11º ESTUDIO DEL ESTADO DEL ARTE DE LA SEGURIDAD EN LA NUBE

Una iniciativa de

isms forum

CSA ES cloud security SPAIN alliance SM

En Colaboración con

ISACA Madrid Chapter

ISACA Lisbon Chapter

Peru Chapter

Noviembre 2023

11º Estudio del Estado del Arte de la Seguridad en la Nube

AUTORES

COORDINADORES	Mariano J. Benito (GMV), CSA-España
	Antonio Cueva (Kairos NET Perú), CSA-Perú
	Maite Avelino (Independiente), Isaca-Madrid
	Josué Delgado (Independiente), Isaca-Lisboa
	Beatriz García (ISMSForum), CSA-España
	Daniel Garcia (ISMSForum), CSA-España
ANALISTAS	Alberto Bernaldez (Liberty Seguros), CSA-ES
	Alfredo Alva (Presidente), CSA-PE
	Cándido Arregui (AENA), CSA-ES
	Daniel Fernandez (LafargeHolcim), CSA-ES
	Diego Fernandez Vázquez (ISDEFE), CSA-ES
	Fernando Iglesias (BBVA Next), CSA-ES
	Javier Carbayo (Deloyers Abogados), CSA-ES
	Javier Diaz Evans (A3sec), CSA-ES
	Jorge Castañeda (Comunicaciones), CSA-PE
	Josep Bardallo (Grupo Recoletas), CSA-ES
	Juan José del Río (TMB), CSA-ES
	Julia Socorro (Islas SEM), CSA-ES
	Luis Ballesteros (WiZink), CSA-ES
	Mara Fernández (DXC Technology), CSA-ES
	Pablo Rodriguez (Naturgy), CSA-ES
	Ramón Codina (Consultant), CSA-ES
	Santiago Minguito (Pepsico), CSA-ES
	Ana Belén Galán (BBVA CIB), CSA-ES
	Concepción Cordón (Independiente), CSA-ES
DISEÑO/ MAQUETACIÓN	Rim Souri (ISMSForum), CSA-España
	Beatriz García (ISMSForum), CSA-España

Índice de Contenidos

Principales Hallazgos del 10º Estudio

El 11º Estudio del Estado del Arte de Seguridad en la Nube se ha realizado en 202 en cooperación entre los capítulos español y peruano de Cloud Security Alliance, y los capítulos de Madrid y Lisboa de ISACA, continúa la serie de estudios realizados en 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021 y 2022. El equipo de analistas que ha preparado desea y confía en que este Estudio y sus contenidos sean de utilidad para sus lectores.

Esta 11ª Edición del Estudio del Estado del Arte de Seguridad en la Nube ha confirmado en primer lugar que la posición dominante en el mercado de los tres CSP Google Cloud, AWS y Azure efectivamente existe, y hay un 97% de organizaciones que se apoyan en alguno de los tres servicios. El consumo de servicios es más extendido en organizaciones de mayor tamaño, mientras que las organizaciones más pequeñas concentran sus apuestas en servicios y proveedores concretos.

En segundo lugar, el estudio detecta que los servicios que se están consumiendo de los CSPs son servicios Core de los procesos de negocio de las organizaciones, por lo que no pueden fallar. Esta relevancia explica la inversión en la tendencia a la baja en las expectativas y requisitos sobre la nube, que vuelven a elevarse. Inversión lógica cuando las organizaciones ya tienen dependencia de estos servicios para sus operaciones diarias y un fallo en los mismos supone una caída del total de los servicios de la empresa. Este factor toma preponderancia frente a otros también relevantes, de forma que para muchas organizaciones la continuidad de negocio prima sobre la soberanía del dato.

También destaca la mejora en la concienciación de seguridad sobre el uso de la nube, impulsado por los estamentos directivos y por las organizaciones de mayor tamaño. Este efecto aún no ha generado suficiente tracción en el resto de los niveles organizativos o entidades.

La gestión de incidentes sigue beneficiándose de la Nube, con una mayor capacidad de detección que hace que el número de incidentes disminuya, aun a costa de un mayor esfuerzo inversor y de recursos por las organizaciones.

Finalmente, los profesionales independientes demuestran un mayor nivel de exigencia en los servicios de la Nube, tanto a nivel expectativas como requisitos y de petición de certificados de seguridad a sus CSPs.

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

Objetivos y Ámbito del Estudio

El objetivo del presente Estudio continúa para 2023 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 2013[1], 2014[2], 2015[3], 2016[4], 2017[5], 2018[6], 2019[7], 2020[8], 2021[9] y 2022[10], y busca investigar y conocer el Estado del Arte de la adopción de la Computación en la Nube, las tendencias históricas establecidas, y el papel que juega la seguridad en la adopción de estos servicios. Todo ello, desde el punto de vista de los Usuarios de Servicios en la Nube, en los mercados hispanohablantes en los países cuyo capítulo local de Cloud Security Alliance ha participado. Ha contado pues con analistas de los Capítulos de CSA señalados, junto con los capítulos de ISACA en Madrid y Lisboa.

Para ello, este 11º Estudio del Estado del Arte de Seguridad en la Nube cierra el análisis de las circunstancias particulares derivados de la pandemia Covid19 para centrar el análisis en aspectos abiertos a debate y a implantación en la actualidad: Gestión avanzada de incidentes en la Nube, extraterritorialidad de la Nube o la valoración de Shadow-IT como una oportunidad o una amenaza.

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 o Shadow IT. También mantiene la investigación en el perfil de usuarios no técnicos detectado en el 8º Estudio, para conocer las diferencias entre estos usuarios frente a los usuarios clásicos de 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/viiiestudioestadoseguridadnubev11602744518.pdf

[9] https://www.ismsforum.es/ficheros/descargas/xiestudiosotacsa2021v31637832356.pdf

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

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. Tipología de Servicios consumidos en la Nube

1.1. Adopción o rechazo de los servicios en la Nube

El primer dato relevante sobre el uso de la nube declarado por los participantes en este 11º Estudio se refleja en la Ilustración 1. En ella se puede detectar que el 90% de las organizaciones participantes han adoptado servicios en la nube y actualmente los están utilizando. Por otra parte, un 4% de los participantes declaran que han descartado su uso, en línea con resultados de estudios anteriores, mientras que el 6% restante están aún de las organizaciones están evaluando la implementación del uso de la nube. El análisis conducido se centrará en los datos ofrecidos por el 90% de usuarios de la Nube, considerando el total de respuestas sólo para el análisis de expectativas y requisitos.

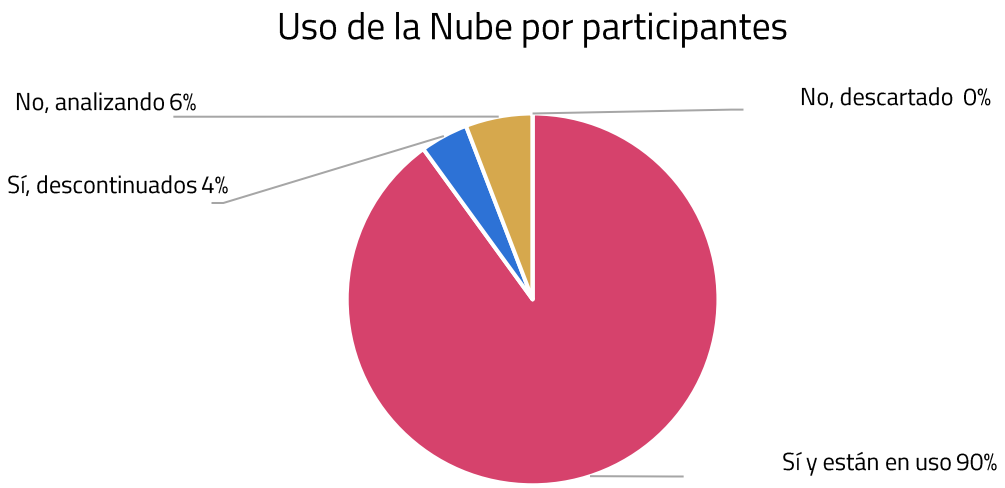


Ilustración 1.- Declaración de participantes sobre su uso de servicios en la Nube

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

En esta 11º edición del Estudio del Estado del Arte de Seguridad en la Nube se ha querido analizar con mayor detalle el perfil de proveedores de servicios en el Nube (CSP) que en los que se están efectivamente apoyando los usuarios. Para ello, se ha consultado a los participantes en el estudio por la identidad de los CSP en los que se apoyan para recibir servicios de ellos. La Ilustración 2 muestra el análisis realizado sobre los datos recogidos.

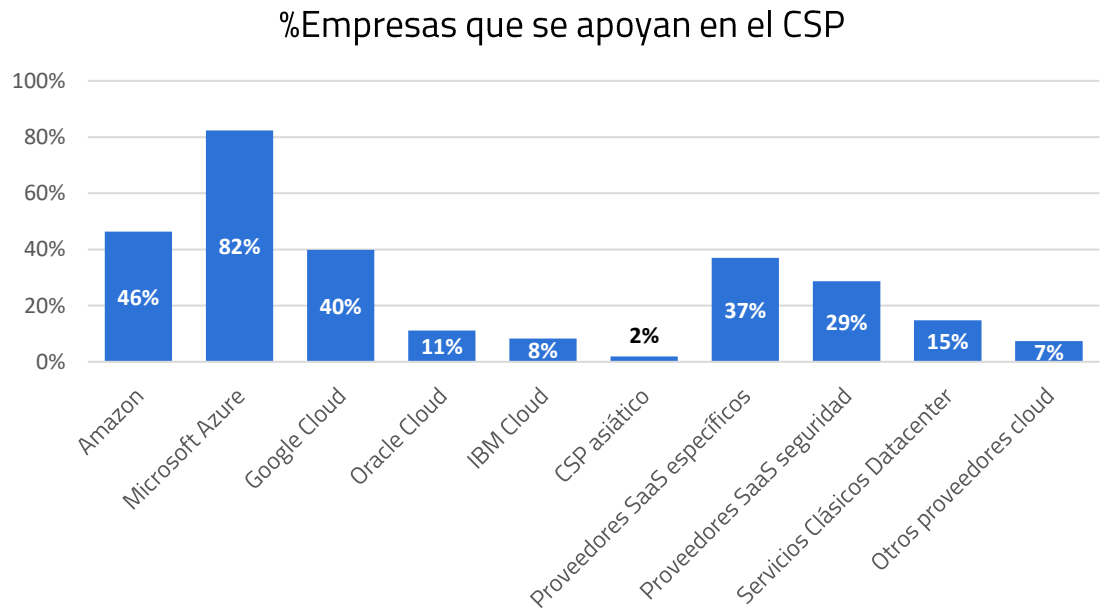


Ilustración 2.- % de usuarios que se declaran usuarios de cada tipo de CSP

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 mayor proporción de usuarios que se declaran usuarios de los servicios de Azure acompañados en el top3 de proveedores por los otros dos, si bien sólo el 14% de las empresas aceptan un entorno multicloud donde utilizan servicios de los tres CSP. Y sólo el 3% de los usuarios de los servicios en la nube no utilizan servicios de ninguno de estos tres proveedores. Estos datos confirman las expectativas previas del estudio sobre la alta dependencia del sector sobre estos tres CSP.

El 97% de usuarios se apoya en servicios de Azure, Amazon y/o Google.

De forma complementaria, el estudio identifica que los proveedores SaaS que proporcionan servicios verticales específicos tienen un grado de aceptación comparable al de alguno de los CSPs públicos señalados. Y que casi uno de cada tres usuarios se declaran usuarios de servicios de Security-as-a-Service (SECaaS), dato que mejora el grado de adopción de servicios respecto del 20% que se declaraban usuarios de estos servicios en el 10º estudio.

El resto de CSP tienen una utilización por parte de los usuarios menor, habitualmente cercando al 10%. Esto incluye el uso de DataCenters clásicos, que sigue siendo un modelo de uso de servicios muy presente y no solo por parte de proveedores de servicios, sino también de usuarios finales. El Estudio no ha recogido información adicional para profundizar en las razones de los participantes para mantener esta presencia en ubicaciones físicas no virtualizadas, por lo que no es posible determinar si estos usuarios finales están a la espera de futuras de decisiones de migración de servicios a la Nube, si se ha tomado la decisión de mantener la relación directa con el DataCenter, o si son servicios desplegados conjuntamente en CSP y en la Nube.

Siguen aumentando los usuarios de servicios de Seguridad desde la Nube (SECaaS).

La Ilustración 3 analiza el uso de las distintas opciones de CSP cuando se considera el tamaño de las organizaciones usuarias de los servicios. Se pueden identificar claramente cuatro tendencias.

- La preferencia de las organizaciones participantes de menor tamaño por los servicios del proveedor Google Cloud. Esta tendencia no había sido detectada hasta la fecha. Analizada en conjunto con los datos de la Ilustración 6, que señalan a las empresas de menor tamaño como máximas usuarias de los servicios de correo de electrónico, parece apuntar a que estas empresas de menor tamaño consideran que un servicio de correo electrónico puede resolver sus necesidades de la manera más efectiva.

- El mayor consumo de todo tipo de servicios en la Nube por las empresas de mayor tamaño, que son usuarias más intensas de casi todos los CSP considerados. En casos como Oracle Cloud, IBM Cloud Services o SECurity-as-a-Service, con una diferencia considerable respecto de las empresas más pequeñas. Como puede verse en la Ilustración , esta notable diferencia responde a un uso más intenso de los CSP apoyándose de media en uno o dos CSPs más que organizaciones de otro tamaño.

- Las empresas de tamaño grande y muy grande son las usuarias más intensas de servicios SaaS sobre Amazon o Azure. Este hallazgo es similar al anterior respecto de la intensidad del uso de estos servicios, y complementa al primero realizado, reforzando la tendencia detectada en estudios anteriores a que las empresas de mayor tamaño consumen servicios a medida y utilizan las capacidades de PaaS e IaaS de la Nube para construir los servicios que precisas y que no encuentran como SaaS.

- El uso de servicios de seguridad desde la Nube aumenta cuando las organizaciones son de mayor tamaño, y se dispara para las de mayor tamaño. En todo caso, el promedio en todo caso está cercano al 30% de utilización de SECaaS, que mejora el anterior 20% de ediciones anteriores del estudio.

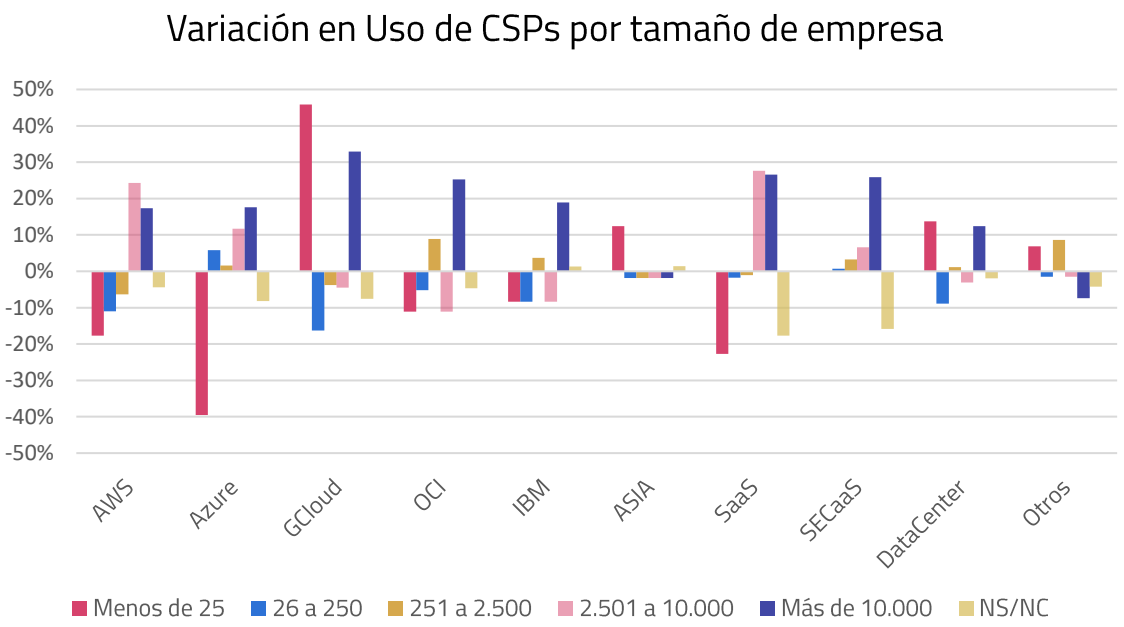


Ilustración 3.- Diferencias en el uso de CSP según el tamaño de la organización

Las grandes empresas se constituyen en las mayores consumidoras de servicios en la Nube, de todo tipo y proveedor. Las empresas más pequeñas concentran su apuesta por la Nube en servicios y necesidades concretas.

El Estudio también ha querido analizar si los usuarios utilizan los servicios de un único proveedor para el total de sus necesidades o si seleccionan a distintos proveedores para distintos servicios. Como puede verse en la Ilustración , sólo uno de cada cuatro empresas tiene un único CSP y estarían expuestas a 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. Las empresas de mayor tamaño también se apoyan en un número mayor de CSPs (ver Ilustración) no están libres de riesgos de *Locked-in*, si bien este efecto puede ocurrir de forma puntual para proveedores y servicios concretos y no para el total de la organización como en el caso de las empresas pequeñas y medianas.

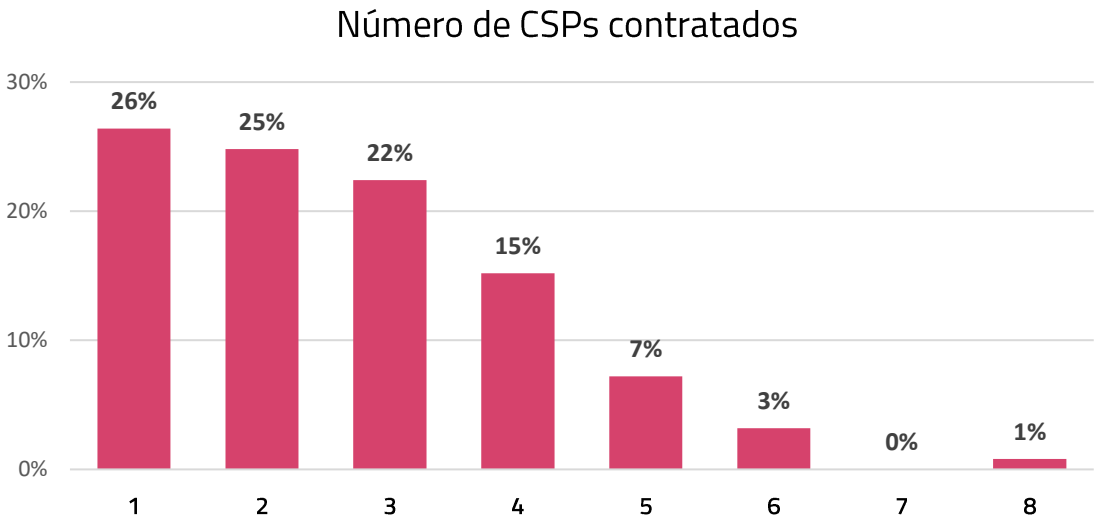


Ilustración 4.- Distribución del número de CSPs contratados

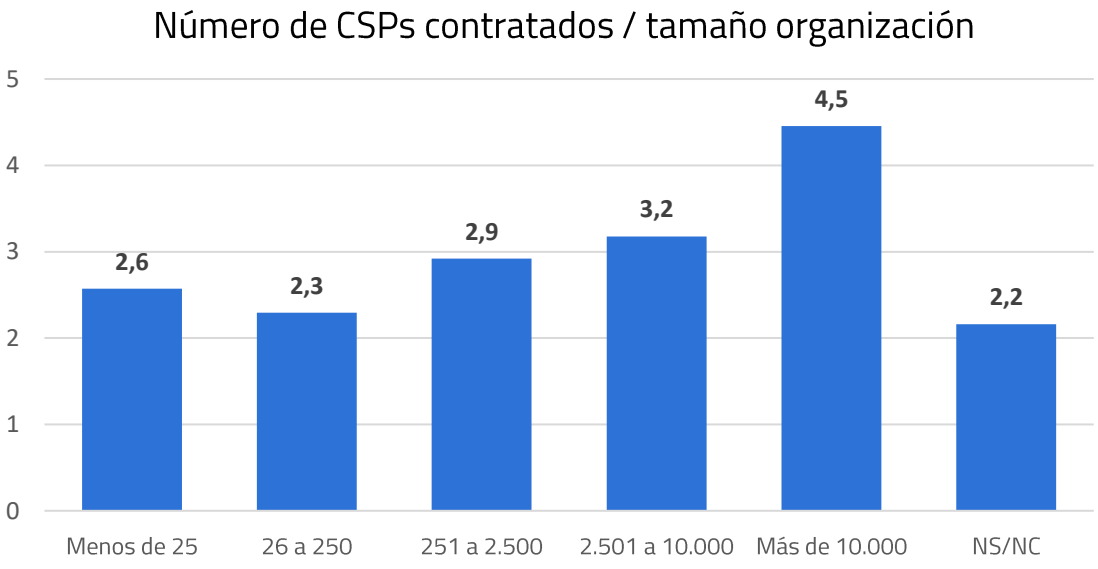


Ilustración 5.- Número de CSPs contratados por las organizaciones, según su tamaño

1.3. Servicios de la Nube demandados por los usuarios

El análisis de los servicios de nube contratados por los distintos usuarios que se muestra en la ilustración 6 confirma el análisis realizado anteriormente para los CSP, donde las empresas de mayor tamaño son las mayores consumidoras de estos, con áreas concretas en las que empresas de otro tamaño concentran su demanda de servicios.

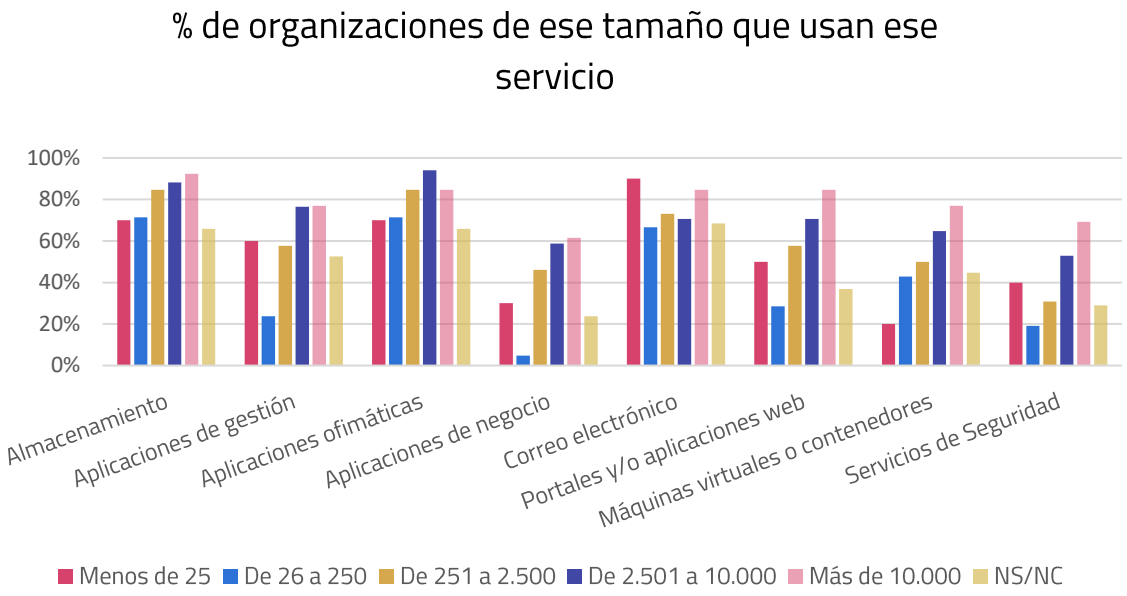


Ilustración 6.- Diferencias en el uso de servicios en la Nube según el tamaño de la organización

En relación con 2022[11], los servicios de Almacenamiento y de Ofimática experimentan un crecimiento en la demanda, pasando del 70% de media de organizaciones usuarias, a valores cercanos al 80% para este Estudio. Junto con el Correo Electrónico, estas aplicaciones representan la mitad de los servicios prestados desde la nube. También se confirma el aumento de consumo de servicios de Seguridad desde la Nube desde el 15% medio de 2022 a subir del 30% de usuarios, incluyendo también servicios especializados de seguridad tipo SASE, CASB, CSPM, CNPA o CWPP que se añaden a otros servicios clásicos.

[11] https://www.ismsforum.es/ficheros/descargas/estudio-estado-arte-seguridad-nube-2022.pdf#page=36

Almacenamiento, Ofimática y Correo Electrónico suponen la mitad de los servicios consumidos en la Nube.

En esta edición, se han introducido en el estudio nuevos servicios prestados desde la nube, los cuales se ha evidenciado que tienen aún un grado de implantación bajo. Estos servicios son DRaaS (Disaster Recovery as a Service), continuidad de negocio y recuperación ante desastres, Blockchain, IoT, Soporte a Procesos Industriales y otros servicios no especificados en las anteriores opciones. Al igual que ocurrió en Estudios anteriores, cabe esperar que algunos de estos servicios se adopten con más intensidad en un futuro cercano.

1.4. 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. El éxito de las mismas está condicionado a 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.

Este 11º Estudio se interesa por los resultados de estas estrategias. La ilustración 7 presenta un escenario de éxito razonable de las mismas, con 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.

El dato anterior no puede ser comparado con el de Estudios anteriores puesto que es la primera oportunidad en que se formula esta pregunta. Sí que puede hacerse un análisis más detallado de las organizaciones que se encuentran en cada escenario si se chequean las respuestas que dan las distintas organizaciones en función de su tamaño. Esta información se muestra en la ilustración 8, donde puede verse que las empresas de menor tamaño son las que han logrado completar la estrategia C*loud-Only* con más éxito, mientras que ese porcentaje de éxito corresponde con un meritorio 10% de empresas de cada tamaño. Y que, en el resto de los casos, las empresas que están en fases iniciales o intermedias es mayor que los que estén en fases avanzadas. Cabe esperar también una evolución de este indicador en línea con las tendencias de adopción identificadas en puntos anteriores y que en próximos estudios se detecte un mayor número de empresas que hayan adoptado ya al menos la mitad de sus servicios en la Nube.

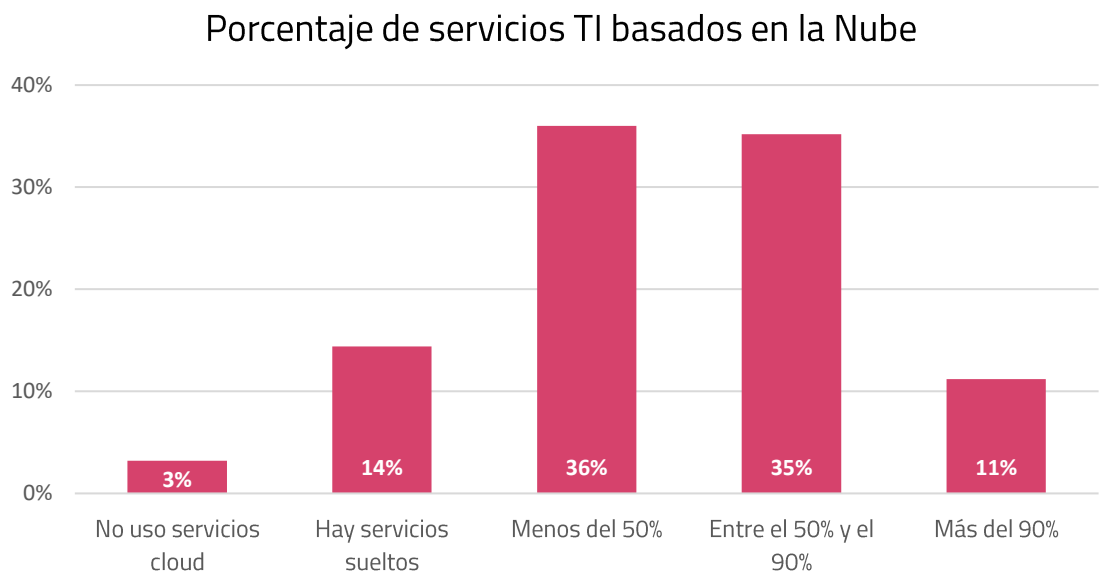


Ilustración 7.- Porcentaje de Servicios TI basados en la Nube de las organizaciones

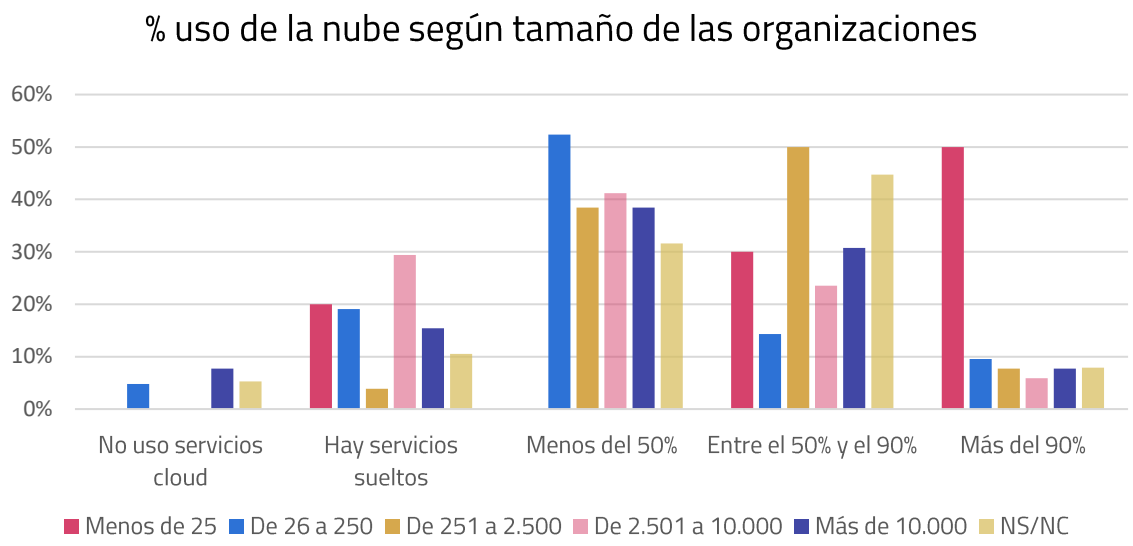


Ilustración 8.- Porcentaje de Servicios TI basados en la Nube de las organizaciones, según su tamaño

Las empresas de menor tamaño son las que han completado en mayor proporción una estrategia Cloud-Only.

2. Análisis de Expectativas de los Usuarios de la Nube

Se analizan a continuación el entendimiento de las necesidades y expectativas que tienen los usuarios con respecto al uso de servicios en la Nube, con independencia de los servicios concretos que luego se utilicen o las condiciones concretas de los mismos. Para discernir el nivel de exigencia de los usuarios, se ha realizado el análisis sobre las principales dimensiones de seguridad de la información y de otros campos relacionados como el cumplimiento, la privacidad o la continuidad del servicio, estableciendo la importancia que les otorgan los usuarios.

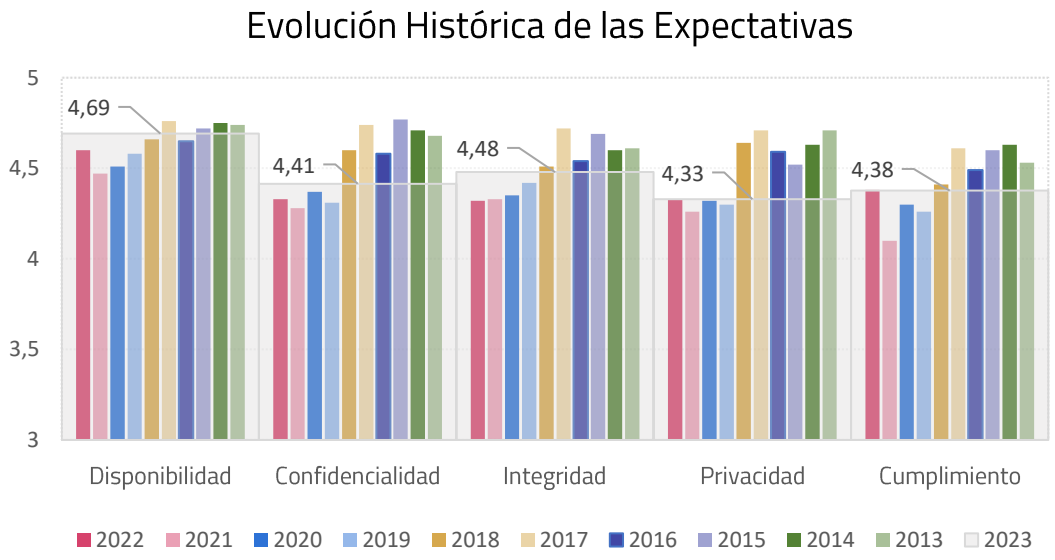


Ilustración 9.- Evolución de Expectativas de Seguridad de los usuarios de servicios en la Nube

El principal resultado del análisis de este primer parámetro es que se confirma la reversión de la tendencia descendente observada en los anteriores 4 años sobre las expectativas de seguridad en la Nube. En el caso de cumplimiento legal y privacidad, esta reversión se completó en 2022 y el estudio confirma que se mantienen los niveles de exigencia ya identificados. Por el contrario, las dimensiones de Confidencialidad, Integridad y Disponibilidad ven crecer las expectativas de forma significativa, llegando a niveles cercanos al máximo de la serie histórica para la disponibilidad, e incrementando de forma más significativa en la integridad.

Las expectativas mantienen el cambio de tendencia, y se incrementan en la Confidencialidad, la Integridad y de forma más intensa en la Disponibilidad de los servicios.

Las causas de esta mejora no pueden achacarse exclusivamente a la aparición de nuevas regulaciones y estándares, como en el año anterior, puesto que las dimensiones de privacidad y cumplimiento no varían. En un análisis más detallado, la Ilustración10 muestra claras diferencias entre las expectativas del personal Directivo, que son consistentemente mayores que los valores medios, y claramente más altas que las expectativas del personal no técnico. Por su parte, analizando la variación de expectativas para los distintos tamaños de empresa en la Ilustración 1, se detecta que las empresas medianas (26 a 2.500 empleados) tienen unas expectativas mayores a la media, y muy divergentes a las del resto de organizaciones. Precisamente, estas empresas declaran en la Ilustración 66 un uso menor de servicios en la Nube.

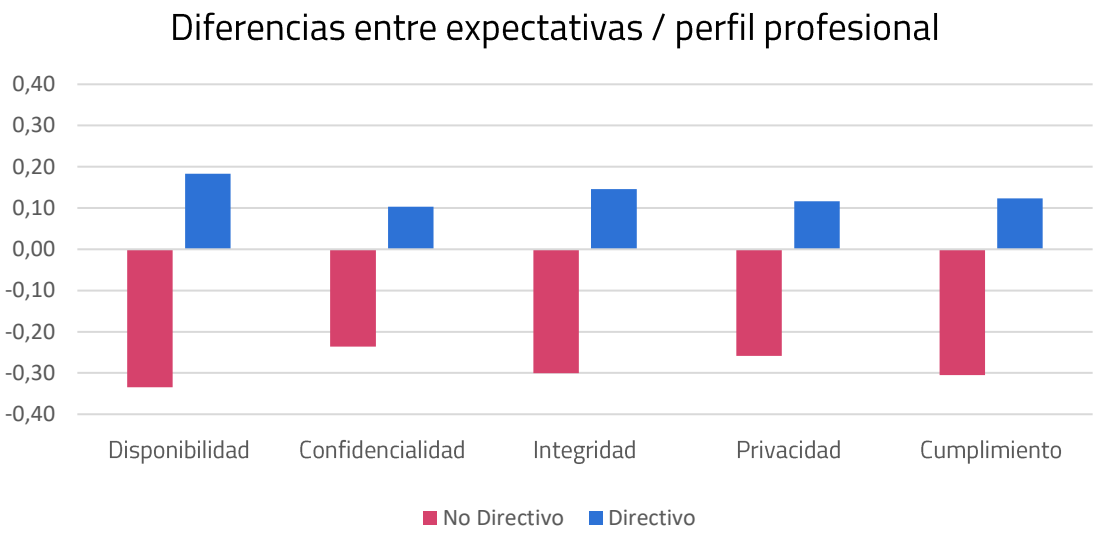


Ilustración 10.- Diferencias de Expectativas sobre la Nube por personal Directivos y No Directivo

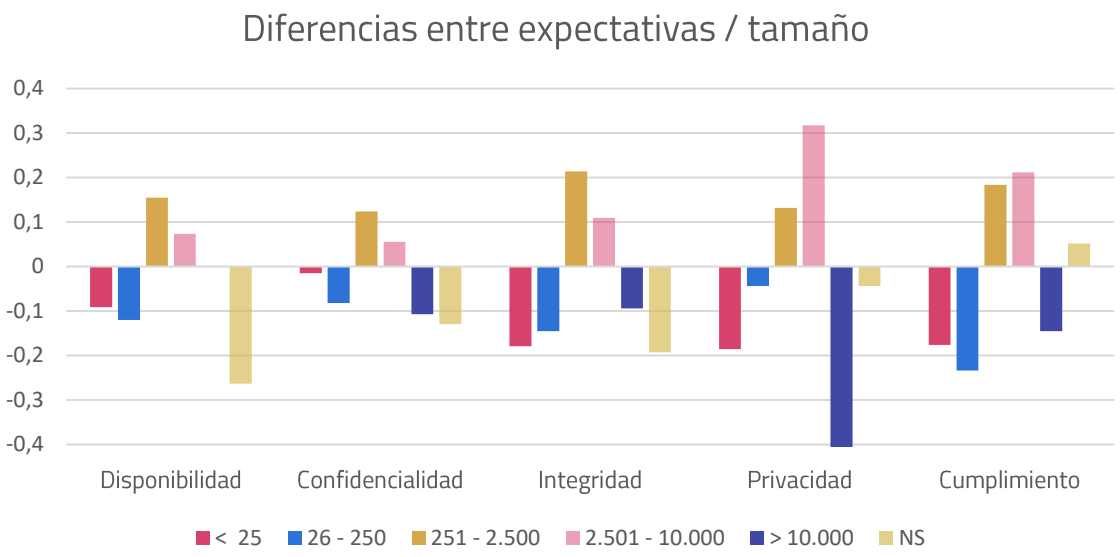


Ilustración 11.- Diferencias de Expectativas sobre la Nube de acuerdo con el tamaño de la organización

Por ello, parece que las expectativas sobre el resultado de la Nube crecen fundamentalmente por un aumento de las expectativas de los perfiles directivos de las empresas medianas. El Estudio interpreta que los distintos CSPs están incrementando su llegada a este tipo de empresas, en las que ahora tienen una presencia menos representativa y que esta acción esté creando el aumento detectado.

Las expectativas crecen por el aumento de las expectativas de los perfiles directivos de las empresas medianas.

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 habitualmente exigibles a un proveedor, de forma que el CSP ofrezca confianza y satisfaga requisitos de seguridad jurídica y de seguridad técnica en la prestación de los servicios contratados. En este capítulo se analiza con qué intensidad se requieren ciertos de estos requisitos antes de iniciar cualquier prestación de servicio en la Nube.

En líneas generales y según se muestra en la Ilustración12, las organizaciones y los consumidores de servicios en la Nube siguen teniendo un nivel de exigencia mayor que alto en todos sus requisitos, derivado de la importancia de todos estos requisitos a la hora de contratar servicios en la Nube.

Se sigue dando importancia a las leyes de privacidad de los datos de carácter personal, como exigir el cumplimiento de la directiva GPDR en Europa, aunque esta se encuentre en el segundo lugar de importancia. Los CSPs de mayor cuota de mercado de la Ilustración 2 están declarando un compromiso con la prestación de servicios locales en los distintos países con la apertura de centros de servicio locales en más geografías (en particular en España), tanto para mejorar su cercanía a sus clientes, como la latencia de sus servicios y para dar mayores garantías y confianza a los consumidores de aseguramiento de la soberanía del dato. Estas decisiones podrían verse plasmados en la mejora de indicadores como la selección de la ubicación física dentro del mismo territorio donde se consumen los servicios en la nube o la facilidad de ofrecer la portabilidad de los datos y efectivamente la Ilustración así lo muestra, siendo los dos únicos requisitos que mejoran en el presente estudio respecto de la anterior edición de este Estudio.

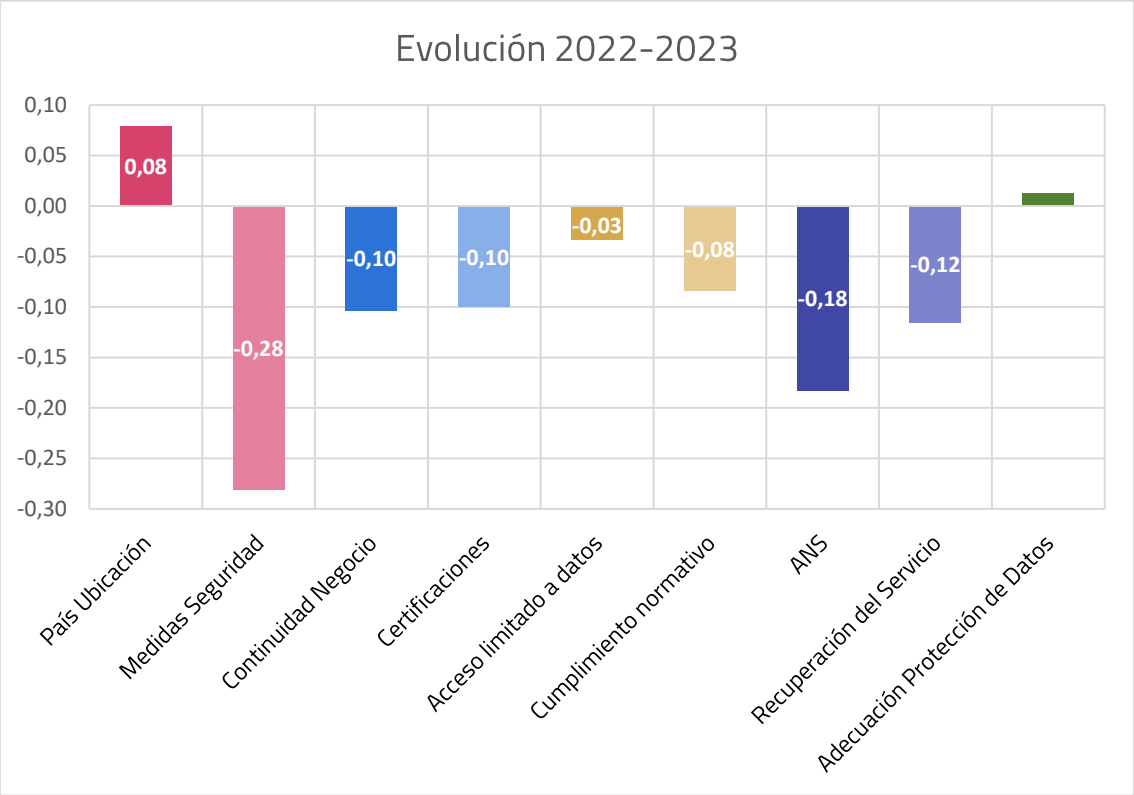


Ilustración 12.- Comparativa años 2022 y 2023

Los requisitos solicitados a los CSP por sus usuarios se han relajado un poco este año

En una visión global de la exigencia de requisitos que se exigen actualmente a los CSP, la continuidad de negocio, la resiliencia ante desastres, es el requisito de más nivel de exigencia. El cumplimiento de GDPR y la existencia de medidas de seguridad también están más cerca de una exigencia "muy alta" que simplemente "alta" y a escasa distancia de la continuidad de negocio. Del resto de parámetros considerados, la exigencia de certificaciones y el acceso a logs del CSP son los de menor nivel de exigencia.

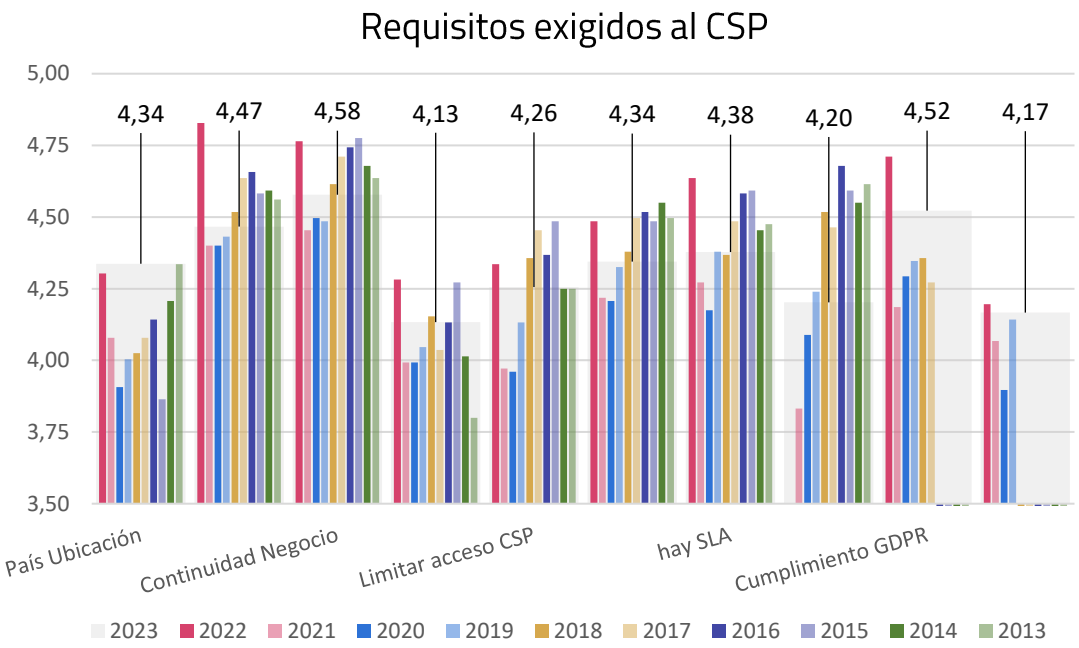


Ilustración 13.- Nivel de exigencia en los Requisitos de Seguridad solicitados por los clientes de Nube en 2023

Los usuarios siguen siendo más exigentes con la continuidad del servicio sobre la "soberanía del dato" u otros requisitos.

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 nuevas funcionalidades recibidas y en cómo ayudan estos servicios a las empresas a conseguir sus objetivos de negocio.

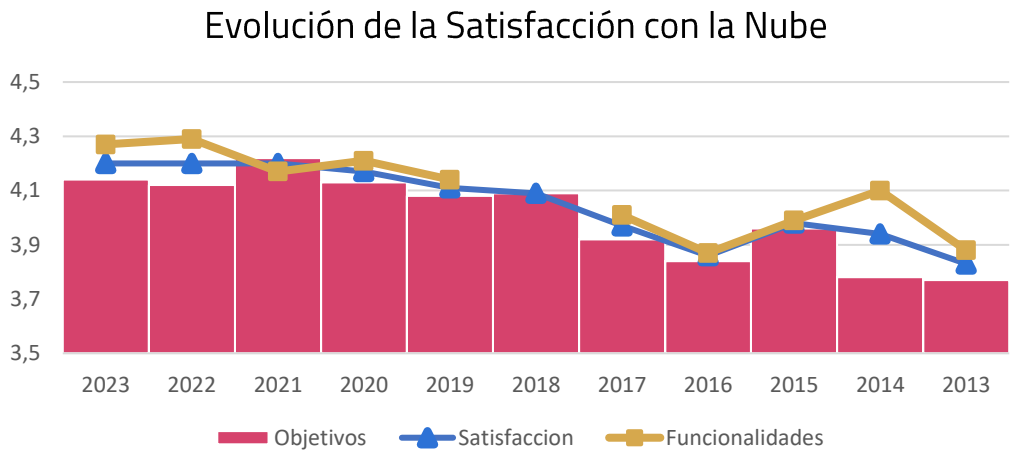


Ilustración 14.- Evolución del Grado de satisfacción según los criterios analizados en 2023

En este año 2023, permanece estable el nivel de satisfacción con los servicios en nube, observándose una ligera bajada en la satisfacción con la funcionalidad que es compensada con una subida equivalente en la satisfacción con los objetivos cumplidos. El nivel de satisfacción sigue siendo muy alto y se mantiene en máximos históricos.

El nivel de satisfacción con los servicios en la Nube permanece estable.

El análisis de la satisfacción por tamaño de empresa muestra una gran diferencia según nos fijemos en las empresas más pequeñas o en las más grandes. Todas las franjas de empresas sufren una ligera disminución en el grado de satisfacción, a excepción de las empresas pequeñas que muestran un gran aumento en el nivel de satisfacción poniéndose a la cabeza tanto en la satisfacción por objetivos como en los logros de funcionalidad. El estudio apunta a que las empresas pequeñas, que tienen menor capacidad de dotarse de recursos TI, se benefician del acceso a servicios de calidad gran empresa a costes más ajustados.

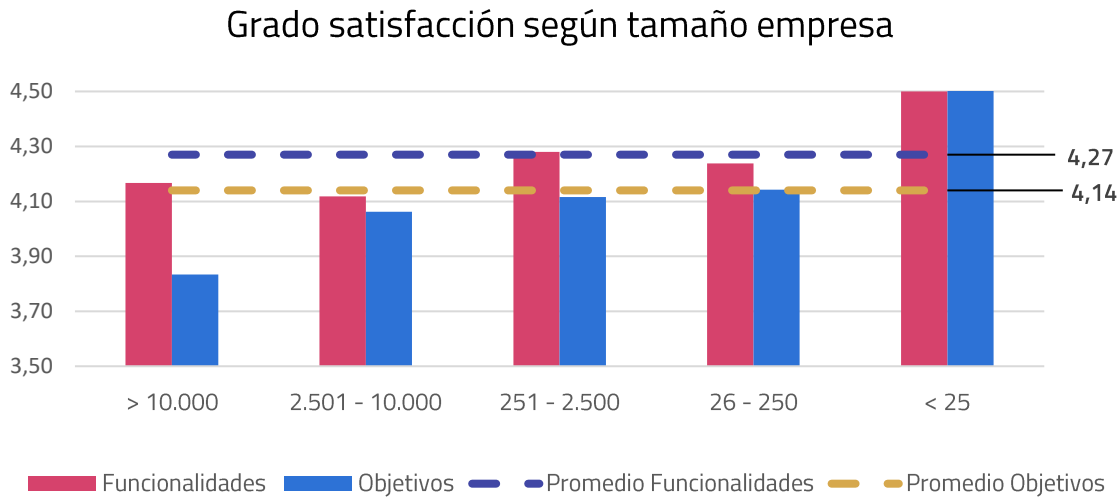


Ilustración 15.- Comparativa de satisfacción de los usuarios en función del tamaño de la empresa.

El grado de satisfacción con los servicios en la Nube disminuye a medida que aumenta el tamaño de la organización.

Por último, el estudio también analiza el grado de satisfacción con los servicios en la Nube según el país en el que se opera. Según las respuestas facilitadas en la encuesta de 2023, los usuarios muestran un grado de satisfacción diferente según el país. Las empresas con actividad en España, Norteamérica y resto de LATAM muestran una mayor diferencia entre la satisfacción por funcionalidad y la satisfacción por la ayuda a la hora de conseguir los objetivos de la empresa, siendo notablemente mayor la satisfacción por la funcionalidad proporcionada. Sin embargo, en empresas que operan en Perú, Argentina, Bolivia, y resto de Europa, el grado de satisfacción es similar en funcionalidad y en objetivos.

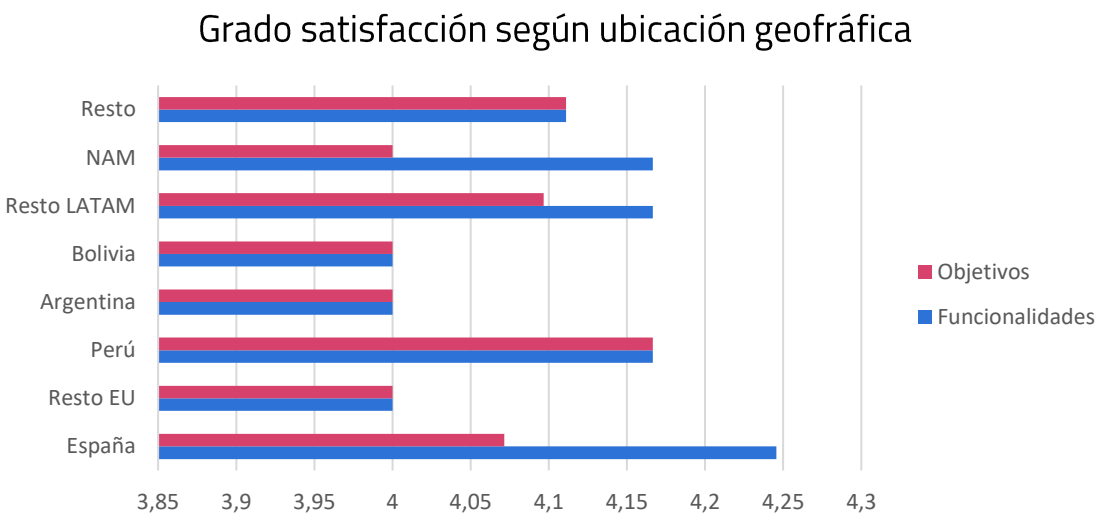


Ilustración 16.- Grado de satisfacción de los usuarios según la ubicación geográfica de la empresa.

Las empresas con actividad en España, Norteamérica y resto de LATAM muestran una mayor diferencia entre la satisfacción por funcionalidad y la satisfacción por la ayuda a la hora de conseguir los objetivos de la empresa.

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 tanto la serie temporal de cada uno de estos factores, como la comparación entre la evolución entre expectativas, requisitos y satisfacción.

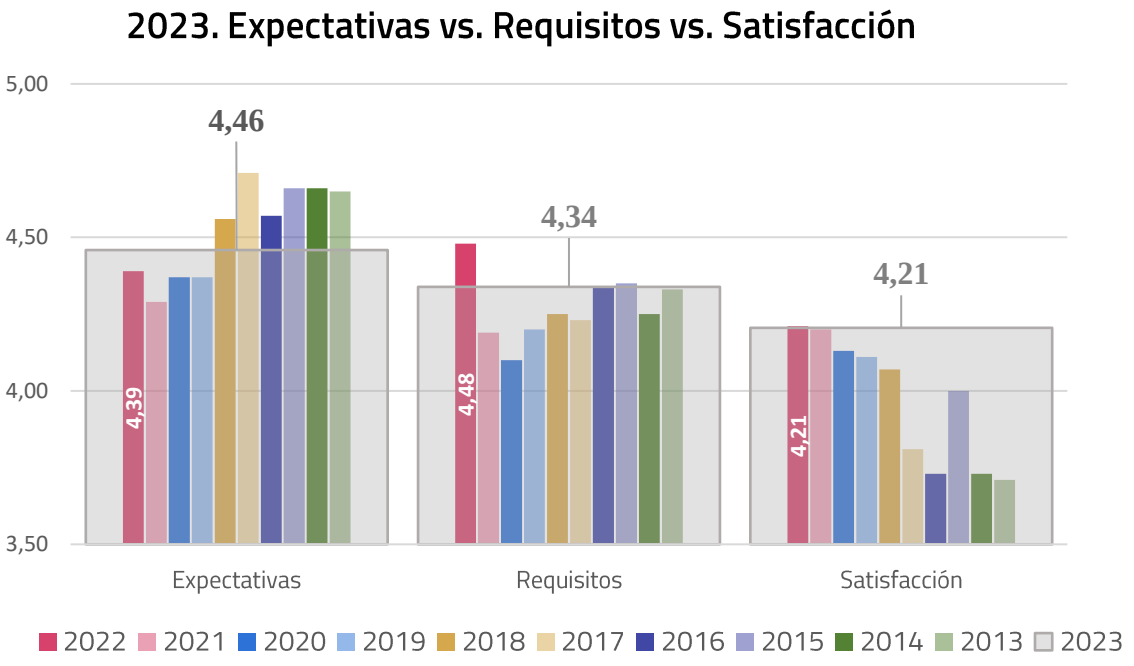


Ilustración 17.- Expectativas vs. Requisitos vs. Satisfacción en 2023

En esta undécima edición del estudio, se recupera la tendencia histórica detectada en ediciones anteriores, y se ensanchan las diferencias entre expectativas, requisitos y satisfacción que, en 2021, llegaron a ser prácticamente testimoniales.

La satisfacción con los servicios prestados sigue en máximos históricos, pero parece haber encontrado un techo en su progresión en valores de 4,20 sobre 5. Este techo a la progresión parece también constituir un suelo a su descenso, por lo que los usuarios siguen estando con una satisfacción más que alta con los servicios que reciben sin que lleguen a encontrar motivos para más satisfacciones.

La evolución de las expectativas sobre la Nube había experimentado un descenso continuado desde el inicio del estudio hasta que la tendencia se invirtió en 2022. Este cambio de tendencia se confirma, haciendo remontar estas expectativas a valores previos a la pandemia Covid19.

Por su parte, la exigencia de requisitos no mantiene el cambio de tendencia abrupto identificado en 2022, sino que retorna a valores más cercanos a los históricos y a máximos dentro de ellos. Quizás el cambio de tendencia fuera más abrupto en 2022 que en el caso de las expectativas, pero también se haya producido.

El análisis de esos datos en el entorno de mayor adopción de la Nube que se detecta en el estudio, con un número mayor de servicios en cada organización adoptados durante el Covid y mantenidos o ampliados a posteriori, debe contextualizarse con los hallazgos realizados sobre la tipología de servicios que se consumen en la Nube, con una fuerte presencia de servicios básicos de la organización, como el correo electrónico o el almacenamiento de datos, frente a una adopción menor de servicios que complementan a la organización pero que no están en el núcleo de sus procesos de negocio. La Nube ha llegado a los servicios TI que no pueden fallar, en los que una indisponibilidad o un incidente de seguridad sobre los datos ralentiza o paraliza la organización. No pueden fallar. Ello se traduce en la mayor exigencia de calidades de servicio sobresalientes en los mismos, que se derivan en una mayor expectativa y en requisitos más exigentes que deben ser satisfechos por la Nube.

La Nube está en el core de los Servicios TI de las empresas. Ya no pueden fallar, y por ello se tienen mayores Expectativas, y se demandan Requisitos más exigentes.

6. Visión sobre Shadow IT

Como punto inicial de este análisis, debe recordarse que la definición establecida de Shadow IT 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"[12]. Dado que estos servicios 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.

Este 11º Estudio presenta dos cambios de tendencia en la opinión sobre el Shadow IT respecto de la 10º Edición del mismo, del año 2022.

Por un lado, en la ilustración 8 se observa una disminución en el número de departamentos en las organizaciones que recurren a la práctica de Shadow IT, en comparación con los años anteriores. Esto sugiere que las organizaciones están tomando medidas más efectivas para controlar y prevenir esta práctica. Además, hubo un aumento en las organizaciones que centralizaban todos sus servicios en el Departamento de IT, lo que significa que estaban utilizando solo tecnología oficial y autorizada. Esto marca una tendencia positiva hacia la reducción de la incidencia de Shadow IT.

Sin embargo, a pesar de estos avances, Shadow IT sigue siendo un desafío en algunas organizaciones, con casos que ocurren ocasionalmente en algunos departamentos. Además, algunas organizaciones aún encuentran difícil detectar estas situaciones, lo que indica que la detección y prevención de Shadow IT sigue siendo un área que necesita mejorar. En general, aunque se están haciendo progresos, todavía hay trabajo por hacer para controlar completamente el fenómeno del Shadow IT.

[12] https://www.gartner.com/en/information-technology/glossary/shadow

Las organizaciones reconocen con claridad en 2023 la necesidad de supervisión de IT, y cambia la tendencia detectada en 2022.

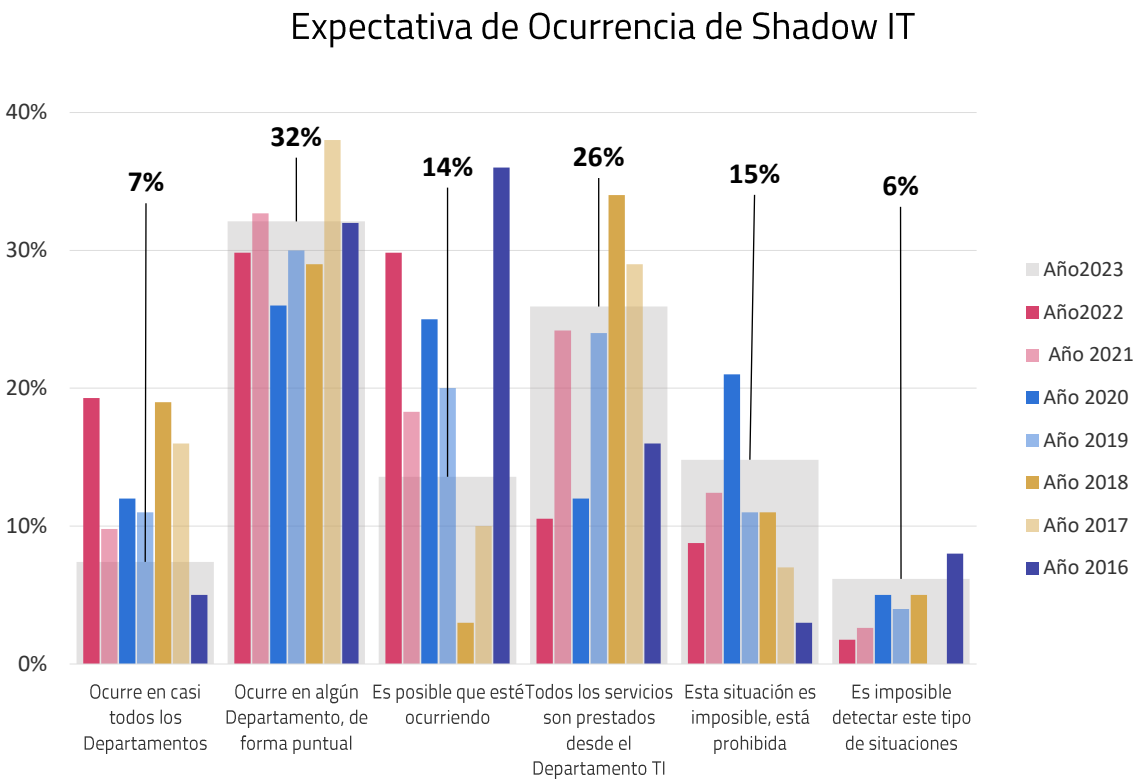


Ilustración 18.- Presencia estimada de Shadow IT en las organizaciones

El segundo cambio de tendencia se puede detectar en la 18 y se refiere a la percepción sobre el Shadow IT. En esta edición, se observa de nuevo una cantidad significativa de organizaciones que percibe la existencia de Shadow IT de manera negativa, manteniendo una postura que ha sido constante en los últimos años, excepto en 2022.

Por otro lado, el aumento de la visión negativa sobre ShadowIT se produce a costa de una disminución notable en comparación con años anteriores en el número de organizaciones que tienen una visión neutral o basada en los resultados de la aplicación de ShadowIT. Esto sugiere que las organizaciones están adoptando una postura más definida sobre la materia, ya sea positiva o negativa.

Finalmente, muy pocas organizaciones ven el Shadow IT de manera positiva, una tendencia que ha disminuido significativamente desde 2020, y que tiende a ser ya muy residual. Esto sugiere que la mayoría de las organizaciones no aprueba la práctica de la Shadow IT, independientemente de los posibles beneficios que pueda ofrecer.

Todo ello induce a pensar en que las tendencias observadas en los estudios anteriores son correctas y que las conclusiones del 10º Estudio corresponden a una ruptura temporal y circunstancial de la misma.

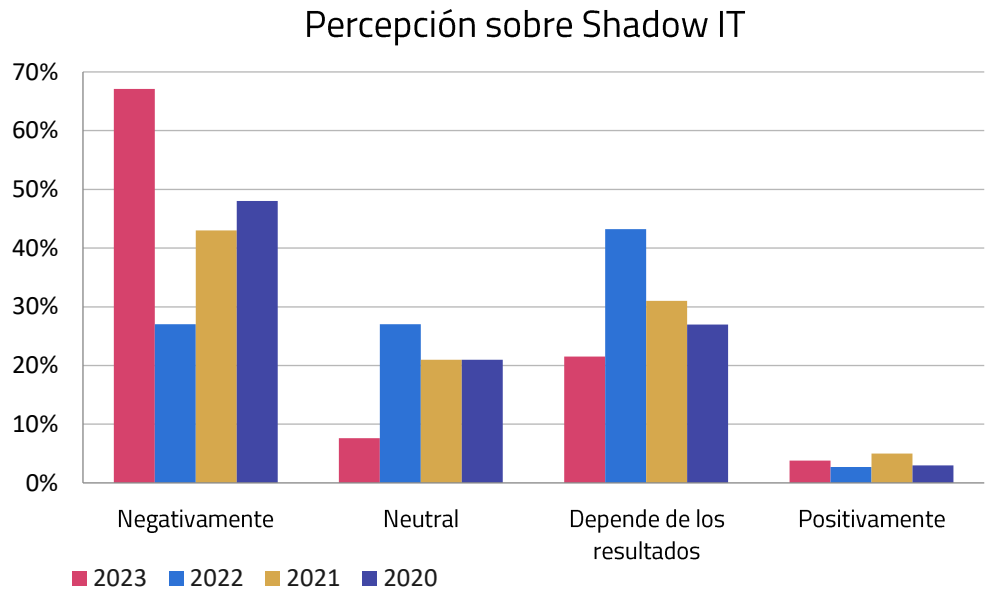


Ilustración 19.- Evolución histórica de la percepción de las organizaciones sobre ShadowIT

Este Estudio quiso recopilar información adicional sobre la visión de las organizaciones sobre ShadowIT para analizar las causas y motivos de la visión más positiva identificada en 2022.

Para ello, consultó a los participantes si sus organizaciones habían identificado CSPs de confianza, de forma que la contratación de servicios estuviera preautorizada a toda la organización.

El resultado obtenido, que se muestra en la ilustración 20, es perfectamente consistente con los datos anteriores, con casi tres cuartas partes de las organizaciones no contemplando esta preautorización, mientras que sólo el 13% de participantes sí que disponen de esa lista.

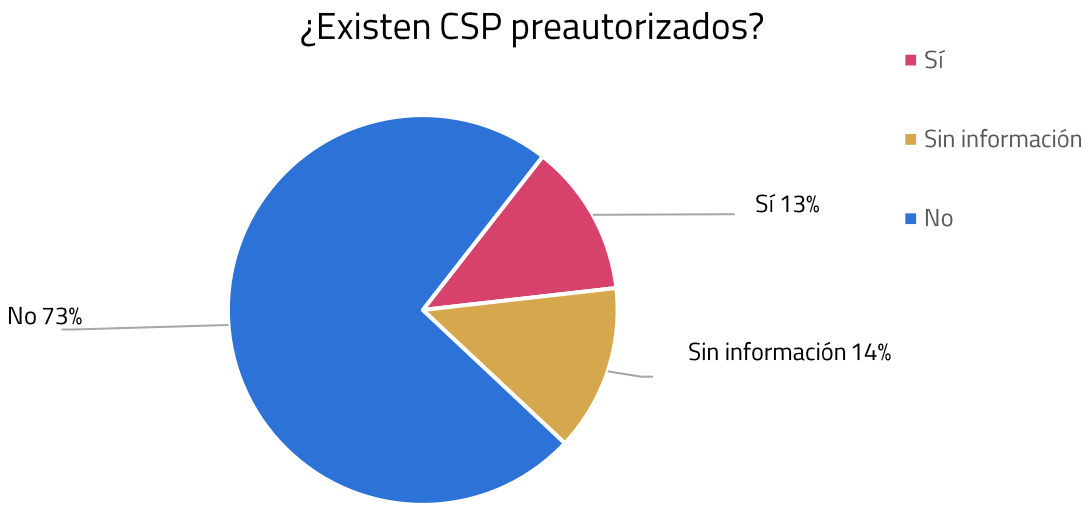


Ilustración 20.- Evolución histórica de la percepción de las organizaciones sobre ShadowIT

La percepción hacia el Shadow IT en 2023 es claramente negativa frente a la visión más tibia en 2022. La visión positiva es residual.

Como complemento del análisis de expectativas de ocurrencia de Shadow IT de la

Ilustración 8, la Ilustración profundiza en esta expectativa desde el punto de vista del tamaño de la organización, mostrando diferencias claras entre las distintas empresas.

Puede detectarse que las empresas de mayor tamaño, que tienen una mayor superficie de exposición y una mayor posibilidad de que una persona o departamento individual se decida por el Shadow IT, por lo que mezclan una apuesta decidida por que su área de TI proporcione todos los servicios, junto con un convencimiento de que hay elementos que no se pueden detectar y el convencimiento de que hay algún área que no está perfectamente controlada.

Por el contrario, las empresas pequeñas tienen la situación mejor controlada, aunque es mayoritaria la opinión de que es posible que haya situaciones de este tipo.

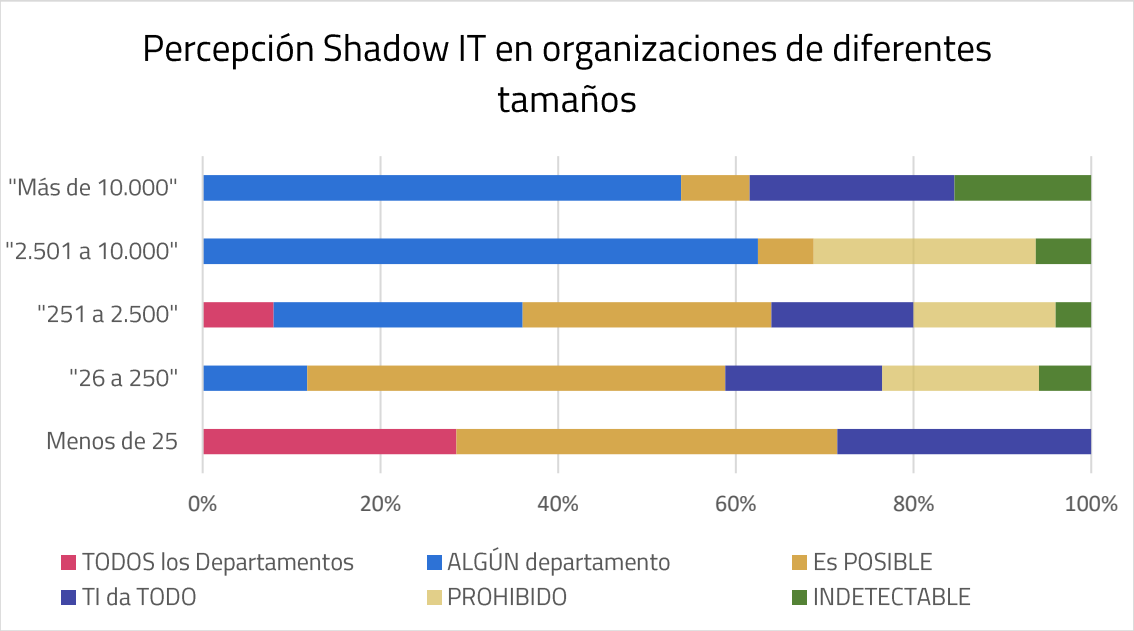


Ilustración 21.- Percepción de las organizaciones sobre ShadowIT en función de su tamaño

Se percibe una mayor presencia de Shadow IT en las organizaciones más grandes, mientras que las PYMES tienen un mayor control.

7. Estado de Concienciación en Seguridad de los Usuarios

En este año 2023 se mantiene la dinámica de estudios anteriores que permite establecer y poner en valor una perspectiva histórica que habilita la proposición de conclusiones en base a la comparativa de los resultados obtenidos en diferentes años. Por tanto, se ha vuelto a realizar el análisis de la concienciación sobre los riesgos de seguridad de los servicios recibidos desde la Nube en base a tres grandes grupos:

- Resultados acumulados para todos los participantes.
- Resultados específicos de los empleados con puestos directivos.
- Resultados específicos de empleados no directivos de su organización.

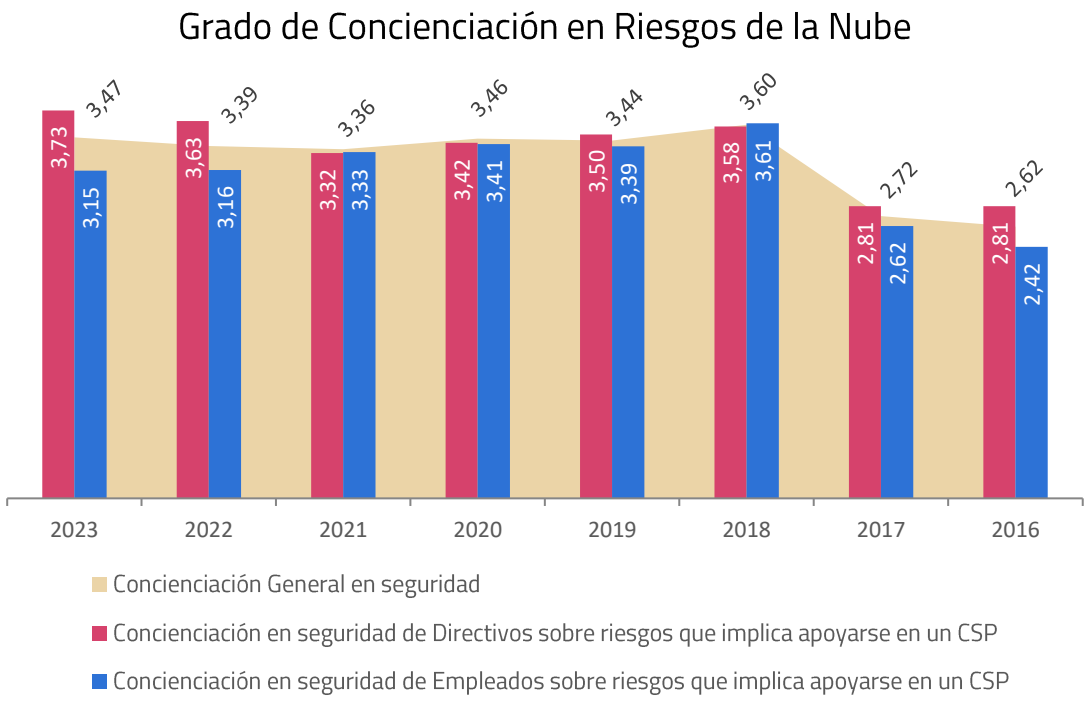


Ilustración 22.- Evolución histórica de concienciación en Seguridad de usuarios de la Nube

Los resultados son muy similares a los del año 2022, por lo que cabe concluir que la tendencia no solo se mantiene, sino que se consolida.
Esta consolidación tiene una vertiente negativa y que pone de manifiesto una divergencia que podría haberse esperado que hubiera mejorado respecto al 2022. En concreto, se trata de la diferencia entre el grado de concienciación de directivos y de empleados.

Si bien podría haberse esperado una reducción de la divergencia, o que si se mantenía hubiera un mayor grado de concienciación en ambas categorías de personal, lo cierto es que su mantenimiento permite reiterar la oportunidad de actividades de concienciación "top-down" que reduzcan esta divergencia antes de que sea mayor, de modo que genere también una mejor concienciación general a todos los niveles.
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.

Por otro lado, la vertiente positiva de los resultados de 2023 es que también puede entenderse la consolidación indicada como un factor que pone de manifiesto la naturalización de los servicios en la Nube, y la disminución de las reticencias internas. Mantener la tensión de las actividades de concienciación sobre riesgos en la Nube, además de que no provoca miedo o rechazo a los servicios que se proveen de tal manera, sigue siendo necesaria para la creciente familiaridad con los mismos.

El diferente grado de concienciación entre directivos y empleados es un factor a superar, para evitar que se convierta en un riesgo en sí mismo.

El análisis de otros elementos consultados a los participantes en el Estudio mantiene las buenas sensaciones respecto en otros indicadores sobre concienciación en Seguridad en la Nube de las organizaciones.

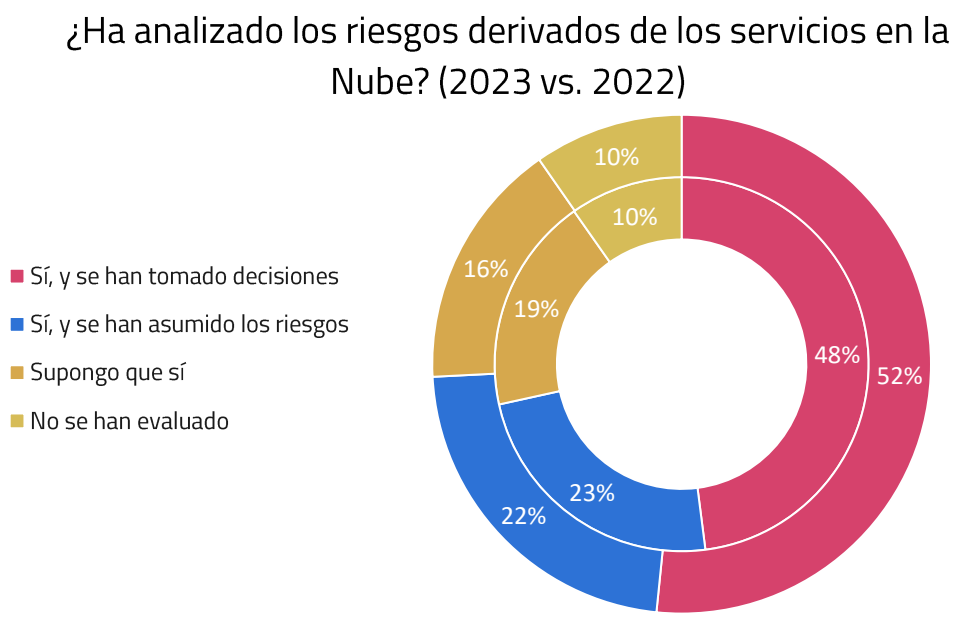


Ilustración 23.- Realización de Análisis de Riesgo previo al uso de servicios en la Nube

En este sentido, aumenta, siquiera levemente, el porcentaje de organizaciones que han realizado un análisis de riesgos previo al uso de estos servicios, lo cual también puede entenderse como una señal de la importancia que dan las Organizaciones a la identificación, valoración y gestión de los riesgos de la migración a la Nube. Y esto frente a ciertas carencias de los procesos de migración en cuanto a riesgos de Seguridad, derivadas en muchas ocasiones de la supuesta facilidad y velocidad de tales procesos.

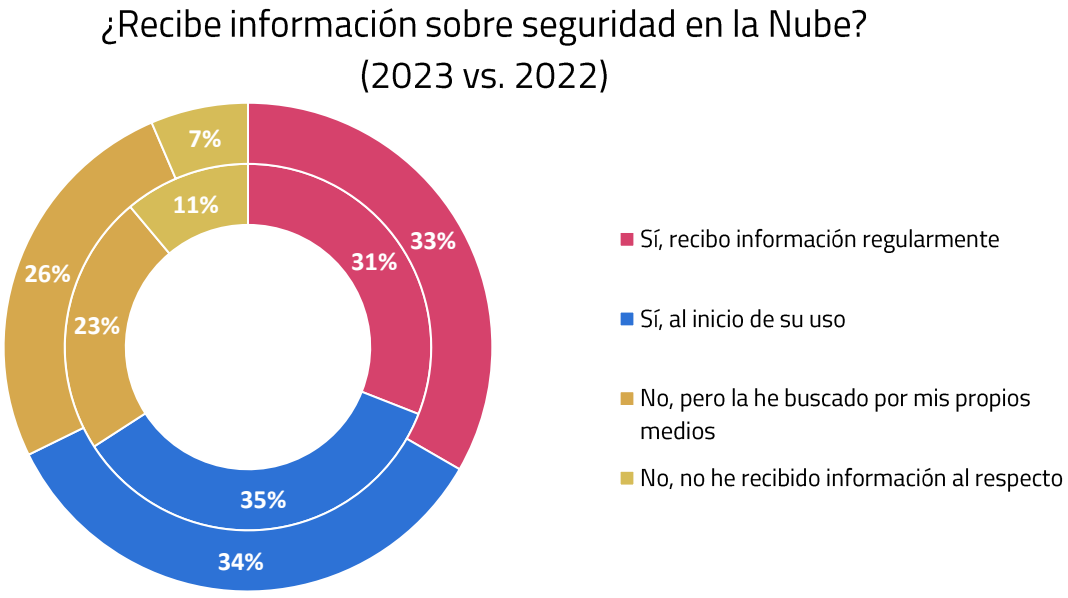


Ilustración 24.- Formación y concienciación a las personas sobre el uso de servicios en la Nube

También hay una evolución similar, pequeña pero significativa, en las actividades e iniciativas de las Organizaciones dirigidas a informar a sus empleados sobre el cambio de paradigma que suponen los servicios de la Nube y sobre los nuevos riesgos que lleva asociados. Implicar a todos los miembros de la Organización en los pasos a dar y los resultados esperados del proceso de migración, conlleva informarles también de los riesgos y hacerles parte de las medidas de mitigación de los mismos.

Cabe añadir que sigue siendo relevante y significativo el número de Organizaciones que no hace análisis de riesgos ni forma a sus empleados. Hay un espacio de mejora que debe ser recorrido 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.

La mejora en los indicadores sobre gestión del proceso de adopción de Servicios en la Nube no debe ser obstáculo para apreciar los espacios de mejora que todavía existen.

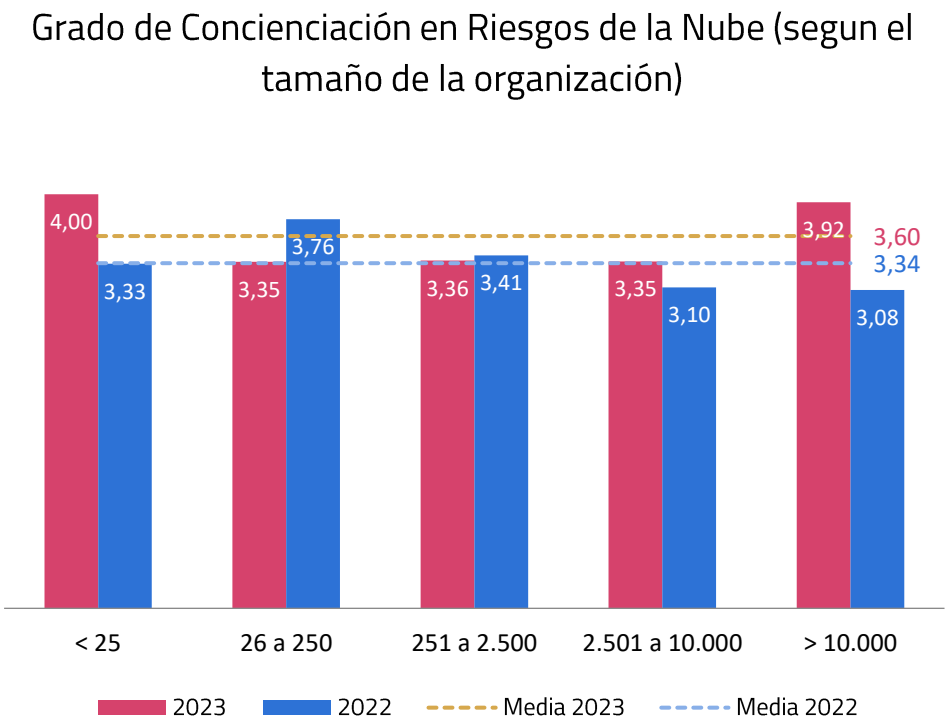
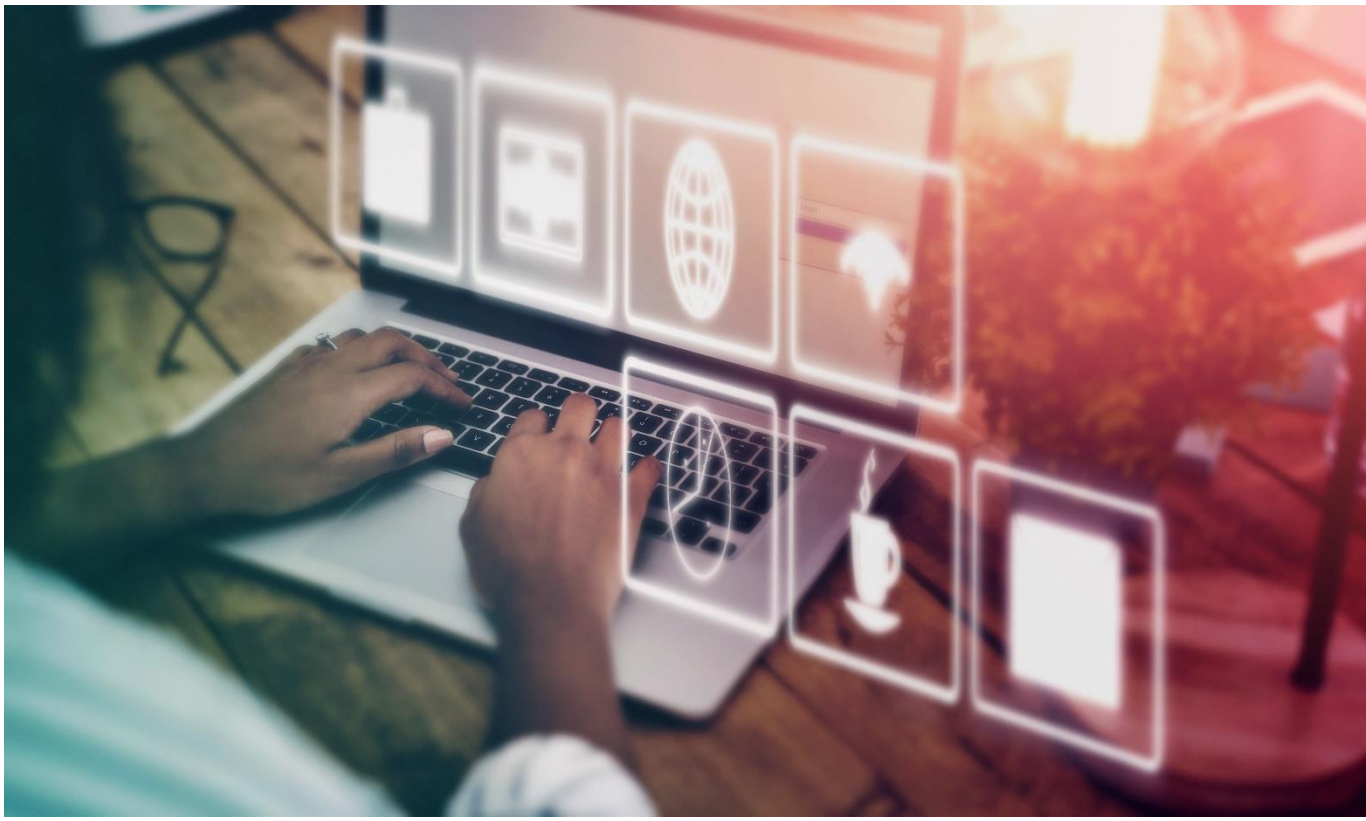


Ilustración 25.- Grado de concienciación en Riesgos de la Nube según tamaño de la organización

Por último, el análisis de la concienciación media en seguridad en las organizaciones en función de su tamaño apunta a un cierto cambio de tendencia en las Organizaciones de mayor tamaño, que parecen haber elevado su nivel de concienciación. Esto no supone que las medianas o pequeñas empresas se hayan descolgado del resto, sino que antes bien también las más pequeñas mejoran sus niveles de concienciación, quizá impulsadas por esa mayor implicación de las grandes empresas.

Las organizaciones de mayor tamaño han "pisado el acelerador" respecto al nivel de concienciación en Seguridad en la Nube, lo cual supone un impulso indirecto al conjunto de organizaciones.



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. Este 11º Estudio contemplará por primera vez, y como factor adicional a los factores contemplados históricamente, la influencia que tiene en esta evolución el porcentaje de servicios que la organización está apoyando 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 va a realizar tomando cada uno de estos factores por separado, para luego realizar un análisis conjunto del mismo.

Respecto del número de incidentes, el análisis de la Ilustración 26 refleja una pequeña variación que puede implicar un cambio de tendencia respecto a años anteriores. Así, el análisis de los datos proporcionados por las organizaciones rompe el equilibrio histórico entre las organizaciones que seguían con el mismo número de incidentes y las que experimentaban una reducción en el volumen de incidentes. La ruptura se produce a favor de las organizaciones que mantienen el número de incidentes después de migrar a la nube. No obstante, estas dos opciones siguen siendo el escenario mayoritario que refleja la opinión de más del 80% de los participantes. La opción de desaparición de los incidentes pierde parte de su apoyo, mientras que se mantiene el número de organizaciones que han tenido un aumento en las mismas.

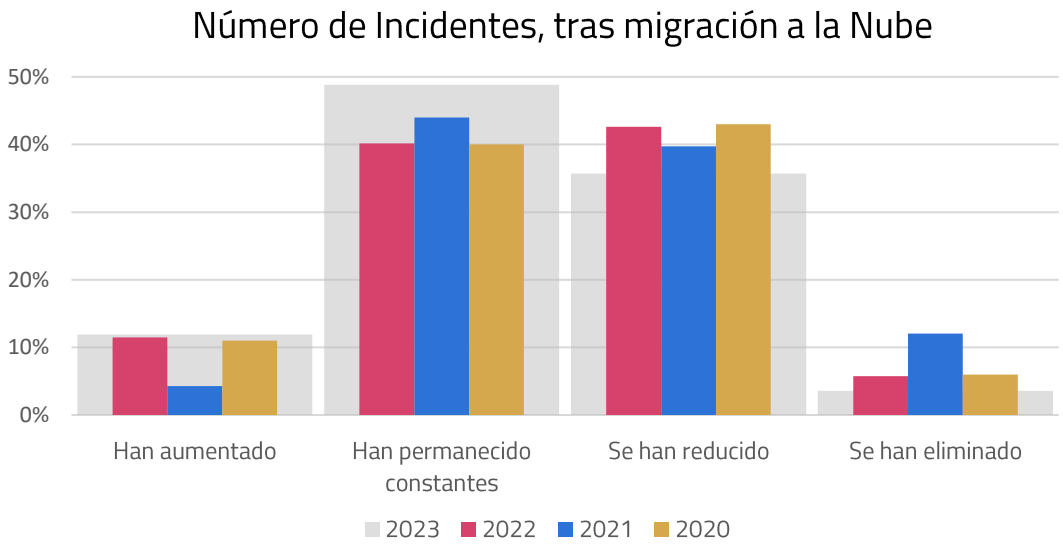


Ilustración 26.- Evolución en 2023 del Número de Incidentes en servicios en la Nube.

Por su parte, la Ilustración 27 analiza este parámetro en función del porcentaje de servicios apoyados en la Nube. Se puede verificar que cada una de las situaciones de evolución de los incidentes es claramente mayoritaria sin que pueda establecerse un patrón común para todas ellas. Así, las entidades que utilizan servicios puntuales o menos de un 50% de los servicios en la Nube siguen el perfil de uso general establecido anteriormente. Por otra parte, las entidades que más declaran un aumento de las incidencias utilizan entre un 50% y 90% de servicios en la Nube, mientras que las que declaran que se han eliminado los incidentes usan el 100% de sus servicios en la Nube. Estas divergencias son menos relevantes de lo que pudiera parecer porque en ambos casos hay más entidades con este porcentaje de uso de servicios que se posicionan en las respuestas más frecuentes, por lo que el Estudio achaca esta diferencia a un efecto estadístico propio de un menor número de respuestas obtenidas en cada una de las opciones. Efecto estadístico que será monitorizado en futuras ediciones del estudio.

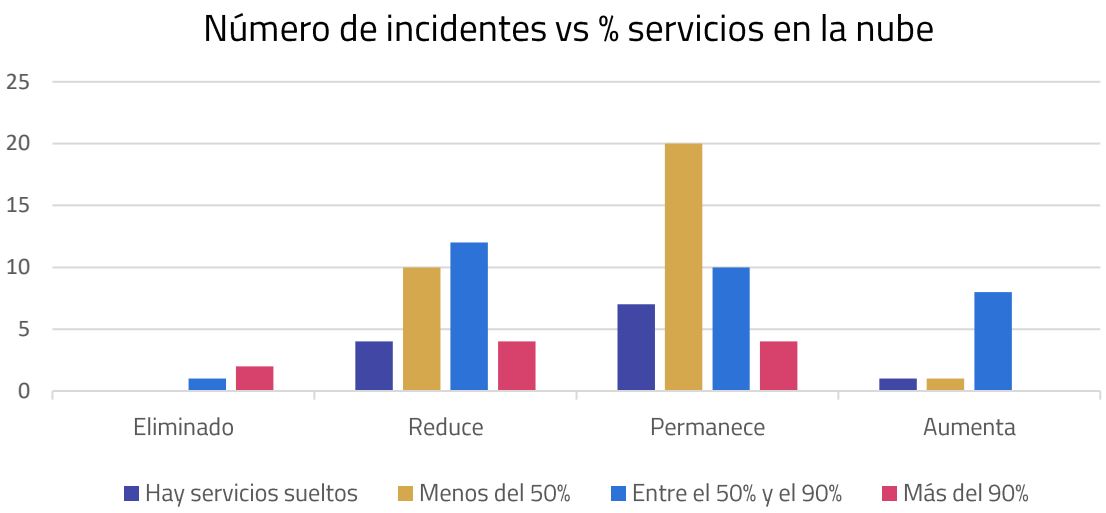


Ilustración 27.- Número de incidentes vs porcentaje de servicios en Nube

Se mantiene la tendencia de mantenimiento o reducción del número de incidentes en los servicios en la nube, con más entidades que mantienen el número de incidentes

Respecto de la criticidad de los incidentes, este 11º Estudio detecta la continuidad de las tendencias y escenarios detectados en ediciones anteriores. Así, el cambio a servicios en la nube no supone un cambio en la criticidad de los incidentes sigue siendo mayoritariamente igual a los escenarios OnPremise, con una ligera tendencia de las empresas a favor de la reducción en la criticidad de los incidentes.

El Estudio también ha realizado una reflexión sobre los actuales escenarios de amenazas y como la evolución de los mismos 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 están apoyándose para la realización de sus actividades en servicios legítimos en la Nube, de forma que los propios CSP pudieran llegar a ser considerados fuentes de ataque, o a que los mecanismos de defensa y la efectividad de los ataques de CSP a CSP o en el mismo CSP sean distintos.

En todo caso, esta edición del Estudio no dispone de información suficiente en este campo, por lo que este punto queda pendiente de estudio para futuras ediciones.

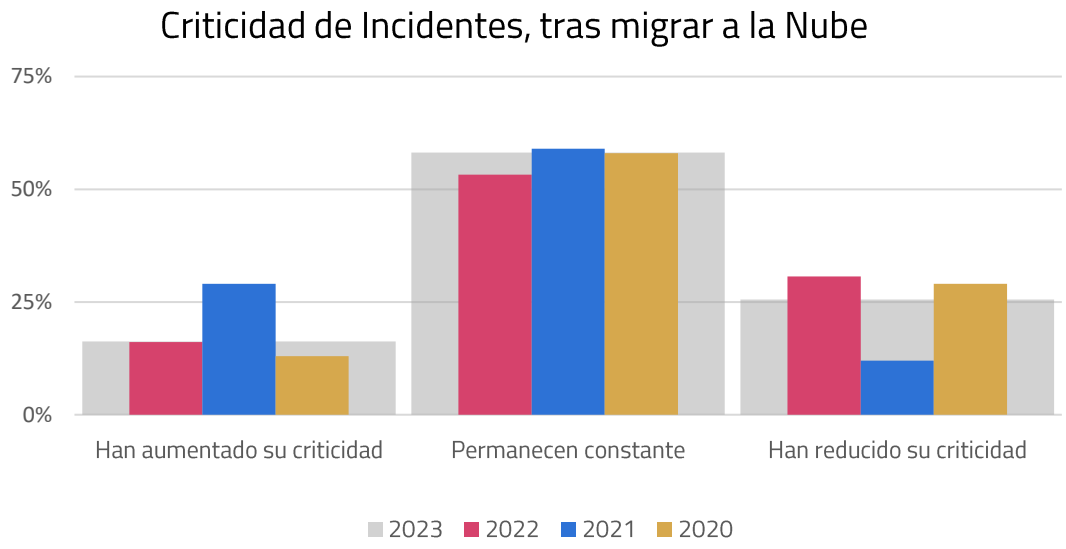


Ilustración 28.- Evolución en 2023 de la Criticidad de Incidentes en servicios en la Nube.

Las organizaciones han mejorado su capacidad de detección de incidentes cuando sus servicios están en la Nube.

Por su parte, la capacidad de detección de incidentes de servicios tras migrar a la Nube sigue ofreciendo una visión esperanzadora, con el predominio de las organizaciones que han igualado o mejorado su capacidad de detección de incidentes de seguridad a través de los servicios y capacidades en la Nube, o por las capacidades propias del servicio en la Nube. En esta edición, se repite el escenario de 2020 y son mayoría las organizaciones que han declarado una mejora en su capacidad de detección frente a las que simplemente mantienen la capacidad de detección previa. Esta situación refrenda el mensaje positivo que se venía observando en el análisis de los demás parámetros de gestión y respuesta a incidentes.

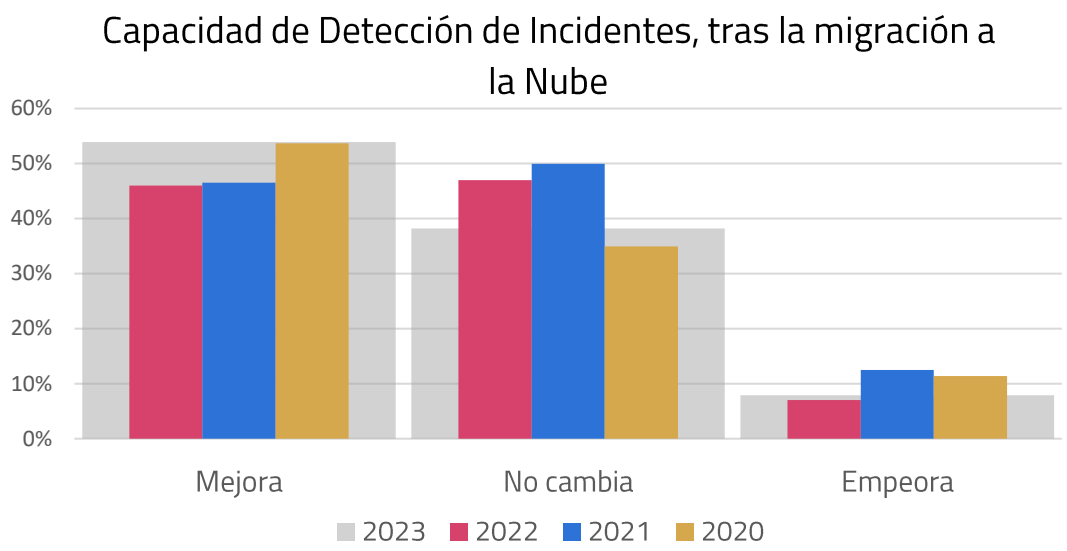


Ilustración 29.- Evolución en 2023 de la Capacidad de Detección de Incidentes en servicios en la Nube.

Este análisis deja algunas preguntas de gran interés pendientes de respuesta. ¿El origen de esta capacidad de mejora se origina en las capacidades nativas de detección de los propios servicios en la Nube? ¿se origina en la facilidad de uso de soluciones SIEMaaS o SOARaaS combinadas con la adopción de servicios en la Nube? ¿hasta qué punto los servicios en la Nube se integran correctamente en las plataformas de gestión de incidentes de sus usuarios?

En cualquier caso, como podemos observar, se produce una relación positiva en cuanto a la capacidad de detección con el aumento de servicios en Nube en el mismo porcentaje: Son las organizaciones que tienen más de un 50% de sus servicios en la Nube las que experimentan estas mejoras.

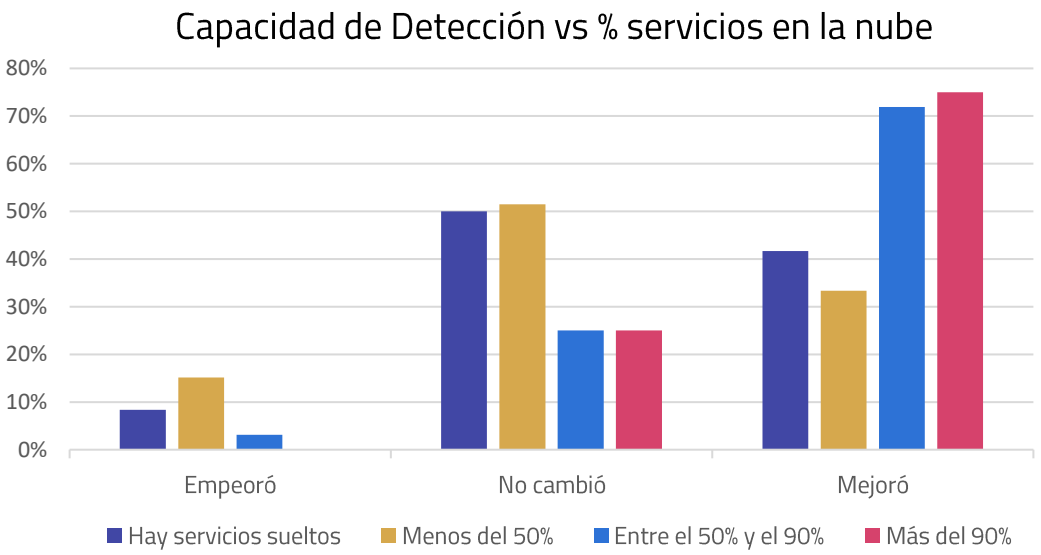


Ilustración 30.- Capacidad de detección Vs Porcentaje de servicios en la nube.

Respecto al volumen de recursos que los usuarios deben dedicar para la gestión de los incidentes, el Estudio detecta una cierta degradación en el rendimiento de este proceso, tendencia que frena la observada en años anteriores donde se apreciaba una situación que partía de un ahorro de costes inicial, pero que sin embargo había empeorado.

Cabe en todo caso valorar si esta estabilización en los costes se debe a una mejora en las capacidades de respuesta a incidentes que detecta más incidentes y demanda de mayores recursos, o si existen otras causas basadas en la estabilización del número y criticidad de los mismos.

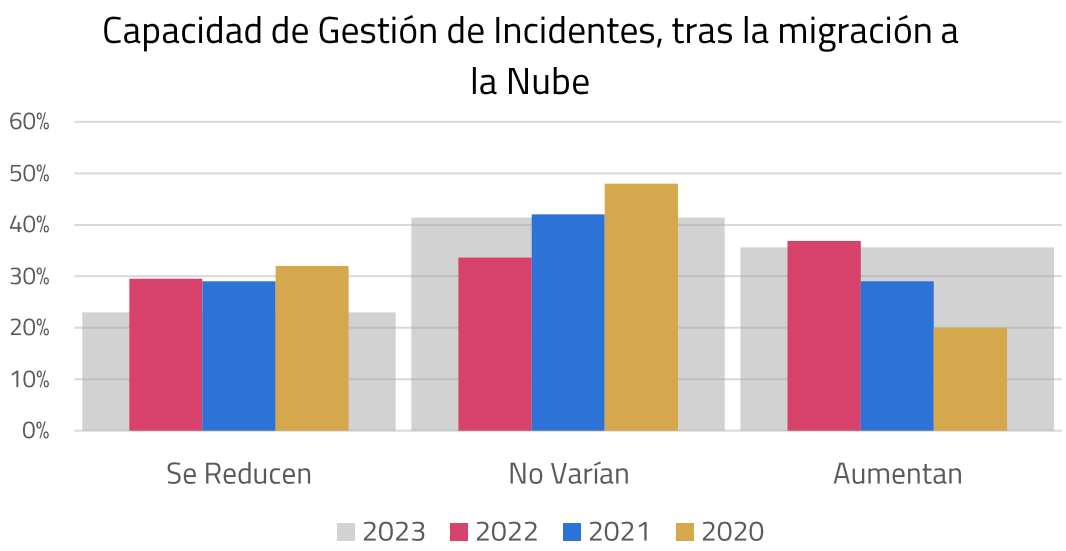


Ilustración 31.- Evolución en 2023 del Coste en la Gestión de Incidentes en servicios en la Nube.

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 los mismos.

En este caso, la situación ha mejorado: casi ha desaparecido el número de usuarios que indican que su CSP no ofrece este tipo de servicios, y se incrementa en paralelo el número de usuarios que contratan estos servicios, sin embargo, ya no se observa incremento significativo entre los CSP que los ofrecen sin coste frente a los que son de pago, siendo la opción predominante. En todo caso, y al tratar esta pregunta con capacidades y servicios ofrecidos por el CSP y sujeto a la evolución de su portfolio de servicios, aún no puede establecerse una tendencia clara en el mercado de los CSP que elimine esta dependencia o la dependencia de los CSP concretos en los que sea apoyan los participantes en el Estudio.

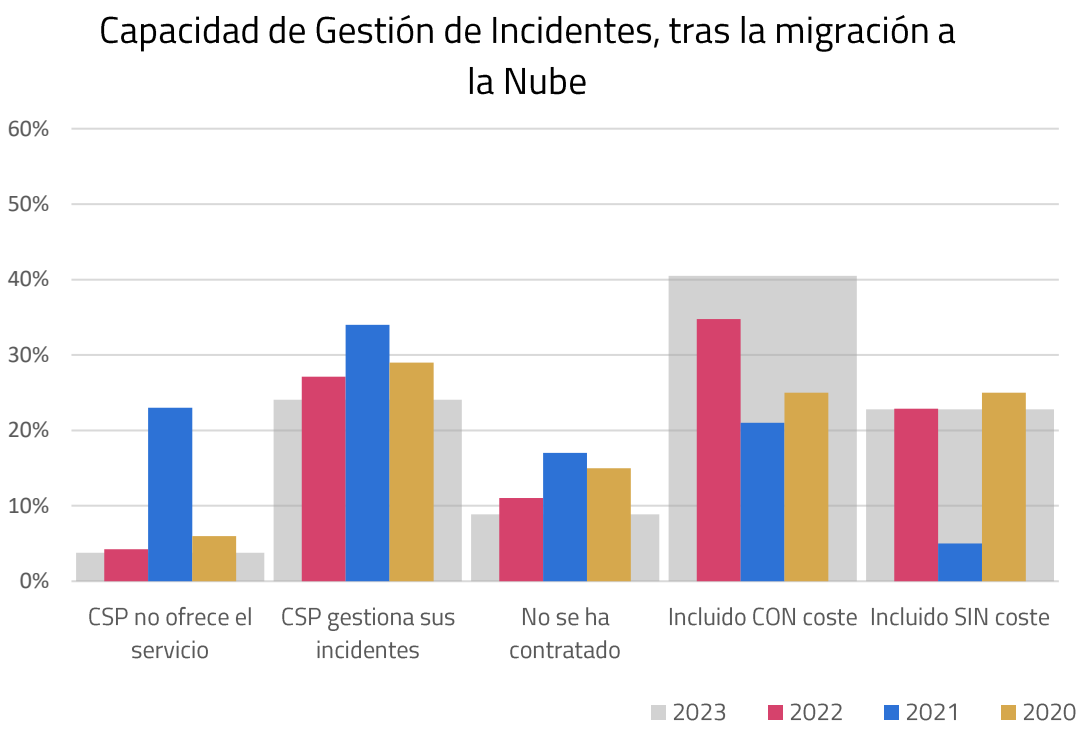


Ilustración 32.- Evolución en 2023 del Apoyo a los usuarios por el CSP en Incidentes en servicios en la Nube.

La gestión de incidentes en la Nube sigue siendo más eficiente que en servicios OnPremise, si bien esta mejora de eficiencia no es tan diferencial como en 2020 y 2021.

9. Análisis de Participantes en el Estudio y sus particularidades

9.1. Caracterización de usuarios no técnicos

La 8ª Edición del Estudio permitió en 2020 identificar y caracterizar el incremento en el uso de soluciones en la Nube por parte de los denominados usuarios no técnicos. Es decir, usuarios que utilizan servicios en la Nube porque les resultan sencillos de contratar, se ajustan a sus necesidades, pero que no 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 profunda, 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.

Entre estos elementos, los profesionales independientes se comportan igual que el resto de las organizaciones respecto del número de CSPs contratados, como se ve en la Ilustración , donde se ve que estas entidades contratan servicios en la media de organizaciones de otros tamaños, sin que haya diferencias reseñables.

También se han detectado actividades en las que estas organizaciones presentan diferencias significativas frente al resto de organizaciones:

- La Ilustración 3 muestra un perfil de uso de CSPs muy distintos, con una amplia proporción de servicios sobre Google Cloud en lugar de Azure o Amazon o SaaS, como para el resto de las organizaciones participantes en el Estudio.
- La Ilustración 6 muestra a estas empresas como las máximas consumidoras de servicios de correo electrónico, estando el resto de servicio en línea con el consumo de resto de servicios.
- La Ilustración señala que las PyMES utilizan la mayor parte de los servicios TI sobre Nube. Es decir, no disponen de infraestructura propia y apoyan la mayoría de sus servicios (de correo y otros) en servicios en la Nube.
- La **¡Error! No se encuentra el origen de la referencia.** muestra que el grado de c oncienciación es más elevado en PyMES que en empresas de tamaño mediano, y a la altura de las empresas de mayor tamaño.

Además, el estudio analiza las diferencias más significativas entre las necesidades y expectativas, requisitos y satisfacción entre los profesionales independientes y el resto de las empresas.

En materia de satisfacción, los profesionales independientes están razonablemente alineados con los niveles de satisfacción generales de las organizaciones, por lo que no se muestra el análisis gráfico de estos datos.

Las diferencias son más ostensibles en las expectativas en los profesionales independientes, que tienen mayor expectativa en todas las dimensiones consideradas (ver Ilustración). La exigencia llaga incluso a ser el máximo posible, con todos los usuarios teniendo una expectativa muy alta en disponibilidad.

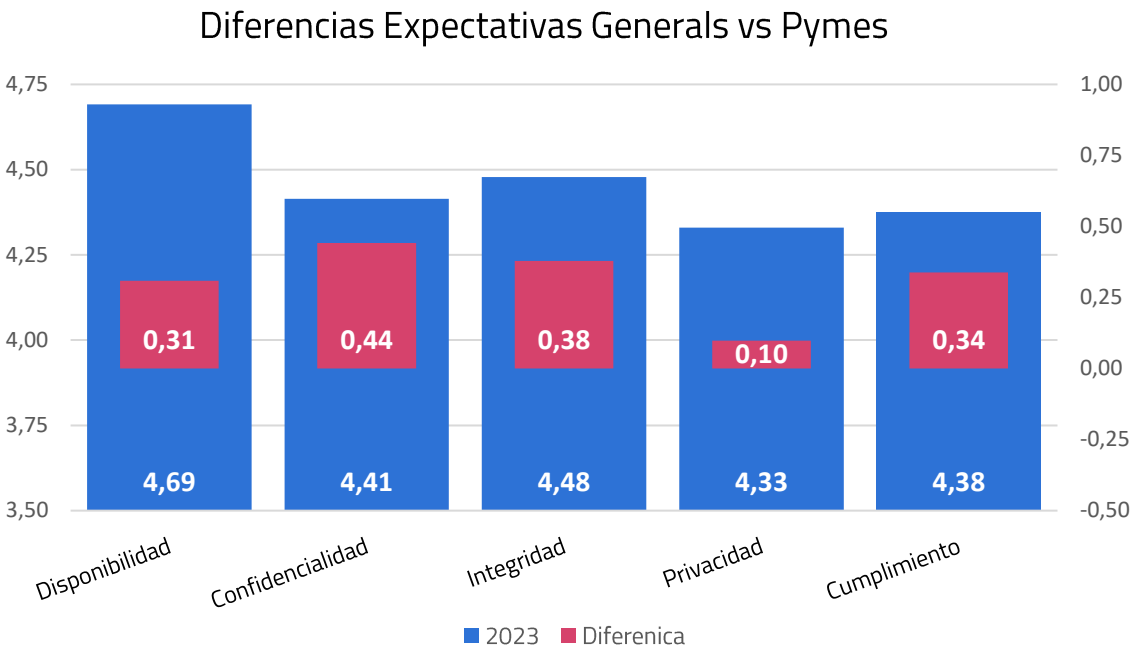


Ilustración 33.- Diferencias en Expectativas de los profesionales independientes frente al total de participantes.

Respecto de los requisitos exigidos por los profesionales independientes que se pueden ver en el Ilustración, de nuevo resultan ser superiores a la media de los participantes en todos los casos menos en dos: controles de seguridad y existencia de ANS. Estos dos casos se explican en combinación con el aumento de los requisitos de certificación y de acceso a los logs. El profesional independiente no tiene recursos suficientes en cantidad o en calidad para hacer verificaciones en profundidad de las condiciones de servicio que ofrecen los CSP, por lo que las demandan con menos intensidad, y en su lugar, recurren a la obtención de certificaciones de seguridad que suplan esas carencias y generen el entorno de confianza adecuado. Y demandan también el acceso a logs que pudieran utilizar en caso necesario como fuente de información alternativa.

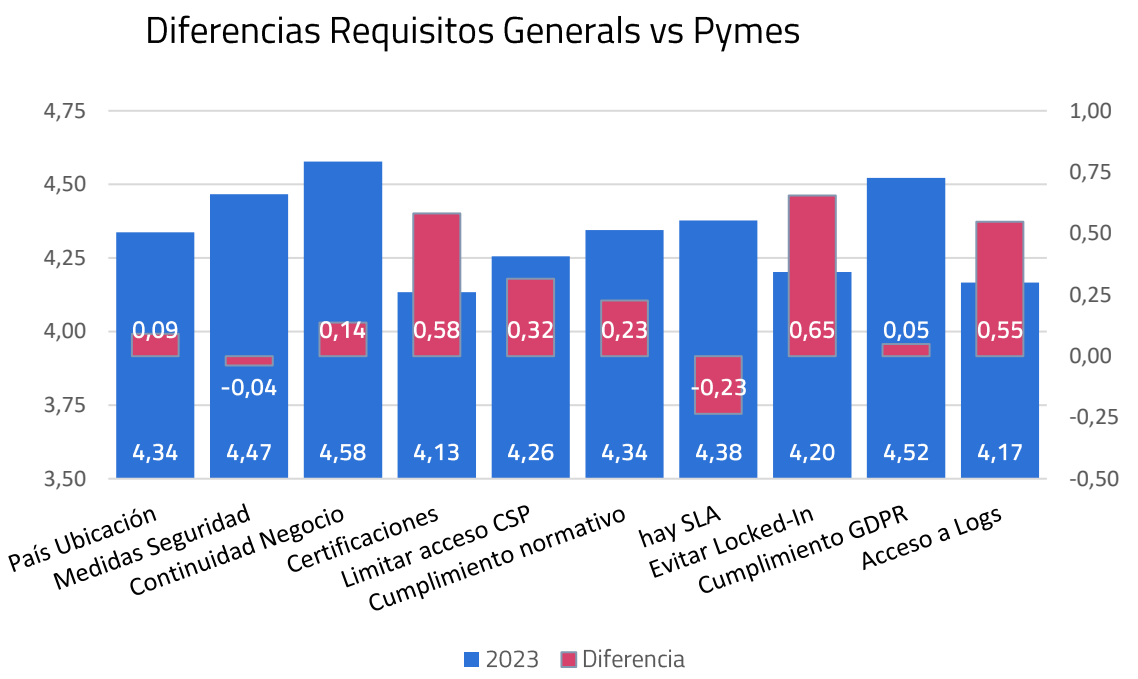


Ilustración 34.- Diferencias en Requisitos de los profesionales independientes frente al total de participantes

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

10. Ficha Técnica del Estudio

El análisis y diseño del Estudio ha sido realizado por los profesionales que figuran en la portada del documento, que forman parte de los Capítulos Español y Peruano de CSA y de los Capítulos de Madrid y Lisboa de ISACA, en colaboración con ISMS Forum.

El Estudio se ha realizado en base a encuestas recopiladas entre el 21 de septiembre y el 4 de octubre de 2023, a través de la plataforma online SurveyMonkey. Se recopilaron un total de 125 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.

El 11º Estudio está abierto a todas las organizaciones, independientemente de su ubicación geográfica, tamaño, madurez tecnológica, estrategia de adopción de la Nube y/o sector. Por ello, se ofrecen estadísticas respecto de la distribución de los participantes en la encuesta, incluyendo el tamaño de las empresas participantes, las áreas de actividad en la que operan y la huella geográfica de los participantes en la encuesta, en cuyos datos se ha basado el análisis realizado en este Estudio.

Los participantes en la encuesta presentan una distribución suficiente de la muestra, en la que no se identifica una tipología predominante que pudiera introducir sesgos geográficos, de tamaño o de sector relevantes.

En este último punto, el sector de telecomunicaciones y tecnología tiene una representación que al menos duplica la de cualquier otro sector y que representa al 25% de participantes. El reparto geográfico de las respuestas también indica una concentración de las respuestas en empresas españolas, sin que de nuevo esta circunstancia signifique un sesgo relevante en la muestra de los datos.

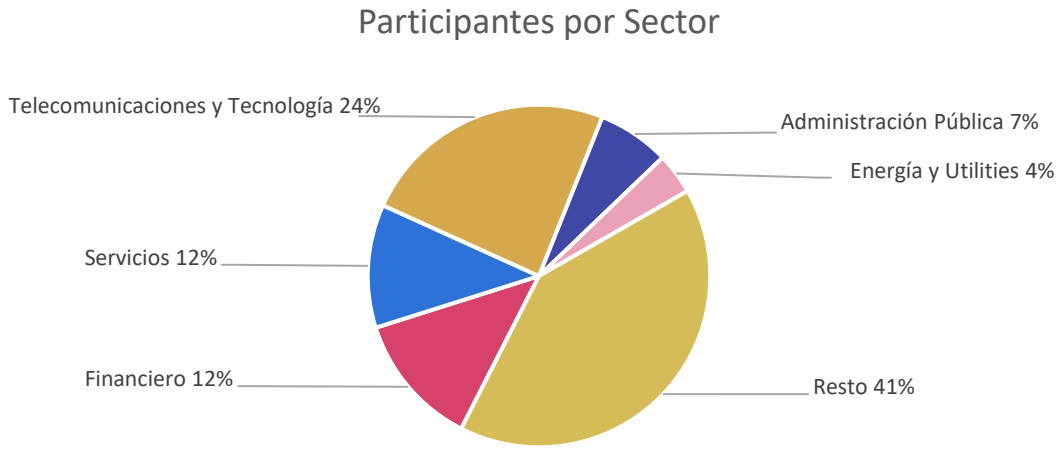


Ilustración35.- Distribución de los participantes en la encuesta por sector económico de actividad

Ilustración 36.- Distribución de los participantes en la encuesta por nivel de responsabilidad en sus organizaciones

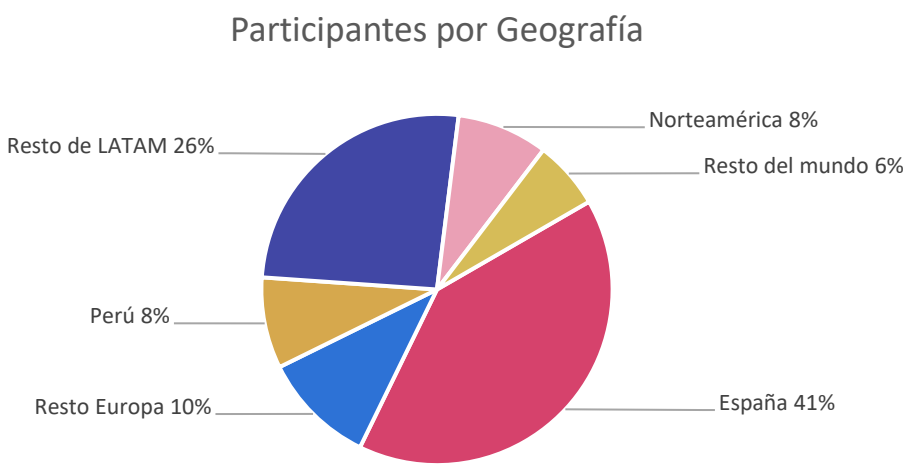


Ilustración 37.- Distribución de los participantes en la encuesta por ubicación geográfica

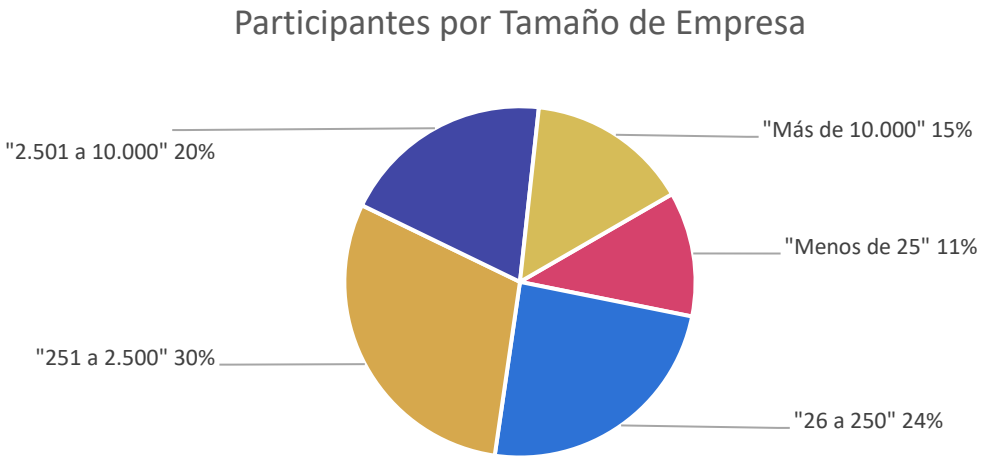


Ilustración 38.- Distribución de los participantes en la encuesta por tamaño de empresa

11º Estudio del Estado del Arte de la Seguridad en la Nube

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


@ISMSForum ISMS Forum

Una iniciativa de

isms forum

CSA Spanish Chapter