegurar el cumplimiento legal siguen no pareciendo suficientes a los clientes de la Nube

Los clientes están algo más satisfechos con los servicios en la Nube, con necesidad de mejorar más en el futuro en Cumplimiento Legal.

La edición de este estudio 2017 analiza de nuevo la satisfacción de los usuarios de la Nube con el rendimiento de estos servicios. Si ya en 2016 se identificó que los usuarios estaban satisfechos con el rendimiento, este aspecto mejora significativamente en esta edición del estudio, posicionando el rendimiento de los servicios como uno de los dos aspectos más satisfactorios para los usuarios, al nivel de la obtención a través de los servicios en la Nube de nuevas funcionalidades

Como conclusión general sobre la satisfacción de los usuarios de los servicios en la Nube, indicar que aparentemente están satisfechos con estos servicios, sin que exista ningún elemento destacado o decisivo para esta satisfacción, y a pesar de las dificultades en materia de cumplimiento legal.

Si se realiza un análisis por sectores de la satisfacción obtenida, puede establecerse conclusiones de mucho interés. Para ello, un análisis de los valores obtenidos para cada una de las mejoras evaluadas en cada uno de los sectores, que muestre en rojo los valores absolutos más bajos, y en verde los más altos, ofrece conclusiones interesantes:

	Mej.Rend	Mej.Coste	Mej.RRHH	Mej.func	Mej.Simpli	Mej.Compl	Mej.NivSeg	Mej.Satis	Mej.ImpSeg	Mej.Neg
Total	3,95	3,88	3,81	4,01	3,73	3,43	3,68	3,93	3,82	3,92
Adm	4,00	3,90	3,87	3,95	3,70	3,53	3,76	3,91	3,90	3,84
telco	4,05	4,09	3,84	4,11	3,89	3,51	3,74	4,07	3,70	4,00
Cons	4,20	4,03	4,00	4,23	4,07	3,71	3,93	4,17	4,20	4,31
finanza	4,00	4,00	3,67	3,94	3,76	3,11	3,67	3,88	3,76	3,88
Resto	3,76	3,71	3,74	3,94	3,55	3,38	3,55	3,77	3,74	3,78

En primer lugar, los sectores más cercanos a la tecnología (consultoría en particular, pero también telco) muestran una mayor satisfacción con los servicios en la Nube que reciben que el resto de sectores. Sobre el valor medio de satisfacción de cada característica, los participantes en el estudio que pertenecen a este sector declaran tener una satisfacción de al menos 0,2 puntos sobre 5 sobre la satisfacción media obtenida en el estudio. Por su parte, los participantes del sector Telco declaran en todos los casos una satisfacción superior a la media, si bien la diferencia es menos amplia.

Los sectores más tecnológicos se declaran más satisfechos con los servicios en la Nube que están consumiendo.

Respecto de los aspectos menos satisfactorios detectados, y siendo en todos los casos el cumplimiento legal el aspecto evaluado como menos satisfactorio, son las entidades financieras quienes encuentran en un entorno de Nube las mayores dificultades para cumplir con las regulaciones que les son aplicables y para soportar sus necesidades de cumplimiento legal. El estudio no dispone de mayor información para analizar los motivos concretos de esta situación, si bien es cierto que las entidades bancarias están sujetas de forma histórica a un mayor número de regulaciones y controles.

	Mej.Rend	Mej.Coste	Mej.RRHH	Mej.func	Mej.Simpli	Mej.Compl	Mej.NivSeg	Mej.Satis	Mej.ImpSeg	Mej.Neg
SaaS	3,95	3,84	3,81	4,04	3,74	3,42	3,65	3,93	3,77	3,92
PaaS	4,04	3,94	3,77	4,16	3,73	3,40	3,61	4,05	3,96	4,09
IaaS	4,03	3,85	3,78	4,03	3,69	3,41	3,69	4,08	3,84	4,05
XaaS	3,83	3,86	3,73	3,67	3,55	3,39	3,65	3,73	3,64	3,64

Respecto de la satisfacción de los usuarios con los distintos modelos de servicios en la nube, esta está en relación con la estabilidad y madurez de los mismos. Así los modelos clásicos (SaaS, PaaS, Iaas) resultan más satisfactorios que los demás modelos de prestación de servicio (denominados genéricamente como XaaS y que pueden incluir cualquier otro modelo de servicio en la Nube), en particular en la satisfacción obtenida con las mejoras de negocio, de los controles de seguridad o la satisfacción general con el servicio.

	Mej.Rend	Mej.Coste	Mej.RRHH	Mej.func	Mej.Simpli	Mej.Compl	Mej.NivSeg	Mej.Satis	Mej.ImpSeg	Mej.Neg
Publica	4,01	3,87	3,85	4,05	3,82	3,45	3,71	3,99	3,84	3,95
Privada	3,85	3,71	3,67	3,94	3,61	3,26	3,54	3,87	3,64	3,87
Híbrida	3,95	3,85	3,69	4,03	3,58	3,44	3,75	3,94	3,74	4,00
Comun	3,93	3,47	3,62	4,00	3,38	2,77	2,94	3,50	3,33	3,73

Respecto de los modelos de Nube usado para la prestación de servicios, , la satisfacción de los usuarios de servicios en nube privada resulta ligeramente menor que la de los usuarios de servicios en nube pública o híbrida. En todo caso, son los servicios sobre nube comunitaria los menos satisfactorios, en particular en términos de cumplimiento legal o de niveles de seguridad obtenidos.

Los servicios en la Nube resultan más satisfactorios cuando son servicios más estables, estandarizados y con mayor permanencia en el mercado

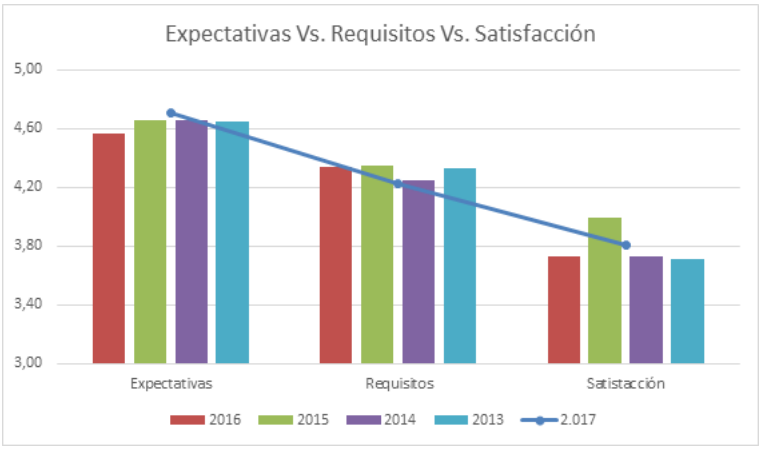
EVOLUCIÓN EXPECTATIVAS VS REQUISITOS VS RESULTADOS

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 no experimenta cambios significativos sobre los resultados obtenidos en estudios anteriores. Si bien es cierto, que tanto las expectativas aumentan levemente sus niveles de exigencia, como que los clientes de los servicios en la Nube están algo más satisfechos con los servicios, como que la exigencia de los requisitos solicitados se relaja algo, sin embargo no se identifican tendencias relevantes en estos cambios.

En ese sentido, el estudio concluye que las exigencias de los clientes son marcadamente más altas que las cualidades o características percibidas de los servicios que ofrecen los proveedores de servicios en la Nube. Así, las muy altas expectativas de los clientes de los servicios en la Nube están claramente por encima del algo más que alto grado de exigencia en los requisitos que los clientes solicitan a los proveedores de los servicios, y del nivel de satisfacción medio-alto con los servicios recibidos.

Por ello, el estudio plantea que el mercado de servicios en la nube necesita seguir mejorando los servicios que proporciona a sus clientes. Eventualmente, el mercado debería encontrar una situación más equilibrada, en la que los proveedores estuvieran proporcionando servicios a la altura de las expectativas de sus clientes, o al menos a la altura de los requisitos que exigen de dichos servicios.

La satisfacción de los usuarios de los servicios en Nube sigue siendo inferior a sus expectativas, y a los requisitos que solicitan a los CSPs.



Los servicios en la Nube 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.

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.

En este ámbito, el primer aspecto destacado por el estudio es que ningún participante asume que Shadow IT sea indetectable.

Más de la mitad de los participantes consideran que ShadowIT es un fenómeno cierto en las organizaciones. Si bien en 2016 (círculo interior) este porcentaje era aun mayor y llegaba a las dos terceras partes de los participantes, ha cambiado el grado de certeza en la afirmación: los que lo consideran simplemente probable pasan del 33% al 9%, mientras que los que piensan que es un fenómeno generalizado suben al 14% desde el 5%, y los que consideran que es un fenómeno puntual aumentan levemente del 29% al 33%; claramente el estudio apunta a una preponderancia en la identificación de existencia de servicios prestados de forma directa por un CSP.

Los participantes que consideran que ShadowIT no está ocurriendo aumentan, en particular aquellos que sostienen que ShadowIT no está ocurriendo porque los servicios son prestados desde el Departamento de TI, que crecen del 9% al 25%.

Por ello, el estudio concluye que Shadow IT es una realidad mejor conocida por las organizaciones y que probablemente se estén dando pasos para que el ShadowIT pase a ser IT, prestada por IT como el resto de servicios.

Shadow IT es una realidad mejor conocida por las organizaciones, que puede ser detectada y debe ser integrada entre los Servicios de IT.

Analizando las razones que podrían justificar la ocurrencia de ShadowIT, el estudio detecta en 2017 una disminución relevante de las causas aducidas para justificar el uso de ShadowIT. En la edición de 2016 del estudio cada participante aportaba un promedio de 2 razones para justificar el uso de ShadowIT. En este edición de 2017 y de forma alineada con el mayor porcentaje de participantes que consideran que ShadowIT no ocurre o no debería ocurrir en sus organizaciones, desciende este valor y se aportan como 1,5 razones por participante como promedio.

Analizando factores evaluados y las aportaciones de los participantes,

• la calidad de la provisión de servicios del Departamento de TI está detrás de las posibles razones para justificar ShadowIT, bien sea porque ShadowIT proporciona servicios de forma más ágil (lo dice un 33% de los participantes aunque en 2016 lo afirmaba un 46%), con mayor libertad en la selección de servicios (un 17% frente a un 25% en 2016) y/o con mejor calidad de servicio (también un 16% frente al 22% de 2016).

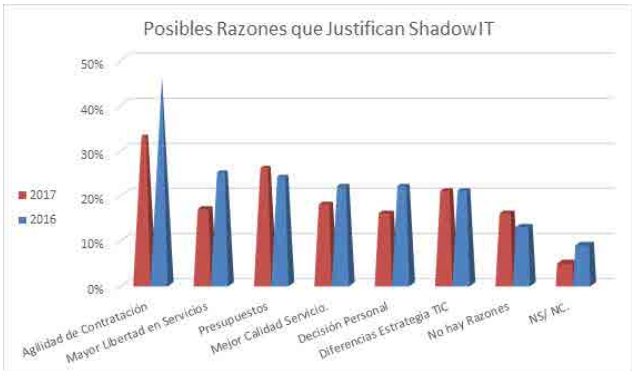
• Frente a ello, las razones presupuestarias son el único factor que se señala con mayor frecuencia en 2017 que

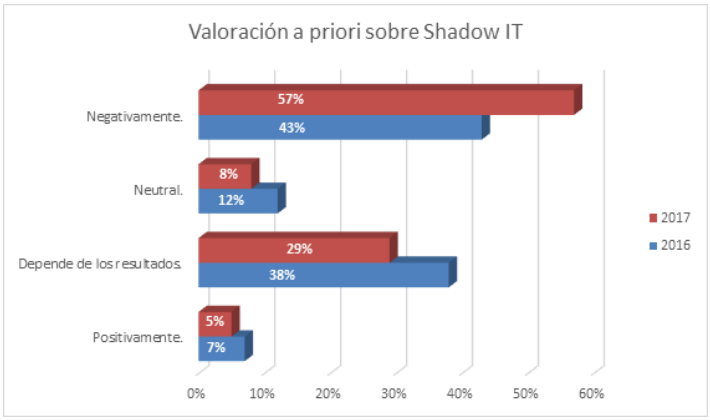
en 2016 y en ambos casos como segunda razón (un 26% en 2017 frente a un 22% en 2016).

• Las causas debidas a la insuficiente coordinación del Departamento de TI y otras áreas de la organización son seleccionadas por uno de cada cinco participantes: resulta preocupante que se repita el 21% de participantes que señalan discrepancias en la estrategia TI de sus organizaciones, o que uno de cada seis señale la decisión personal del usuario del servicio Shadow como motivo para adoptar ShadowTI. Estos casos deberían generar reflexiones más generales en la organización sobre el diseño y la implantación de los Planes y Estrategias de la organización, puesto que aparentemente no siempre son suficientemente compartidos, o directamente pueden ser obviados.

• Por último, uno de cada seis participantes declara que no existen razones para justificar ShadowIT en las organizaciones. Si bien este porcentaje aumenta desde el 13% de 2016, sigue representando casi tres veces más que los usuarios que declaraban que ShadowIT estaba prohibido, y la mitad de los que declaran que estas actividades deben ser ejecutadas por el Departamento TI, sin que se hayan identificado más relación entre estas respuestas.

De todo ello, el estudio detecta un equilibrio entre las razones que prospectan una adecuada interacción del Dcepartamento TI y por el otro las razones que expresan desacuerdos con dicho Departamento.

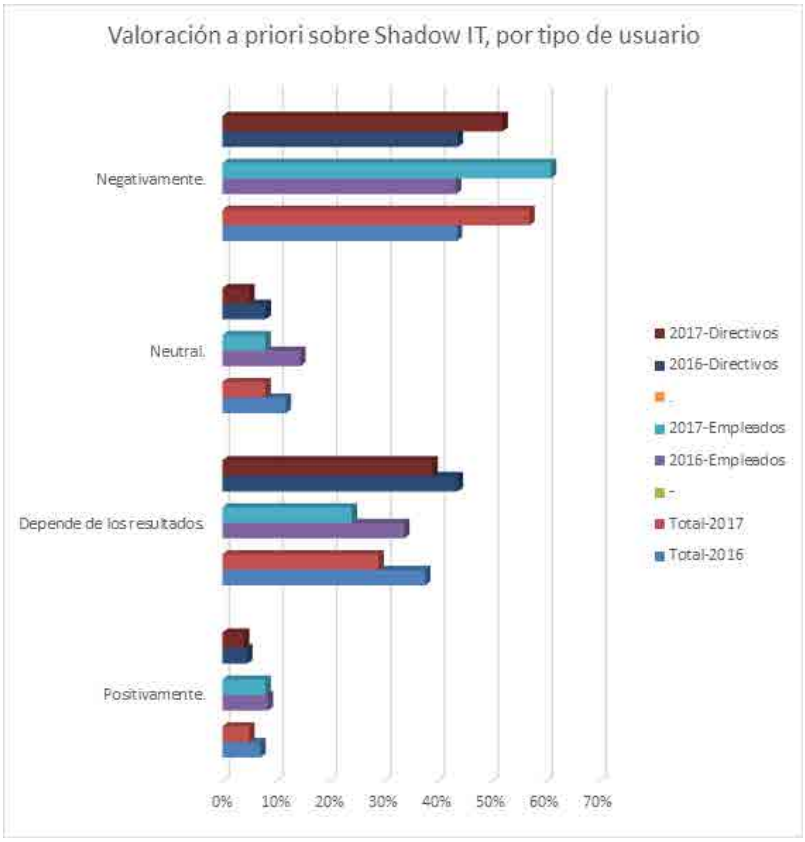




Por último, la visión que se tiene sobre el fenómeno ShadowIT es crecientemente negativa, a pesar de las numerosas razones aducidas anteriormente. La consideración de ShadowIT como una circunstancia negativa crece claramente, de forma que más de la mitad de los participantes comparten esta visión, mientras que se reducen el apoyo por los participantes a todas las demás opciones. En particular, una cuarta parte de los participantes que condicionaban su visión a los resultados obtenidos ya no mantienen esta posición.

El estudio también analiza estos datos en relación de la función en la organización del participante en la encuesta. El estudio de 2016 detectó diferentes respuestas según la función en la organización de los participantes, con las funciones directivas menos receptivas ante el fenómeno ShadowIT y las posibilidades de que efectivamente estuviese ocurriendo, mientras que las funciones más operativas afirmando que sí que está ocurriendo y con una visión más positiva sobre el fenómeno. La situación en 2017 cambia significativamente. Los estamentos directivos se posicionan claramente en el rechazo a ShadowIT, o dando oportunidades para esperar resultados, mientras que los empleados rechazan de forma más nítida ShadowIT, reduciéndose el apoyo al resto de opciones.

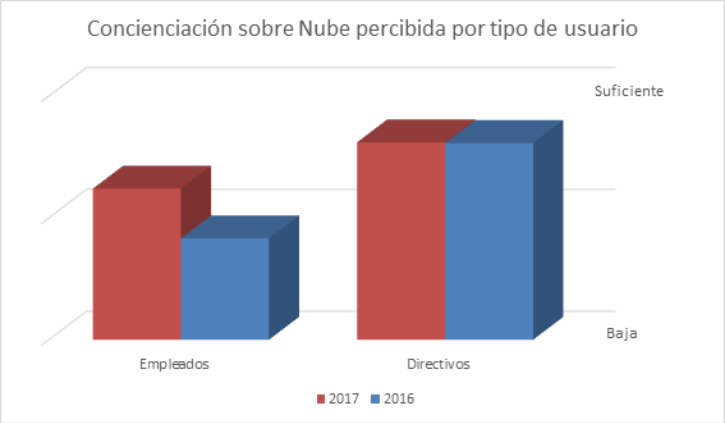
La existencia de Shadow IT en las organizaciones es vista crecientemente como un aspecto negativo en las organizaciones.



ESTADO DE CONCIENCIACIÓN EN SEGURIDAD DE LOS USUARIOS

El estudio en 2017 repite el análisis iniciado en 2016 sobre el grado de concienciación de las organizaciones respecto de los servicios prestados desde la Nube.

El estudio detecta una situación similar a la encontrada en el estudio anterior. El grado de concienciación sigue siendo insuficiente en todos los estamentos, si bien se puede detectar durante este año una mejora clara en la concienciación por parte de los empleados, frente a una situación estable por parte de los Directivos.



Analizando estos datos de forma más detallada y con la perspectiva de años anteriores, el estudio detecta que no existen movimientos significativos entre las distintas categorías de usuario que permitan identificar los motivos o movimientos de fondo para las mejoras obtenidas.

La ausencia de cambios más significativos en la concienciación percibida por el personal contrasta con la abundancia de noticias de impacto en medios de comunicación sobre incidentes de seguridad, que han aumentado de facto la concienciación de las organizaciones en seguridad. Estos incidentes han afectado tanto a estamentos directivos de las organizaciones (Equifax), como al total de los empleados (Wannacry). La expectativa a priori del equipo de analistas apuntaba a un incremento en la concienciación a todos los niveles, que ya se está detectando y produciendo en el mercado. Posiblemente, este impacto que se ha centrado en áreas de cyberseguridad no se haya trasladado aun a la seguridad en la Nube. Y, por otro lado, puede haber aumentado la preocupación de directivos y empleados de las organizaciones sobre la seguridad, de forma que niveles anteriormente evaluados como suficientes, ahora fuesen evaluados como bajos.

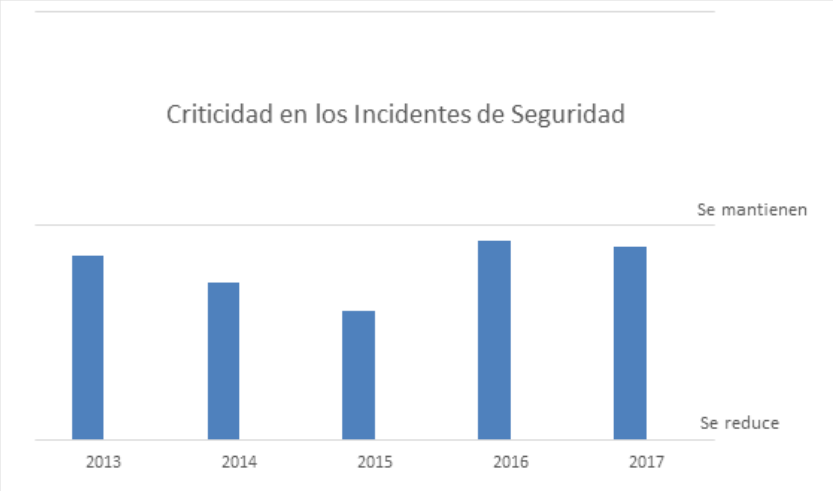
Las Organizaciones siguen viéndose como insuficientemente concienciadas sobre los riesgos de seguridad en los Servicios en la Nube.

El estudio también ha analizado el proceso de toma de decisiones en las organizaciones sobre los riesgos de los servicios en la Nube. NO se han extractado conclusiones relevantes sobre esta acción.

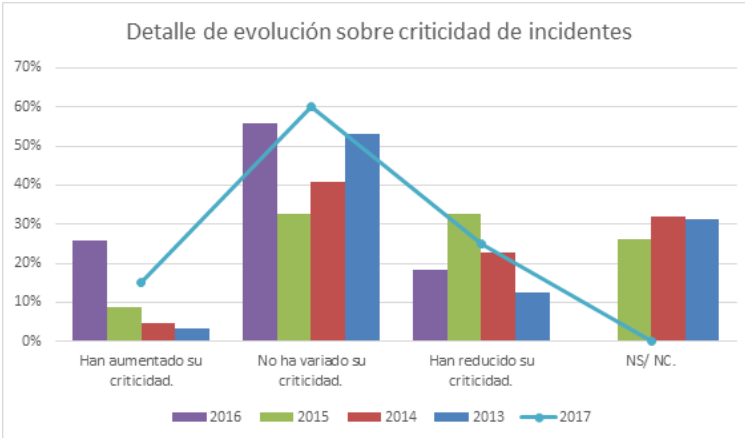
EVOLUCIÓN DE LOS INCIDENTES DE SEGURIDAD EN SERVICIOS EN LA NUBE

Este V 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 y criticidad de los incidentes de seguridad, se han analizado las variaciones en los recursos dedicados a la gestión de incidentes, y en la capacidad de detección de incidentes de seguridad: Estos dos aspectos son recurrentemente señalados por los CSPs como mejoras derivadas de la adopción de sus servicios, y se identificó el interés en su análisis para conocer cómo esta afirmación era recibida por los usuarios de los servicios en la Nube.

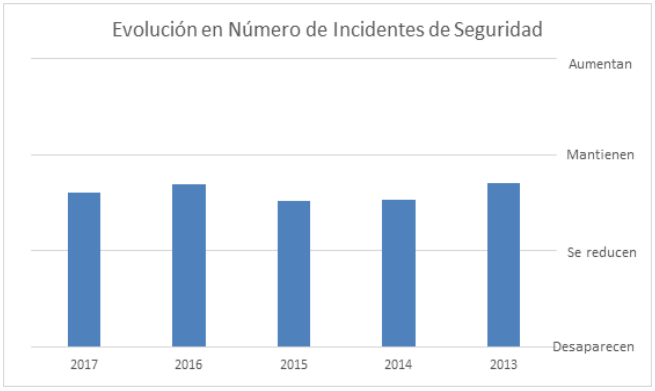
En primer lugar, al analizar de forma histórica la evolución de la criticidad de los incidentes de seguridad tras la migración a servicios en la Nube podemos observar que esta migración supone una reducción en la criticidad de los incidentes, y en particular, una reducción en el último periodo estudiado.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

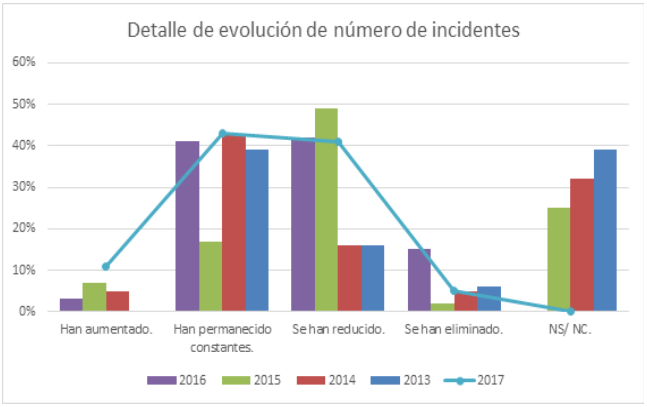


Analizando las opiniones particulares, tres de cada cinco usuarios opinan que no ha habido cambios en la criticidad de las incidencias detectadas, por lo que el descenso en la criticidad se basa en los usuarios que valoran los incidentes como menos críticos (uno de cada cuatro), que los que los valoran que son más críticos (uno de cada seis). Esta posición invierte la que se había detectado por primera vez en 2016, que señalaba por primera vez una mayoría de usuarios que identificaban un incremento en la criticidad de los incidentes.



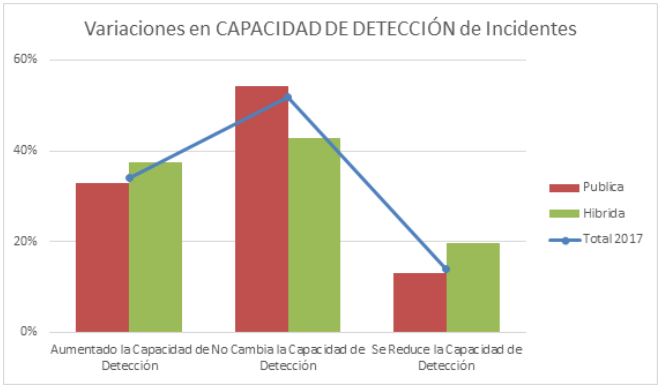
Al analizar el número de incidentes detectados que perciben los usuarios, el estudio sigue concluyendo que el uso de servicios en la Nube conlleva en general una reducción del número de incidentes de seguridad, reducción no achacable a una falta de compromiso del CSP respecto de la notificación de incidentes. Es una tendencia que se sostiene a lo largo de los sucesivos estudios, si bien en este año se es algo menos optimista sobre esta reducción que en años anteriores.





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

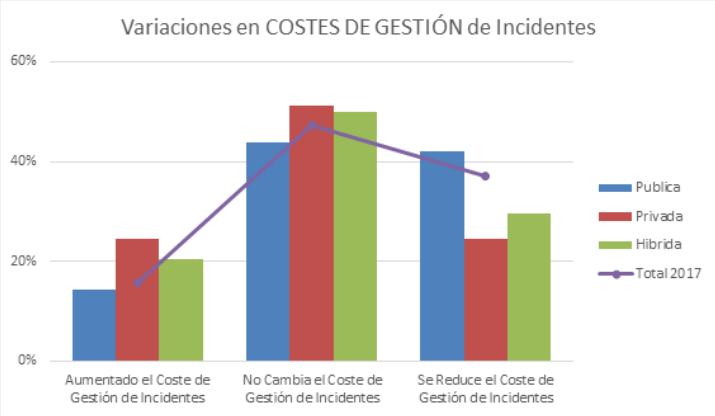
En todo caso, el análisis en el número de incidentes de seguridad, aun siendo revelador, plantea una duda. ¿Es la variación en el número de incidentes consecuencia exclusiva del cambio de modelo de servicios, o se debe al cambio en las capacidades de detección de incidentes de que se dispone por el cambio a servicios en la Nube? Los resultados expresados por los participantes en la materia son positivos, en tanto que se reporta un aumento de la capacidad de detección por uno de cada tres usuarios.



Este aumento en la capacidad de detección no sigue ninguna tendencia diferenciada. Los resultados son equivalentes independientemente del tamaño de la compañía, ubicación geográfica o tecnologías de Nube utilizadas (XaaS). En particular, al analizar este resultado en base al modelo de servicio (Nube Pública, Privada, …) no se aprecian diferencias relevantes en este parámetro entre la situación general o la que corresponde a cada uno de estos modelos de servicio. Este resultado ha contradicho las expectativas previas del equipo de analistas, en tanto que la Nube Pública o Híbrida deberían ofrecer una mejora más significativa por estar apoyándose de forma más intensa en los recursos de un CSP que en el caso de nubes Privadas o Comunitarias, cuando en realidad, la mejora es apreciable en todos los casos.

El uso de servicios en la Nube permite aumentar levemente las capacidades de detección de incidentes, y reducir algo los recursos dedicados a su gestión.

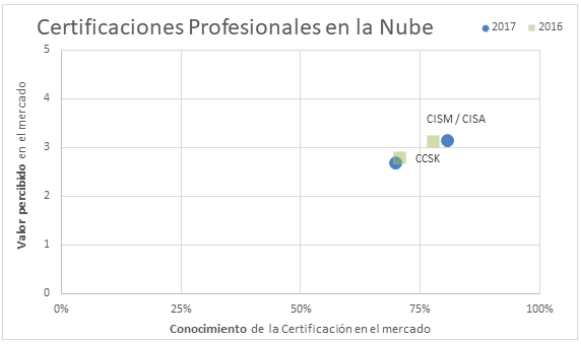
Por último, se ha analizado como varían los costes en las organizaciones derivados de la gestión de incidentes con el uso de servicios en la Nube. Como valoración general, La mayoría de los encuestados respondieron que siguen dedicando el mismo volumen de recursos de la organización para la gestión de incidentes que el estudio anterior y un grupo del 10 a 15 % cree que se necesita dedicar más recursos de su organización en esa tarea.



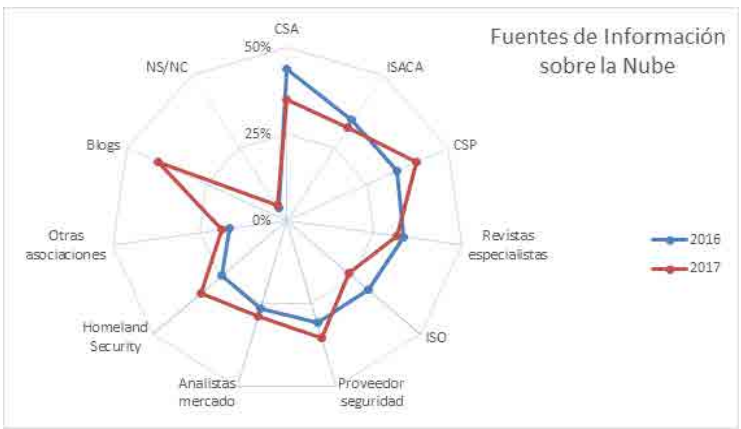
Analizando más en detalle estos resultados, de nuevo esta mejora es independiente de geografías, tamaño de la organización u otros parámetros. Salvo en una situación: A efectos de reducción de costes en gestión de incidentes, la nube pública o híbrida SÍ ofrecen mejoras para los usuarios de los servicios en Nube.

FORMACIÓN E INFORMACIÓN DE PROFESIONALES

El estudio analiza también el grado de conocimiento en el mercado y el valor que aportan a los profesionales algunas certificaciones existentes. Todas las certificaciones identificadas tienen un nivel de reconocimiento alto en todos los casos, con ligeras variaciones en su reconocimiento y grado de utilidad (ligeramente mayor en el caso de CISA o CISM frente a CCSK). Sin embargo, el conocimiento en el mercado de estas certificaciones es aun mejorable, dado que al menos el 20% de los participantes no se posiciona sobre el valor de estas certificaciones por resultarles desconocida.

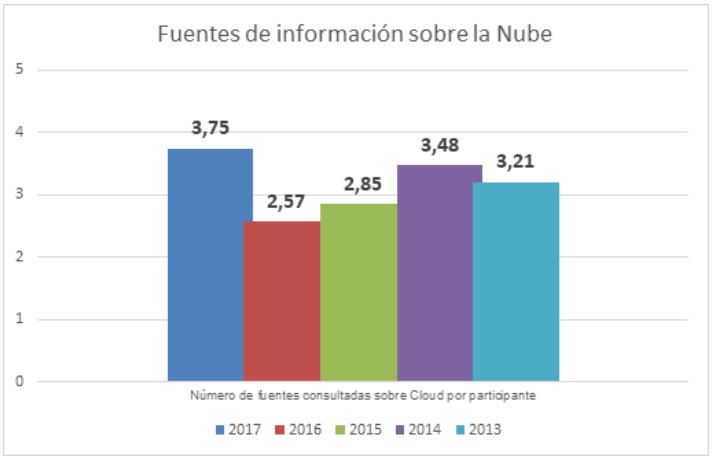


Por otra parte, el estudio ha identificado que 74% de los encuestados determina que la información sobre la Nube tiene una disponibilidad alta o muy alta, mientras que menos del 10% considera que sea baja o muy baja. La fuente de información más consultada son los Blogs de Seguridad o de Cloud, luego la información facilitada por los propios los Proveedores de servicios Cloud (CSP) seguido de la información facilitada por CSA en la cuarta posición.



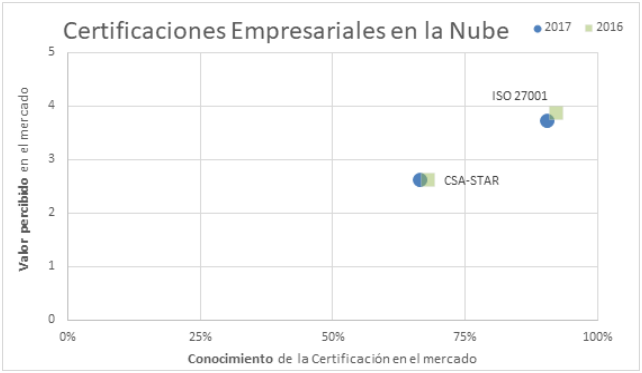
Los datos anteriores se confirman porque, de acuerdo con los resultados de la encuesta, cada persona encuestada consulta entre 3 y 4 fuentes distintas para informarse sobre los servicios en la Nube y esa tendencia muestra un crecimiento en el interés sobre la seguridad sobre la nube.

Los blogs especializados aparecen como la más consultada de las 4 fuentes de información como media que consultan los usuarios de servicios en la Nube.

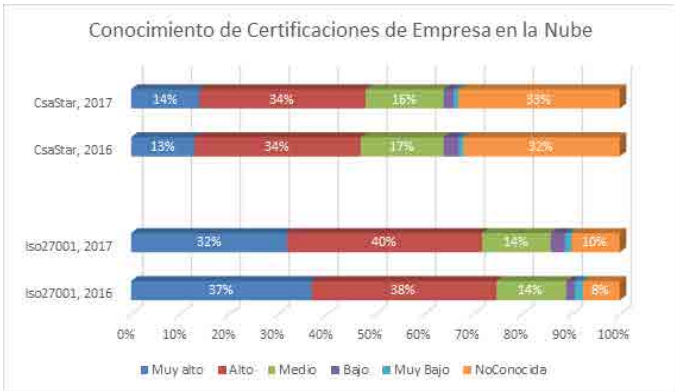


CERTIFICACIÓN DE SERVICIOS OFRECIDOS POR LOS CSP

El estudio ha detectado que la certificación ISO27001 tiene mayor relevancia para los usuarios de los servicios en la Nube, siendo considerada como de utilidad alta. Por su parte, el valor percibido por para la certificación CSA-Star es menor, quedándose en una utilidad media.



Esta situación está en relación directa con el grado de reconocimiento en el mercado que tienen cada una de las certificaciones: ISO 27001 es conocida prácticamente por la totalidad de los encuestados, mientras que la certificación CSA-Star resulta desconocida para una tercera parte de los participantes.



El estudio también ha detectado que tanto el conocimiento de estos esquemas de certificación de proveedores de servicios en la Nube, como el grado de utilidad, como el desglose de la visión sobre este tema por los participantes en la encuesta no experimenta apenas cambios desde el estudio anterior.

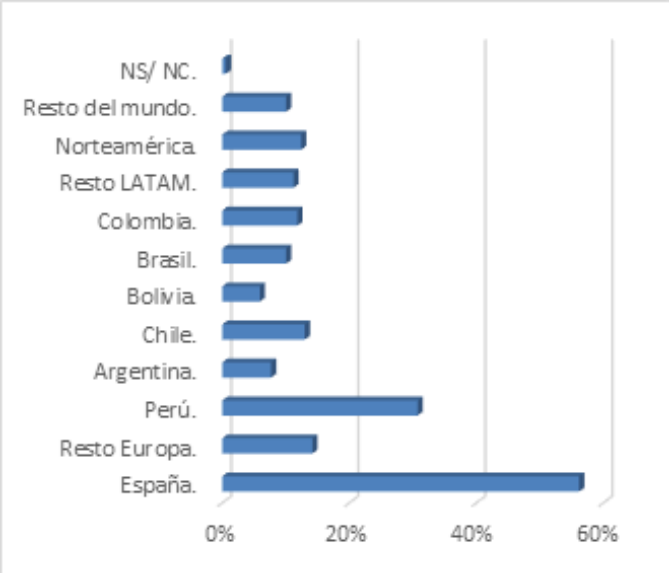
Las certificaciones de seguridad de los servicios en la Nube para profesionales y organizaciones no experimentan cambios.

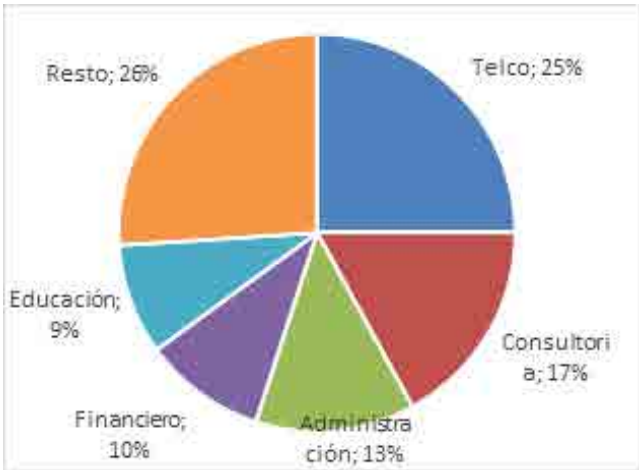
FICHA TÉCNICA DEL ESTUDIO

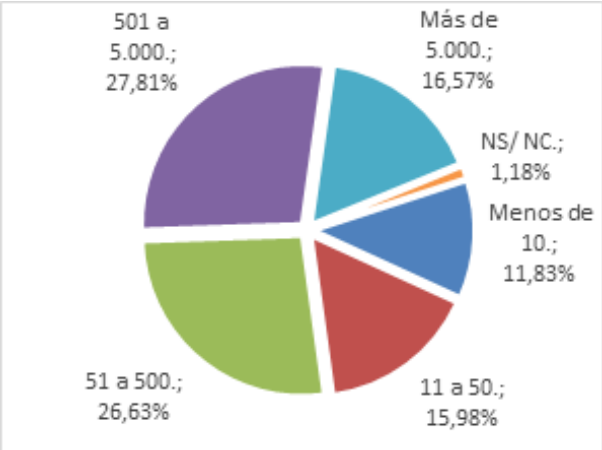
Los resultados del análisis y el diseño del estudio ha sido realizado por los profesionales que figuran en la portada del documento, que forman parte de los Capítulos Español, Peruano, Argentino, Chileno, Boliviano, Brasileño y Colombiano de CSA y del Capítulo de Madrid de ISACA, en colaboración con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

El estudio se ha realizado en base a encuestas recopiladas entre el 5 y el 28 de septiembre de 2017, a través de la plataforma online SurveyMonkey. Se recopilaron un total de 273 respuestas de profesionales y organizaciones.

Con respecto a la distribución de las respuestas por geografía, en la edición 2017 hay que destacar la amplia 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, financiero o educación. Las organizaciones participantes en el estudio cubren de forma equilibrada el total del espectro de tamaños de organizaciones.