Estudio del Estado del Arte de la Seguridad en la Nube

Iniciativa de

CSA ES cloud security alliance SM SPAIN

CSA PE cloud security alliance SM PERU

CSA cloud security alliance SM ARGENTINA CHAPTER

ISACA Sistemas de información fiables y valiosos Madrid Chapter

ISACA Confianza y valor en los sistemas de información Lima Chapter

En colaboración con

isms forum spain

Estudio del Estado del Arte de la Seguridad en la Nube 2016

Estudio elaborado con la colaboración de los siguientes profesionales y organizaciones:

Coordinadores
Mariano J. Benito (GMV), CSA-España Manuel Caldas (Independiente), CSA-Perú Julio César Balderrama (Independiente), CSA-Argentina Antonio Ramos (Vicepresidente), ISACA-Madrid Daniel García (ISMS Forum)

Analistas	Analistas
Aldo Carlessi (ATMOSPHERA	Juan García Galera (CEMI-Ayuntamiento de Málaga)
Alejandro del Río (Aubay)	Omar Crespo (CA), CSA-PE
Daniel Zapico (Grupo SIA)	Rafael Antonio Vasquez Sanchez (Montana), CSA-PE
Enrique Aristi (Grupo UCI)	Rafael Navajo (GMV)
Grupo de Trabajo Cloud Computing, ISACA-Madrid.	Walter Cabanillas (IBM), CSA-PE
Jorge Antonio Rojas Arévalo (Independiente)	

Índice

Índice de Gráficas

Resumen ejecutivo

El IV Estudio del Estado del Arte de Seguridad en Cloud Computing, realizado en 2016 en cooperación entre los capítulos Español, Peruano y Argentino de Cloud Security Alliance, y los capítulos de Madrid y Lima de ISACA, continúa la serie de estudios realizados en 2013 y 2014 para España, y en 2015 para España y Perú.

El estudio **consolida** las tendencias identificadas en años anteriores respecto de las expectativas sobre la Nube, los requisitos que se exigen a estos servicios y la satisfacción final con los servicios recibidos. Así, las expectativas de seguridad sobre la Nube son muy altas (aunque con un leve descenso), y siguen siendo más altas que los requisitos que se piden (que se mantienen) y más altas aún que la satisfacción final de los usuarios de los servicios de Nube, que también se mantienen.

El estudio ha tomado foco específico sobre ShadowIT. Este fenómeno había producido datos quizás inconsistentes en ediciones anteriores del estudio, por lo que se ha abordado desde una óptica diferente. Desde este nuevo enfoque, se ha estimado que **ShadowIT está ocurriendo de forma amplia**, a pesar de que hay una opinión generalizada negativa sobre su idoneidad. La causa fundamental para el uso de ShadowIT sería la **mayor agilidad** en la prestación de servicios de la Nube frente a otros escenarios. La Dirección de las organizaciones desconfiaría de ShadowIT o consideran el fenómeno contrario a las políticas corporativas, mientras que otros estamentos de la organización ven ShadowIT como un fenómeno más normal.

Como nuevo elemento de interés en este IV Estudio, se ha investigado el grado de concienciación de seguridad sobre la Nube que tienen las organizaciones que usan estos servicios. El grado de **concienciación** se ha determinado **como bajo e insuficiente**, si bien este nivel es algo más elevado en los estamentos directivos que en los no directivos.

El estudio ha ampliado también los posibles requisitos exigibles a los proveedores de servicios en la Nube y puntos satisfactorios, sin que hayan surgido nuevos elementos que condicionen significativamente las decisiones en seguridad.

Respecto de la satisfacción de los usuarios de la Nube, el estudio ha establecido una relación inversa entre el nivel de **satisfacción** y el **tamaño de la organización** usuaria. Por otra parte, los usuarios menos satisfechos son los que requieren mayor grado de control y verificación de los servicios recibidos. Varios de estos usuarios insatisfechos son también las organizaciones que han participado en el estudio después de haber dejado de usar servicios en la Nube.

El estudio de los **incidentes** de seguridad en las organizaciones que utilizan servicios en la Nube ha revelado, por su parte, que las organizaciones de **menor tamaño sí se benefician** de un número menor de incidentes y de menor relevancia. Sin embargo, las organizaciones de más tamaño sufren de más incidentes, y de mayor criticidad cuando usan servicios en la Nube.

Respecto de la información disponible para los servicios en la Nube, esta se considera en general suficiente, consultando los usuarios de servicios en la Nube una media de entre 3 y 4 fuentes de información diferentes.

El estudio ha contado con la aportación de información de casi 150 empresas, con presencia en mayoritaria en los mercados de interés para el equipo de analistas, así como en otros mercados internacionales.

Objetivos y Ámbito del 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, peruano y argentino, ampliando el alcance a otros mercados en la medida en que las empresas participantes en el mismo han facilitado información sobre ellos. Esta decisión se origina en el interés de los respectivos capítulos de CSA y de los Capítulos de ISACA en Madrid y Lima, para tener un mejor conocimiento de sus mercados locales, y como base para extrapolar a otros mercados su situación de la seguridad en la Nube.

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, tanto a nivel Español y Peruano (alcance del estudio 2015[1]), como Español (alcance de los estudios de 2014[2] y 2013[3]).
- Particularidades específicas del estudio, analizando los datos específicos aplicables a ámbitos geográficos concretos, frente al análisis general del total de los datos.

[1] 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

[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] 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).

Conclusiones del Estudio

Como se ha mencionado anteriormente, el estudio se enfoca en el conocimiento del Estado del Arte en Seguridad Cloud, estructurado en cuatro ejes principales:

- Aspectos relacionados directamente con la prestación de servicios en la Nube: expectativas, los requisitos solicitados o la satisfacción final con los servicios recibidos.
- La concienciación de seguridad relativa a la Nube y los riesgos adicionales que implica.
- ShadowIT
- Otros elementos de interés asociados a los servicios en la Nube: Formación, certificación, disponibilidad de información, incidentes en la Nube, etc.

Disminución leve de las expectativas de los usuarios en la Nube

El estudio parte del reconocimiento de que los usuarios presentes o futuros de los servicios en la Nube parten de unas expectativas respecto de dichos servicios y de la seguridad que van a ofrecerse en estos servicios.

El estudio investiga en primer lugar los 5 factores sobre los que los usuarios pueden tener expectativas de seguridad (Ilustración 1), localizando que, en todos los casos, los usuarios siguen teniendo expectativas muy altas sobre los servicios en la Nube (4,5 puntos sobre 10), si bien los valores de las expectativas han descendido levemente, mostrando los valores más bajos de la serie histórica considerada.

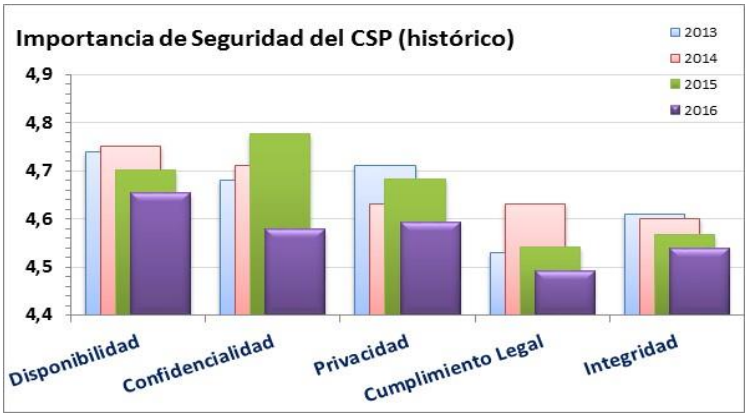

Ilustración 1.- Importancia de Seguridad del Proveedor (Global)

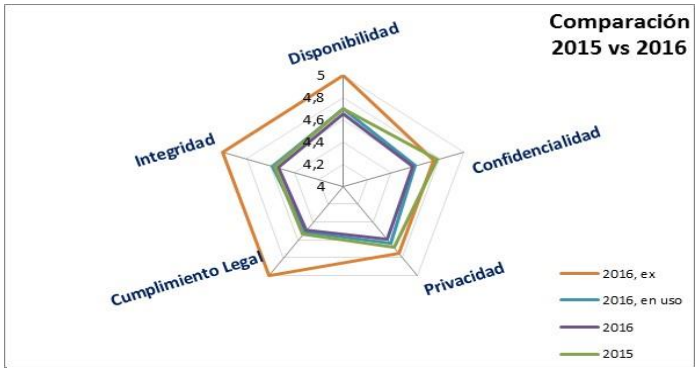

Ilustración 2.- Comparación expectativas 2015 vs 2016

El análisis más detallado de estos resultados (Ilustración 2) revela que las expectativas son ligeramente más altas para las organizaciones que ya son usuarios efectivos de los servicios de Nube, que para el total de participantes de la encuesta. En cualquier caso, ambos colectivos tienen expectativas menos elevadas que las que se tenían el año pasado.

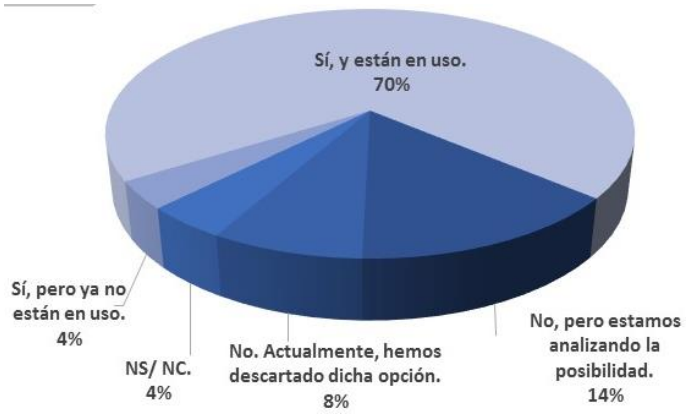

Ilustración 3.- Estado de Adopción de Servicio en la Nube

Por otra parte, el colectivo más exigente en sus expectativas sobre la Nube es precisamente el de usuarios de servicios en la Nube que la han abandonado, dejando de usar sus servicios. Este colectivo alcanza el 4% de los participantes en el estudio, también corresponde con el perfil de usuarios insatisfechos de la Ilustración 8. Remarcar que no todos los usuarios insatisfechos han dejado de usar los servicios en la Nube, ni todos los usuarios que han dejado de usar los servicios en la Nube corresponden al perfil de usuario insatisfecho. Pero si existe esa relación.

Conclusión #1. Leve disminución de las expectativas de los usuarios de la Nube, que aun así siguen siendo muy altas.

Conclusión #1.1. Los usuarios que han dejado la Nube son mucho más exigentes en sus expectativas que el resto de participantes.

Estabilización de requisitos para los Servicios en la Nube

Las expectativas anteriormente estudiadas han de traducirse en requisitos de seguridad que deberían ser satisfechos por los servicios en la Nube que los usuarios utilicen. En la presente edición del estudio se han analizado dos posibles requisitos adicionales a los ya analizados en años anteriores: la transferencia de riesgos entre usuarios y proveedores de Nube, y el impacto de la cadena de suministro en el proveedor de servicios en la Nube.

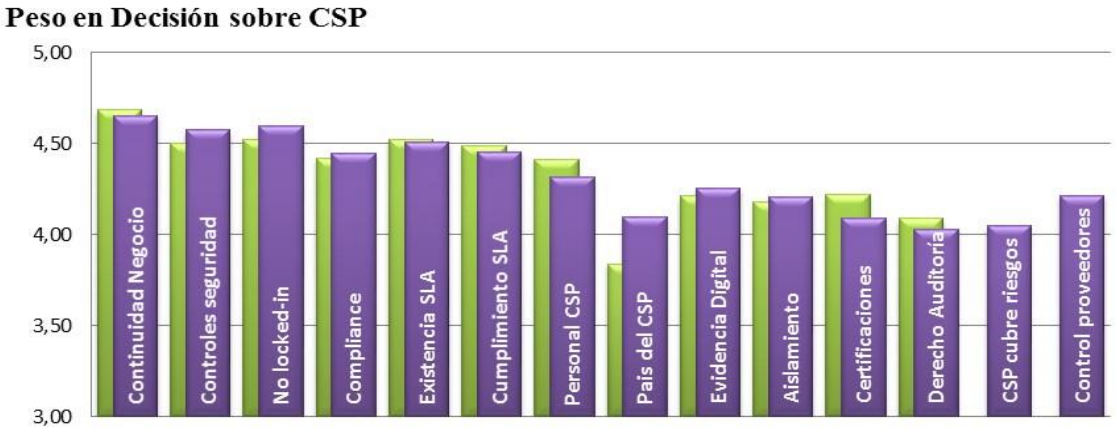

Ilustración 4.- Importancia de los diversos factores en la decisión sobre CSP.

El análisis de estos factores que se muestra en la Ilustración 4 ofrece escasas conclusiones relevantes, vista la estabilidad de todos ellos de forma individual y como conjunto, y las ligeras variaciones que se producen. El análisis más profundo de los datos, combinados con otros puntos de vista considerados (tipo de servicio, tamaño de empresa, etc), tampoco ofrece diferencias significativas.

Por ello, los requisitos más importantes siguen siendo (i) la Continuidad de Negocio del proveedor de servicios en la Nube, seguido de (ii) la no existencia de efecto lock-in[4], (iii) los controles de seguridad que implementa el proveedor, (iv) la existencia y cumplimiento de un SLA y (v) las garantías de cumplimiento legal por el proveedor y para el cliente. Destacar también que (a) los dos factores nuevos se ubican entre los requisitos menos relevantes, apuntando a que el estudio ya identificó los requisitos más considerados por los clientes; y (b) la ya citada estabilidad de los requisitos pedidos.

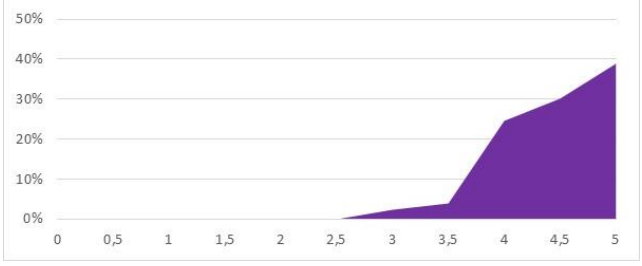

Ilustración 5.- Número Organizaciones por nivel de Requisitos

Si se analizan la distribución de las organizaciones que piden un determinado nivel medio de requisitos, puede verse que las organizaciones que no piden requisitos altos o muy altos son muy pocas (Ilustración 5). Son organizaciones del sector servicios, que utilizan únicamente servicios SaaS en Nubes Públicas y que finalmente quedan satisfechas a un nivel medio.

Conclusión #2. Estabilidad de los requisitos pedidos a los servicios en Nube, que siguen siendo altas o muy altos.
Conclusión #2.1. Las organizaciones que menos requisitos piden usan SaaS Públicas y obtienen una satisfacción también de nivel medio.
Conclusión #2.2. No han identificado nuevos requisitos exigibles a los servicios en la Nube, más relevantes que los ya identificados.

[4] https://en.wikipedia.org/wiki/Cloud_computing_issues#Vendor_lock-in

Estabilización de satisfacción con los Servicios en la Nube

Se analiza a continuación cual es la satisfacción que generan en los usuarios los servicios en Nube que se les prestan. Este análisis resulta de gran interés, en la medida en que esta satisfacción sirve como indicador general del resultado de todos los esfuerzos realizados por la organización para "subirse a la Nube" y la valoración sobre si fue un esfuerzo válido o no.
En este IV estudio, el análisis incorpora un elemento de satisfacción adicional, que es la aportación que los servicios en la Nube hacen al negocio.

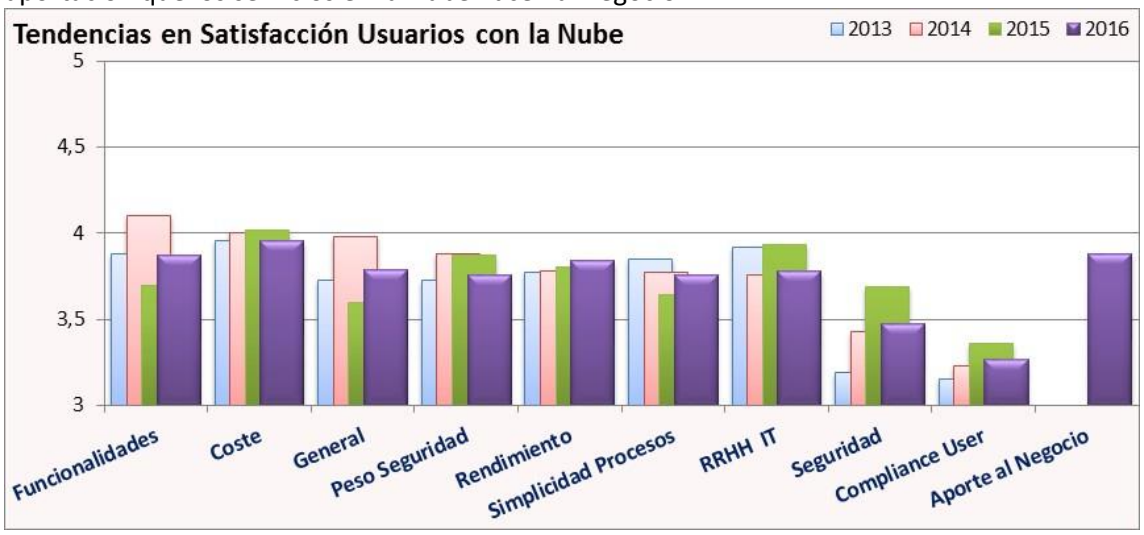

Ilustración 6.- Satisfacción de los usuarios de servicios en la Nube con distintos elementos

Se observan en la Ilustración 6 que los posibles elementos de satisfacción identificados no siguen un patrón común de evolución. Sí cabe destacar que el coste sigue siendo el elemento más satisfactorio de todos los considerados, y que el resto de elementos siguen estando ligeramente por detrás de él, salvo la satisfacción con los niveles de seguridad proporcionados y las facilidades dadas por el proveedor para el cumplimiento legal. Esos dos elementos están más cerca de un nivel de satisfacción medio, que el nivel de satisfacción casi alto en el que están los demás elementos.

Ilustración 7.- Nivel medio de satisfacción de las organizaciones vs tamaño

Señalar también que el nuevo elemento considerado ("Aporte al Negocio") queda encuadrado en ese segundo escalón dentro de los niveles de satisfacción que se ha identificado, por lo que se debe considerar como un elemento de satisfacción a considerar.
El análisis detallado de los parámetros de satisfacción identificados ofrece también información reveladora.

Así, el nivel de satisfacción de las diversas organizaciones está inversamente relacionado con el tamaño de la organización: las organizaciones de menor tamaño tienen un nivel de satisfacción mayor que las organizaciones de mayor tamaño, siendo la diferencia de 0,2 puntos sobre cinco

(Ilustración 7). Esta relación también se observa si se mide el tamaño de la empresa en función de su volumen de facturación.

Por otra parte, al contabilizar el número de organizaciones en los distintos niveles de satisfacción (Ilustración 8), puede detectarse un predominio del nivel alto de satisfacción, con una deriva hacia niveles medios, e incluso casos de satisfacción baja. El análisis de estos casos, permite caracterizar estos usuarios de servicios en la Nube que están menos satisfechos: son usuarios que exigen una verificación más tangible y de primera mano sobre el estado de sus servicios (reclaman más con más intensidad requisitos sobre ubicación de los datos, su aislamiento, generación de evidencias, derecho a auditar y SLAs de servicios; y valoran con menor intensidad certificaciones, controles de seguridad). Usan por encima de la media de aplicaciones de negocio en la Nube y están más abiertas a apoyarse en diversos modelos de Nube (pública, privada, comunitaria o híbrida) y usan nubes privadas con más intensidad.

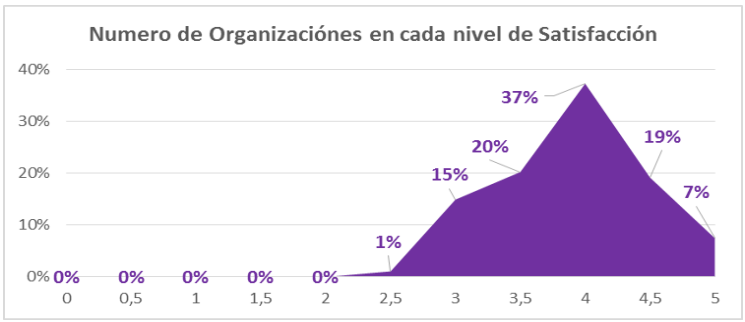

Ilustración 8.- Número de Organizaciones en cada nivel de Satisfacción

> *Conclusión #3. La satisfacción de las empresas con los servicios en la Nube es inversamente proporcional a su tamaño.*
>
> *Conclusión #3.1. Las empresas menos satisfechas son las que más requieren información y verificación en primera persona de sus servicios en la Nube.*

Análisis conjunto de expectativas, requisitos y satisfacción con los Servicios en la Nube

Una vez analizados cada uno de los tres factores por separado, procede realizar un análisis conjunto de todos ellos y con una perspectiva histórica (Ilustración 9). Este análisis dibuja un escenario de gran estabilidad, en la que los parámetros analizados se mantienen en niveles similares a lo largo del periodo observado.

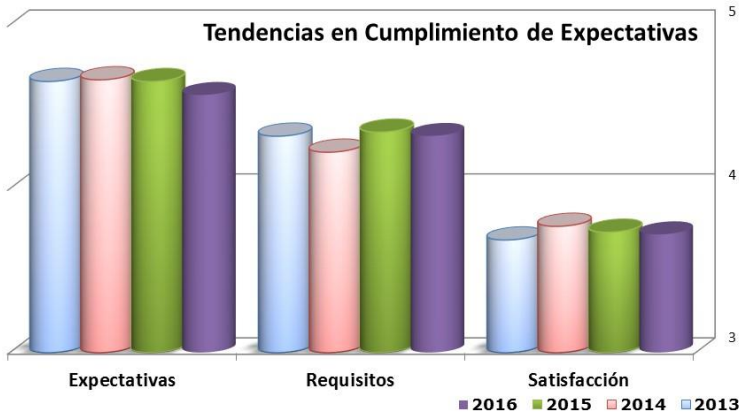

Ilustración 9.- Comparación expectativas vs. Requisitos vs. Satisfacción

Conclusión #4. Estabilidad en la relación entre expectativas, requisitos para la Nube y satisfacción con los servicios recibidos.

Certificaciones para la Nube: Personales y Empresariales

Una de las medidas consideradas para aumentar el éxito de los servicios en la Nube está relacionada con el conocimiento de las personas involucradas en esta acción. Para ello, se han identificado los esquemas de certificación de personas no asociados a fabricantes o tecnologías concretas que el equipo de analistas ha considerado como más relevantes, evaluando el reconocimiento que tienen los profesionales con esa certificación, y el conocimiento que esta certificación en si tiene en el mercado (Ilustración 10).
Siguiendo este mismo esquema, se han analizado los esquemas de certificación de servicios, corporaciones y/o instalaciones aplicables a entornos de Nube, seleccionando de nuevo los más relevantes a criterio del equipo de analistas, y evaluando de nuevo su reconocimiento y conocimiento (Ilustración 11).

Ilustración 10.- Conocimiento y Reconocimiento de Certificaciones EMPRESARIALES

Ilustración 11.- Conocimiento y Reconocimiento de Certificaciones PERSONALES

Respecto de las certificaciones personales, todas las certificaciones identificadas tienen un nivel de reconocimiento alta en todos los casos, con ligeras variaciones en su reconocimiento dado que son desconocidas para entre el 20% y el 30% de los encuestados, según el caso
Respecto de las certificaciones empresariales, sí que se han identificado diferencias más claras entre las certificaciones consideradas, siendo ISO 27001 la certificación más popular y más valorada.

Disponibilidad de información sobre la Nube

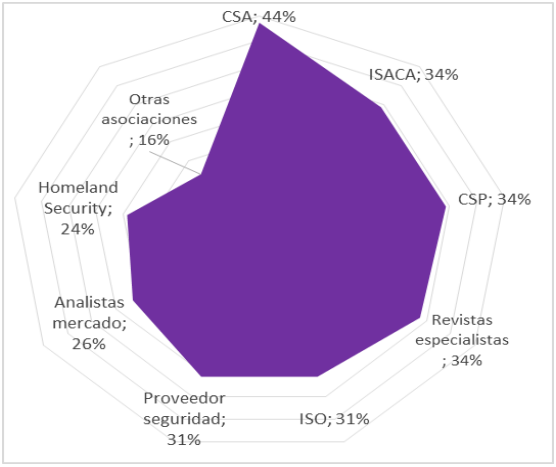

Ilustración 12.- Fuentes de Información disponibles

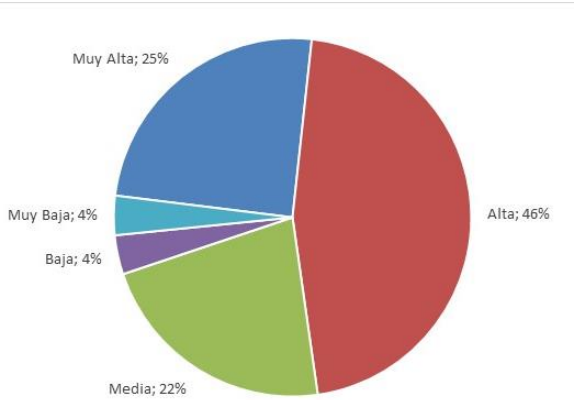

Ilustración 13.- Accesibilidad de Fuentes de Información

Por otra parte, el estudio ha identificado que un 75% 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. CSA es la fuente más consultada, mientras que ISACA, ISO, los proveedores de servicios de Nube o las revistas especializadas son consideraras válidas por uno de cada 3 encuestados. Estos datos se confirman porque, de acuerdo con los resultados de la encuesta, cada encuestado consulta entre 3 y 4 fuentes distintas para informarse sobre los servicios en la Nube.

Conclusión #5. Se consultan entre 3 y 4 fuentes de información distintas para estar información sobre la Seguridad en la Nube

Concienciación en el uso de los servicios en la Nube

Como elemento novedoso de este IV estudio, se ha analizado la percepción que se tiene en las organizaciones del grado de concienciación de los distintos niveles organizativos sobre el uso de los servicios en la Nube.

Los resultados obtenidos (Ilustración 14) indican que se tiene la percepción de que los órganos de dirección de las compañías realizan con más frecuencia análisis de riesgos formales previos a la adopción de servicios en la Nube (uno de cada cuatro), frente a una menor consciencia espontánea o inducida del personal no directivo sobre estos riesgos, que sólo se percibe en uno de cada seis empleados.

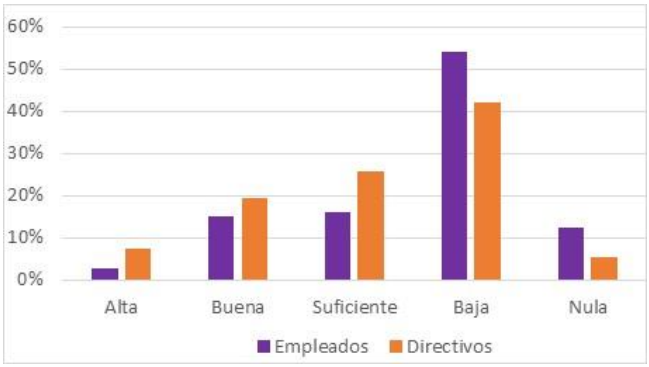

Ilustración 14.- Grado de Concienciación ante la Nube

En todo caso, la concienciación por parte de ambos niveles se juzga como baja para uno de cada dos directivos y para dos de cada tres no directivos.

Una primera explicación a este escenario podría extractarse de una falta mutua de confianza entre ambos roles, de forma que cada uno de ellos pensase que está adecuadamente concienciado y es el otro rol quien no lo está. Afortunadamente, esta explicación NO es correcta. La Ilustración 15 desglosa la información anterior con este criterio, y permite identificar que todos los roles de la organización perciben esa mayor concienciación en la dirección que en el personal no directivo. Con matices interesantes. En particular, las áreas técnicas (CTO, CISO, Administradores, Desarrolladores) son más escépticas sobre la concienciación que hay en las empresas, mientras que el CEO, los responsables de Departamento y los Jefes de Proyecto tienen una visión más positiva.

Ilustración 15.- Grado de Concienciación ante riesgos de servicios en la Nube, según el rol.

Conclusión #6. El grado de concienciación en las organizaciones ante los servicios en la Nube es aún bajo e insuficiente.

Incidentes y Servicios en la Nube

La capacidad de detección y respuesta de los usuarios para incidentes en sus servicios en la Nube es foco habitual del estudio, en tanto que los CSP de Nube Pública aducen como ventajas una mayor capacidad para aplicar controles de seguridad y de responder a incidencias, al disponer de economías de escala que permiten dedicar recursos específicos a esta tarea. Aparentemente, este objetivo permite reducir el número de incidentes (Ilustración 17), pero en esta edición del estudio, la criticidad de los incidentes aumenta (Ilustración 16).

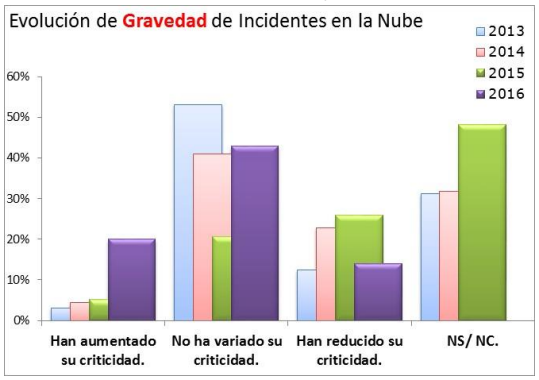

Ilustración 16.- Evolución de Criticidad de Incidentes en Servicios en la Nube

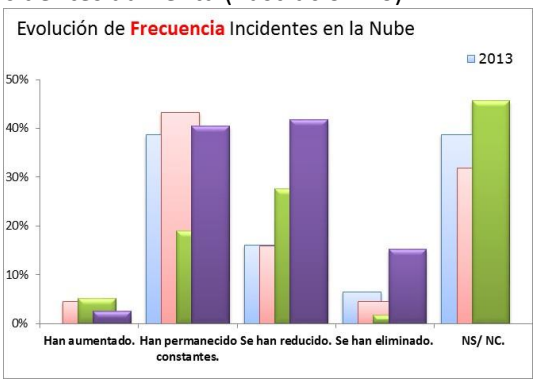

Ilustración 17.- Evolución de Frecuencia de Incidentes en Servicios en la Nube

Desconociendo la identidad y tipo de los incidentes concretos detectados en cada organización, un análisis más detallado permite identificar que los incidentes son más y más numerosos a medida que el usuario de los servicios en la Nube crece en tamaño. De hecho, para empresas de más de 500 empleados, la criticidad media de los incidentes en servicios en la Nube es mayor que la de los incidentes previos, y para empresas de más de 5.000 empleados, el número total de incidencias es mayor (Ilustración 18)

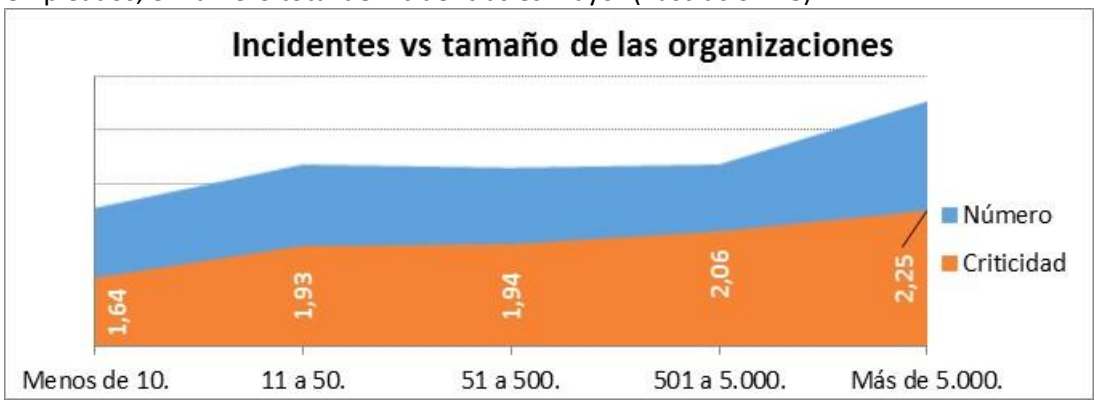

Ilustración 18.- Criticidad de Incidentes en la Nube vs. Tamaño del Usuario.

Si bien la información disponible no permite un análisis más profundo, el equipo de analistas plantea como hipótesis que los incidentes de seguridad es una de las razones por las que las empresas de mayor tamaño estaban menos satisfechas con los servicios en Nube (Ilustración 7). Por otra parte, las empresas de mayor tamaño son más complejas (por lo que en todo caso deberían tener ya más incidentes de seguridad que una empresa pequeña), y posiblemente dispongan de equipos internos especializados en gestión de incidentes, por lo que el servicio adicional que pueden recibir de un CSP puede menos diferencial, o incluso peor.

Conclusión #7. A efectos de incidentes, las empresas pequeñas sí se benefician de un entorno en la Nube. Las empresas grandes tienen por el contrario más incidentes y de mayor gravedad.

ShadowIT

El estudio también ha abordado la viabilidad del Shadow IT, es decir, 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.
Este aspecto ha merecido especial interés por el equipo de analistas, en tanto que las conclusiones a las que se llegó en el III estudio no correspondieron con las expectativas previas identificadas. Por ello, el problema se ha abordado desde una óptica diferente, que asume de principio la posibilidad de que sí exista ShadowIT y busca confirmarlo y encontrar sus causas.

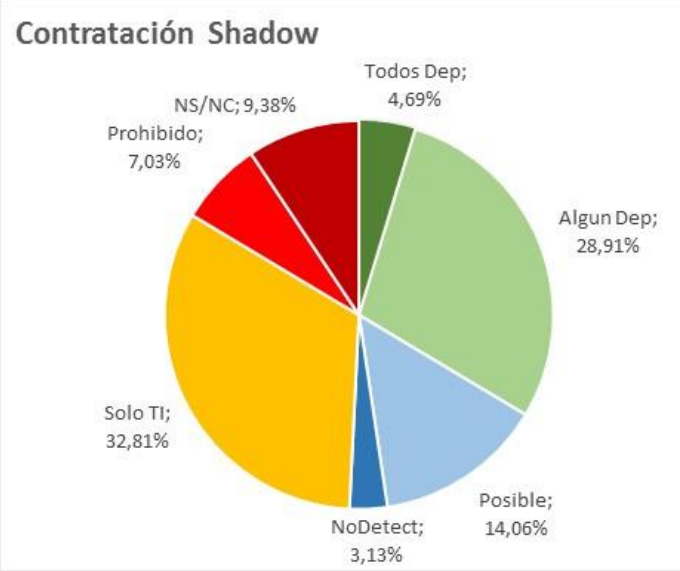

Ilustración 19.- Existencia o no del fenómeno Shadow IT

Con este nuevo enfoque (Ilustración 19), se ha detectado que cerca del 40% de los participantes opinan que ShadowIT no ocurre en las organizaciones porque está prohibido o porque está especificado que TI realiza estas funciones. Por el contrario, un 33% cree que el fenómeno existe, bien puntualmente, bien de forma generalizada. Por último, un 20% tiene dudas, bien porque lo sospecha bien porque no cree que se pudiera detectar.

Asumiendo que las cifras apuntan a que efectivamente existe ShadowIT en las organizaciones, cabe realizarse dos preguntas: ¿Qué razones pueden esgrimirse para que poder justificar internamente el uso de ShadowIT en una organización? Y si existiese, ¿Sería una situación deseable o no deseable?

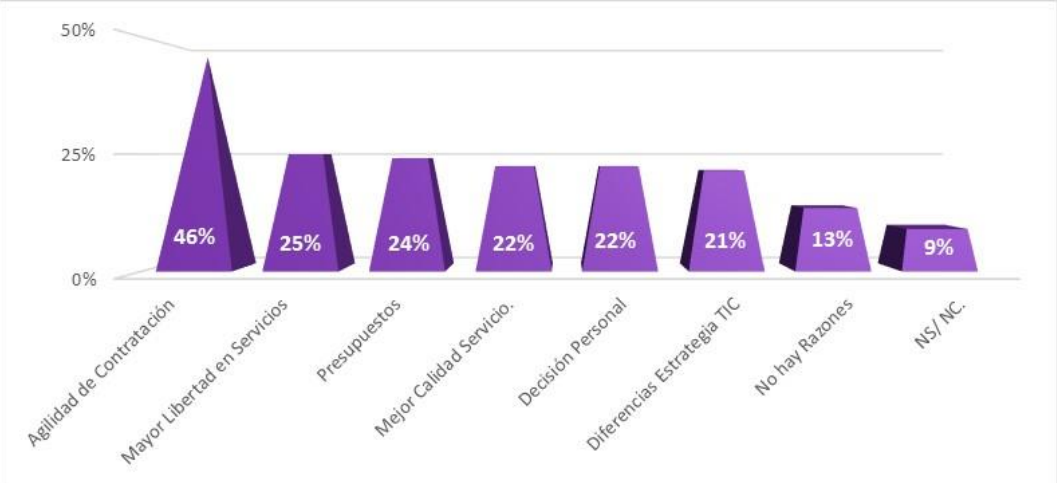

Ilustración 20.- Motivaciones identificadas para ShadowIT

Respecto de las posibles justificaciones (Ilustración 20) se han ofrecido a los participantes 6 posibles razones que podrían usarse para justificar el uso de Shadow IT, junto con una última posibilidad que señale que, sencillamente, no hay razones para usar ShadowIT. De entre las razones presentadas, los participantes han señalado casi dos razones diferentes como promedio. Y de entre todas ellas, hay una razón principal que predomina claramente sobre todas las demás: La agilidad de contratación de servicios en ShadowIT. El resto de razones son

seleccionadas por uno de cada cuatro participantes, por lo que no pueden desdeñarse como posible justificación para el uso de ShadowIT. Porque cualquiera de ellas es más frecuente que la opción "no hay razones" que también se ofrece.
Analizando estos dos factores de forma conjunta frente al rol en la organización de la persona, se verifican algunos aspectos interesantes:

- No hay diferencias en los hallazgos realizados en función del tamaño de la compañía.
- Las figuras más cercanas a la directiva en una organización (excepto el CISO) tienden a ser más escépticos con el fenómeno ShadowTI que las figuras no directivas.

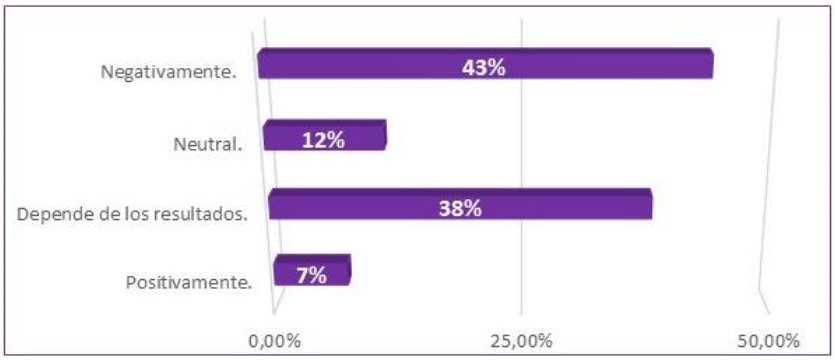

Ilustración 21.- Valoración a priori sobre ShadowTI

Por último, el estudio analiza (Ilustración 21) cual es la posición a priori sobre ShadowIT, sin tener en cuenta otros factores. Para verificar que solo el 7% ver ShadowIT como un fenómeno positivo en todos los casos, mientras que la visión negativa es la mayoritaria. Destacar la existencia también de un porcentaje relevante de opiniones que condicionan la posición a los resultados que se obtengan.

Conclusión #8. ShadowIT está ocurriendo de forma amplia, a pesar de que hay una opinión generalizada negativa sobre su idoneidad.

Conclusión #8.1. ShadowIT se origina fundamentalmente por presiones en el TimeToMarket en las organizaciones, que aparentemente resuelven mejor los Servicios en Nube Externos que los departamentos TI internos. Aunque es fácil que alguien encuentre otras justificaciones.

Conclusión #8.2. La Dirección confía en las políticas corporativas, los procedimientos internos y por ello, desconfía del fenómeno. Que en otros niveles se ve con más normalidad.

Servicios y Modelos de Servicio más demandados desde la Nube

Como último elemento del estudio, se analizan los servicios que se están utilizando por los participantes en el estudio. Hay un aumento en el uso de prácticamente todos los servicios, y en particular, de soluciones ofimáticas y de servicios Web.

Además, se ha vuelto a detectar que el uso de servicios de almacenamiento es mucho más habitual en usuarios de Nube Privada que en los usuarios de Nube Pública. La situación se invierte para los servicios de correo electrónico, donde los usuarios de Nube Pública usan servicios de Correo con más frecuencia que los usuarios de Nube Privada.

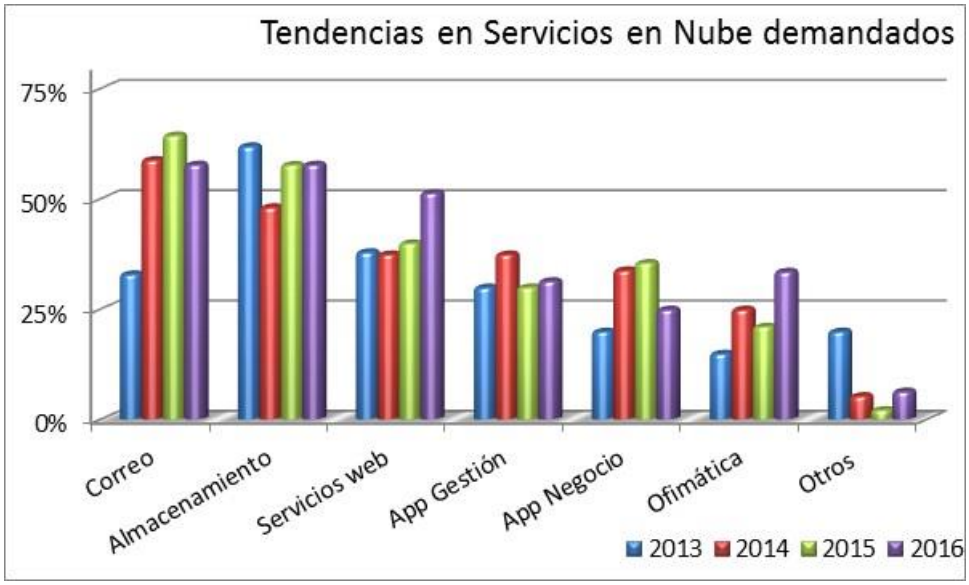

Ilustración 22.- Uso de Servicios en la Nube detectado.

Consideraciones Particulares desde CSA-España

Las conclusiones presentadas hasta el momento afectan al total del estudio. El análisis particular de las contribuciones realizadas desde España ofrece algunas conclusiones específicas, aplicables al mercado local, que merecen ser destacadas.

CSA-ES. Tipología de Nube utilizada

En líneas generales, el uso de la Nube en las empresas españolas es ligeramente mayor que al total de empresas encuestadas.

Esta diferencia se debe principalmente al uso de aplicaciones tanto de almacenamiento como de ofimática en la nube, bastante más utilizadas en las empresas que se encuentras en España que en el global.

Tal como muestra la Ilustración 23, la tipología que más diferencias presenta son las híbridas, en las cuales parte de los servicios en la Nube son públicos, pero otra parte de los servicios son privados.

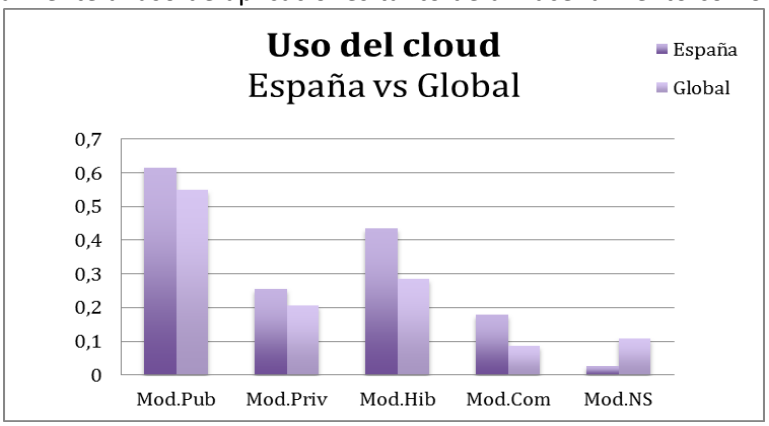

Ilustración 23.- CSA-ES. Diferencias en Uso de Modelos

Además, todos los tipos de tecnología de Nube, es decir SaaS, IaaS y PaaS son más usados en las empresas que se encuentran en territorio español que en el global.

CSA-ES. Garantías de seguridad

En la Ilustración 24 se puede identificar que, atendiendo a las posibles expectativas analizadas en el estudio, el mercado español tiene un horizonte menos ambicioso frente a otras geografías. Con la excepción de la confidencialidad, donde el mercado español sí es más exigente que el resto de mercados.

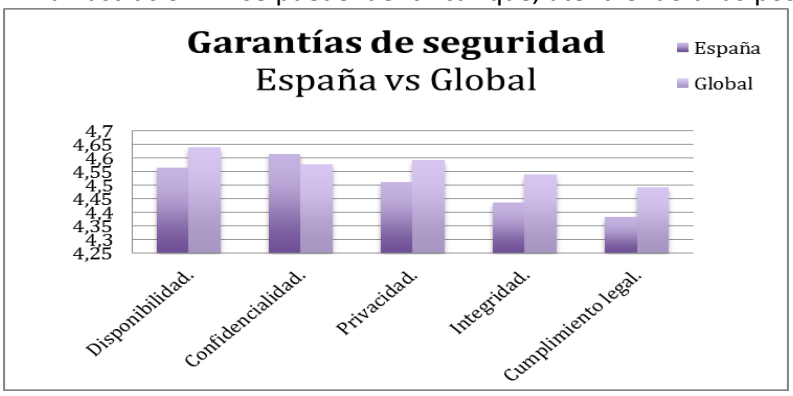

Ilustración 24.- CSA-ES. Diferencias en Expectativas de Seguridad

Merece también ser comentado el descenso en el cumplimiento legal. Como ya se apuntaba en el III estudio, en el año 2015, esta situación puede resultar paradójica frente a la importancia recurrente que se ha indicado respecto del cumplimiento de las regulaciones españolas y europeas. Como ya se apuntaba en años anteriores, las empresas españolas ya han aprendido a gestionar su cumplimiento legal, incluso en la Nube, lo que hace que este tema pierda algo de su relevancia anterior.

CSA-ES. Shadow IT

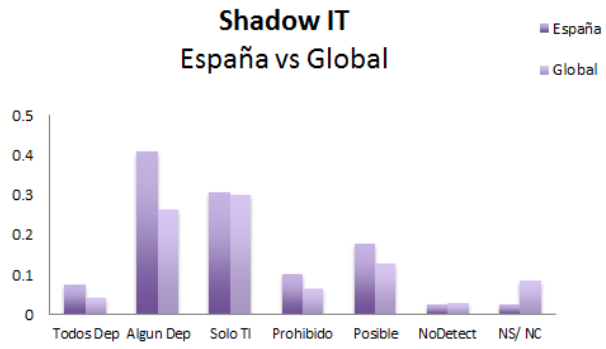

Ilustración 25.- CSA-ES. Diferencial en Incidencia de ShadowIT

Como consideración general, la ocurrencia en el mercado español del fenómeno de ShadowIT es más frecuente que en los resultados generales, donde la identificación del ShadowIT ocurre más en España que en la globalidad de encuestados (Ilustración 25). Esto se ve en que todos los valores son mayores, excepto para el de "no sabe, no contesta". En particular, la mayor diferencia se observa en el valor "Está actualmente ocurriendo en algún departamento", por lo que se asume en muchos casos que el fenómeno ya está ocurriendo, aunque quizás no se conozca con precisión donde.

En cuanto a las razones para la aparición de ShadowIT (Ilustración 26), el análisis para el mercado español apunta diferencial y nítidamente hacia el uso de ShadowIT para la contratación más ágil y menos constreñida de servicios, sin recurrir al apoyo en servicios y/o departamentos corporativos.

Por otro lado, en España no se percibe que la contratación de servicios en ShadowIT obedezca a un incremento en la calidad de servicio recibido.

Ilustración 26.- CSA-ES. Diferencial en razones para ShadowIT

En un análisis combinado de motivaciones e incidencia para ShadowIT, podemos concluir que en el mercado español existe una fuerte intuición sobre la mayor incidencia del fenómeno, motivado por la sospecha extendida de que existen Departamentos no desean interactuar con el Departamento de TI, bien porque consideran que el proceso es inadecuado, bien porque los servicios ofrecidos no son los correctos.

> *Conclusión CSA-ES.#1. Hay una sospecha extendida de que ShadowIT existe en España por reticencias con el Departamento de TI, bien sobre los servicios que ofrece, bien por su proceso de gestión del servicio.*

Consideraciones Particulares para Perú

De forma análoga a como se realizó en el capítulo anterior para España, se analizan y particularizan para el caso de Perú las conclusiones específicas de este mercado que difieren de las conclusiones generales presentadas.

Específicamente los términos más relevantes con respecto al estudio resaltan con respecto a los requisitos sobre los proveedores de Nube (CSP) relacionadas principalmente con la "Continuidad del Negocio" y la Seguridad, Niveles de Servicios (SLA) y la Capacidad de auditar al CSP.

La Superintendencia de Banca, Seguros y AFP (SBS), publicó los circulares G-139-2009 y G-140-2009, referidos a la Gestión de Continuidad del Negocio y Gestión de Seguridad de la Información, respectivamente.

La circular G-139-2009 se refiere al cumplimiento obligatorio para que las empresas del sector financiero Peruano (incluidos los bancos, cajas municipales de ahorro y crédito, financieras, compañías de seguros y administradoras de fondos de pensiones), definan los criterios mínimos para elevar el nivel de preparación de las organizaciones de tal forma que se pueda hacer frente a eventos externos que puedan interrumpir sus actividades críticas, así como contar con la capacidad para recuperar dichas actividades en el menor tiempo posible.

Dentro de sus exigencias, las entidades de este sector financiero, se ven obligadas a realizar auditoría de inspección a sus proveedores, quienes también deberán contar con los criterios mínimos de continuidad de negocio y seguridad de la información.

Ello conlleva a que las empresas que brindan servicios a las empresas financieras, deban de contar con los controles técnicos de seguridad y continuidad, como las brindadas por la Nube. Esto explica el resultado para Perú reflejado globalmente obtenido en la Ilustración 4.

Es sin duda necesario enfatizar la difusión y conocimiento de la Nube, evangelizando a las empresas en las necesidades de establecer controles de seguridad y continuidad en sus negocios.

Otro punto resaltante es que en el Perú, las certificaciones empresariales están más direccionadas hacia la norma internacional ISO; siendo ISO 27001 la certificación que tiene un impacto positivo localmente y que es promovido por el estado peruano en la Normas Técnicas Peruanas (NTP).

Sin embargo se observa de manera significativa la importancia de la certificación ISO 27018 para el proveedor de la Nube (CSP) tan igual como ocurre globalmente en la Ilustración 10.

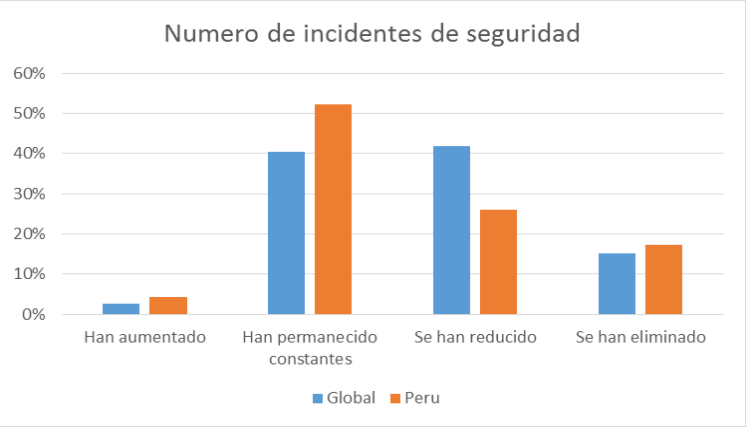

Ilustración 27.- Diferencias en Número de Incidentes Perú

Finalmente, entendemos que de manera particular se dan las siguientes observaciones para el Perú con respecto a la evolución y cantidad de los incidentes de seguridad tras la migración a la Nube.

Se encontraron ciertas diferencias notorias en las respuestas sobre Incidentes de seguridad que respondieron el total de encuestados versus los encuestados peruanos.

Observamos que más del 50% de los encuestados peruanos dicen que el número de incidentes ha permanecido constante, frente a un 40% de las respuestas globales. De otro lado, solo un

25% de encuestados peruanos mencionan que se han reducido los incidentes, frente a un 40% de respuestas globales.
Es curioso notar también que las respuestas que establecen que han aumentado y se han eliminado permanecen constantes en ambos casos.

Sobre la criticidad de los incidentes de seguridad, hay una notable diferencia en los encuestados que afirman que los incidentes han aumentado su criticidad, para el caso de Peru son más del 40% frente a un 25% de respuestas globales.
Asimismo, las personas que indican que no ha variado su criticidad son menos para el Perú, representando solo un 30%, frente a un 55% de respuesta globales.

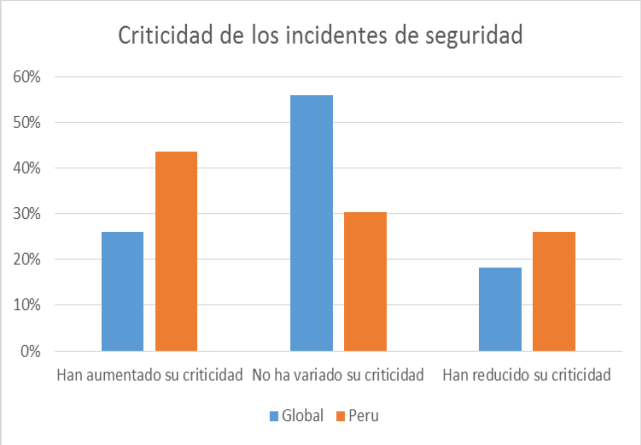

Ilustración 28.- Diferencias en Criticidad de Incidentes, Perú

La conclusión es que los peruanos están ligeramente más satisfechos en torno a incidentes de seguridad, sin embargo, también dicen que su criticidad es mayor cuando suceden.

Consideraciones Particulares de ISACA-Madrid

Finalmente, se incluyen a continuación las conclusiones específicas obtenidas desde la óptica del capítulo de Madrid de ISACA

La Nube se han convertido en pieza fundamental para la prestación de servicios de compañías de todos los tamaños y en todos los sectores gracias a que:

- Hace que las organizaciones sean más ágiles y eficientes
- Permite que los servicios sean más innovadores y competitivos
- Reduce los costes operativos globales

Esta circunstancia hace que el gobierno de la nube se haya convertido en un aspecto fundamental para los Directivos de las organizaciones[5]: ¿Qué nivel de confianza se puede tener en que los planes de la Dirección alcanzaran los beneficios esperados? ¿Cómo podemos saber si los riesgos que se asumen no excederán los beneficios?

En relación a estas preguntas, los resultados de la encuesta han puesto de manifiesto datos muy relevantes:

- La disponibilidad del servicio es la expectativa más elevada de los usuarios de la Nube, en contraste con el cumplimiento normativo. Este dato soporta el hecho mencionado de que los servicios en la Nube cada vez son más críticos para los usuarios de los mismos.
- Además de la continuidad de servicio por parte del proveedor, el segundo requisito más valorado por los encuestados han sido los 'controles implantados por el proveedor' (un 64,8% lo ha valorado con la máxima importancia). Este dato refleja que los usuarios de la Nube están concienciados de la necesidad de evaluar el nivel de riesgo asumido, lo que pasa, indudablemente, por conocer la robustez de los controles implantados por el proveedor.
- La aportación de valor de los servicios en la Nube es, como no podía ser de otra forma, un elemento claro para evaluar la satisfacción del usuario respecto al servicio, ya que, como hemos comentado previamente, estos servicios son una pieza fundamental para la estrategia de las compañías.
- En la parte negativa, destacar que, como se ha destacado como conclusión sexta, "*el nivel de concienciación en las organizaciones ante los servicios en la Nube es aún bajo e insuficiente*", por lo que debemos perseverar en el esfuerzo de asegurar que, especialmente, la Dirección comprende y considera los riesgos asociados a la utilización de los servicios en la Nube[6].

Finalmente, en cuanto a una de las actividades fundamentales de ISACA, como asociación de profesionales, esto es, la acreditación de profesionales, vemos como existe un conjunto de certificaciones que son utilizadas por los profesionales de la seguridad y gestión del riesgo, entre las que destaca CISM como una de las más utilizadas. Este dato, junto a la creciente importancia de los servicios en la Nube para la consecución de los objetivos de negocio, reitera la necesidad de implementar mecanismos adecuados de gobierno de la seguridad que aseguren la aportación de valor gestionando los riesgos y utilizando los recursos de manera eficiente, elementos en los que se basa la gestión de la seguridad que acredita el CISM y que derivan directamente de los principios de COBIT 5©.

[5] "Guiding Principles for Cloud Computing Adoption and Use", ISACA, 2012

[6] "Cloud Governance: Questions Boards of Directors Need to Ask", ISACA, 2013

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 y Peruano de del CSA en colaboración con ISMS Forum.

El estudio se ha realizado en base a encuestas recopiladas entre el 12 y el 29 de septiembre de 2016, a través de la plataforma online SurveyMonkey. Se recopilaron un total de 140 respuestas de profesionales y organizaciones.

Con respecto a la distribución de las respuestas por geografía, en la edición 2016 hay que destacar la equilibrada distribución de los participantes por distintas geografías, y la aparición de organizaciones ubicadas en los ámbitos geográficos incluidos por primera vez en el estudio, en particular en LATAM.

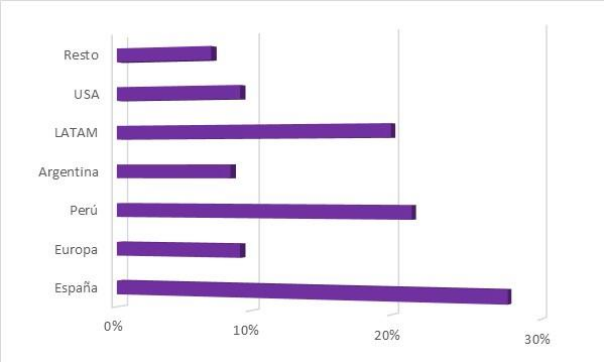

Ilustración 29.- Participantes en la Encuesta (Geografía)

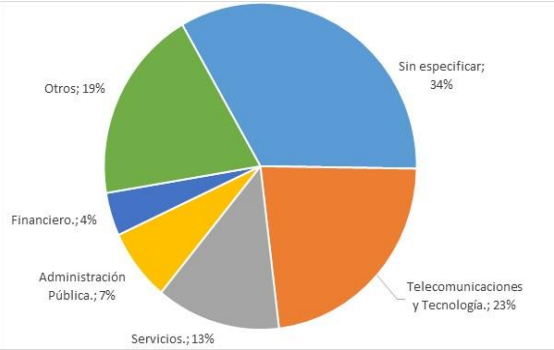

Ilustración 30.- Distribución de participantes por sector

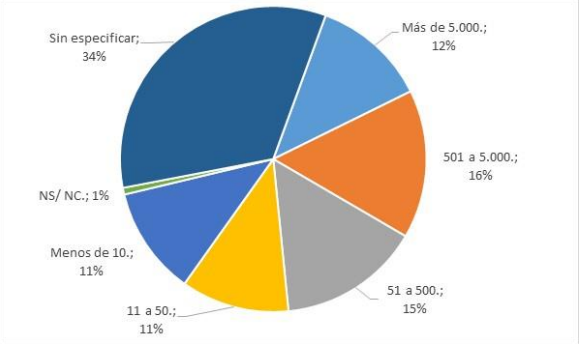

Ilustración 31.- Distribución de participantes por tamaño

En términos de características de las empresas participantes, la mayoría desarrollan su actividad de negocio en el sector de las telecomunicaciones y de la tecnología (23%). Las organizaciones participantes en el estudio cubren de forma equilibrada el total del espectro de tamaños de organizaciones.

Paseo de la Habana, 54,
2º Izquierda 1.
28036 Madrid - España
Tlf :+34 91 563 50 62

+info:
info@ismsforum.es
www.ismsforum.es
@ISMSForumSpain