



**12° ESTUDIO DEL
ESTADO DEL ARTE DE LA
SEGURIDAD EN LA NUBE**

Una iniciativa de:

isms
FORUM

En colaboración con:



CSA

Bolivia
Chapter



ISACA
Madrid Chapter

Enero 2025

12º Estudio del Estado del Arte de la Seguridad en la Nube

Copyright

Todos los derechos reservados. Puede descargar, almacenar, utilizar o imprimir el presente Estudio 12º Estudio del Estado del Arte de la Seguridad en la Nube, 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.

AUTORES

COORDINADORES

Mariano J. Benito
Antonio Cueva
Abdel Fedora Aliaga Villalobos
Maite Avelino
Ricardo Urbina Miranda
Julio C. Balderrama
Juan Carlos Carrillo
Trinidad de Miguel
Raquel de Saá
Daniel García

ANALISTAS

Alberto Bernáldez
Alejandro Agudelo
Alejandro García
Alfredo Alva
Ana Belén Galán
Cándido Arregui
Carlos Lopez Blanco
Carlos Samaniego
Concepción Cordón
Diego Fernandez Vázquez
Fernando Iglesias
Fran Garcia Martínez
Gonzalo Flores
Gabriela Romo
Javier Carbayo
Jorge Castañeda
Josep Bardallo
Juan Antonio González
Juan José del Río
Julia Socorro
Luis Ballesteros
Manuel Estevez
Manuel Fernandez
Mara Fernández
Ramón Codina
Santiago Minguito

DISEÑO/ MAQUETACIÓN

Marta Barroso
Beatriz García

Índice de Contenidos

Principales Hallazgos del 12º Estudio	5
Objetivos y Ámbito del Estudio	7
¿Están las organizaciones abandonando la Nube?	8
1. Tipología de Servicios consumidos en la Nube	16
1.1. Relevancia de los Proveedores de Servicios en la Nube (CSP).....	16
1.2. Servicios de la Nube demandados por los usuarios.....	20
1.3. Estrategias Cloud-First y Cloud Only	21
2. Análisis de Expectativas de los Usuarios de la Nube	24
3. Requisitos exigidos por los usuarios a los prestadores de servicios en la nube	29
4. Satisfacción de los Usuarios con los Servicios en la Nube.....	35
5. Evolución Expectativas vs Requisitos vs Satisfacción	39
6. Visión sobre Shadow IT	41
7. Estado de Concienciación en Seguridad de los Usuarios	45
8. Evolución de Incidentes de Seguridad en Servicios en Nube	50
9. Análisis de Participantes en el Estudio y sus particularidades	58
9.1. Caracterización de usuarios no técnicos.....	58
9.2. Diferencias en Resultados de Usuarios No Técnicos	58
10. Ficha Técnica del Estudio	63
10.1. Consideraciones sobre posibles sesgos en la información analizada	64
10.2. Perfiles que han participado en el Estudio	66
10.3. Consideraciones Temporales sobre el Estudio	68

Principales Hallazgos del 12º Estudio

El 12º Estudio del Estado del Arte de Seguridad en la Nube se ha realizado en 2024 en cooperación entre los capítulos español, peruano, boliviano, chileno, argentino y mexicano de Cloud Security Alliance, y el capítulo de Madrid de ISACA, continúa la serie de estudios realizados en 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022 y 2023. El equipo de analistas que ha preparado desea que este Estudio y sus contenidos sean de utilidad para sus lectores.

Esta 12ª Edición del Estudio del Estado del Arte de Seguridad en la Nube se planteó resolver una **percepción existente entre los analistas** al inicio de los trabajos: Que muchas organizaciones estaban **abandonando los servicios en la Nube** y retornando a la prestación desde instalaciones propias o de terceros geográficamente localizadas. El Estudio ha podido identificar que se están produciendo movimientos de este tipo, al identificar que una quinta parte de los participantes habían abandonado total o parcialmente servicios en la Nube. Las organizaciones que retornan de la Nube aducen razones de coste de estos servicios, mientras la disponibilidad del servicio y la flexibilidad de uso son las características más apreciadas por los usuarios de la Nube.

El Estudio analizó de nuevo el perfil de **servicios consumidos** desde la Nube, obteniendo **resultados similares** a años anteriores: Los usuarios consumen de forma abrumadora servicios de Almacenamiento, Ofimática y/o Correo electrónico, proporcionado por tres CSP (Azure, AWS, Google Cloud). En el caso de empresas pequeñas, muy basado en los servicios básicos de Google. También se mantiene un uso amplio de servicios de Seguridad desde la Nube (SECaaS). Pero aparecen la cuota de uso de Oracle Cloud Infraestructura en grandes empresas, que es comparable al de los tres CSP; o el 33% de participantes que usan servicios de IA en Nube.

El Estudio también detectado que las **expectativas** en el mercado sobre el uso del mercado, la exigencia de los **requisitos** solicitados a los proveedores y el grado de **satisfacción** con los servicios recibidos siguen siendo **altos o muy altos**. El Estudio detecta **leves retrocesos** en todos los campos, y una ampliación de las diferencias entre los valores detectados, con expectativas más altas que la exigencia de requisitos y ambos mayores que la satisfacción con los servicios.

Esta edición ha permitido contemplar una **evolución positiva** en las organizaciones en su grado de **concienciación** sobre cómo afrontar los riesgos de la Nube y, mientras que la no aceptación de escenarios de ShadowIT y de gestión de incidentes no han experimentados cambios.

La situación evoluciona de forma proporcional al tamaño de la empresa, siendo las empresas de mayor tamaño las más exigentes y que hacen un uso más intensivo de los servicios en Nube.


Confiamos en que los detalles de este Estudio sean de su interés.

Objetivos y Ámbito del Estudio

El objetivo del presente Estudio continúa para 2024 la serie de estudios sobre el Estado del Arte en la Seguridad de los Servicios en la Nube que se vienen desarrollando en los años 2013¹, 2014², 2015³, 2016⁴, 2017⁵, 2018⁶, 2019⁷, 2020⁸, 2021⁹, 2022¹⁰ y 2023¹¹, busca investigar y conocer el Estado del Arte de la adopción de Servicios en la Nube en los mercados español y LATAM, analizando las tendencias históricas establecidas y el papel que juega la seguridad en la adopción de estos servicios. Esta investigación se enfoca al punto de vista de los Usuarios de estos Servicios, y se ha realizado con la participación de analistas voluntarios de los Capítulos de CSA señalados y del capítulo de ISACA en Madrid.

Este Estudio amplía sus ámbitos de interés sobre los de versiones anteriores para el entendimiento de las motivaciones que tienen las organizaciones para adoptar servicios en la Nube o para rechazar su uso. Este análisis cubrirá también a las organizaciones que han cambiado en su estrategia de adopción de servicios en la Nube, incluyendo a organizaciones que han abandonado total o parcialmente estos servicios después de usarlas, y a las organizaciones que no usan servicios en la Nube, pero quizás los usen en el futuro.

Además, se mantienen otras líneas de investigación clásicas del Estudio: expectativas, requisitos y satisfacción de los usuarios con los servicios en la Nube, incidentes en los servicios, concienciación de los usuarios, condiciones geográficas de los servicios o Shadow IT, o la diferencias y semejanzas que tienen los usuarios corporativos de estos servicios frente a sus usuarios particulares o individuales.

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*). Estas organizaciones incluyen mayoritariamente a actuales usuarios de servicios en la Nube, junto a organizaciones que han dejado de utilizar estos servicios, a organizaciones que han decidido no utilizarlos y a organizaciones que aún no han adoptado una estrategia de servicios en la Nube. 

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>

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

⁶ <https://www.ismsforum.es/ficheros/descargas/6o-estudio-cloudsecurity-esarsenu-2018.pdf>

⁷ <https://www.ismsforum.es/ficheros/descargas/vii-estudio-sobre-el-estado-del-arte-de-seguridad.pdf>

⁸ <https://www.ismsforum.es/ficheros/descargas/viii-estudio-estado-seguridad-nube-v11602744518.pdf>

⁹ <https://www.ismsforum.es/ficheros/descargas/xi-estudiosotacsa2021v31637832356.pdf>

¹⁰ <https://www.ismsforum.es/ficheros/descargas/estudio-estado-arte-seguridad-nube-2022.pdf>

¹¹ <https://www.ismsforum.es/ficheros/descargas/sota-2023-definitivo1701434704.pdf>

¿Están las organizaciones abandonando la Nube?

Al inicio de los trabajos de preparación de esta 12ª Edición del Estudio, varios analistas expresaron una preocupación común. Basándose en conversaciones informales, casos dispersos e inconexos y experiencias propias de los analistas voluntarios del estudio, existía una percepción compartida entre muchos de ellos: las empresas estaban ejecutando actividades de *cloud repatriation*. Es decir, que había organizaciones que, tras haber usado servicios en la Nube, han decidido discontinuar este uso.

En anteriores ediciones del Estudio, se detectó un cierto número de participantes se declaraban como no usuarios de servicios en la Nube. En total, se trataba de un número de participantes poco significativo sobre el total (un 5% de los participantes). Esas ediciones no investigaban ni las razones que conducían a las organizaciones a esa decisión ni su evolución temporal ni la firmeza de las organizaciones que tomaban esta decisión.

Esta 12ª edición decidió abordar y analizar el fenómeno de *Cloud Repatriation*, estableciendo su extensión, impacto en las organizaciones, identificando y analizando tanto las motivaciones de las organizaciones que lo aplican como las de las organizaciones que siguen usando servicios en la Nube, y como estos factores evolucionan en las distintas organizaciones según el sector y geografías en que operan, su tamaño y la visión de los distintos estamentos internos sobre el fenómeno.

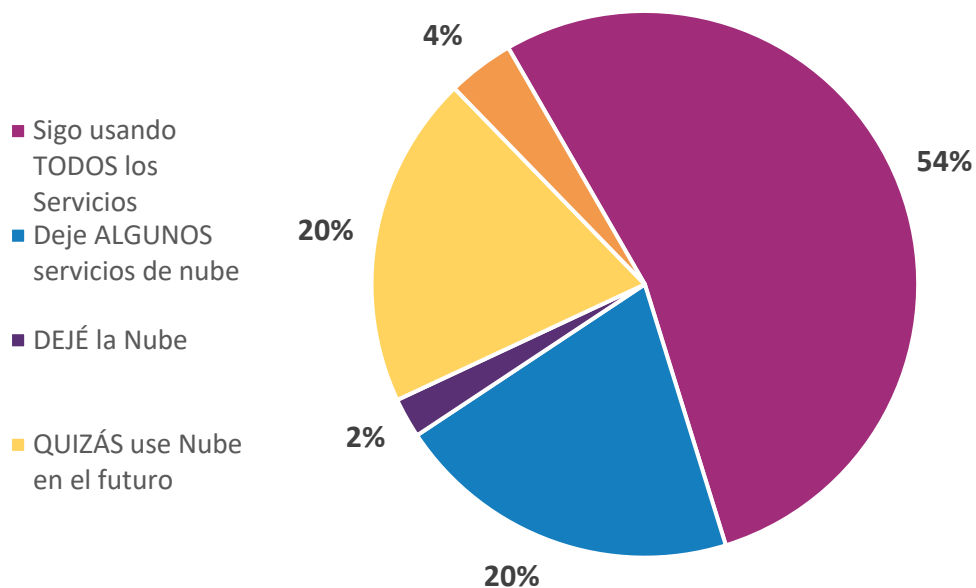


Ilustración 1.- Postura sobre Cloud Repatriation en las organizaciones

La Ilustración 1 muestra el estado de adopción de servicios de la Nube por las organizaciones, en función de su postura respecto de *Cloud Repatriation*. El Estudio identificó cinco posibles posiciones de las organizaciones ante este fenómeno.

- A. Organizaciones que adoptaron servicios de la Nube y que siguen usando todos ellos, que totalizan un 54% de los participantes del Estudio
- B. Organizaciones que adoptaron servicios en la Nube y que, si bien siguen usando varios de ellos, han decidido abandonar el uso de algunos de ellos. El estudio decidió no abordar en esta edición cual era la motivación original para el uso de estos servicios (prueba de nuevos servicios, sustitución de servicios On-prem u otras razones), ni la nueva ubicación de los servicios que se han retirado en la Nube (servicio discontinuado, prueba fallida, internalización de servicios, movimiento a otras Nubes u otras razones), que se abordarán en su caso en futuras ediciones. El estudio detectó que el 20% de los participantes en el estudio se identificaban con esta postura.
- C. Organizaciones que adoptaron servicios en la Nube pero que han decidido abandonar por completo el uso de servicios en la Nube. De nuevo, es el estudio no profundiza ni en la motivación inicial del uso de la Nube, ni el modelo posterior de consumo de servicios de TI. Sólo un 2% de las organizaciones se identificaron con este escenario.
- D. Organizaciones que no han adoptado aun servicios en la Nube, pero que no descartan adoptar estos servicios en el futuro. Un 20% de los usuarios se identifican con esta postura.
- E. Finalmente, las organizaciones que no están usando servicios en la Nube actualmente, ni prevén usarlos en el futuro. El 4% de los participantes del estudio declaran que esta es la postura que han adoptado sobre el uso de la Nube

Los resultados de la Ilustración 1 ofrecen información de gran interés. Ciertamente, más de la mitad de los participantes siguen usando servicios en la Nube con toda su intensidad. Sin embargo, un 20% de los participantes ya no usan algún servicio en la Nube y aunque el abandono total de estos servicios es aún incidental y no frecuente, sí que constituye un volumen de usuarios suficiente para establecer en el mercado la sensación de que el fenómeno de *Cloud Repatriation* está efectivamente ocurriendo, y ha podido ser detectado por los analistas. La tendencia así identificada no se había detectado en ediciones anteriores, ni podía deducirse su presencia de los datos recopilados en ese momento. Por ello, constituye una novedad en el Estudio que corrobora la impresión y expectativa inicial de los analistas.

El Estudio ha profundizado también en el perfil de participantes que podrían participar en este fenómeno de *Cloud Repatriation*, sin que se haya identificado parámetros o características comunes que pudiera perfilar este fenómeno, o asociarlo a casuísticas concretas que pudieran profundizar más en sus causas.

Por otra parte, la información de esta edición del Estudio sobre las organizaciones que declaran que nunca usarán la Nube y las que no rechazan el posible uso futuro, continúa los resultados obtenidos en años anteriores, manteniendo porcentajes de participantes en valores comparables a las de anteriores ediciones.

Este análisis comprende los datos de los encuestados que continúan con la muestra histórica contemplada en ediciones anteriores del Estudio.



Hay usuarios de la Nube, de distintos tipos, que han iniciado un proceso de *Cloud Repatriation*, aunque siguen siendo mayoría las organizaciones usuarias de estos servicios.

Derivada de la inquietud por la existencia del *Cloud Repatriation*, el equipo de analistas pidió a los participantes en el Estudio que compartiesen, según su casuística de uso de los servicios en la Nube, las motivaciones que se aducían para abandonarlos o no utilizarlos (pregunta formulada a todos los usuarios salvo al 54% que son usuarios de todos los servicios y cuyas respuestas se muestran en la Ilustración 2), y las ventajas que encuentran los usuarios de los servicios, que incluyen el 74% que suman los usuarios de todos los servicios y los usuarios que han abandonado alguno, que se muestran en la Ilustración 3. De esta forma, los analistas buscan determinar las características más apreciadas y menos satisfactorias de estos servicios y los elementos que deberían reformarse o reforzarse para mejorar su grado de adopción o sus características de seguridad, para incrementar el valor de uso.

En este sentido, la Ilustración 2 muestra las motivaciones que conducen al abandono de los servicios en la Nube. Cada organización podía indicar varias, por lo que el resultado de cada columna es el porcentaje de participantes que aducían esta motivación, y el total agregado llega a un 185%, por lo que las organizaciones dejan la nube o sus servicios por varias razones.

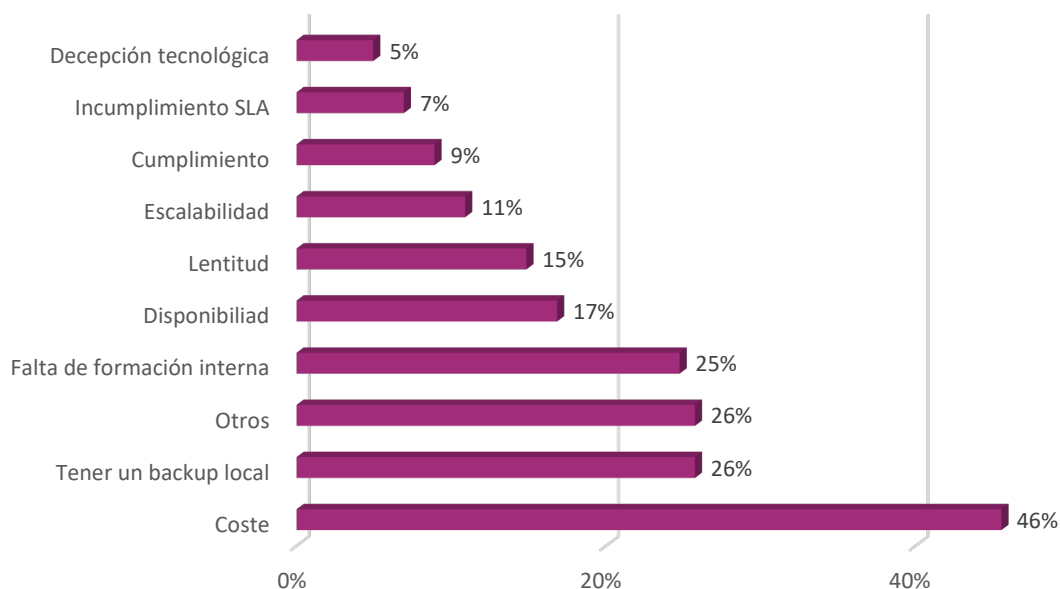


Ilustración 2.- Motivaciones aducidas para dejar servicios en la Nube

El análisis de los valores de la Ilustración 2 apuntan a un motivo principal para este abandono: El coste económico.

Este resultado, que inicialmente podría parecer como contraintuitivo, no fue tal para el equipo de analistas del Estudio. Muchos de ellos llevan utilizando servicios en la Nube desde hace años y han podido verificar el impacto real del coste del servicio recibido. Diversos¹² estudios¹³ apuntan a que el TCO (*Total Cost of Ownership*) de los servicios en la Nube se incrementa a medida que se prolonga su uso y que se iguala con el TCO de servicios On-prem y lo supera en periodos pocos años. En contraste con este mensaje, muchos proveedores de servicios destacan el coste de sus servicios como ventaja competitiva de estos servicios.

El Estudio permite conciliar los dos puntos de vista añadiendo la variable temporal. Si queremos explicar de una forma muy simplificada la evolución del coste de servicios a lo largo del tiempo en cada una de las modalidades, los servicios On-prem requieren de una fuerte inversión inicial (CAPEX) que es mucho menor en los servicios en la Nube puesto que solo debe hacerse cargo de los costes de migración y/o configuración inicial de los servicios en la Nube. Sin embargo, el coste de operación y mantenimiento (OPEX) de los servicios On-prem suele ser menor que en los servicios en la Nube, puesto que el proveedor reparte sus inversiones en CAPEX a lo largo del tiempo. En este contexto, si el consumo de servicios en la Nube se prolonga suficientemente en el tiempo, llegará un momento en el que compense la diferencia inicial entre los CAPEX y el TCO sea finalmente menos favorable para los servicios Cloud.

Este escenario puede no ocurrir o tardar más en ser detectado en servicios con consumos más variables en el tiempo o en servicios de bajo consumo. También puede ser detectado con el uso de las aplicaciones de cálculo del TCO de servicios en la Nube que ofrecen muchos proveedores de servicios en la Nube, si el usuario de servicios en la Nube las utiliza para analizar el TCO del servicio a varios años vista. El Estudio concluye que ese 46% de entidades no usuarias de la Nube que aducen el coste de los servicios como motivo de rechazo a la Nube se debe a una de estas dos causas, sea para abandonar servicios previamente contratados.

Como causas secundarias del no uso de los servicios, se destacan tres. En primer lugar, la necesidad de backup local expresa, según el criterio de los analistas, una falta de confianza de los usuarios en los servicios en la Nube, que les motiva a disponer de entornos locales de trabajo, que resultan complejos y costosos de operar y mantener en condiciones correctas. Este trabajo que redundante es difícilmente sostenible en el tiempo, y termina creando confianza en los servicios en la Nube y el abandono del entorno local: Pero en otros casos (27% de los encuestados), termina generando la decisión contraria y el abandono de los servicios en la Nube. En ambos casos, esta razón apunta a las dificultades que tienen algunos servicios para conseguir generar la confianza necesaria en sus capacidades y en su solidez. Algunos analistas apuntan a que la limitada transparencia de los proveedores sobre la prestación real de sus servicios que se deriva de la aplicación de los modelos de responsabilidad compartida¹⁴ en la parte que corresponde al proveedor dificulta proporcionar visibilidad sobre este punto, y permite que algunos consumidores puedan establecer dudas que no pueden resolver ni asegurar sobre si el servicio que están recibiendo es correcto en todos sus términos, más allá

¹² <https://cloudsecurityalliance.org/blog/2011/03/22/hey-you-get-off-of-my-cloud>

¹³ <https://cloudsecurityalliance.org/blog/2023/08/31/what-is-a-hyperscaler-are-they-really-cost-effective>

¹⁴ <https://cloudsecurityalliance.org/blog/2021/02/04/the-evolution-of-cloud-computing-and-the-updated-shared-responsibility>

de la disponibilidad y funcionalidad que sí que pueden medir. En particular, cuando el servicio tiene errores y fallos de disponibilidad que no pueden ser esclarecidos a plena satisfacción del consumidor, y con garantías completas de transparencia, trazabilidad, monitorización y/o generación evidencias sobre sus causas y sus soluciones.

En segundo lugar, se señalaba la falta de formación interna. Este factor incluye tanto la ausencia en suficiente cantidad y calidad de perfiles cualificados para trabajar con servicios en la Nube en los equipos de los usuarios de servicios en la Nube, como la dificultad de los usuarios de servicios para que su personal especialista en TI sea capaz de operar y gestionar correctamente servicios On-prem. Este factor se presentaba como motivo para abandono de la Nube para organizaciones de tamaño medio. Algunos analistas habían adelantado este resultado y la relevancia de este factor, aunque fue una sorpresa para los demás.

En tercer lugar, los participantes en el estudio señalan a “Otros Factores” que no habían sido previamente identificados por los analistas y ofrecidos como opción de respuesta. Este aspecto debe ser estudiado en futuras ediciones del estudio, para tratar de identificar estos factores que pueden estar ocultos y merecerían ser identificados y destacados, o para establecer que corresponde a múltiples y variadas razones que no son significativas de forma individual, pero sí cuando se contabilizan de forma conjunta.

El resto de los factores propuestos tenían una importancia no menor, pero no se analizan en profundidad por ser menores relevantes.



El coste de la Nube está expulsando a usuarios actuales, y disuadiendo a usuarios futuros.

De forma similar a las razones para el abandono, la Ilustración 3 muestra los motivos que declararon los usuarios que usaban los servicios en la Nube. De nuevo, cada columna refleja el porcentaje de participantes que declara este motivo, por lo que el resultado de nuevo excede el 100%. En este caso, un 324% de cumplimiento, por lo que los motivos de satisfacción son más abundantes que los de queja, que eran de un 185%.

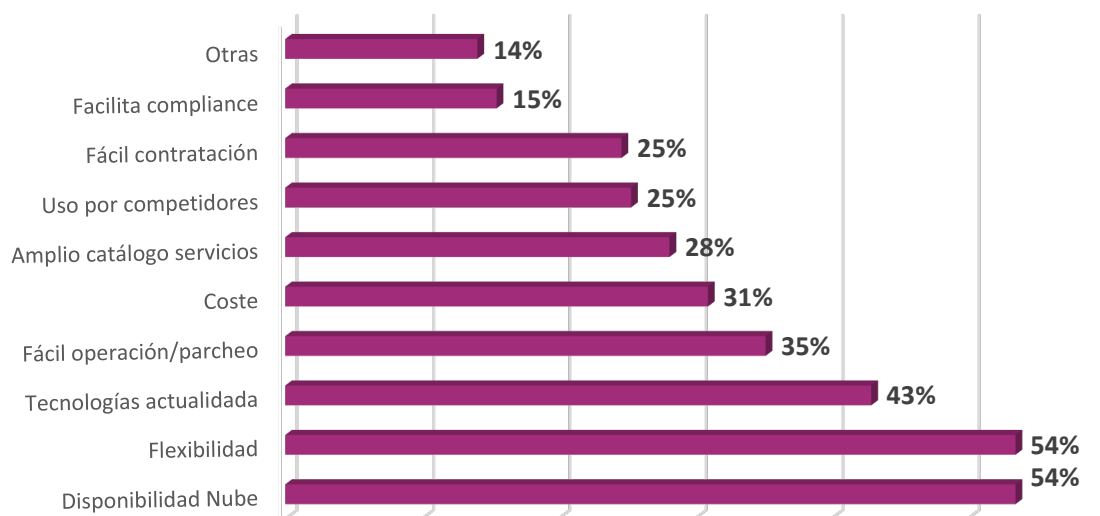


Ilustración 3.- % de organizaciones que fundamentan el uso de Nube en cada característica identificada

El análisis de motivos aducidos en la Ilustración 3 posiciona como elementos más apreciados dos características propias de las características técnicas propias de la Nube: la disponibilidad de servicio y la flexibilidad y escalabilidad del consumo de servicios.

En segunda posición aparecían otras características de fuerte contenido tecnológico, centrado en la operación de las actividades que dependen de la Nube, como es la capacidad de actualización de los servicios y plataformas desde lo que se prestan, como la facilidad de la operación y parcheo de los servicios. En ambos casos, los analistas habían identificado que eran actividades que pueden resultar menos complejas para el usuario de servicios de usuario que para esa misma entidad cuando tiene estos servicios en On-prem, por lo que este resultado confirmó la expectativa.

Por otra parte, las expectativas de los analistas estaban sobreestimadas para tres factores: Coste, uso por competidores y facilidad de contratación.

Respecto del coste, un 30% de los participantes en el Estudio declaran su satisfacción, pero las expectativas eran más altas. Respecto del coste, este 30% es compatible con el 54% de participantes que lo declaran motivo para abandonar la Nube, si bien se esperaba una mayor satisfacción debido a la insistencia en este mensaje por parte de los proveedores.

Respecto del uso por los competidores, este parámetro trataba de identificar a las entidades que tomaban la decisión de uso de servicios en la Nube por imitación de decisiones similares de sus competidores. Este efecto de viaje a la Nube por mimetismo suele corresponder con organizaciones más susceptibles de no haber evaluado correctamente sus necesidades de servicio, los riesgos derivados de este viaje, las necesidades y requisitos específicas que se desean satisfacer, y, por lo tanto, la probabilidad de que las organizaciones contraten servicios que luego finalmente no son necesarios y generen insatisfacción el gasto generado por los servicios contratados y que no fueron de utilidad. Sin embargo, el 25% de organizaciones resulta un número por debajo de las expectativas, evidenciando que las organizaciones reflexionan con más intensidad sobre su decisión en el viaje a la Nube.

Respecto de la facilidad de contratación, el 25% de usuarios que señalan la fácil contratación es también un valor menor del esperado. Los analistas esperaban que las capacidades de auto provisión que ofrecen los proveedores de Nube facilitasen la contratación de nuevos servicios y que esta característica fuera apreciada y utilizada. Sin embargo, esta operación favorecería una mayor frecuencia en el uso de servicios en ShadowIT, aspecto que se evalúa más adelante como un factor negativo. Por ello, el valor obtenido es consistente con los resultados de otros campos de la encuesta, y las expectativas de los auditores no estaban fundadas.

El resto de los factores no merecen un análisis más detallado ni ofrecen conclusiones de valor.

Los motivos operativos (disponibilidad, flexibilidad, operaciones) fundamentan las razones de uso de Nube por las organizaciones

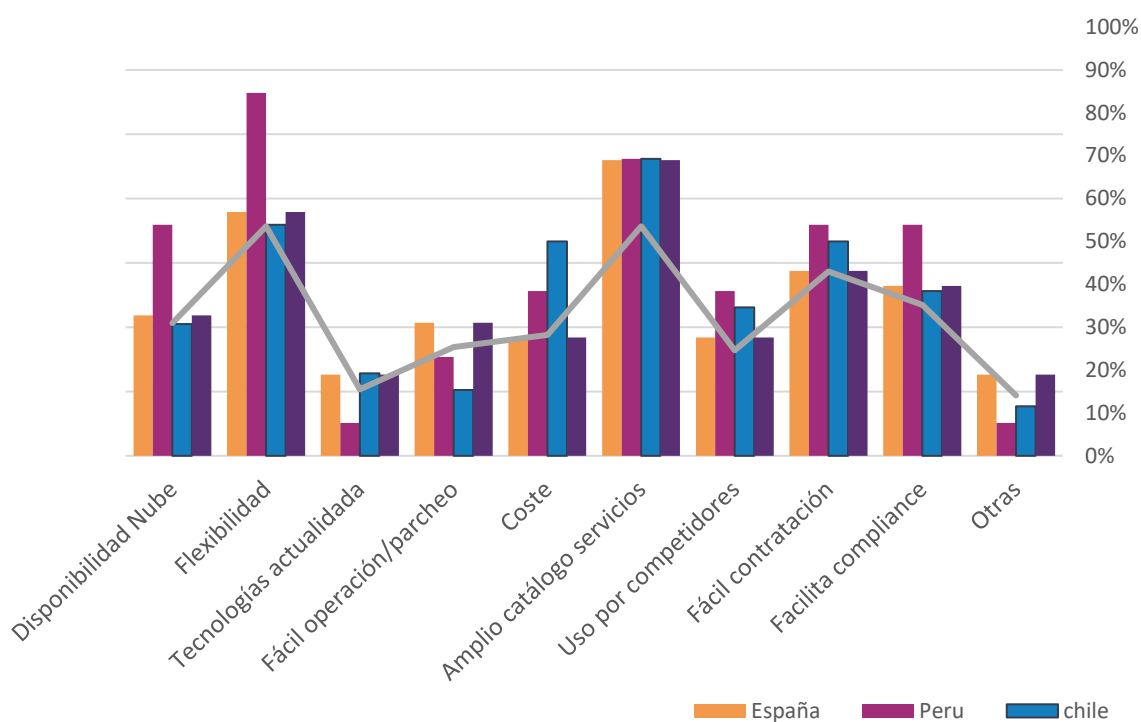


Ilustración 4.- % organizaciones por geografía que fundamentan el uso de Nube en cada característica identificada

La Ilustración 4 muestra un análisis de los datos de la Ilustración 3 introduciendo el factor geográfico, para aquellos países que han aportado una muestra de datos significativa. Este análisis aporta algunos elementos de interés, como:

- La importancia que prestan las empresas peruanas por encima de otros países al coste de los servicios, la actualización de tecnologías y parches, la disponibilidad del servicio.

- Chile valora también la flexibilidad de servicios y el catálogo de servicios.
- Los valores de España y Chile no tienen discrepancias significativas.



Los motivos operativos para uso de la Nube tienen una dependencia limitada de factores geográficos.

1. Tipología de Servicios consumidos en la Nube

Tras analizar el estado de adopción de los servicios en la Nube por las organizaciones, y los distintos escenarios y casos de uso y de no uso identificados, este capítulo del Estudio se centra en entender qué servicios se demandan, como se consumen y qué proveedores de servicios en la Nube tienen una mayor demanda por sus consumidores

1.1. Relevancia de los Proveedores de Servicios en la Nube (CSP)

El Estudio indaga en detalle el perfil de proveedores de servicios en el Nube (CSP) que en los que se están efectivamente apoyando los usuarios y el grado de consumo de sus servicios por los participantes en el Estudio.

La Ilustración 5 muestra el porcentaje de participantes en el Estudio, comparando el peso relativo de cada uno de ellos, y comparándolo con los valores obtenidos para estos parámetros en el 11º Estudio en el año 2023. El análisis de los datos dibuja un escenario razonablemente estable, con tres proveedores principales (Amazon, Azure y GoogleCloud) que prestan servicio respectivamente a dos (Google), tres (Amazon) y cuatro (Azure) de cada cinco de los participantes del Estudio que se declaran usuarios de la Nube. Y, combinando a los tres, el 95% de estos participantes se declaran usuarios de alguno de ellos. De hecho, un 24% de ellos se declaran usuarios de estos tres proveedores.

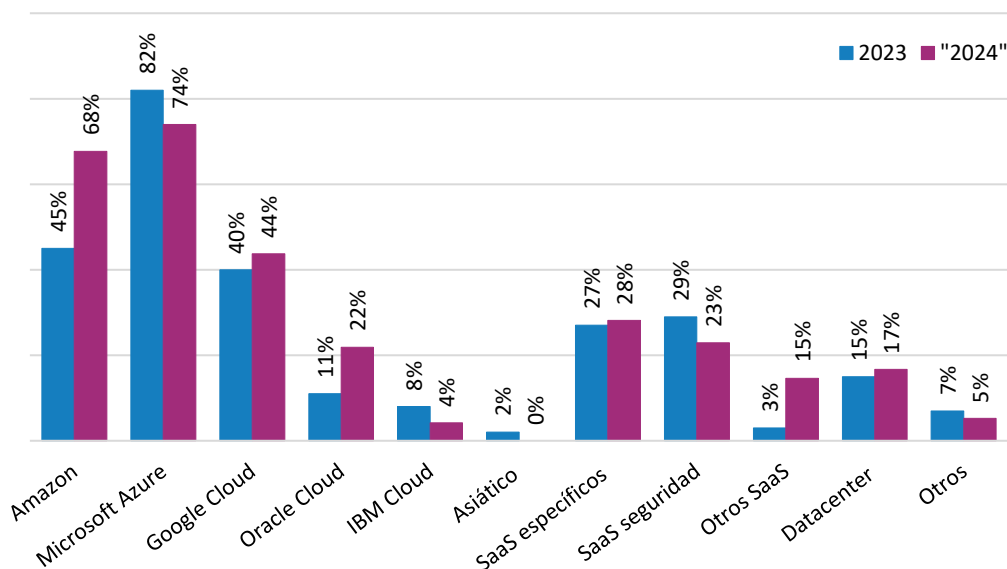


Ilustración 5.- % de penetración de los CSP en las organizaciones

Estos resultados confirman la expectativa previa respecto de la mayor cuota de mercado centrada en tres CSPs: Amazon, Azure y Google Cloud. En este caso, con una ligera bajada en la proporción de los servicios de Azure y subidas de los otros dos proveedores.



El 94% de usuarios se apoya en servicios de Azure, Amazon y/o Google.

El análisis detallado del uso de proveedores de servicios en la Nube en relación con el tamaño de la organización que los consume se muestra en la Ilustración 6. Como era de esperar, la relación en el uso de los proveedores es consistente con el diagnóstico realizado anteriormente. Pero pueden observarse algunos elementos relevantes.

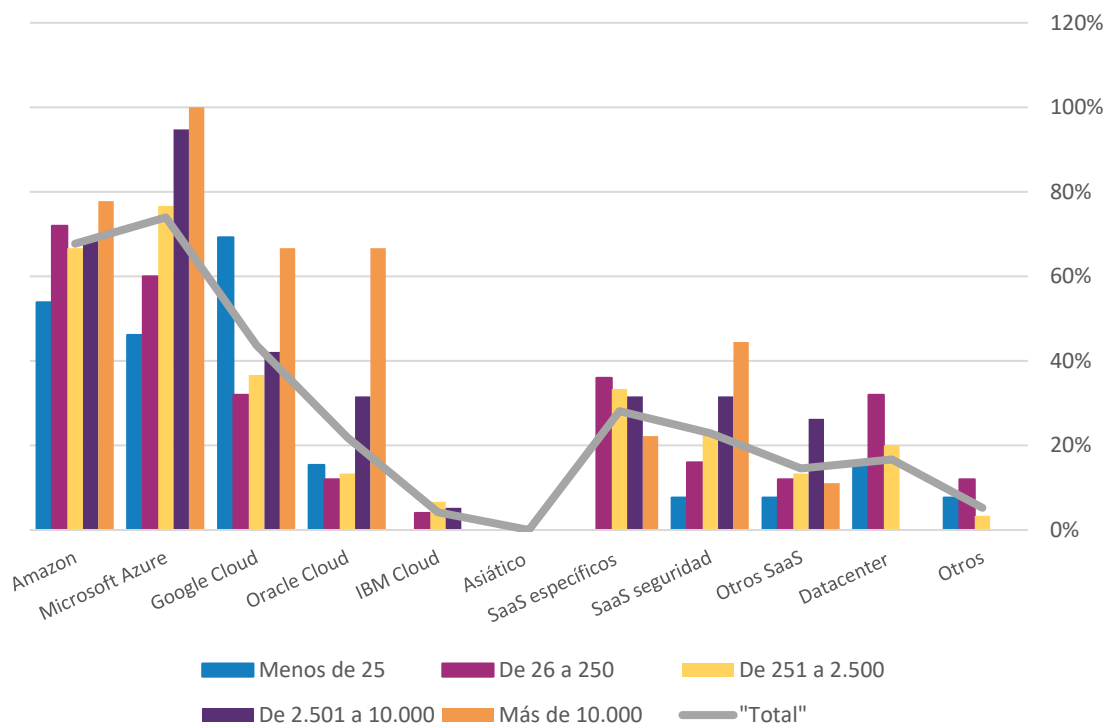


Ilustración 6.- Intensidad de Uso de Proveedores de Nube por Tamaño de Organización que los consume

Un de ellos es que las organizaciones de menor tamaño (menos de 25 empleados) son las mayores usuarias de servicios de Google, con gran preferencia sobre el resto de los proveedores. Las empresas de mayor tamaño también hacen un uso intensivo de servicios de este CSP. Por otra parte, Azure es la preferida por las empresas de tamaño medio y grande, con porcentajes de penetración que ronda o supera el 80% y que llega al 100% en las empresas de mayor tamaño.

Estas empresas de más de 10.000 empleados apuntan a ser los usuarios más frecuentes de los servicios en la Nube.

Abundando en este argumento, también debe destacarse el uso de la Nube del proveedor Oracle, que está por encima del 60% en las organizaciones de más de 10.000 personas. Este modelo está en la misma intensidad de uso que los otros tres grandes proveedores, rondando el 70% de los usuarios. También se detecta una mayor intensidad de uso en IBM Cloud Services.

El uso de SaaS específicos que no son de seguridad tiende a utilizarse más a medida que la organización es más pequeña, rozando el 40% en el caso de las PYMES y sobre el 20% para organizaciones muy grandes. Las empresas de menos de 25 usuarios no usan apenas estos servicios ni los servicios de Datacenter clásico, que siguen también este mismo perfil de uso.

El uso de CSP específicos que proveen de servicios de seguridad desde la Nube aumenta cuando las organizaciones son de mayor tamaño, y se sobrepasa el 40% para las de mayor tamaño.

Este escenario es generalmente consistente con los resultados obtenidos en ediciones anteriores del Estudio, incluso en los matices destacados del uso de SECaaS y de Oracle Cloud y el uso de servicios de Google por empresas de menor tamaño.



Las empresas de mayor tamaño consumen servicios en la Nube con más intensidad, mientras que las empresas de menos de 25 empleados usan sobre todo GoogleCloud.

El Estudio también ha analizado la intensidad de uso de servicios Cloud en las organizaciones.

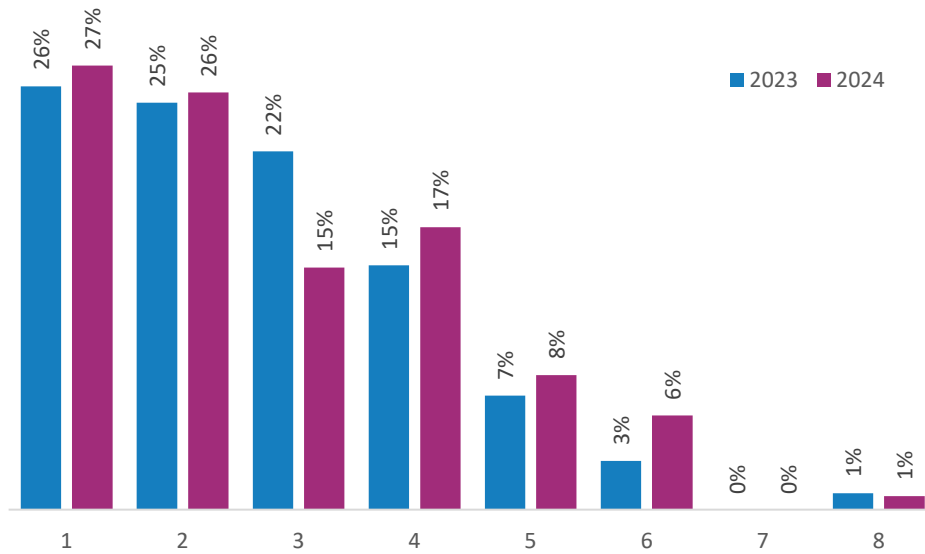


Ilustración 7.- Distribución del número de CSPs contratados

La Ilustración 7 recoge la distribución de los participantes en la encuesta según el número de CSPs cuyos servicios utiliza. En ella se observa que sólo uno de cada cuatro empresas tiene un único CSP y tienen un mayor riesgo de efecto Locked-in global con su CSP. Las empresas con este perfil de riesgo corresponden con las empresas pequeñas y medianas, puesto que en general tienen un número menor de proveedores. La Ilustración permite detectar un ligero desplazamiento de las empresas que utilizan tres CSP distintos para, en general, utilizar un número mayor de ellos. Este efecto puede deberse al uso mayor de servicios SaaS de distintos tipos que se ha detectado.

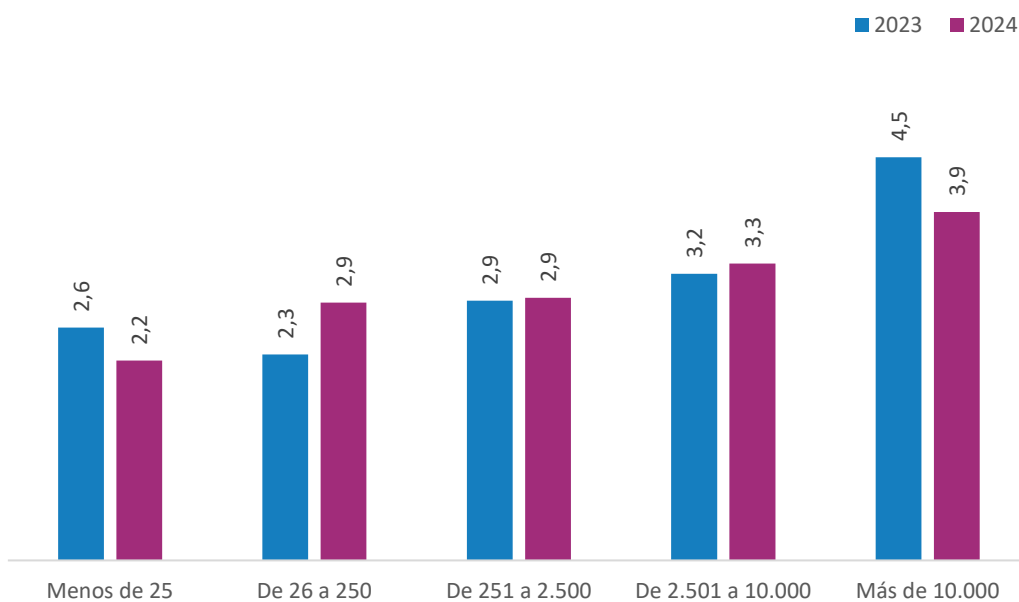


Ilustración 8.- Número de CSPs contratados por las organizaciones, según su tamaño

Por otra parte, si analizamos el número de CSP utilizados por cada organización en función de su tamaño que se muestra en la Ilustración 8, se observa que son las empresas de mayor tamaño las que tienen un uso más intenso de los servicios en la Nube. Esta valoración es consistente con los valores obtenidos en los análisis realizados anteriormente para otros parámetros. En una perspectiva histórica, el número medio de proveedores en la Nube aumenta en las organizaciones de tamaño mediano, mientras que en las empresas de mayor y menor tamaño disminuye este número promedio de CSPs.



Las organizaciones trabajar mayoritariamente en entornos multicloud con múltiples CSPs.

1.2. Servicios de la Nube demandados por los usuarios

La Ilustración 9 muestra el distinto uso de los Servicios en la Nube que hacen los participantes en el Estudio. La ilustración muestra el porcentaje de empresas participantes en el Estudio que están usando este servicio en particular, para luego desglosar ese uso en función del tamaño de las empresas. Esta ilustración aplica los criterios definidos para la misma en la 11ª Edición del Estudio del año 2023, valorando las organizaciones que se han declarado usuarias actuales de los servicios en la Nube, y con las consideraciones geográficas establecidas para esta edición.

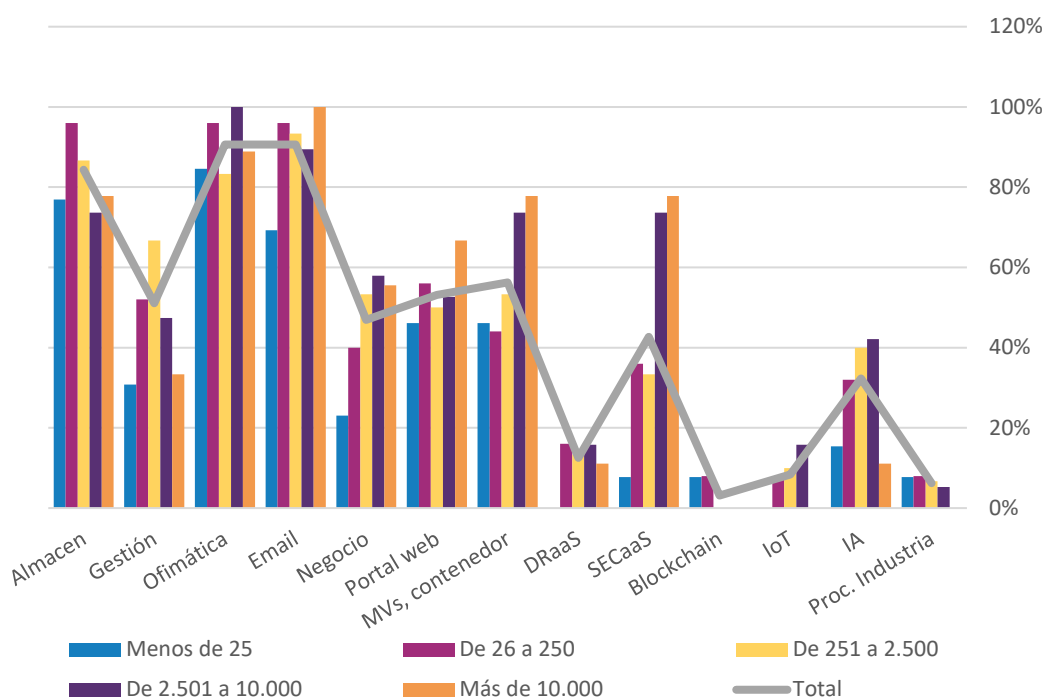


Ilustración 9.- Diferencias en el uso de servicios en la Nube según el tamaño de la organización

En primera instancia, la Ilustración 9 confirma algunas conclusiones ya establecidas anteriormente, como el uso de soluciones de SECaaS por los participantes en empresas de mayor tamaño. También el uso de soluciones de contenedores y máquinas virtuales es mayoritario en este perfil de empresas.

Por otra parte, la trilogía de servicios “correo electrónico” + “ofimática” + “almacenamiento” es el servicio más consumido por las organizaciones, en todos los tamaños de las empresas, llegando a tasas de uso superiores al 90% de los participantes. Este grado de uso sigue la tendencia detectada en el anterior estudio, donde ya eran los servicios más utilizados con un 80% de los usuarios y un crecimiento en 10% porcentuales sobre el 10º Estudio, realizado en 2022.

Esta 12ª Edición consultaba a los participantes por primera vez sobre su uso de la Nube como soporte para los servicios de IoT, Blockchain, Disaster-Recovery-as-a-Service, IA y soporte a procesos industriales. En casi todos los casos, se ha detectado un uso puntual de estas tecnologías que se queda en el 10% de usuarios, salvo en el caso de los servicios IA, para los que uno de cada tres participantes en el Estudio se declaran usuarios, con mayor intensidad de uso en empresas de mayor tamaño. Estas empresas son las que con más frecuencia han mostrado casos de uso y aplicaciones prácticas de su adopción de estas tecnologías, conclusión a la que se suma el Estudio. Esta intensidad de uso se alinea con las expectativas creadas en todos los sectores entorno a la Inteligencia Artificial Generativa.



Almacenamiento, Ofimática y Correo Electrónico son los servicios en la Nube más consumidos. Los servicios de IA en la Nube también tienen un uso creciente.

1.3. Estrategias Cloud-First y Cloud Only

Son numerosas las organizaciones que, a lo largo del tiempo, han declarado o establecido que todos los servicios TI de su organización deben ser prestados desde la Nube (estrategia *Cloud-Only*) salvo, cuando tras valorar el servicio en la Nube, sea imposible o ineficiente hacerlo de esta forma frente a otras opciones (Estrategia *Cloud-First*). Estas dos estrategias son dos opciones ampliamente valoradas por las organizaciones para dirigir la adopción de estos servicios. Su éxito está condicionado por la complejidad de la arquitectura previa de servicios TI de la organización y a la tipología de servicios concreta. En este sentido, las organizaciones de reciente creación parten de un escenario que facilita estas estrategias, mientras que las organizaciones de mayor tamaño, complejidad y madurez pueden encontrarse con más dificultades y con más escenarios particulares.

La Ilustración 10 desglosa a los participantes en el Estudio que se han declarado usuarios de la Nube de acuerdo con la intensidad en su uso de los servicios de la Nube, y comparando la situación en el 11º Estudio (año 2023) con la detectada en esta edición.

Esta Ilustración 10 añade un elemento más de refuerzo al incremento del uso de servicios en la Nube detectado previamente, con reducción del número de organizaciones que hacen un uso puntual de la Nube, utilizando algún servicio individualizado, mientras que aumenta significativamente respecto del año pasado las organizaciones que usan la Nube en el 90% de sus servicios TI. Aun así, la mayoría de las organizaciones hacen un uso menos intenso de la Nube, con un equilibrio entre las organizaciones que tienen en la Nube más de la mitad de sus servicios con aquellas que aún no tienen ese porcentaje de servicios prestado desde la Nube. En ambos casos, esencialmente mantienen los datos obtenidos en la anterior edición del estudio.

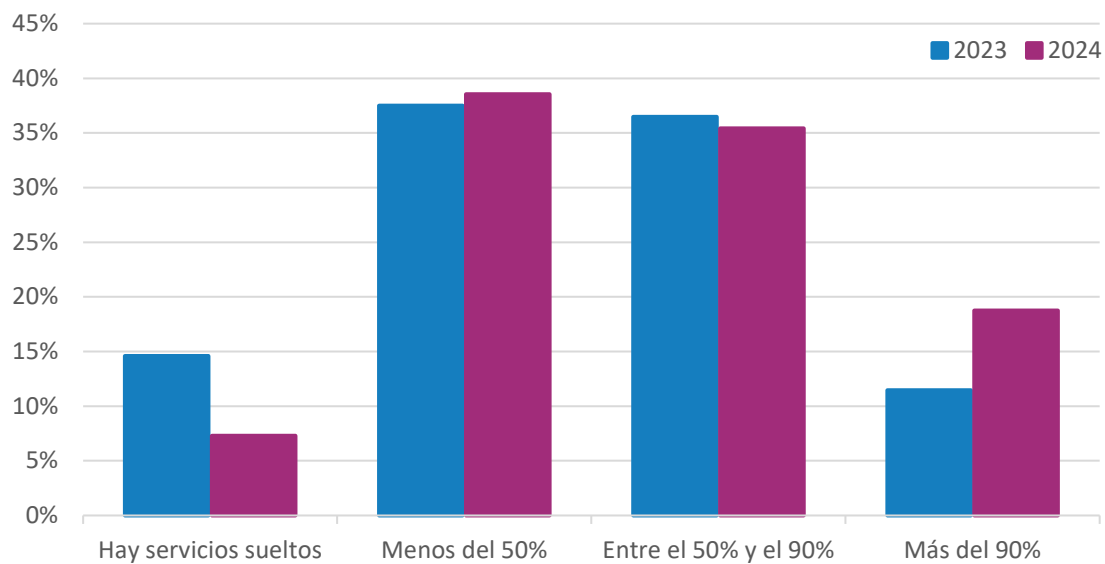


Ilustración 10.- Intensidad de uso de Servicios en Nube sobre el total de Servicios TI



Si bien aumenta quienes aplican estrategias Cloud-First o Cloud-Only, sigue predominando un uso medio de estos servicios.

Analizando la dependencia del tamaño de la organización usuaria respecto de su uso de los servicios en la Nube, la Ilustración 11 muestra que las organizaciones de menor tamaño son las que han logrado completar la estrategia *Cloud-Only* con más éxito, probablemente porque el número de servicios que precisa una organización de ese tamaño es menor, y, además, pueden ser obtenidos de forma rápida y cómoda a través de servicios SaaS en la Nube. De hecho, en la

Ilustración 9 se identificaba que estas empresas estaban utilizando fundamentalmente servicios de correo, almacenamiento y ofimática que son todos los servicios que necesitan muchas empresas de este tamaño. Quizás sí que precisen aplicaciones específicas de negocio o de gestión propias de su sector, y por ello en algunas organizaciones declaran un uso menos interno.

Por el contrario, las organizaciones de más tamaño tienen una mayor dispersión en el número de servicios que utilizan, y la probabilidad de que precisen de servicios más especializados se incrementa. En las organizaciones de más tamaño, muchos de estos servicios (SECaaS, virtualización y otros) se pueden apoyar en servicios en la Nube, por lo que el uso de servicios puntuales queda más reducido que en las organizaciones de miles de usuarios.

Según se muestra en la Ilustración 11, no hay una tendencia clara en relación con los servicios TI adoptados en la Nube, ya que si bien parece que la tendencia es que el porcentaje de organizaciones con más del 50% de los servicios TI en la Nube crezca según el tamaño de estas, esta tendencia se rompe con la gran empresa entre 2.500 y 10.000 empleados. Este hallazgo es razonable, en tanto que las organizaciones de menor tamaño precisan de un número menor de servicios para operar y se trata de servicios básicos (correo, almacenamiento, ofimática) que son consumidos por muchas organizaciones. De esta forma, y por mero efecto estadístico, el porcentaje de organizaciones con aproximaciones *Cloud-Native* y *Cloud-First* es más elevado que en otras organizaciones que consumen un mayor de servicios y por ello, estos servicios significan una proporción numéricamente inferior por ser mayor el total de servicios.

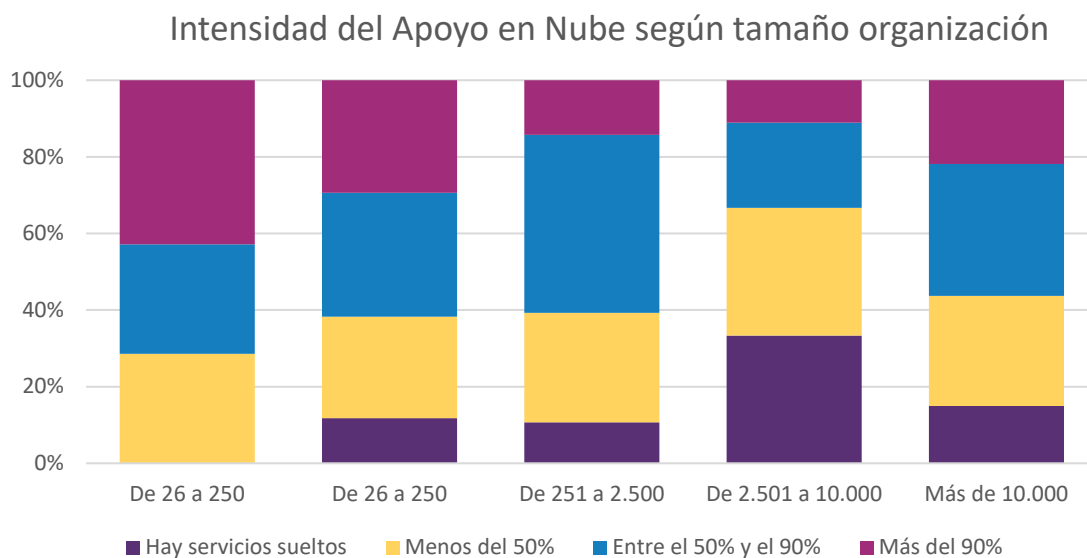


Ilustración 11.- Porcentaje de Servicios TI basados en la Nube de las organizaciones, según su tamaño



Las empresas de menor tamaño son las que han completado en mayor proporción las estrategias *Cloud-Only* o *Cloud-First*.

2. Análisis de Expectativas de los Usuarios de la Nube

Este capítulo presenta el análisis de las expectativas sobre la seguridad que manifiestan los participantes en el Estudio. Este análisis incluye al total de estos, tanto los que actualmente están usando servicios en la Nube como los que ya han dejado de usarlos (pero los han utilizado alguna vez) o no se plantean hacerlo.

Para ello, se analizan las principales dimensiones de seguridad de la información además de otros campos relacionados como el cumplimiento legal o la privacidad, estableciendo la importancia que les otorgan los usuarios.

El primer análisis realizado presenta la evolución histórica desde el año 2019 de la importancia otorgada a estas dimensiones. Como se explica en el capítulo “Consideraciones sobre posibles sesgos en la información analizada”, la serie histórica de datos tiene diferencias en la muestra de datos analizada frente a la muestra de esta edición del estudio. Por ello, la Ilustración 12 ha utilizado los datos que continúan la muestra eliminando los sesgos adicionales.

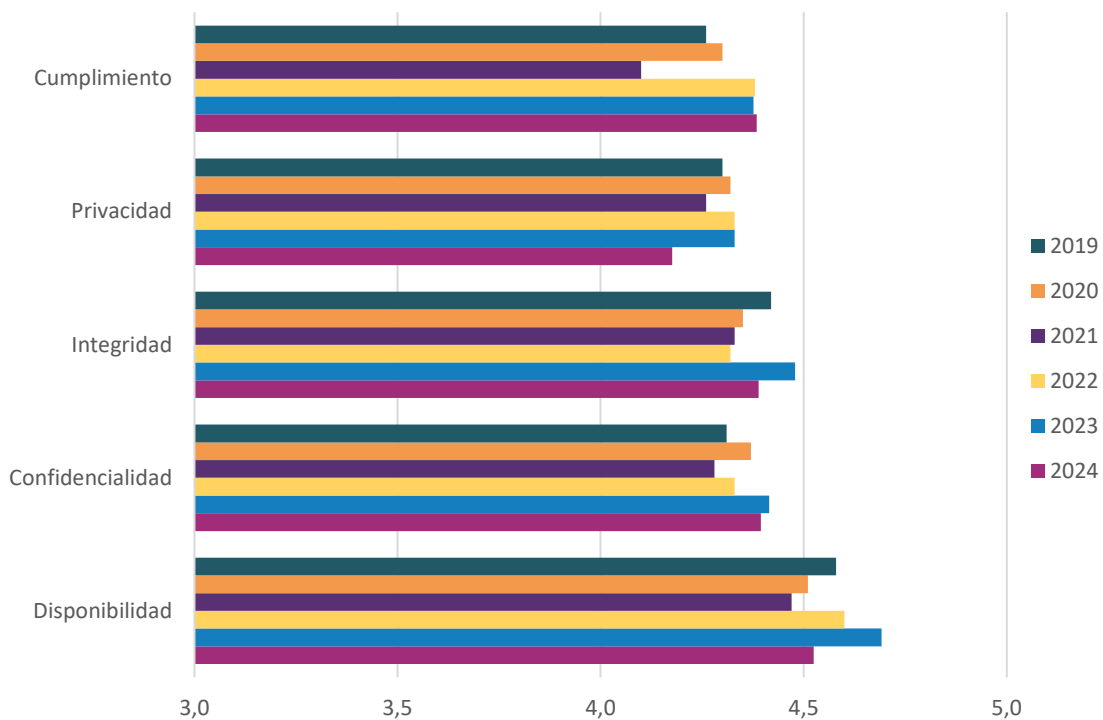


Ilustración 12.- Evolución de Expectativas de Seguridad de los usuarios de servicios en la Nube

El principal resultado del análisis es la reducción de todas las expectativas de seguridad con respecto a la 11ª edición del estudio, correspondiente al año 2023. El descenso es prácticamente

nulo en la dimensión de cumplimiento, y más acusado en la privacidad, mientras que el decrecimiento de las demás dimensiones de los parámetros es pequeño.

El equipo de analistas del Estudio no ha encontrado un patrón o motivo para esta variación en los resultados de esta edición, aunque quizás pueda estar en el impacto que ha supuesto la adopción de técnicas de IA por las organizaciones. En realidad, los valores que toman estos parámetros son comparables a los de años anteriores, por lo que puede interpretarse que este descenso leve no tiene una motivación más allá y que los valores se encuentran dentro de los márgenes de error estadísticos.



Las expectativas mantienen valores comparables a los de anteriores Estudios, con un leve retroceso. Las expectativas en privacidad descienden algo más.



En cuanto a las expectativas de seguridad por países, las expectativas son distintas en cada lado del Océano Atlántico. Mientras que, en el lado europeo y español, estas expectativas están en valores muy altos, por encima de los 4,7 puntos de valoración, los valores en el lado americano están más cerca de unas expectativas Simplemente altas (4 puntos de valoración). En este ámbito, las expectativas en Chile son las más exigentes en Chile, rondando los 4,5 puntos, mientras que Bolivia no llegan a este valor alto y en Argentina las expectativas se desploman hasta quedarse en un nivel medio. Estos están claramente impactados por regulaciones locales en algunas geografías o sectores o para empresas de la Administración Pública Bolivianas o sector financiero chileno, que exigen la presencia local de nodos de Nube en el país para poder consumir sus servicios, y que hacen más compleja la adopción de servicios en la Nube.

Estas diferencias son más notables en el caso del Cumplimiento y la Privacidad, mientras que la exigencia en Disponibilidad son las más altas en casi todos los países.

El Estudio apunta a que las diferentes presiones regulatorias en cada una de las geografías, tanto en el ámbito de privacidad (GDPR) como en otros ámbitos (NIS2, DORA, directivas de ciberseguridad y otras) han creado un escenario de mayor concienciación en las organizaciones respecto de las consecuencias de no cumplimiento de estas regulaciones, ya sea en las organizaciones como en su cadena de suministro. Incluyendo en ella a los proveedores de servicios en la Nube.



Ilustración 13.- Expectativas sobre los Servicios en la Nube, desglosado por países



Las expectativas sobre los servicios en la Nube son más elevadas en Europa que en América. La diferencia es más acusada en Cumplimiento Legal y Privacidad.

Respecto al tamaño de la organización, se aprecia que las expectativas crecen con arreglo al tamaño de la organización. Las organizaciones de menor tamaño se limitan a tener expectativas simplemente altas, mientras que las de mayor tamaño tienen expectativas significativamente más altas. Las organizaciones de más de 10.000 empleados bajan algo sobre las de tamaño inferior. El Estudio deduce que estas organizaciones suelen tener una huella eminentemente internacional, que las obliga al cumplimiento de una disparidad de criterios, reglamentos y regulaciones en ocasiones contradictorias, y que reducen la expectativa sobre la capacidad de cumplimiento de todos ellos. La Ilustración 14 muestra la evolución de los indicadores descrita anteriormente.

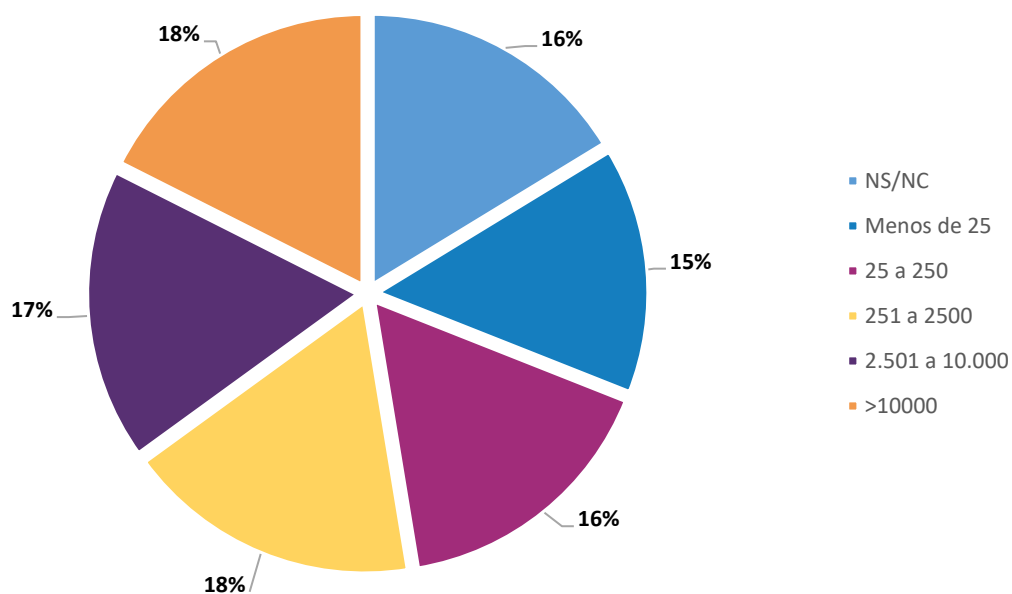


Ilustración 14.- Expectativas sobre los Servicios en la Nube, desglosado por Tamaño de Organización



Las organizaciones tienen expectativas más modestas sobre la seguridad de los servicios en La Nube cuando tienen un tamaño a su vez más modesto.

Finalmente, se analiza la dependencia que tienen las expectativas de los usuarios de la Nube en función de sus expectativas de uso futuro de la Nube, o del uso presente de la misma. Para ello, y como se han tratado en el capítulo “¿Están las organizaciones abandonando la Nube?”, se analizan por separado a las organizaciones que están usando todos los servicios en la Nube, lo que usan servicios, aunque han abandonado alguno, los que han dejado la Nube después de

usar servicios, y los que no están usando servicios en la Nube, sea porque ya han decidido descartar su uso o sea porque hay una puerta abierta a un uso futuro.

La Ilustración 15 muestra este análisis, donde se identifica con claridad como las expectativas sobre el uso de la Nube está directamente relacionada con la decisión tomada respecto del uso de estos servicios. Así, los usuarios de Nube que mantienen todos sus servicios son los más exigentes en sus expectativas, y los que no se plantean usar la Nube en ningún caso tienen las expectativas menos exigentes, quedándose en un nivel medio alto. El Estudio deduce que este parámetro está derivado de la experiencia de usuario (real, supuesta, o percibida a través de terceros) sobre los servicios en la Nube y su capacidad de satisfacer todos los requisitos.

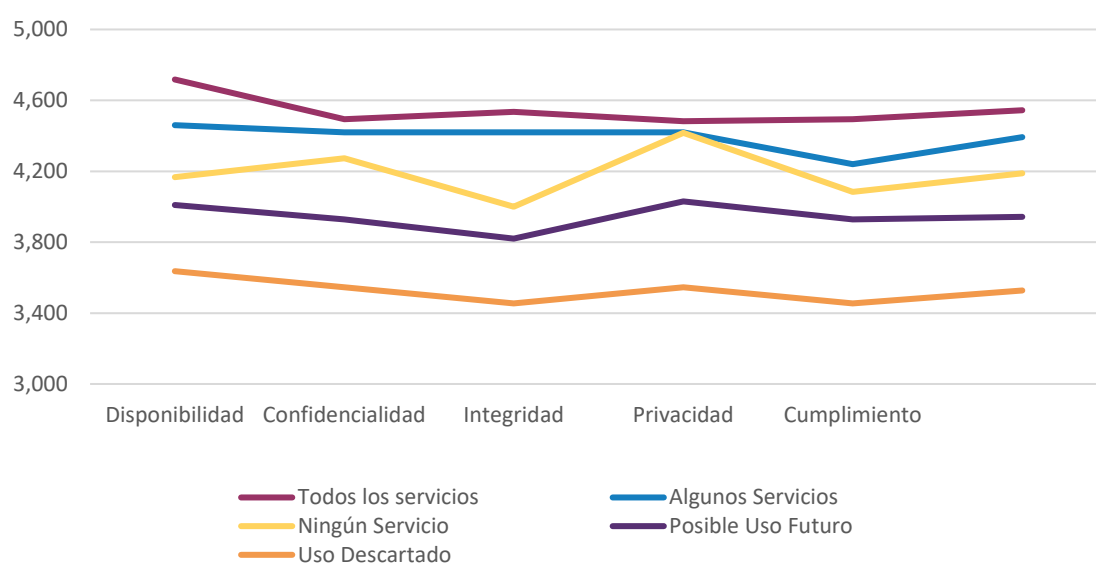


Ilustración 15.- Expectativas sobre los Servicios en la Nube, según su estrategia de Nube



El nivel de expectativas sobre el uso de servicios en la Nube está directamente relacionado con estrategia de adopción de la Nube: Las estrategias más intensas generan mayores expectativas.

3. Requisitos exigidos por los usuarios a los prestadores de servicios en la nube

El uso de servicios en la Nube supone de facto la contratación de la prestación de servicios TI por la organización en un tercero, en el CSP. Esta contratación de servicios está sujeta a las necesidades exigibles por las organizaciones a sus proveedores. El CSP por ello debería ofrecer garantías y confianza de que va a satisfacer los requisitos de seguridad jurídica y técnica exigidas por el usuario al prestar los servicios contratados. No obstante, los servicios de la Nube y sus proveedores no siempre pueden satisfacer en toda su extensión el total de requisitos deseados por el usuario de la Nube, ya sea porque ha diseñado sus servicios en ciertas condiciones que no son exactamente y en todos sus detalles coincidentes con los deseados por el usuario. En otros casos, es el propio usuario quien modula sus expectativas iniciales de seguridad y no las exige en toda su intensidad inicial, renuncia a ciertos requisitos, o prioriza el cumplimiento de estos requisitos. Por último, algunos requisitos pueden ser satisfechos, pero los recursos precisos para ello son simplemente excesivos o no rentables, y se renuncia a ellos.

Por todas estas razones, resulta viable analizar los requisitos concretos que los usuarios piden que sean satisfechos por los CSPs con sus servicios, y separar el análisis del realizado en el capítulo anterior **“Análisis de Expectativas de los Usuarios de la Nube”**.

La Ilustración 16 muestra la evolución en el último año del nivel de exigencia en los diversos requisitos exigibles por los usuarios de servicios en la Nube a sus proveedores.

Como primer resultado, no es fácil apreciar un patrón claro de evolución de estos indicadores, porque prácticamente hay tantos indicadores que evolucionan al alza, como los que evolucionan a la baja. Sin embargo, la evolución del nivel medio de exigencia de requisitos sí evoluciona a la baja, con un descenso de algo más de una décima en el valor promedio. De hecho, en el año 2023 todos los requisitos superaban el nivel de exigencia alto (valor 4), mientras que sólo 5 de los 10 criterios lo consiguen en este año. La horquilla de valores oscila en este año entre los valores 3,73 y 4,25, mientras que en el año 2023 los requisitos estaban en la horquilla entre el 4,13 y el 4,58. Por ello, El promedio baja del 4,34 al 4,21, un 7,6%. La Ilustración 23 muestra esta evolución con mucho más detalla que la Ilustración 16. Los analistas interpretan este descenso en el nivel de requisitos desde una perspectiva histórica, y con la vista en el Covid19.

Durante ese periodo, el nivel de exigencia en los requisitos aumentó significativamente en ese periodo por la dependencia crítica en los servicios en la Nube que tenían los procesos de trabajo remoto implantado como respuesta a esta crisis. Como resultado, muchas organizaciones incrementaron su consumo de estos servicios, la dependencia de las organizaciones en ellos y la importancia de mantener la continuidad y seguridad de los servicios. Pero, aunque se ha establecido esa mayor necesidad, repercusión y dependencia de los servicios en la Nube, la crisis Covid19 ha remitido y con ella se ha limitado la excepcionalidad del uso de servicios en la Nube

y la preocupación de las organizaciones por sus requisitos. Son mayores que antes de la pandemia, porque hay mayor consumo de servicios en la Nube, pero no son tan acuciantes como durante la crisis. Por ello, el nivel de requisitos se relaja respecto de 2023.

La pregunta que se plantea para futuros estudios es si este descenso de exigencia continuará en el tiempo y recuperará la tendencia histórica previa al Covid19, y este periodo quedará como una situación excepcional, o si establecerá una nueva tendencia con valores medios más altos en el nivel de exigencia de estos requisitos.

La segunda tendencia tiene que ver con la evolución de unos de los requisitos: El control de acceso de la información del usuario de servicios en la Nube por el personal del proveedor de servicios en el Nube. Este valor desciende de forma abrupta, desde una exigencia muy alta a no llegar apenas a alta. El análisis más detallado de la evolución de este indicador no ofrece ninguna indicación de las razones para esta caída o la tipología de organizaciones que modifican su valoración: El descenso en la exigencia de este requisito es generalizado para todas las geografías, tamaños de empresas y sectores. El equipo de analistas tampoco ha podido identificar otra causa externa (incidente, regulación, evolución de porfolio de servicio de los proveedores, cambio de modelo u otras) que pudieran explicar este cambio. Simplemente, cambia de forma abrupta.

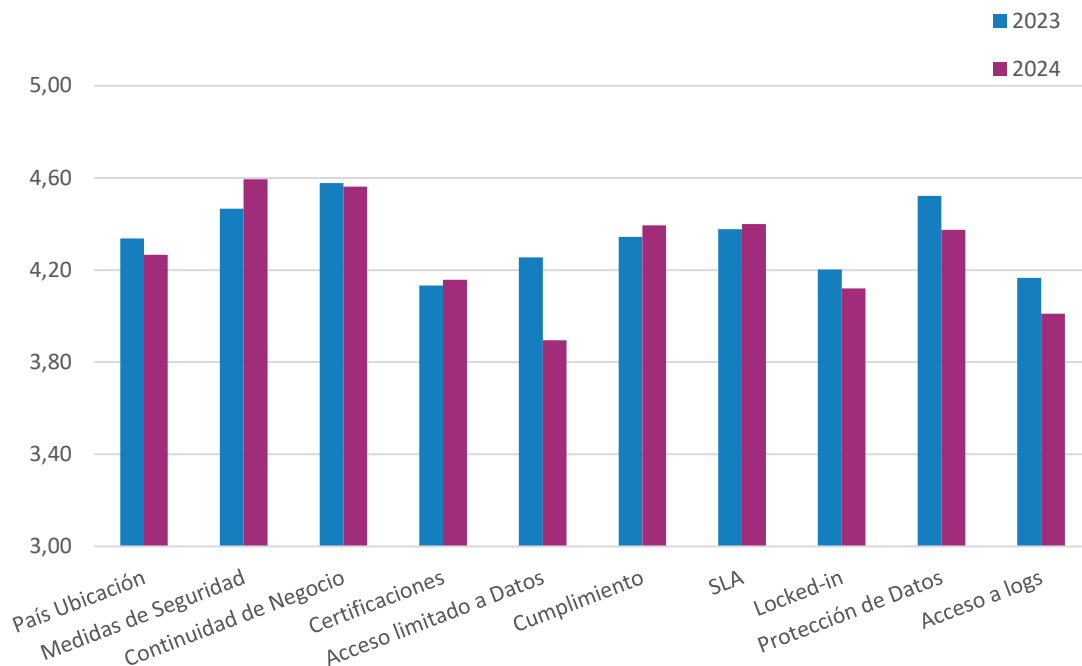


Ilustración 16.- Comparativa de Requisitos entre el año 2023 y 2024

El tercer análisis se centra en los requisitos donde los usuarios son más exigentes. Los encuestados siguen destacando entre los tres criterios mejor valorados la continuidad de negocio del CSP y las medidas de seguridad que proporciona el proveedor, siendo las medidas de seguridad las que en 2024 son mejor valoradas. Este dato puede ser el resultado de considerar al proveedor de Nube también como un proveedor que proporciona altas capacidades en sus propias herramientas de seguridad.

Otra de las razones podría ser la reducción de costes operativos que puede significar unificar en un solo proveedor las operaciones de elementos de seguridad, así como la operación de otras tecnologías.

Se observa también que varía la importancia que se concede a otros requisitos de seguridad. Además de lo ya indicado sobre las medidas de seguridad y la continuidad, se valora mejor que en el año 2023 el cumplimiento de normativas en general y de certificaciones del proveedor, y sin embargo el cumplimiento del reglamento de protección de datos baja al 5º puesto desde el 2º, aunque las diferencias no son grandes.



La exigencia en requisitos desciende en promedio, en particular en el acceso del proveedor a los datos de sus usuarios. Las medidas de seguridad y las garantías de continuidad de negocio de los proveedores siguen siendo los requisitos con mayor exigencia.

El análisis de la exigencia de requisitos en función del tamaño de las organizaciones, que se muestra en la Ilustración 17, resulta tan revelador como alineado con conclusiones obtenidas previamente para las expectativas de usuario (en la Ilustración 17): Hay una relación prácticamente directa entre el tamaño de la empresa y el nivel de exigencia de requisitos, siendo las organizaciones de mayor tamaño las que la demandan con más intensidad.

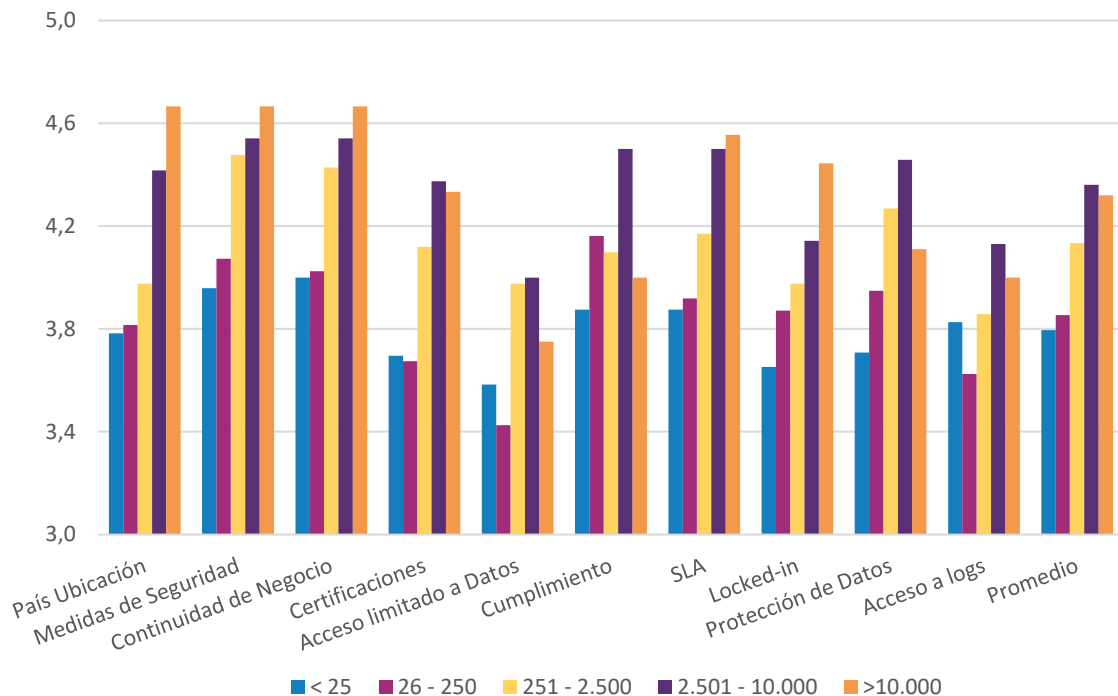


Ilustración 17.- Nivel de exigencia en los Requisitos de Seguridad en función del tamaño de la empresa

Existen algunas mínimas discrepancias en estos valores para algunos requisitos, con cambios de orden entre las organizaciones de más de 10.000 empleados y las de más de 2.500 empleados, y entra las empresas de más o menos de 25 empleados. Únicamente cabría destacar el nivel de exigencia en cumplimiento legal de las empresas de mayor tamaño, que está muy por debajo de las empresas de 2.500 empleados, y también por debajo de las organizaciones de tamaño medio. Probablemente, porque estas empresas de más tamaño son multinacionales con presencia y necesidad de cumplimiento de múltiples legislaciones y no tienen altas expectativas respecto de la complejidad y dificultad del cumplimiento de todas y cada una de las legislaciones, tanto propio como de proveedores.



La exigencia en requisitos se incrementa a medida que crece el tamaño del usuario de servicios en la Nube.

Resulta también aclaratorio replicar este análisis valorando la influencia del perfil profesional de la persona que proporciona la información del uso de servicios en la Nube por su organización. Este análisis, que se muestra en la Ilustración 18, establece claramente una relación muy asimilable entre el nivel de responsabilidad de la persona con la exigencia en requisitos.

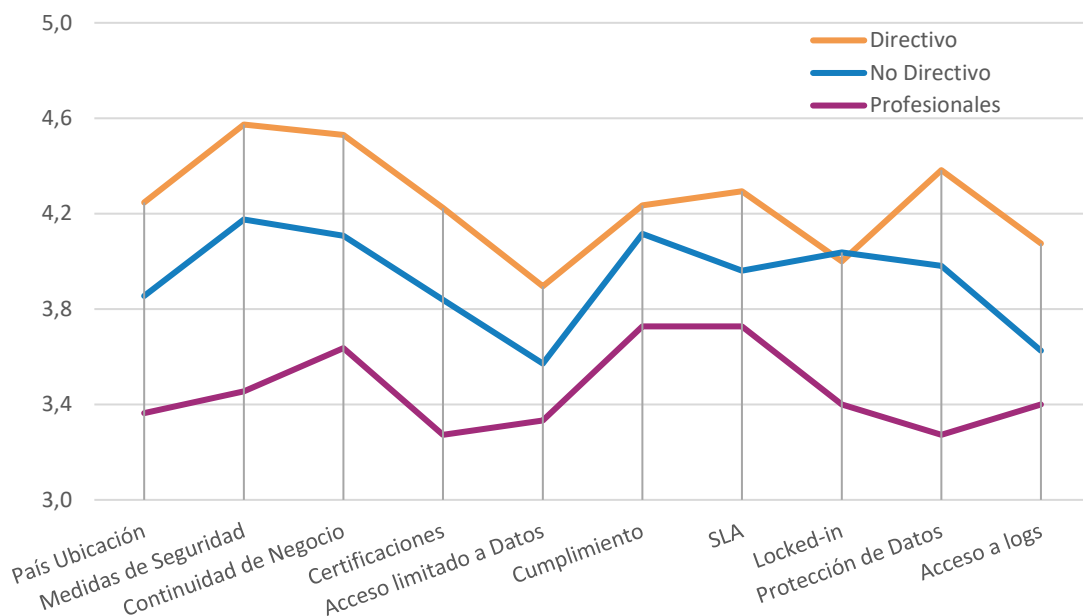


Ilustración 18.- Nivel de exigencia en los Requisitos de Seguridad por perfil de responsabilidad en la Empresa

Son los perfiles directivos los más exigentes en el establecimiento de estos requisitos, con una diferencia de incluso dos décimas sobre los perfiles técnicos de las organizaciones, salvo por el efecto Locked-in, que quizás sean más fácilmente entendibles y generan un mayor sufrimiento (cuando ocurren) en los perfiles técnicos que conviven con los proveedores. Los analistas del Estudio plantean que esta diferencia en el Estudio se genera por las posibles derivadas y responsabilidades para los directivos que supone una incorrecta selección de proveedores de servicios en la Nube. Por ello, la demanda de requisitos es mayor en estos perfiles.

El tercer perfil que aparece en la Ilustración 18 corresponde con los profesionales independientes y expertos que desempeñan sus funciones a título personal. Estos profesionales tienen una exigencia de requisitos menor, que los analistas establecen derivada del menor impacto de sus actividades por afectar a organizaciones con menos recursos y de menor valor, por lo que las consecuencias del uso de la Nube son menores y es aceptable que usen un menor nivel de exigencia.



La exigencia en requisitos es más elevada para los perfiles directivos, seguido de los perfiles técnicos y del requerido por los profesionales independientes.

Finalmente, la Ilustración 19 muestra el análisis de los requisitos exigidos en función de la formación y capacitación profesional de la persona que facilita la información.

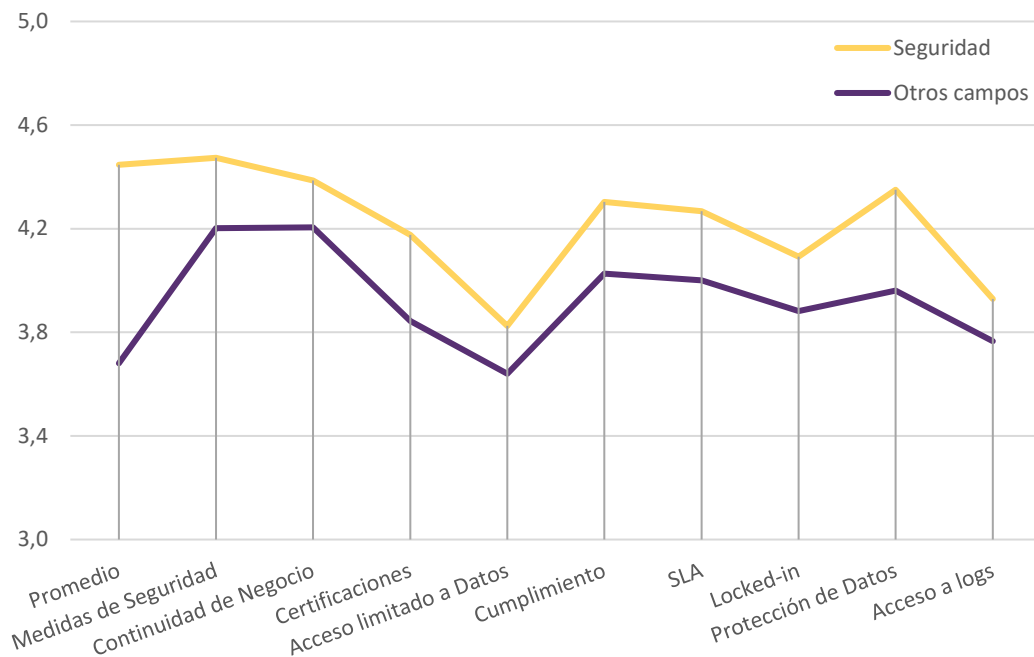


Ilustración 19.- Nivel de exigencia en los Requisitos de Seguridad en función del perfil técnico

En este caso, los resultados obtenidos están alineados con las expectativas previas, y son los profesionales que se desempeñan en áreas de seguridad de la información exigen un mayor nivel de exigencia en los requisitos.



Los profesionales de ciberseguridad demandan requisitos más exigentes a los servicios de la Nube que el resto de los profesionales.

4. Satisfacción de los Usuarios con los Servicios en la Nube

El Estudio analiza en este apartado el grado de satisfacción de los usuarios con los servicios en Nube, concretamente con la satisfacción con las funcionalidades recibidas y en cómo ayudan estos servicios a las empresas a conseguir sus objetivos de negocio.

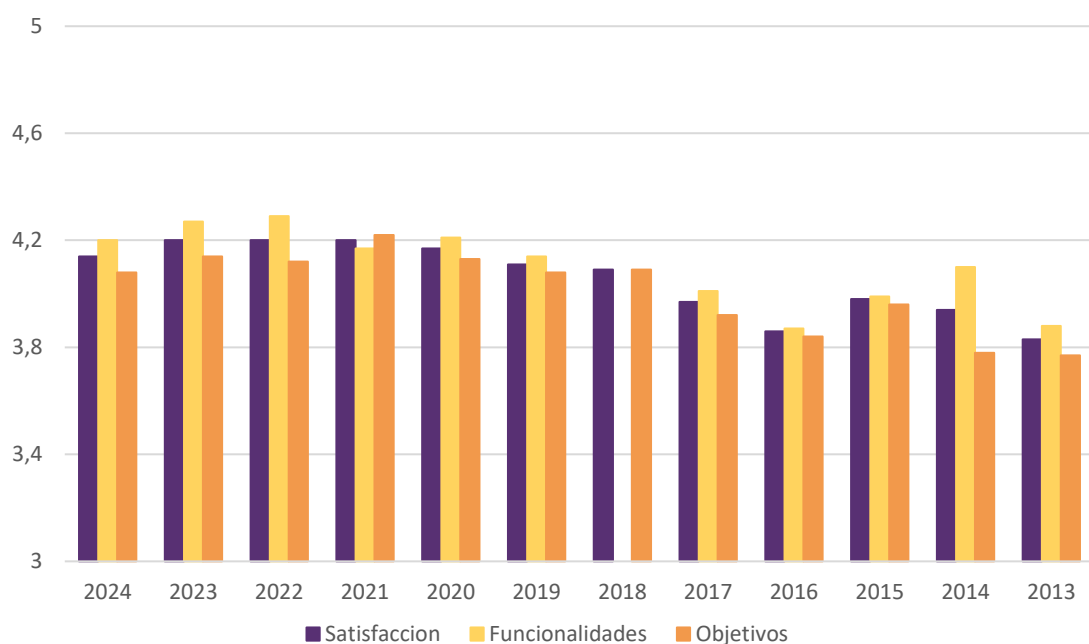


Ilustración 20.- Evolución del Grado de satisfacción según los criterios analizados en 2024

Los resultados recopilados en esta 12ª Edición permiten apuntar a un posible cambio de tendencia en la satisfacción de las empresas que hacen uso de la Nube, tanto en las funcionalidades recibidas como en la ayuda de la Nube para conseguir los objetivos de la empresa. Tras varios años con una satisfacción media de un 4,2 sobre 5, este año muestra una satisfacción media de un 4,14. Este dato se considera relevante ya que hay que remontarse al año 2019 para ver un valor similar. La Ilustración 20 refleja la variación detectada y la evolución de este parámetro a lo largo de las distintas Ediciones del Estudio.

La variación detectada no es en cualquier caso excesivamente significativa ni marcada, por lo que no puede establecerse con completa fiabilidad la existencia de un cambio de tendencia respecto de la satisfacción de los clientes con los servicios recibidos desde la Nube.

Y, en todo caso, el nivel de satisfacción seguirá siendo más que alto, resultado que debe valorado positivamente una edición más.



***Se detecta una disminución leve del grado de satisfacción.
Sigue alto, pero con leve retroceso.***

El análisis de la satisfacción por tamaño de empresa de la Ilustración 21 muestra diferencias notables en la situación declarada en las organizaciones en función de su tamaño. Las empresas de mayor tamaño declaran mayor satisfacción, en particular con las funcionalidades disponibles, pero superior a la media en todos los casos. Las empresas medianas declaran niveles de satisfacción alineados con los valores generales, mientras que las empresas de menor tamaño son las que se encuentran menos satisfechas, que no llegan al nivel alto que se supera en mayor o menor medida en el resto de las organizaciones.

Esta dependencia del tamaño de empresas está alineada con tendencias similares detectadas en las expectativas de los usuarios (Ilustración 17) y en los requisitos exigidos a los proveedores (Ilustración 17). En este caso, el cambio de valor es más acusado, puesto en el Estudio de 2023, las empresas de este tamaño (menos de 25 empleados) eran las que se declaraban como más satisfechas. El análisis de estas organizaciones no ofrece información adicional del cambio detectado, sino que simplemente refrenda la variación sin aportar otras claves que permitan entenderlo.

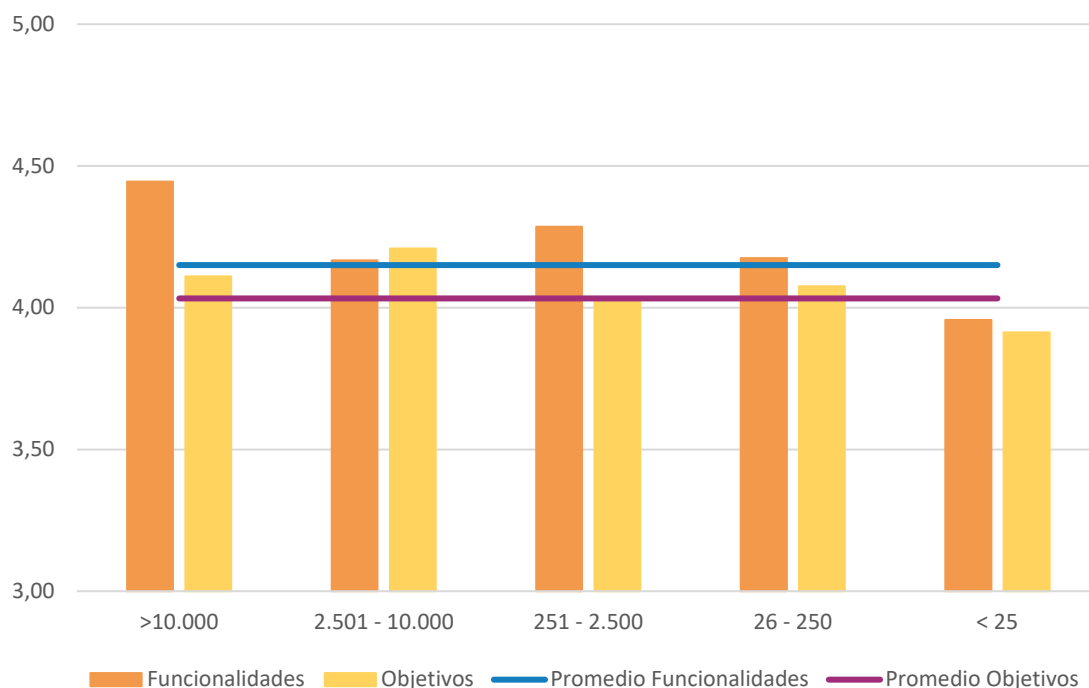


Ilustración 21.- Comparativa de satisfacción de los usuarios en función del tamaño de la empresa



Las empresas de menos de 25 empleados declaran una satisfacción más reducida que el resto de las empresas y que en años anteriores.

El Estudio también analiza el grado de satisfacción con los servicios en la Nube según el país en el que se opera, puesto que se detectaron variaciones relevantes en ediciones anteriores en la satisfacción en función de la huella geográfica de la organización. La Ilustración 29 muestra de forma combinada la satisfacción tanto la satisfacción como el grado de adopción de la Nube acumulando las geografías menos representadas en Resto EU y Resto Latam, respectivamente. En este caso, es Perú quien declara una mayor satisfacción con los servicios en Nube, llegando casi a nivel de satisfacción muy alta, con una amplia diferencia sobre el resto de las geografías que son de nivel alto o algo superior. Únicamente Bolivia se queda en un nivel de satisfacción que no llega a alto. Por otra parte, la encuesta de este año se observa que en algunos casos las diferencias se hacen cambios notables. Esta situación está alineada con los valores de las gráficas anteriores, en tanto que las organizaciones bolivianas que han participado en el Estudio tienen un tamaño medio inferior al de otras geografías. Estos valores están, por otra parte, desacoplados del nivel de uso o de abandono de servicios en la nube, que se analiza.

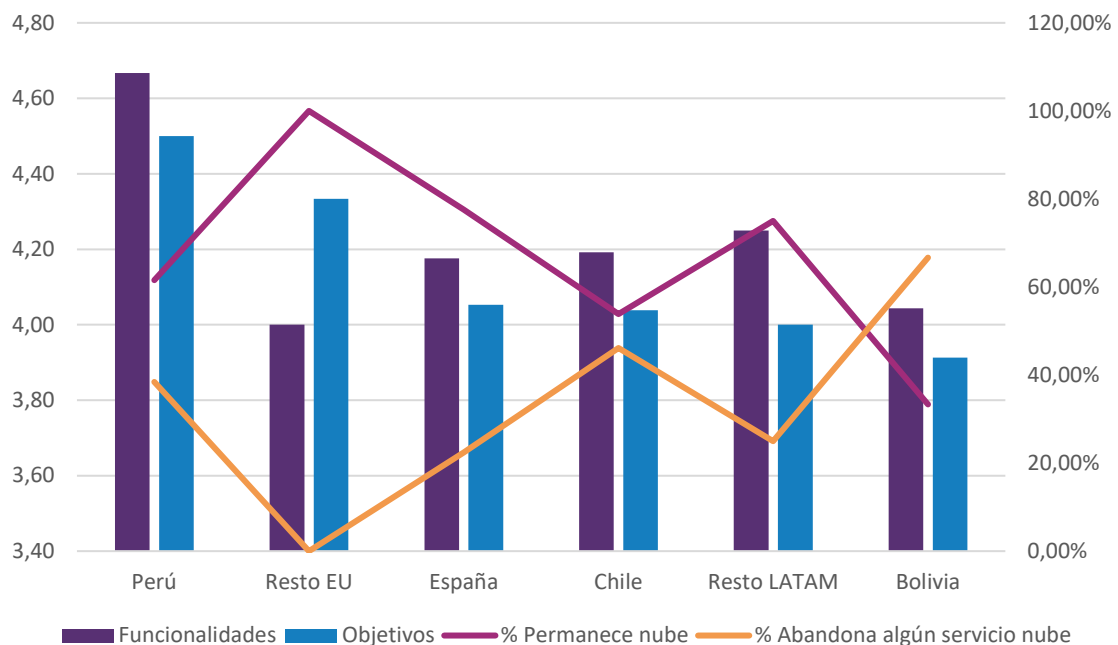


Ilustración 22.- Grado de satisfacción de los usuarios según la ubicación geográfica de la empresa



Perú mantiene un alto nivel de satisfacción, mientras que Bolivia muestra el menor grado de satisfacción con los servicios en la Nube.



5. Evolución Expectativas vs Requisitos vs Satisfacción

Se analiza a continuación la evolución histórica de los tres parámetros principales del Estudio: expectativas de los usuarios de la Nube, requisitos que los usuarios solicitan al CSP, y satisfacción de los usuarios sobre los servicios recibidos de su CSP.

Estos parámetros son el elemento que, a juicio de los analistas, resumen con mayor completitud el estado general de adopción de la Nube y las necesidades y motivaciones que los usuarios de la Nube tienen cuando adoptan sus decisiones de utilización de servicios en la Nube o de ciertos servicios y proveedores frente a otros.

El Estudio analiza la serie temporal de estos factores y la comparación entre expectativas, requisitos y satisfacción.

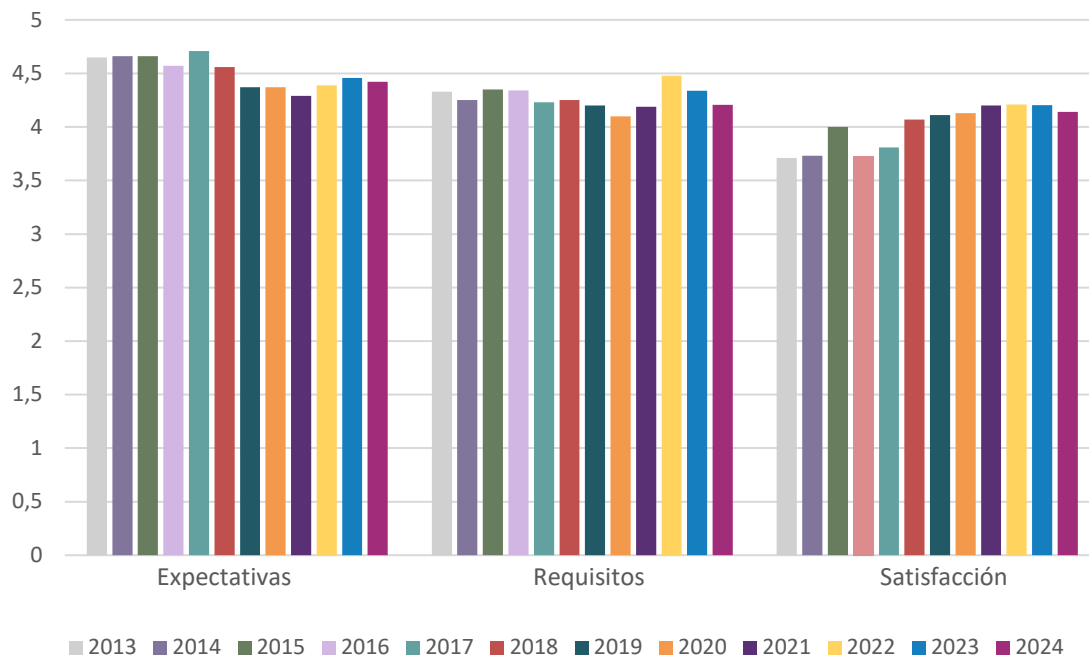


Ilustración 23.- Expectativas vs. Requisitos vs. Satisfacción en 2024

La evolución de la tendencia histórica global de estos parámetros que se muestra en la Ilustración 23 presenta un escenario de estabilidad, con todos los indicadores en nivel alto (valores mayores que 4). En todo caso, parece que tanto las expectativas, como los requisitos y niveles de satisfacción de los usuarios en la Nube siguen decreciendo tras la previa subida experimentada con la pandemia del Covid-19.

El descenso producido no es intenso en ninguno de los tres parámetros (0,04 para las expectativas, 0,14 para los requisitos y 0,07 para la satisfacción), pero se produce. Sólo en el caso de los requisitos es el segundo año en el que se detecta este descenso, por lo que aún es pronto para establecer una tendencia de más largo plazo.

En cualquier caso, la evolución de los tres parámetros continua con la tendencia histórica, en la que el nivel de expectativas de seguridad está en nivel muy alto, y es mayor que el nivel de exigencia de requisitos solicitados, que es a su vez mayor que la satisfacción de los usuarios de los servicios. Estos valores, que llegaron a converger en valores similares durante el Covid19, pero la evolución desde entonces ha vuelto a restablecer las diferencias entre los mismos, de forma que ahora es casi de tres décimas en los indicadores medidas.

A pesar de ello, debe seguirse atentamente la evolución en años futuros, puesto que, a pesar de los valores actuales y las diferencias existentes entre los parámetros, tanto el valor de las expectativas como las de requisitos están cerca de sus valores mínimos de su serie histórica.



Las expectativas de uso de la Nube son más altas que los requisitos solicitados y que la satisfacción con los servicios recibidos.

6. Visión sobre Shadow IT

Es preciso establecer la definición de ShadowIT corresponde con “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 con la ocultación deliberada de esta contratación”¹⁵. El ShadowIT es una consecuencia de la característica de Auto provisión exigible a la Nube que habilita el acceso de los departamentos No IT a servicios TI que, en un entorno OnPremise, no están disponibles de ninguna manera sin el concurso del departamento IT. Dado que los servicios en ShadowIT son contratados sin el conocimiento del Departamento de TI, y en muchos casos, sin el conocimiento de otros departamentos como Seguridad, Privacidad o Cumplimiento Legal, no es viable que estas áreas consideren este servicio en el alcance de sus actividades: No se puede proteger lo que se desconoce. Sin embargo, de cara al exterior, los atacantes pueden identificarlo como un posible punto de ataque a la organización. Por eso se considera relevante como consideran las organizaciones este aspecto de cara reforzar la seguridad en la Nube.



¹⁵ <https://www.gartner.com/en/information-technology/glossary/shadow>

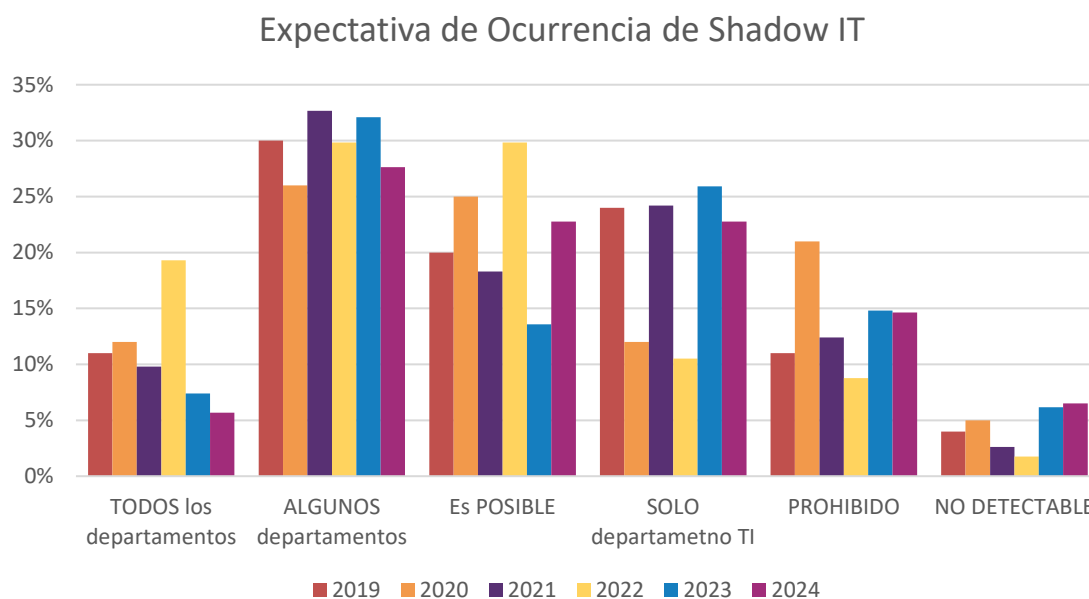


Ilustración 24.- Presencia estimada de Shadow IT en las organizaciones en 2024

La propia naturaleza del ShadowIT implica la ausencia de reporte formal del uso del servicio y una dificultad de detección, cuando no ocultación de su existencia. Por ello, la medición de la ocurrencia del fenómeno es intrínsecamente imprecisa. La Ilustración 24 muestra la opinión de los participantes en el 12º Estudio en comparación con los participantes de estudios anteriores. Del análisis de estos datos, los analistas han establecido tres conclusiones principales

En primer lugar, la percepción de los usuarios sigue estableciendo que hay un uso frecuente de ShadowIT. La percepción crece respecto del año pasado en tanto que aumentan los participantes que declaran que “es posible” el uso de ShadowIT, y este aumento recoge el descenso de los participantes que opinan que el shadow IT ocurre en “todos los departamentos”, los que opinan que ocurre en “algunos departamentos”, pero también el descenso de los que opinan que “sólo el departamento TI” debería realizar estas acciones, que también disponible. Precisamente esta disminución marca el crecimiento de la sensación de uso de la Nube, puesto que esta disminución refleja el cambio de participantes que consideran que no existe el ShadowIT, frente a los que consideran que sí que existe este fenómeno. En todo caso, el ShadowIT sigue siendo un fenómeno que se percibe como posiblemente frecuente.

En segundo lugar, aunque la percepción del uso de ShadowIT crece, la intensidad de ese uso sería menor que en la anterior edición. La disminución en los participantes que consideran que el uso es el “todos” o en “algunos” departamentos disminuye, frente a los que opinan que “es posible”. Esta percepción debe apoyarse en el conocimiento por le participante de casos de uso de ShadowIT concreto, que pasa de estar identificados o tener certeza sobre los mismos, a simplemente tener la sospecha (fundada o no) de ese uso. En varios casos, puede corresponder con uso de ShadowIT que eran conocidos en 2023 y que se han descontinuado en el año. Por ello, cabe concluir que el numero de casos de uso de ShadowIT ha disminuido.

Por último, y relacionando la conclusión anterior (hay menos casos de ShadowIT que puedan ser confirmados) con el aumento del número de casos de servicios en la nube que se refleja en la

Ilustración 7, los analistas concluyen que parte de la reducción de la frecuencia de uso de ShadowIT se debe a que las organizaciones están visibilizando y sacando del ShadowIT algunos casos de uso anteriores. Por ello, las organizaciones han ganado control sobre su uso de las TI.

Finalmente, el incremento en la percepción de ocurrencia de ShadowIT apunta a que el fenómeno sigue estando razonablemente aceptado (o al menos asumido) por las organizaciones.



El fenómeno ShadowIT se percibe como más frecuente y aceptado, pero con menos casos de uso en cada ocurrencia. Se da visibilidad algunos usos de ShadowIT anteriores.

El 12º Estudio también analiza la percepción que se tiene sobre ShadowIT, con independencia de la ocurrencia o no del fenómeno. Esta Edición presenta un escenario prácticamente similar al de la edición anterior, con una mayoría clara de participantes que lo perciben como un fenómeno negativo. Prácticamente dos de cada tres participantes así lo señalan en la Ilustración 25.

En esa línea continuista sobre el escenario detectado, los participantes que valoran el ShadowIT como un fenómeno neutral o que depende de los resultados siguen en niveles comparables a los resultados de 2023, experimentando leves variaciones que no se consideran relevantes. Por ello, los analistas concluyen que se consolida el cambio de tendencia en la percepción de ShadowIT que se intuía en la 11º Edición del Estudio.

También la variación de los participantes que lo perciben como un fenómeno positivo es menor, si bien en este caso este indicador marcaría un valor máximo de la serie. Dentro de la escasa proporción de participantes que declaran esta visión positiva, es una tendencia que debería monitorizarse en años posteriores.

En este sentido, el análisis de los participantes que declaran esta percepción positiva de ShadowIT en función de otros parámetros no permite identificar si existe algún sector concreto donde esta percepción sea más marcada, sea en función del tamaño de la organización, su presencia geográfica, sector económico o perfil profesional del participante en el Estudio.

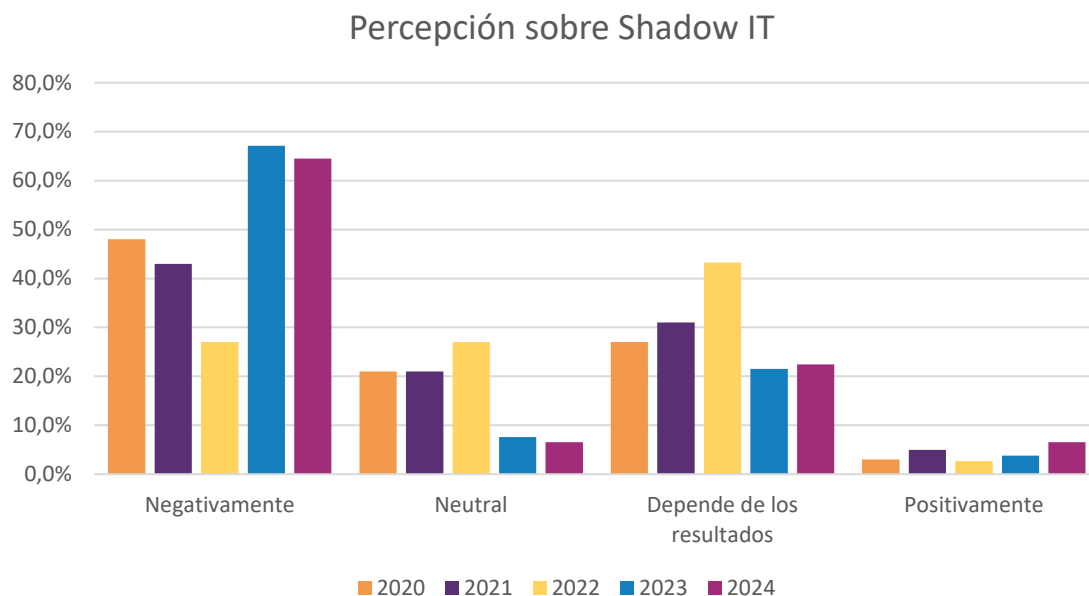


Ilustración 25.- Evolución histórica de la percepción de las organizaciones sobre ShadowIT



Shadow IT se sigue percibiendo como un fenómeno negativo, aunque crezca los que lo ven como positivo.

El Estudio ha considerado en esta edición descartar el concepto de CSP preautorizados para los que no es preciso solicitar permiso de uso y, por lo tanto, nunca serían ShadowIT. La Edición de 2023, que sí consideró esta cuestión, concluyó que esta herramienta se usaba en casos muy puntuales y poco extendidos, y que el análisis de esta cuestión no iba a aportar mayor nivel de detalle o riqueza en la visión del Estado de la Nube.

7. Estado de Concienciación en Seguridad de los Usuarios

En este año 2023 se mantiene la dinámica de estudios anteriores que permite establecer La sucesión de ediciones del Estudio permite mantener la aproximación orientada a la realización de un análisis basado en la perspectiva histórica. La visión comparada en el tiempo permite proponer conclusiones tanto respecto al año inmediatamente anterior, como, cuando es posible, respecto a otros momentos temporales más lejanos en el tiempo.

En este sentido, como en anteriores ediciones, se propone un primer análisis de la concienciación sobre los riesgos de seguridad de los servicios recibidos desde la Nube basado en las siguientes agrupaciones:

- Todos los participantes.
- Empleados con puestos directivos.
- Empleados no directivos.

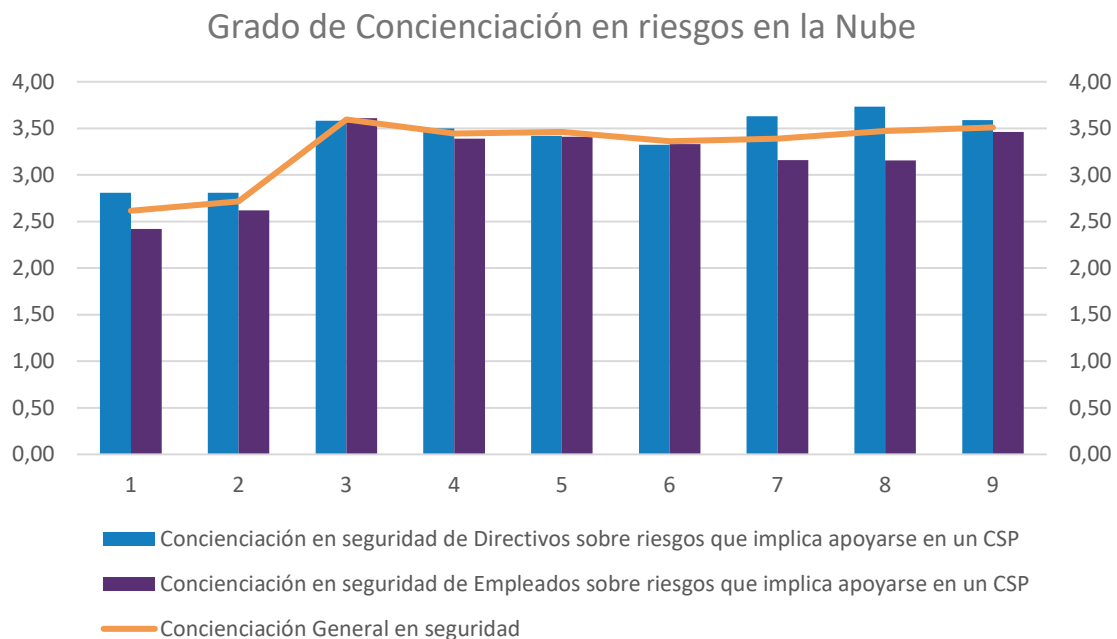


Ilustración 26.- Evolución histórica de concienciación en Seguridad de usuarios de la Nube

La Ilustración 26 refleja una mejor media general en 2024 frente a 2023, si bien los factores en que se basa esa media muestran las dos caras de una misma moneda. Por un lado, en los perfiles directivos el grado de concienciación ha sufrido una pequeña bajada. Por otro lado, en los perfiles no directivos sí es significativo el avance, lo cual sin duda es una buena noticia.

Teniendo en cuenta que un factor esencial de la concienciación es que sea *top-down*, los resultados de esta edición suponen una pequeña llamada de atención, porque, como veremos más abajo en este apartado, concuerdan con una percepción de que la concienciación de origen corporativo no es suficiente en ocasiones. Por tanto, se podría concluir con la oportunidad y conveniencia de que la concienciación se base en acciones corporativas lideradas por los niveles más alto de la organización y que la mayor concienciación por parte de los estamentos directivos está logrando un efecto de arrastre del resto de empleados hacia niveles más altos de concienciación en Seguridad en la Nube.

La concienciación es una línea de defensa compuesta por diversos elementos, por lo que las carencias en alguno de ellos afectan y debilitan al conjunto de manera inevitable.



Una mayor concienciación de los directivos está arrastrando a otros empleados a mayor nivel de concienciación en Seguridad en Nube.

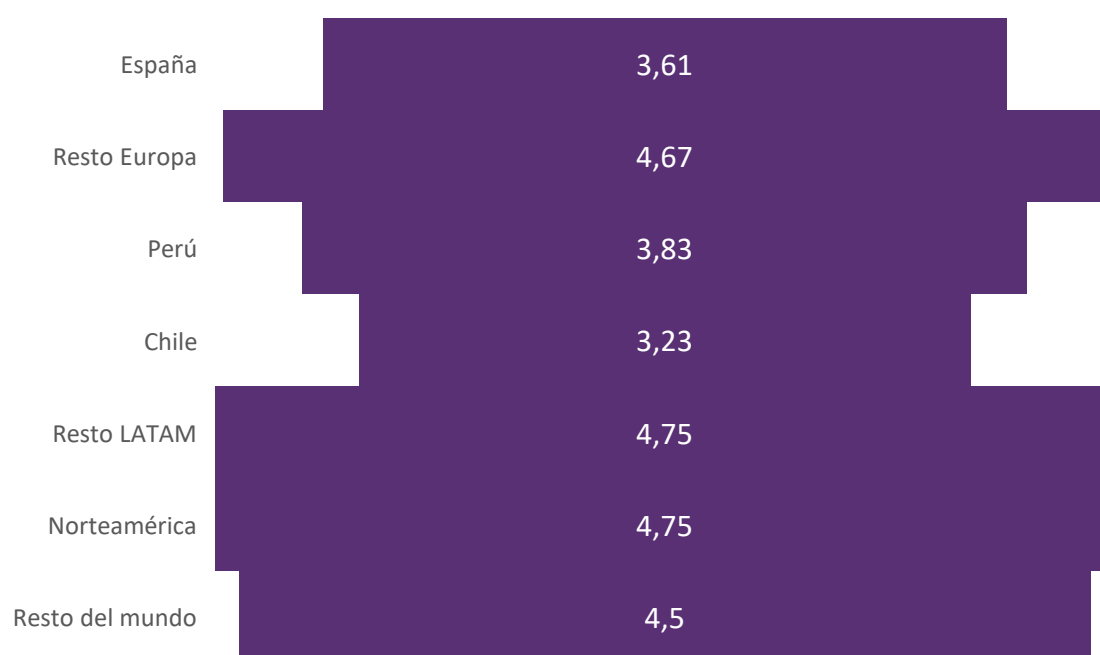


Ilustración 27.- Grado de concienciación en riesgos de la Nube por área geográfica

Resulta también interesante apreciar los resultados obtenidos con relación al indicador de grado de concienciación basado en las diferentes áreas geográficas en las que se han obtenido respuestas a la consulta. La Ilustración 27 recoge la variación del indicador de concienciación media en función de las geografías consideradas en el estudio, acumulando zonas geográficas a aquellos países que han tenido un número menor de participantes y que, por lo tanto, no puede

considerarse que ofrezcan una muestra estadísticamente representativa. La Ilustración 42 muestra en más detalle esta distribución detallada por geografías.

El análisis de la Ilustración 27 muestra una relación inversa entre el número de participantes en el estudio y el nivel del indicador de concienciación media. Par el caso de España, Perú o Chile, las cifras están por debajo de lo esperado. Los analistas consideran que no es necesariamente negativo, puesto que estos mismos países tienen también mayores expectativas sobre la seguridad de los servicios en la Nube (ver Ilustración 13) y esto se ha de trasladar a un mayor grado de autoexigencia, como también se asocia a un mayor número de respuestas.

Ahora bien, esto no debe evitar la oportunidad de poner el foco en aquellos grados de concienciación que tienen un recorrido de mejora considerable. Siendo resultados a nivel de país, esto también permite proponer que la elevación de ese nivel de concienciación no es solo una labor y un compromiso individual de las entidades públicas y privadas, sino que también debería ser un objetivo de las Administraciones públicas en su conjunto. Y ello porque todos los participantes, directos e indirectos, en el ecosistema digital en la Nube son partícipes en promover una adecuación concienciación en materia de riesgos en la Nube en el conjunto del tejido económico y empresarial.



La mejor concienciación a nivel nacional se fortalece con una mayor exigencia y con el respaldo de las Administraciones Públicas.

Hay otros elementos sobre los que se ha preguntado a los participantes en el Estudio que aportan sensaciones y conclusiones que se pueden calificar como negativas, en cuanto a concienciación en Seguridad en la Nube de las organizaciones.

Así, la Ilustración 28 analiza si el grado de concienciación de las organizaciones tiene traducción práctica respecto de la toma de posición de riesgo en las organizaciones en la adopción de la Nube, verificando si se traduce en la realización de un análisis de riesgos previo a la adopción de estos servicios y qué consecuencias se siguen de este ejercicio. La Ilustración 28 muestra un aumento significativo en las situaciones donde los riesgos derivados de los servicios en la Nube no han sido analizados (23%) o no hay certeza de que se hayan evaluado (34%) mientras que, por primera vez en la serie histórica, no llegan a la mitad las organizaciones que hicieron el viaje a la Nube.

Podríamos hacer la suposición de que la evolución y ampliación en la adopción de servicios en la Nube ha disminuido la necesidad de llevar a cabo el análisis de los riesgos asociados. Es posible que esta situación corresponda con la propia madurez de la adopción de los servicios en la Nube, que se realizó hace ya varios años (incluso antes de la pandemia Covid19) y por ello ya está

asumida e incluso olvidada. También puede deberse a que se trata de nuevos servicios en los que los riesgos ya han sido analizados, de manera total o parcial, o así se considera.

En todo caso, el aumento tan importante de las respuestas que indican que no se han analizado los riesgos es una señal de alarma importante, en cuanto a la adopción de servicios en la Nube sin una adecuada valoración de riesgos. Sobre todo, porque se ha producido un cambio significativo en esta Edición del Estudio. La tendencia de asumir los riesgos sin identificarlos adecuadamente es preocupante y sugiere una falta de valoración previa a la adopción de servicios en la Nube.

¿Recibe información sobre seguridad en la Nube?

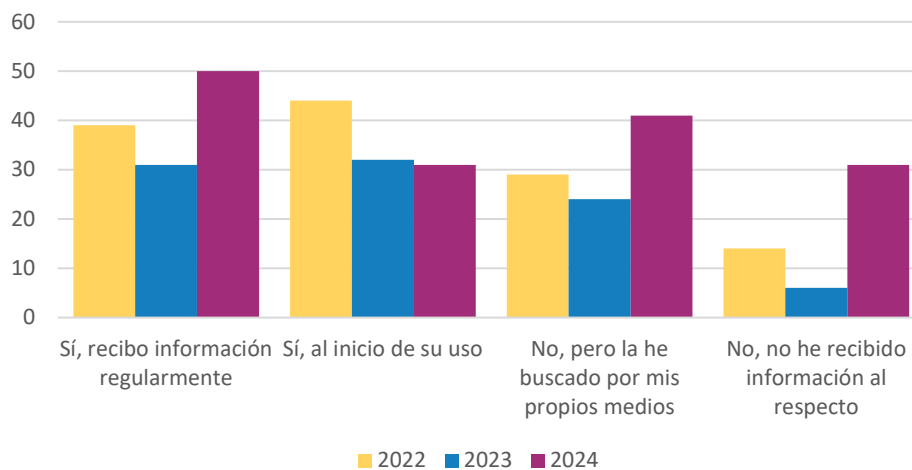


Ilustración 28.- Formación y concienciación a las personas sobre el uso de servicios en la Nube

Ciertamente, no es una buena noticia. Los analistas del estudio reiteramos la necesidad de implicar a todos los miembros de la organización en los pasos a dar en la adopción de servicios en la Nube, para que todo el mundo comprenda y asuma tanto los cambios operativos como los cambios en los riesgos y como los resultados esperados del proceso de migración a la Nube. De esta forma, pueden cooperar en la detección, gestión y tratamiento de estos nuevos riesgos y hacerles parte de las medidas de mitigación de estos.

Volviendo sobre el criterio, ya expresado, de concienciación *top-down*, el enfoque y los recursos corporativos deben ser elementos esenciales, permanentes y adecuadamente dimensionados para no caer en escenarios que puedan quitar valor o disminuir los beneficios esperados al final del camino de adopción de los servicios en la Nube.



Se debe adoptar la Nube tras un análisis de riesgos y aplicando medidas adecuadas de formación y concienciación para las personas.

Y deben mantenerse en el tiempo.

Por último, el análisis de la concienciación media en seguridad en las organizaciones en función de su tamaño, que se muestra en la Ilustración 30, apunta a inversión en la tendencia anterior, con el retorno al escenario en el que las organizaciones de mayor tamaño son las que tienen un nivel de concienciación más bajo. Las organizaciones medianas y pequeñas mejoran o consolidan sus resultados. Los analistas consideran que esta situación es consecuencia de las conclusiones obtenidas en la Ilustración 29 y en la Ilustración 28, que ya apuntaban a una reducción de la intensidad en la formación y concienciación de las personas. Estadísticamente, el impacto de esta reducción del esfuerzo es más notable en las empresas de mayor tamaño y con mayor número de empleados demandando o precisando de esa información.

En la edición anterior, se señalaba como el aumento de concienciación en las organizaciones de mayor tamaño podía haber creado un impulso indirecto en el conjunto de las organizaciones. Sin embargo, la disminución en este año del nivel de concienciación de tales organizaciones no ha tenido un efecto contagio sobre el resto. Esto permitiría concluir que la concienciación no depende ya tanto de dinámicas de tamaño, sector, posición en la cadena de valor, etc., sino de la propia interiorización de la necesidad por cada organización a nivel individual, lo cual es un salto de madurez importante. Si la hipótesis planteada por los analistas fuese cierta, la edición de 2025 del Estudio debería ver reflejada una disminución de la concienciación de las empresas de menor tamaño.

Grado de Concienciación en Riesgos de la Nube (según el tamaño de la organización)

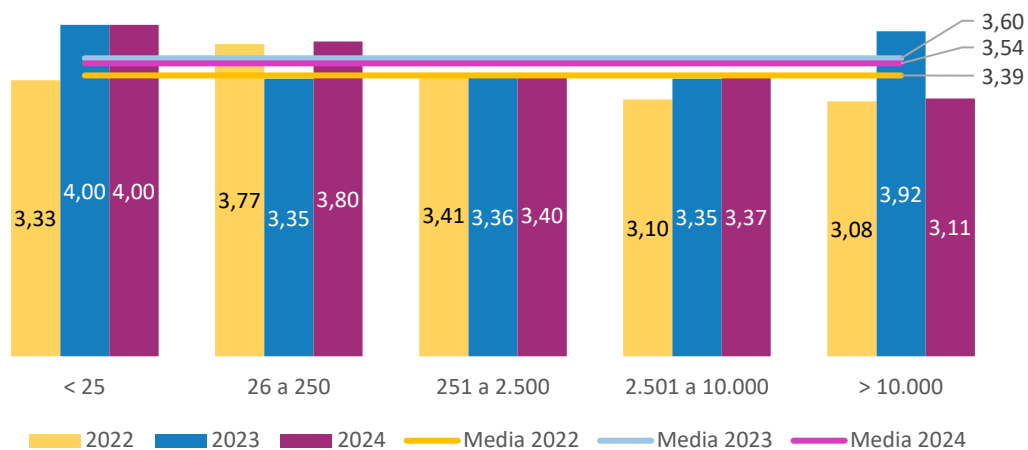


Ilustración 29.- Grado de concienciación en Riesgos de la Nube según tamaño de la organización



El nivel de concienciación en Seguridad en la Nube parece depender cada vez menos del tamaño de la organización y más de la implicación de cada organización concreta.

8. Evolución de Incidentes de Seguridad en Servicios en Nube

Se analiza en este apartado la evolución de los incidentes de seguridad en las organizaciones que usan servicios en la Nube, frente a la situación previa de las organizaciones sin apoyo en servicios en la Nube.

El análisis de la evolución de los Incidentes en la Nube a partir de los datos proporcionados por los participantes en la encuesta se realizará tomando cada factor por separado, para luego realizar un análisis conjunto de este.

Respecto del número de incidentes, la Ilustración 31 muestra cómo se mantiene la tendencia en la que las organizaciones siguen experimentando un número de incidentes similar o más reducido tras su transición a la Nube. En esta edición, la mayor madurez de las organizaciones en su adopción en la Nube hace que las organizaciones que mantienen su número de incidentes tras migrar a la Nube lleguen al máximo de la serie histórica. Este valor se compensa fundamentalmente con la reducción del resto de casuísticas. De seguir esta tendencia, la tendencia de empresas que mantienen incidentes crecería a lo largo del tiempo, a medida que más y más organizaciones pasar a ser usuarias *Cloud-First* o *Cloud-Native* y pierdan la referencia con su estado de incidentes antes de estar en la Nube.

Hay que destacar también que ninguna organización señala que los incidentes hayan desaparecido. Este evento ya era minoritario en anteriores ediciones y pasa a tener un valor testimonial. Señalar, por otro lado, que hay un ligero descenso en las organizaciones que identifican un aumento de incidentes, conservando los valores anteriores. En cualquier caso, siguen destacándose las dos opciones de permanencia y reducción de incidentes de seguridad, constituyendo más del 90% de los participantes.

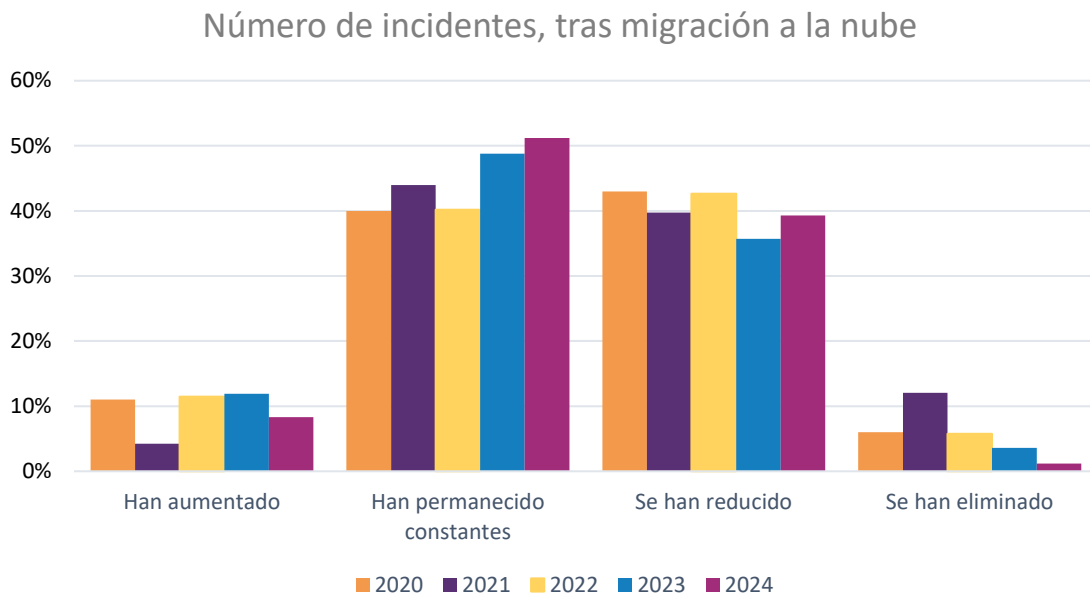



Ilustración 30.- Evolución en 2024 del Número de Incidentes en servicios en la Nube.


El número de incidentes en los servicios en la Nube se mantiene o tiende a bajar

Por su parte, la Ilustración 32 analiza como varían los incidentes en función del grado de utilización de servicios en la Nube. En ese sentido, la expectativa de los analistas era que el volumen de incidentes fuera independiente del tamaño.

Sin embargo, puede verse en Ilustración 32 que las entidades que tienen más del 50% de sus servicios en la Nube son las que declaran que tienen más incidentes en la Nube, mientras que ninguna entidad que usa menos del 50% de servicios en la Nube experimenta aumento. Por el contrario, las entidades que utilizan servicios puntuales o disponen de menos de un 50% de los servicios en la Nube, siguen el perfil de uso general establecido anteriormente, con una mayor proporción de entidades que siguen manteniendo el mismo número de incidentes. Los analistas no han encontrado una explicación sólida a este evento, salvo un mal entendimiento por los participantes en el estudio sobre el motivo de la pregunta que haya hecho responder pensando en el total de incidentes en servicios en Cloud y en OnPremise, que sería claramente superior en ese caso.

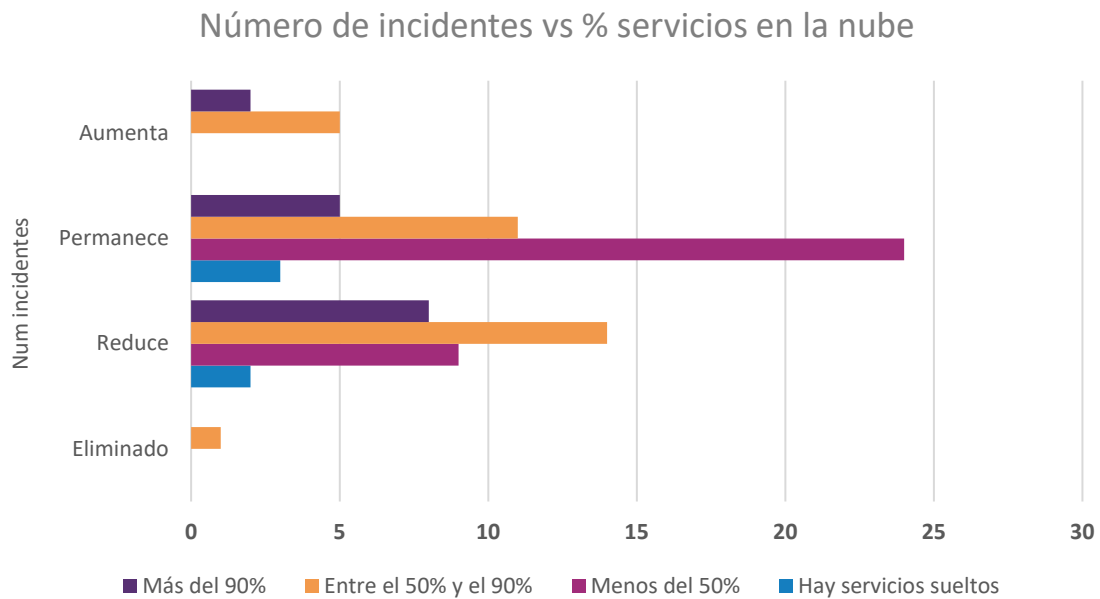


Ilustración 31.- Número de incidentes vs porcentaje de servicios en Nube



Solo las organizaciones con un uso más intensivo de la Nube declaran aumento de los incidentes, lo que rompe anterior tendencia.

Respecto de la criticidad de los incidentes, este 12º Estudio detecta la continuidad de las tendencias y escenarios detectados en ediciones anteriores. Así, y como puede verse en la Ilustración 33, el cambio a servicios en la Nube no supone un cambio en la criticidad de los incidentes que sigue siendo mayoritariamente igual a los escenarios OnPremise, aumentando el número de entidades que declaran que los incidentes siguen teniendo la misma criticidad y siguen siendo más abundantes las empresas que han reducido la criticidad de sus incidentes.

El Estudio también ha realizado una reflexión sobre los actuales escenarios de amenazas y como la evolución de estos pudiera estar impactado en el análisis de los datos. Es decir, es posible que el cambio en la criticidad de los incidentes pueda verse afectado no solo por la migración o no de servicios a la Nube, sino por el cambio y evolución propia de los tipos de ataques que se realizan y su impacto sobre los servicios en la Nube. En particular, porque algunos actores de ataque se apoyan para realizar sus actividades en servicios legítimos en la Nube, así que los CSP pudieran considerarse fuentes de ataque, o a que los mecanismos de defensa y la efectividad de los ataques de CSP a CSP o CSP sean distintos. En todo caso, este cambio en las técnicas utilizadas no parece afectar a la criticidad de los incidentes producidos, sino más bien a la probabilidad de éxito en la materialización de estos.

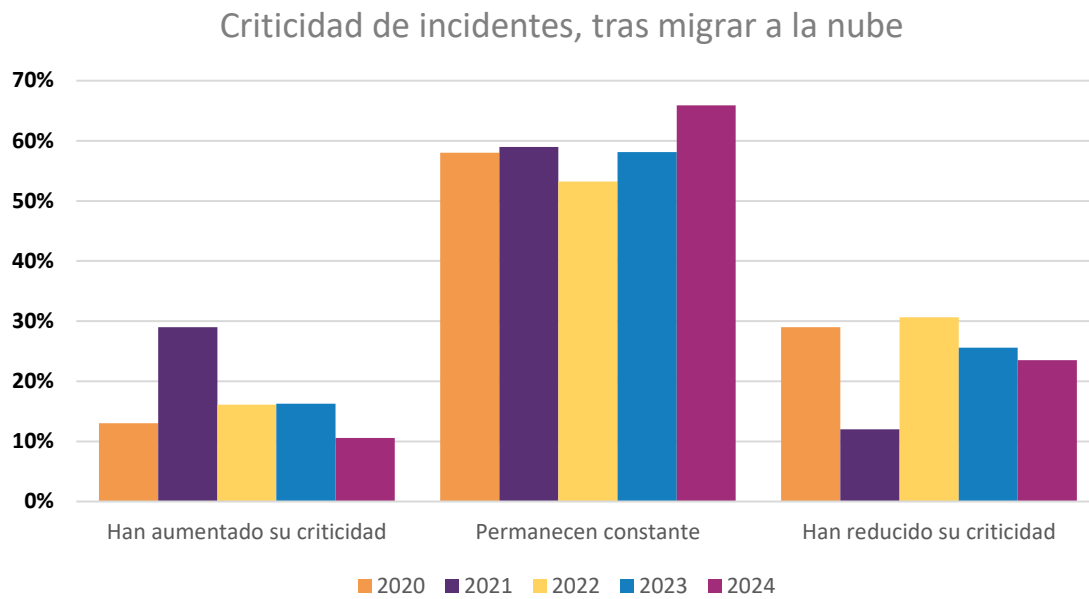


Ilustración 32.- Evolución en 2024 de la Criticidad de Incidentes en servicios en la Nube.



La criticidad de las incidencias en la Nube se mantiene, o quizás se reduce levemente.

Por su parte, la capacidad de detección de incidentes de servicios tras migrar a la Nube sigue siendo mejor que con sus respectivas capacidades en OnPrem. Así siguen siendo mayoría las empresas que mejoran, aunque con una diferencia menos elevada que en 2023. La Ilustración 34 muestra esta evolución.

En este caso, simplemente debe destacarse que se mantiene la tendencia de años anteriores, por lo que son aplicables las conclusiones establecidas en años anteriores.

Capacidad de detección de incidentes, tras la migración a la nube

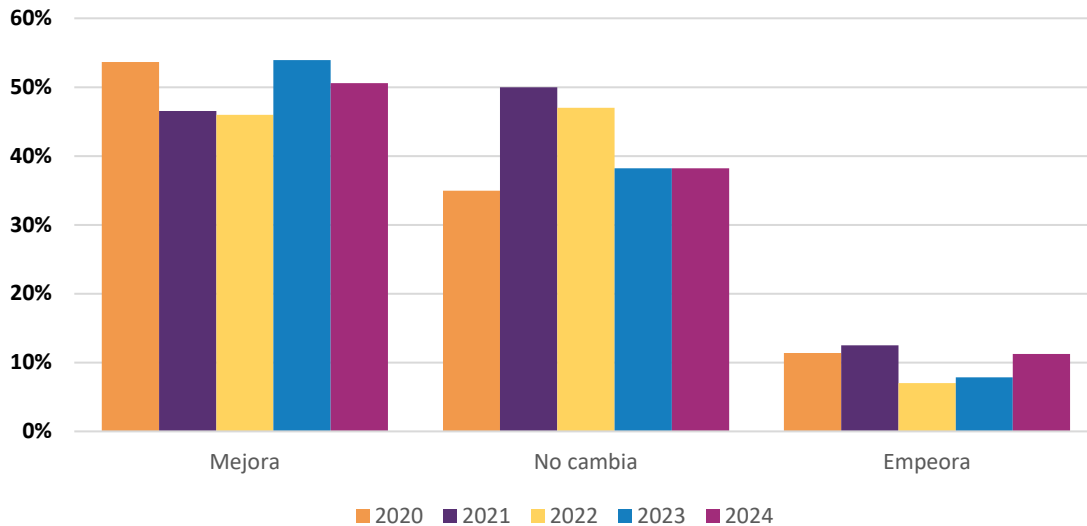


Ilustración 33.- Evolución en 2024 de la Capacidad de Detección de Incidentes en servicios en la Nube.



Las organizaciones siguen mejorando sus capacidades de detección de incidentes al utilizar servicios están en la Nube.

Al analizar la variación de las capacidades de detección en función de la intensidad de uso de los servicios en la Nube, sí que se detecta en la Ilustración 35 una dependencia directa entre el uso de la nube y la mejora obtenida, donde claramente se mejora esta capacidad en los usuarios que hacen un uso más intensivo de la Nube. En particular, en las empresas de más de un 90% de uso de servicios en la Nube, quienes posiblemente estén consumiendo servicios de *SIEM-as-a-Service* como parte de ese porcentaje, lo que facilita el despliegue de capacidades de monitorización Cloud.

Por otra parte, la relación negativa en las capacidades de detección con el aumento de servicios en Nube se presenta en organizaciones que tienen más de un 50 % de sus servicios en la Nube. Esta tendencia puede estar influyendo en las empresas con menor grado de uso de Nube para la adopción de *Cloud Repatriation*.

Capacidad de detección de incidentes vs % de servicios en la nube

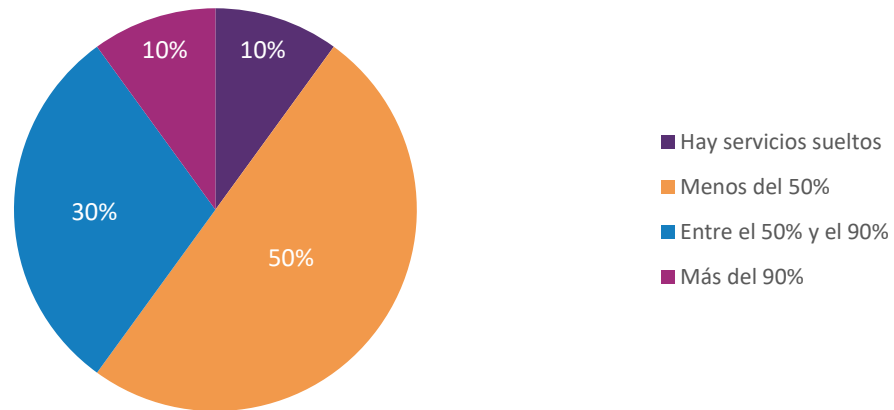


Ilustración 34.- Capacidad de Detección de Incidentes Vs Porcentaje de servicios en la Nube.



Las organizaciones que más usan la Nube también mejoran más sus capacidades de detección de incidentes.

Respecto al volumen de recursos que los usuarios deben dedicar para la gestión de los incidentes, el Estudio detecta un aumento de las organizaciones que declaran que el coste de gestión de los incidentes ha aumentado. La Ilustración 36 muestra los datos obtenidos en este 12º Estudio. Hay un 16% de usuarios que antes declaraban que los costes de gestión de incidentes decrecían, y ahora señalan que sus costes han aumentado.

Esta tendencia podría no estar atada a la migración de servicios a la Nube, más sí directamente relacionada con el constante incremento de actores de amenaza, especialización de los adversarios y constantes incidentes presentados en reconocidas empresas que obligan a las organizaciones a fortalecer sus equipos de respuesta a incidentes. Esta mayor consciencia de las organizaciones respecto de su necesidad de disponer de capacidad de gestión de incidentes, ocurran estos o no, y de dotarse de más y mejores herramientas para realizar esta gestión no puede realizarse sin un aumento de la dotación de recursos a esta tarea, y que explicaría este significativo aumento.

Coste de los incidentes, tras migrar los servicios a nube

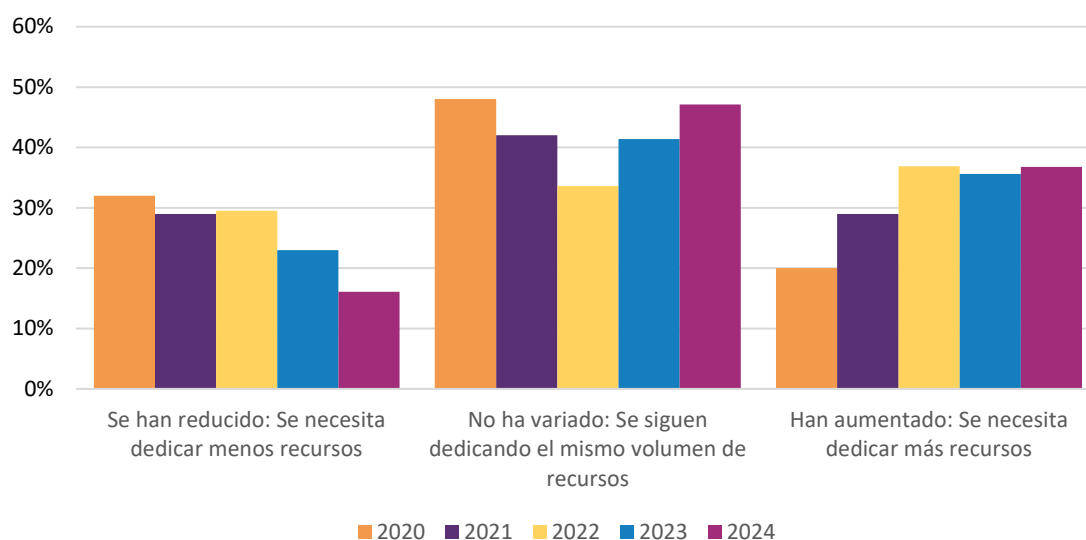


Ilustración 35.- Evolución en 2024 del Coste en la Gestión de Incidentes en servicios en la Nube.



La mayor diversidad de incidentes y más necesidad de recursos especializados aumenta el coste de gestión de incidentes. También para los usuarios de servicios en la Nube.

Por último, se analizan las capacidades que ofrece el CSP a sus usuarios para asistir en su respuesta a incidentes y la disponibilidad y/o facilidad de uso de estos. La Ilustración 37 muestra el resultado de este análisis.

La tendencia ahora es que sea un servicio complementario que se contrata con el CSP disminuyendo también el porcentaje de empresas que indican que está incluido sin coste adicional. Realizando un estudio más particular de este cambio de tendencia, no se identifican cambios en las tendencias de CSP contratados por las empresas.

Capacidad de Gestión de Incidentes, tras la migración a la Nube

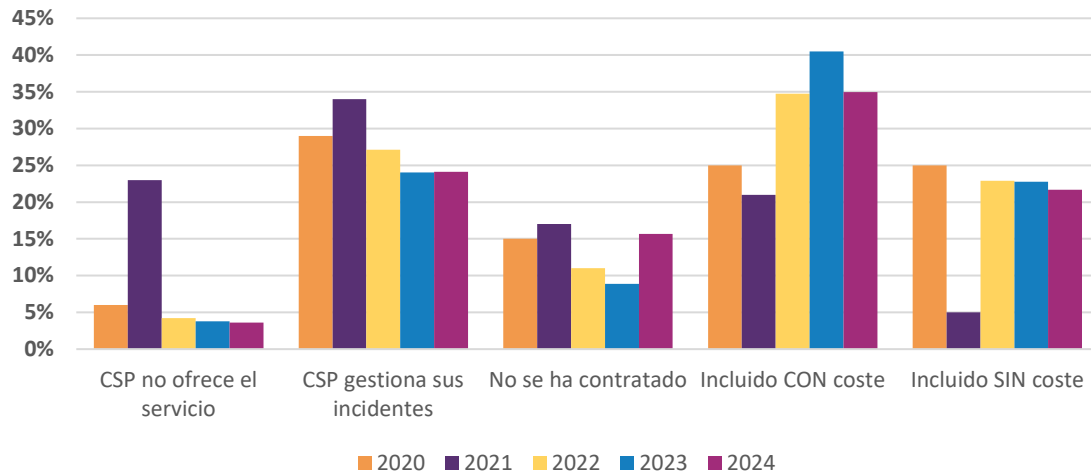


Ilustración 36.- Evolución en 2024 del Apoyo a los usuarios por el CSP en Incidentes en servicios en la Nube.



La gestión de incidentes ocurridos en la Nube supone un coste adicional a las organizaciones



9. Análisis de Participantes en el Estudio y sus particularidades

9.1. Caracterización de usuarios no técnicos

El estudio ha identificado recurrentemente que, además de los usuarios corporativos que se apoyan en servicios de Nube, existía otro perfil de usuario muy distinto, tanto en sus capacidades técnicas y organizativas, como en sus mecanismos para activar los servicios números. Estos usuarios se han identificado como “Usuarios No Técnicos”.

Se trata de usuarios que utilizan servicios en la Nube porque les resultan sencillos de contratar y se ajustan a sus necesidades TI para el desarrollo de sus propias actividades de negocio, pero que no siempre tienen un conocimiento técnico de cómo estos servicios se prestan o cuales son los elementos técnicos de la Nube. Son usuarios puros de Servicios en la Nube. Su conocimiento técnico de la base tecnológica que soporta la prestación de servicios en la Nube no tiene por qué ser profundo, puesto que su interés principal es el consumo de estos servicios. Y, por lo tanto, pueden tener exigencias, expectativas y condicionantes diferentes a los de los usuarios técnicos.

Por ello, el Estudio conservará la definición hecha en anteriores estudios para un Usuario No técnico, que corresponde con participantes en la encuesta que cumplen estos criterios:

- Organizaciones de menos de 25 participantes y menos de 1 M€ de facturación, donde el participante es el CEO de la organización.
- El participante se declara como usuario no técnico / profesional independiente.

9.2. Diferencias en Resultados de Usuarios No Técnicos

Una vez caracterizados los usuarios no Técnicos, el Estudio identifica y evalúa las diferencias que tienen estos usuarios respecto de los usuarios técnicos, y reevalúa las conclusiones a las que se llegaron en aquel momento.

Parte de estas conclusiones ya se han identificado a lo largo de este documento. Así, se han detectado elementos que serían aplicables a esta tipología de empresas, generalizando los resultados de empresas de menos de 25 usuarios.

En primer lugar, se pretende identificar cual es la postura de los usuarios no técnicos sobre su adopción de la Nube. La Ilustración 38 particulariza el escenario global descrito en la Ilustración 1 para estos usuarios, y se puede ver que la postura de estos usuarios sobre el uso o abandono de la Nube es muy similar a la global, con la diferencia de que no hay ningún usuario particular que haya dejado la Nube ni que se niegue en rotundo a utilizarla. En ese sentido, muchos de estos usuarios encuentran en la Nube un acceso sencillo a servicios TI de calidad suficiente, coste asequible y que no requieren un despliegue de grandes

infraestructuras por su parte, por lo que cabría esperar (y en años anteriores así se ha detectado) un grado de adopción mayor en estos perfiles. No obstante, los analistas concluyen que esta diferencia no es significativa ni revela otras tendencias.

Uso de la nube

- Sigo usando TODOS los Servicios
- Deje ALGUNOS servicios de nube
- DEJÉ la Nube
- QUIZÁS use Nube en el futuro
- NUNCA la usaré

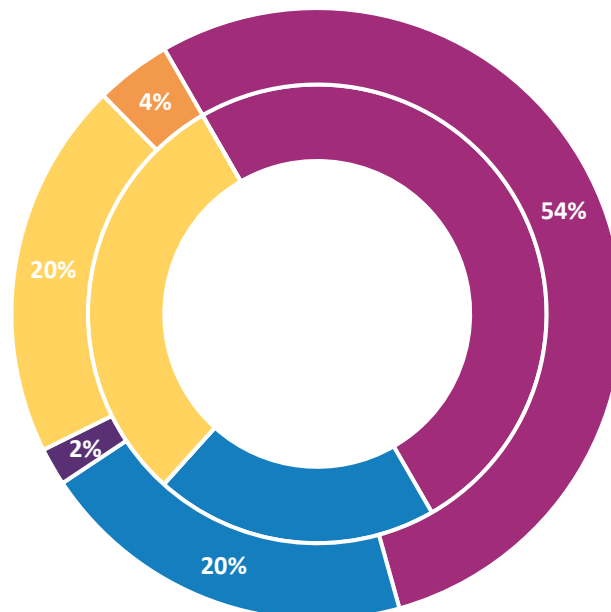


Ilustración 37.- Postura sobre Cloud Repatriation en las organizaciones, Usuarios No técnicos



Los Usuarios no Técnicos tienen una postura sobre la Cloud Repatriation similar a la del resto de participantes.

También se quiere destacar cual es el cambio de expectativas sobre los servicios en la Nube para los usuarios no Profesionales. La Ilustración 39 desarrolla en detalle los datos obtenidos por el Estudio para su análisis.

Mientras que los cambios en Confidencialidad, Integridad y Disponibilidad de los servicios son menores, las expectativas en Privacidad son claramente menores y, sorprendentemente, las expectativas en Cumplimiento Legal de los servicios son mucho más altas. Los analistas no han encontrado fundamento ni motivación en estas diferencias tan ostensibles en áreas tan cercanas a los aspectos más legales de los servicios. Como hipótesis no demostrables, algunos analistas han apuntado a una baja expectativa de la privacidad derivada por las noticias, redes sociales, ciberataques que se publican sobre la Nube, mientras que la expectativa en cumplimiento venga

derivada del posicionamiento comercial de los CSP sobre sus servicios y las garantías de cumplimiento que señalan como ventaja. En ambos casos, el desconocimiento en detalle del funcionamiento técnico de la Nube impide que estas opiniones puedan ser ponderadas con más precisión.

Los analistas también han apreciado diferencias significativas respecto de los datos de Estudios anteriores en esta área, en los que las expectativas de los usuarios no Técnicos eran significativamente más altas¹⁶.

Expectativas : PYMEs vs Media

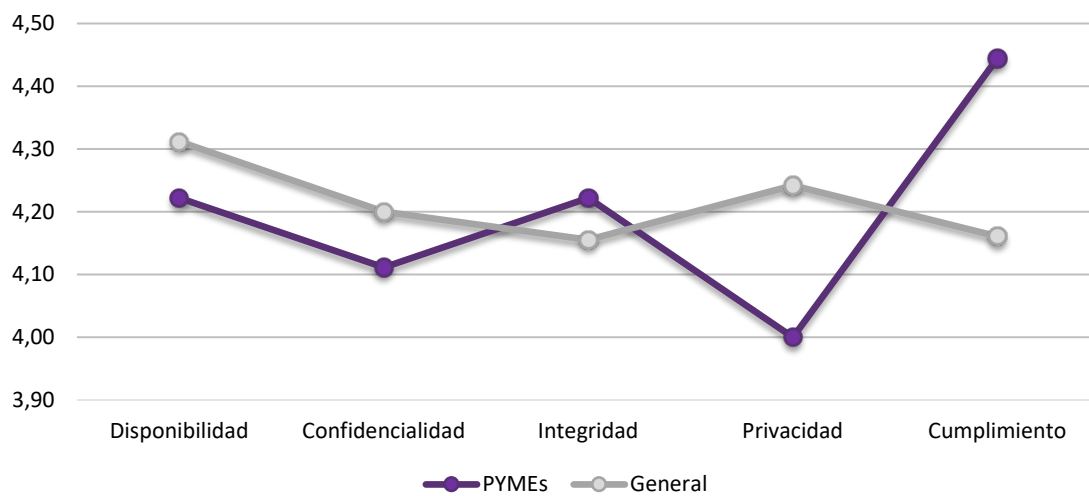


Ilustración 38.- Diferencias en Expectativas de los profesionales independientes frente al total de participantes.

Respecto de los requisitos exigidos por los profesionales independientes que se pueden ver en la Ilustración 41, estos resultan ser superiores en todos los casos a la media de los participantes, salvo para el parámetro "País de Ubicación". Este escenario de nuevo presenta diferencias frente a los resultados de años anteriores, y cierta inconsistencia frente a los datos de expectativas, en particular en el cumplimiento de GDPR, que resulta en esta ocasión netamente superior. Los analistas solo pueden seguir aplicando las hipótesis anteriores no comprobadas. El uso de términos más fácilmente identificables por los usuarios (Seguridad, Continuidad, GDPR, logs, ...) puede haber ayudado a calibrar con más exigencia el grado de conocimiento.

¹⁶ <https://www.ismsforum.es/ficheros/descargas/sota-2023-definitivo1701434704.pdf?page=51>

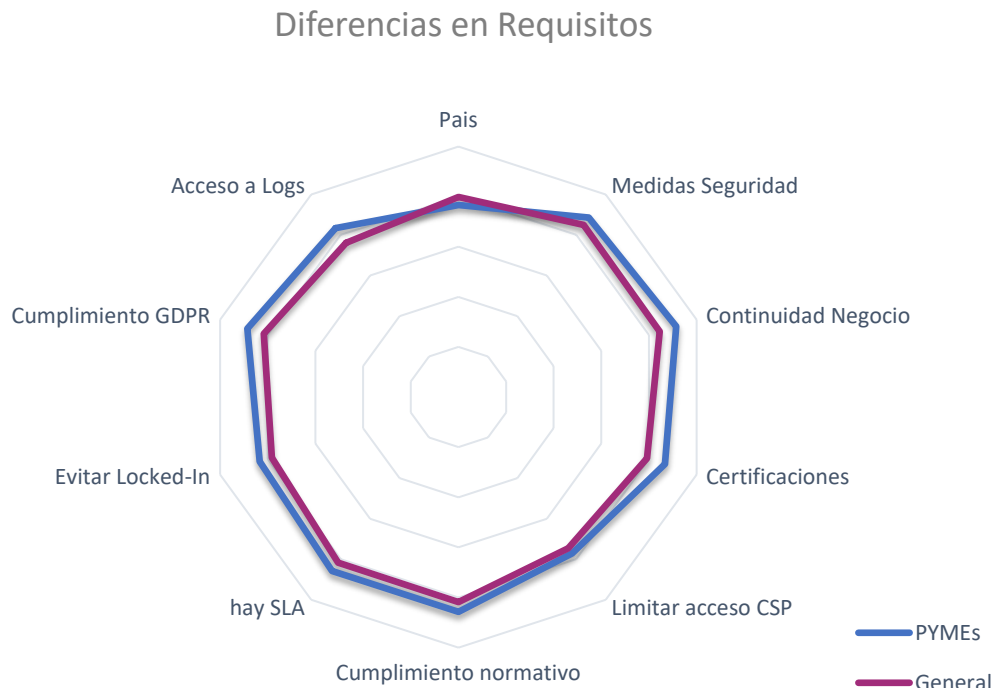


Ilustración 40.- Diferencias en Requisitos de los profesionales independientes frente al total de participantes



Los usuarios no técnicos de la Nube son, en general, más exigentes que el promedio de participantes en el Estudio.

Por último, los datos ya analizados permiten extraer conclusiones adicionales.

Respecto del uso de la Nube por estos usuarios no técnicos, el análisis combinado de la Ilustración 6 (CSPS) y la Ilustración 9 (servicios en Nube) dibujan un escenario en el que los usuarios no Técnicos se perfilan como usuarios frecuentes de servicios de ofimática, correo y almacenamiento sobre Google, con mucha más intensidad que el resto de los usuarios. No se niegan al resto de proveedores y servicios, pero lo hacen con menos intensidad que otros, particularmente que las grandes empresas. Este escenario es consistente con la Ilustración 8, donde se ve que están consumiendo una media de 2,2 CSPS.

Todos estos datos dibujan un escenario en el que estos profesionales utilizan un stack tecnológico sencillo con:

- Una cuenta de Gmail, con sus servicios básicos incluidos, como elemento fundamental de trabajo,
- que complementan con algún servicio de gestión o de seguridad o propio montado sobre Azure/AWS vertical de su sector de actividad,
- Y con servicios en Nube contratados o puestos a su disposición por los terceros a los que prestan sus servicios y que no identifican como servicios en Nube, sino del cliente.
- Y con una base técnica OnPremise muy limitada o inexistente, que en muchos casos se centraría en su EndPoint con algún servicio para su securización.



Los usuarios no técnicos satisfacen muchas de sus necesidades con servicios de ofimática, almacenamiento y correo sobre Google.

10. Ficha Técnica del Estudio

Este Estudio ha sido diseñado y ejecutado por los profesionales que figuran en la portada de este documento. El diseño ha incluido la identificación, selección y ponderación de los aspectos que se querían investigar durante su ejecución, de acuerdo con los aspectos que estos profesionales han propuesto y sugerido como de mayor interés y apoyo a la profesión. Asimismo, se han encargado del análisis de la información recogida de usuarios y no usuarios de servicios en la Nube a partir de una encuesta, para establecer las conclusiones que figuran en este documento.

Los profesionales participantes en este Estudio forman parte de los Capítulos Español, Peruano, Boliviano, Chileno, Argentino y Mexicano de Cloud Security Alliance, y del Capítulo de Madrid de ISACA, en colaboración con ISMS Forum.

El Estudio se ha realizado en base a encuestas recopiladas entre el 8 y el 22 de mayo de 2024, a través de la plataforma online SurveyMonkey®. Se recopilaron un total de 225 respuestas de profesionales y organizaciones. La encuesta y el acceso al mismo se realizó mediante listas de correo y otros servicios de mensajería, boletines de ISMSForum y sitios Web, grupos de LinkedIn y canales de twitter oficiales de los participantes en el Estudio.

Este 12º Estudio está abierto a todas las organizaciones con presencia en el mercado Latinoamericano y Español, con independencia su huella geográfica, tamaño, madurez tecnológica, estrategia de adopción de la Nube y/o sector. Esta sección del Estudio describe las características específicas de las empresas que han aportado su visión para la preparación de este estudio, de forma que se puedan sostener la aplicabilidad de los datos y conclusiones obtenidas por ser representativa respecto del tamaño de las empresas participantes, las áreas de actividad en la que operan y la presencia geográfica.

10.1. Consideraciones sobre posibles sesgos en la información analizada

La Ilustración 42 muestra la distribución geográfica de los participantes en el Estudio. En ella se establece el porcentaje de organizaciones que han participado en el Estudio, y que han declarado tener presencia en esa geografía. Así, cuando una organización ha declarado tener huella geográfica simultánea en varias geografías a la vez, se ha contabilizado la presencia en todas y cada una de ellas. Por ello, la suma de los porcentajes presentados en la Ilustración supera el 100%, reflejando así fielmente la presencia de las organizaciones en las zonas geográficas consideradas en el Estudio.

Este Estudio tiene una distribución de participantes significativamente diferente respecto de ediciones anteriores. Ha registrado un aumento significativo de participantes con presencia en Bolivia, que concentra en esta edición más de la mitad de los participantes. En el resto de las geografías se conserva el peso relativo entre los participantes en cada una de ellas, con mayor representación de organizaciones en España, Chile y Perú, en este orden.

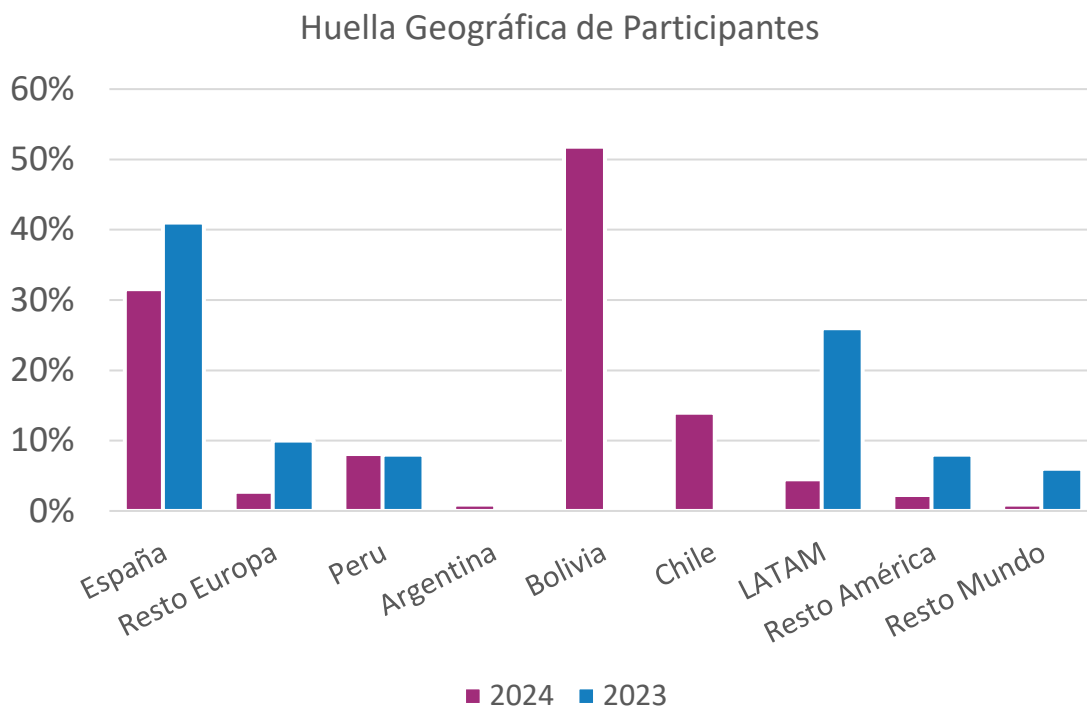


Ilustración 41.- Huella geográfica de las organizaciones que han participado en el Estudio

En un análisis más detallado de los participantes con presencia en Bolivia, el Estudio ha detectado diferencias relevantes entre los perfiles en Bolivia y los perfiles del resto de geografías.

Por ejemplo, la Ilustración 43 analiza el nivel de responsabilidad de los participantes en el Estudio. Mientras que los perfiles directivos representan el 20% de los participantes en Bolivia, suponen el 50% de los participantes del resto de geografías. Por otro lado, la proporción de participantes con perfil No Técnico y No Directivo también es mucho más relevante en este Estudio. La distribución de participantes en estudios anteriores es más cercana al acumulado de geografías, excluyendo a Bolivia.

Por su parte, la Ilustración 44 revela que los participantes con presencia en Bolivia se declaran mayoritariamente como no usuarios de los servicios de Nube, mientras que los usuarios del resto de huellas geográficas se declaran usuarios de servicios en la Nube en un 80%.

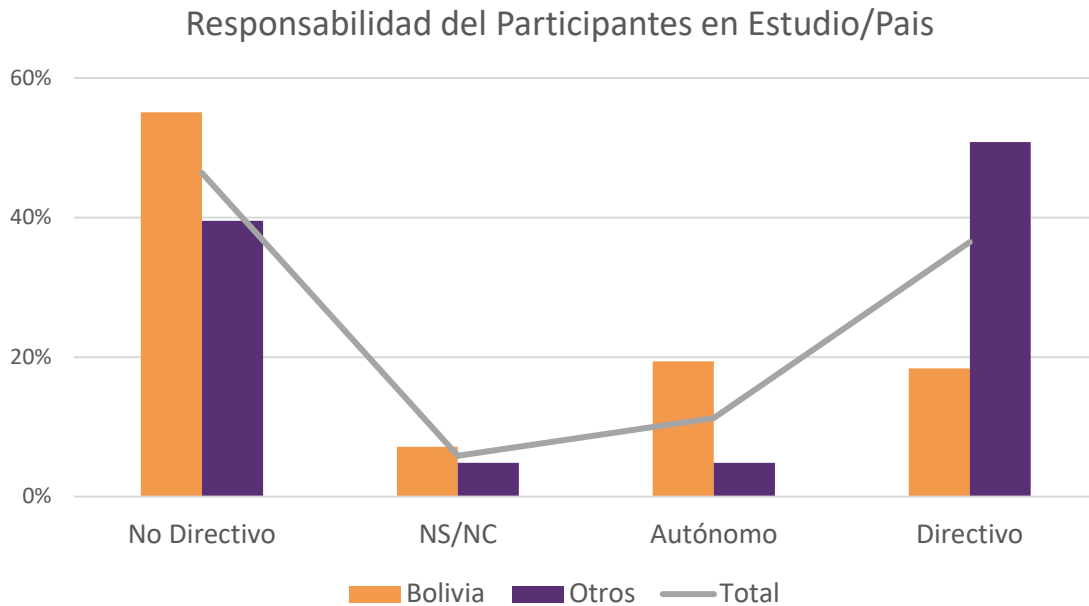


Ilustración 42.- Nivel de Responsabilidad de participantes en el Estudio por geografía: Bolivia, resto de países, total

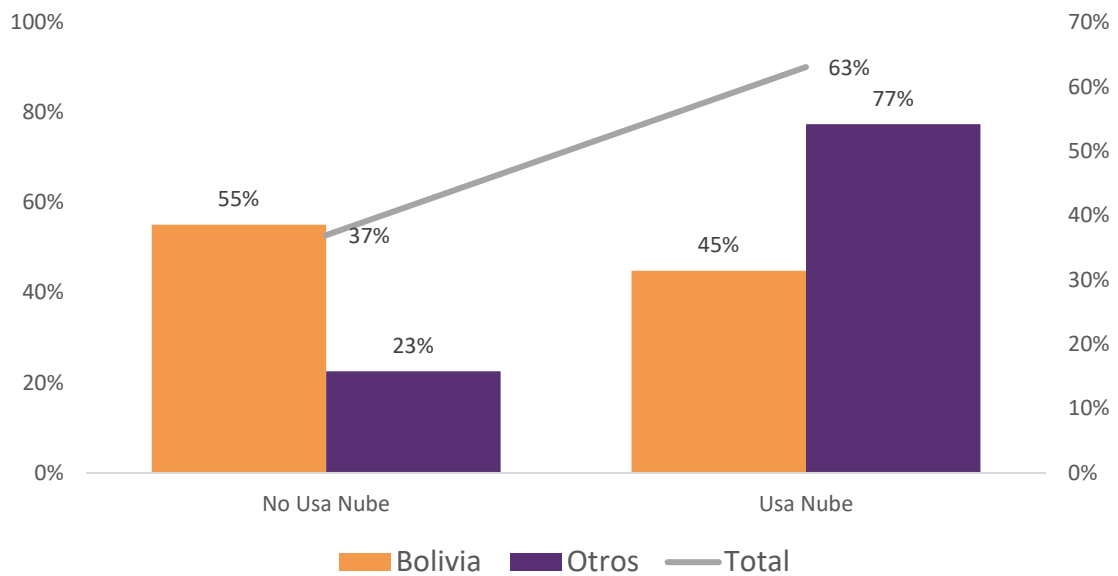


Ilustración 43.- Uso declarado de Servicios en Nube, por geografía: Bolivia, resto de países, total

En base a este análisis, los analistas del Estudio han determinado que la información proporcionada por los participantes de la encuesta incorpora algunos sesgos y diferencias que podrían afectar en la obtención de conclusiones del Estudio. En particular, en el análisis y evaluación de las series históricas de algunos parámetros analizados. En algunos casos, se han

obtenido conclusiones separadas para la muestra total analizada y para la muestra sin considerar los datos de Bolivia.

Así, el Estudio ha ido indicando en cada una de las conclusiones si ese hallazgo concreto se ha establecido contemplando el total de la muestra de información facilitadas, o sólo aquella parte que es comparable a la de la secuencia histórica.

10.2. Perfiles que han participado en el Estudio

La Ilustración 42, que aparece anteriormente en este documento, muestra la distribución geográfica de los participantes en el Estudio. Las conclusiones del análisis de estos datos ya se han abordado.

Respecto del sector en el que se desempeñan las organizaciones, la Ilustración 45 presenta la distribución del total de participantes. En ella se observa una mayoría de participantes del sector Telco, seguido por organizaciones de administración pública y por consultorías. Las empresas del sector de financiero también tienen una representación significativa. La participación de otros sectores no fue suficientemente representativa en ningún caso, si bien la representación acumulada de todos ellos alcanza una tercera parte de todos los participantes.

Estas consideraciones son razonablemente similares en la participación total y en la participación sin considerar a Bolivia, si bien la mayoría de las empresas del sector financiero que participaron no tienen presencia en este país.

Esta muestra de participación es también similar a la de anteriores estudios del Estado del Arte de Seguridad en la Nube.

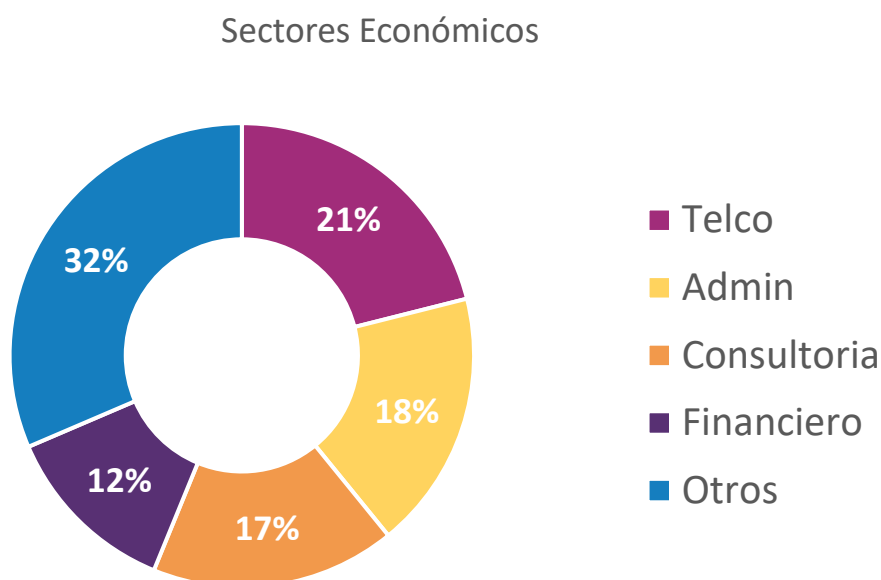


Ilustración 44.- Distribución sectorial de participantes en el Estudio

Respecto de la distribución de las empresas participantes en el Estudio respecto de su tamaño, esta 12ª edición mantiene la relación entre los participantes, con una muestra representativa de organizaciones de todas las dimensiones y una mayor representación de las empresas de tamaño mediano, entre los 25 y los 2.500 empleados. En este sentido, esta edición del Estudio mantiene la línea continuista sobre ediciones anteriores. La Ilustración 46 muestra el análisis de la muestra del Estudio bajo esta óptica.

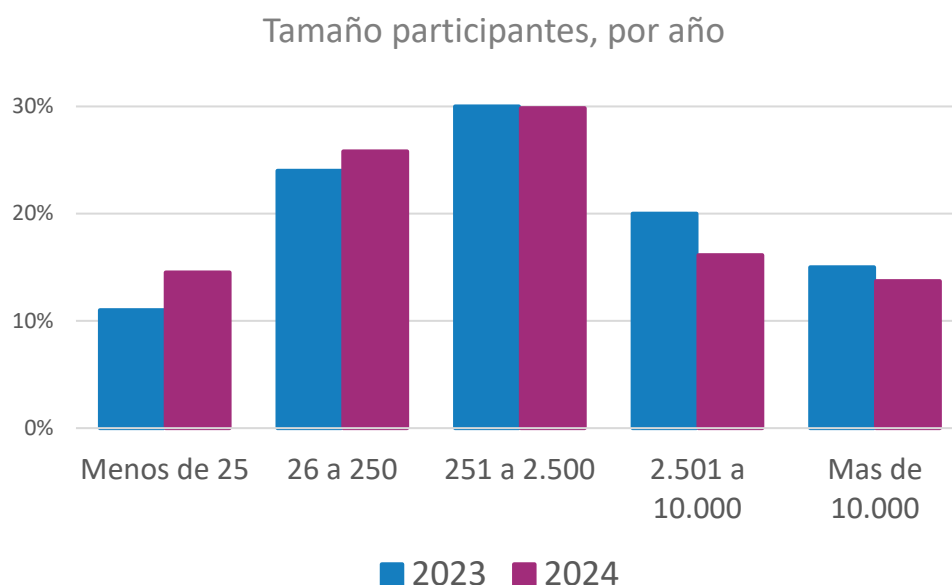


Ilustración 45.- Distribución de los participantes en la encuesta por tamaño de empresa excluyendo Bolivia. Comparación entre años

Cuando se analiza el tamaño de las empresas participantes respecto de su ubicación geográfica, el tamaño predominante de las empresas ubicadas en Bolivia es el de pequeña empresa, con más de un 60% de los participantes de un tamaño inferior a los 250 participantes, mientras que las empresas de mayor tamaño tienen un peso significativamente menos en la muestra. La Ilustración 47 compara la muestra de participantes con presencia en Bolivia, frente a la muestra de participantes sin presencia en ese país. Estas diferencias de tamaño de los participantes refuerzan el análisis realizado anteriormente sobre las diferencias entre los participantes en esta geografía, los posibles sesgos que pueden aportar al Estudio y la decisión de realizar en algunos casos un análisis individualizado de los resultados de la Estudio incluyendo u obviando este factor.

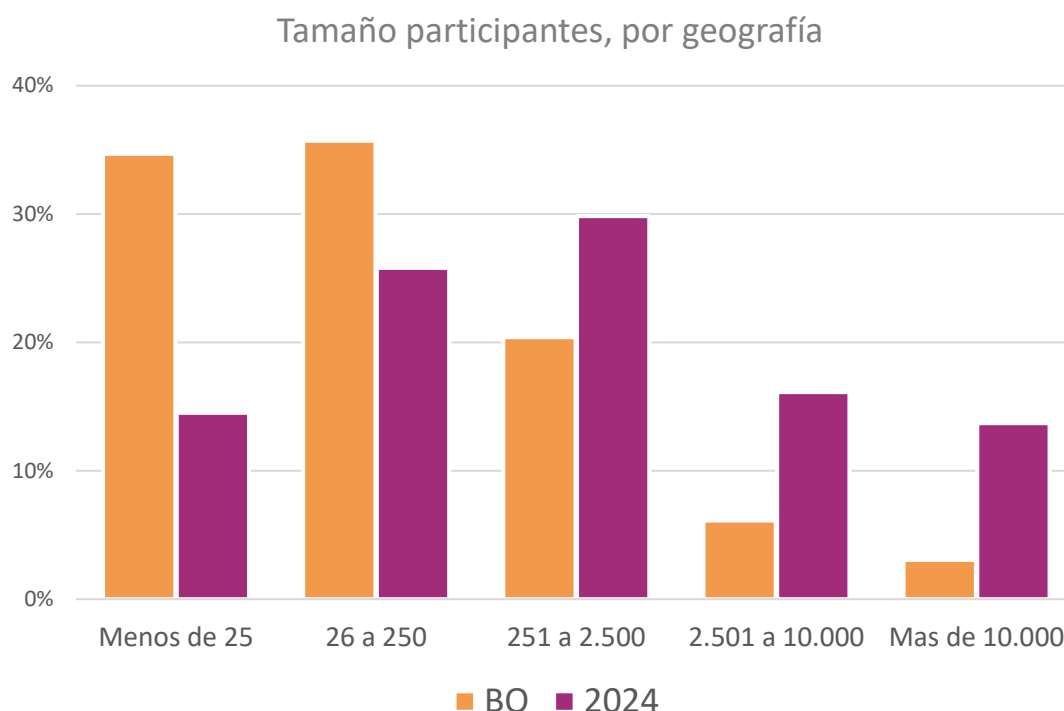


Ilustración 46.- Distribución de los participantes en la encuesta por tamaño de empresa. Bolivia vs otras geografías

10.3. Consideraciones Temporales sobre el Estudio

Como se ha señalado en el capítulo “Consideraciones Temporales sobre el Estudio”, la información analizada en este estudio se recopiló entre el 8 y el 22 de mayo de 2024.

Esta fecha debe ser considerada en contexto respecto de algunos eventos ocurridos en el mercado de seguridad y de servicios en la Nube, en tanto que pudieran haber influido en los participantes en la encuesta y en sus respuestas.

- Incidente Snowflake, en el mes de mayo¹⁷, que supuso la revelación de filtraciones de datos de los clientes de este proveedor en la Nube, si bien el medio utilizado para realizar la intrusión, la naturaleza de la información obtenida en la misma y los clientes del proveedor afectado fueron conocidos progresivamente a lo largo del mes. Es posible que este incidente pudiera influir en la información recogida durante la encuesta.
- Incidente CrowdStrike de 19 de Julio¹⁸, que causó caídas de múltiples sistemas a nivel mundial. La recopilación de la información se había completado cuando ocurrió el incidente, pero el análisis de esta información se estaba aún realizando.

Las conclusiones del Estudio pudieran, por ello, haber variado desde su fecha de producción hasta su fecha de publicación. Y por ello, serán abordadas de nuevo en futuros Estudios.

¹⁷ <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/fuga-de-informacion-en-snowflake>

¹⁸ <https://www.crowdstrike.com/technical-details-on-todays-outage-latam/>



Una iniciativa de:



www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62



@ISMSForum