Soberanía del Dato y Estrategia Cloud

Cómo optimizar la inversión en la nube y facilitar la Soberanía del Dato a las organizaciones

Índice

Resumen ejecutivo

De cara al futuro más inmediato el objetivo de las organizaciones tendrá puesto el foco en fortalecer la infraestructura tecnológica existente, mejorar la eficiencia de los sistemas y aplicaciones, así como implementar nuevas soluciones que permitan optimizar nuestros procesos y ofrecer una experiencia superior a nuestros clientes. Así, el objetivo final en el área de TI y Comunicaciones será **evolucionar y optimizar** su funcionamiento buscando mejorar continuamente los sistemas, procesos y tecnologías para mantenerse competitivo y adaptado a las demandas del mercado. Además, se reconoce la necesidad de reducir costes y lograr eficiencias en nuestras operaciones para maximizar el valor y la rentabilidad de nuestras inversiones.

Basado en la puntuación asignada a la infraestructura de TI en la nube, se estima que entre el 10% y el 30% del presupuesto total se destinará a abordar o evolucionar la **estrategia y tecnología cloud** en 2023. Esto refleja la importancia otorgada a este desafío tecnológico en la asignación de recursos financieros, aunque no se ha asignado más del 30% del presupuesto.

Los participantes del estudio revelan una diversidad de enfoques en las organizaciones en cuanto al modelo utilizado para la estrategia de infraestructura. La adopción de una **multi nube híbrida** es la opción más popular, seguida de cerca por la nube pública/centros de datos de terceros y la nube privada/centro de datos propio. Cada modelo tiene sus ventajas y desafíos, y es importante evaluar cuidadosamente las necesidades de la organización al seleccionar el enfoque adecuado. La flexibilidad y la estructura de costes son consideraciones clave que deben tenerse en cuenta al diseñar y ejecutar una estrategia de infraestructura de estas características así como la capacidad de la organización de soportar las exigencias necesarias en materia de seguridad y control.

Se observa una valoración significativa de la importancia del **desarrollo propio de tecnologías y servicios digitales** en la Soberanía Digital. La mayoría de los participantes está de acuerdo en que el desarrollo propio es crucial para garantizar la independencia, la seguridad y la protección de los intereses nacionales en el ámbito digital. Estos resultados respaldan la necesidad de fomentar la innovación local, invertir en investigación y desarrollo, y promover el desarrollo de talento nacional en tecnología. Al mismo tiempo, es importante tener en cuenta las perspectivas de aquellos participantes que asignaron puntuaciones más bajas, ya que pueden aportar ideas valiosas y enriquecer el debate sobre el equilibrio entre el desarrollo propio y la colaboración con compañías extranjeras en el contexto de la Soberanía Digital.

La implementación de una estrategia de Soberanía Digital enfrenta **desafíos culturales, legales, de estandarización y técnicos.** Estos desafíos deben abordarse de manera integral para garantizar la protección de los datos, la seguridad y la autonomía en un entorno digital cada vez más interconectado. Promover una cultura de seguridad y Soberanía Digital, establecer marcos legales claros y armonizados, fomentar la estandarización y desarrollar capacidades técnicas sólidas son elementos clave para superar estos desafíos y lograr una implementación exitosa de una estrategia de Soberanía Digital. Es importante que las organizaciones y los países aborden estos desafíos de manera colaborativa y busquen soluciones innovadoras para proteger la privacidad y la seguridad en el entorno digital en constante evolución.

Los resultados ponen de manifiesto la **preocupación por las políticas de privacidad y protección de datos en el contexto de la Soberanía Digital.** Los participantes consideran adecuado que los estados inviertan en investigación y desarrollo de tecnología, valoran las políticas de privacidad y protección de datos de España y la UE, abogan por fomentar la creación de empresas tecnológicas nacionales y señalan la necesidad de una regulación más activa de las empresas de tecnología extranjeras. Estos resultados respaldan la importancia de implementar políticas efectivas en estos ámbitos para garantizar una Soberanía Digital sólida y proteger los intereses nacionales en el entorno digital.

1 – Infraestructura y Estrategia

1.1 – La inversión en tecnología y comunicaciones es prioritaria

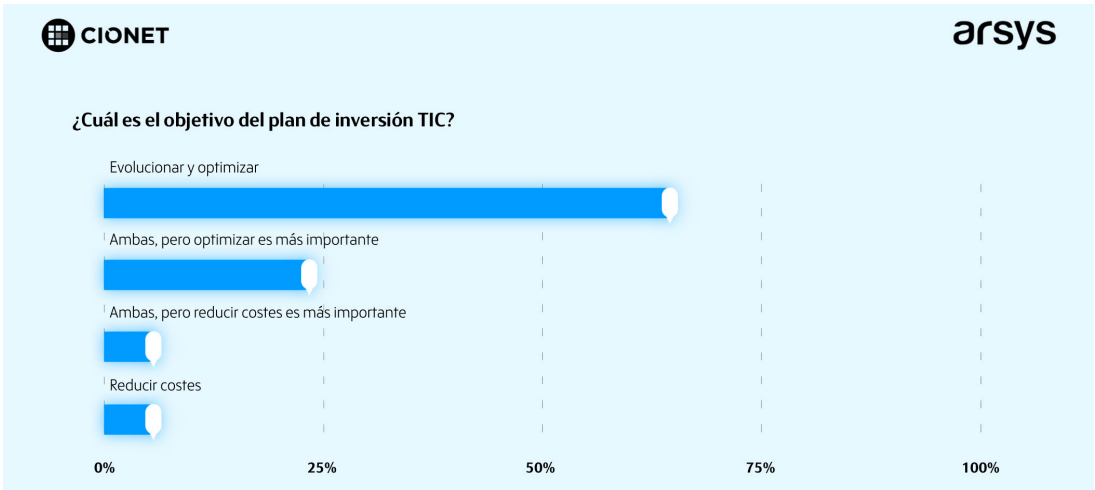
La inversión en tecnología y comunicaciones es prioritaria y está alineada con la estrategia de las organizaciones. Así, el área de TI y Comunicaciones ocupa una posición de alta prioridad dentro del plan de estrategia e inversión de las organizaciones participantes en el estudio para el año 2023. El **82,4%** de los encuestados considera que esta área se encuentra dentro de las 4 **prioridades principales de la compañía**. Esto refleja el reconocimiento de la importancia y el impacto significativo que tiene la tecnología de la información y las comunicaciones en nuestro negocio.

En un entorno competitivo cada vez más digitalizado, el área de TI y Comunicaciones desempeña un papel fundamental para garantizar la eficiencia operativa, la innovación y el crecimiento sostenible de las organizaciones. La inversión estratégica en tecnología y comunicaciones permite mejorar la productividad, optimizar los procesos internos, impulsar la colaboración entre equipos y aumentar la satisfacción del cliente.

En este sentido, las metas y objetivos corporativos para el año 2023 incorporan de manera destacada la transformación digital y la mejora continua de las infraestructuras tecnológicas manifestando, apenas el 17,6% de los participantes que su prioridad es media, es decir, está entre los objetivos de la compañía pero no resulta una prioridad.

1.2 – Optimizar es lo prioritario

El objetivo final de las organizaciones participantes en el estudio en relación al área de TI y Comunicaciones es **evolucionar y optimizar su funcionamiento**. Según los resultados obtenidos, el 64,7% de los encuestados considera que esta es la meta principal, lo que pone de manifiesto la visión de buscar constantemente mejoras en los sistemas, procesos y tecnologías con foco en la productividad y adaptación a entornos competitivos en constante cambio.



Si bien la optimización es el enfoque principal, también se reconoce la **importancia de lograr eficiencias en las operaciones**. El 23,5% de los encuestados considera que ambas metas son importantes, pero la optimización es el aspecto más relevante. Esto implica que buscamos lograr una mejor utilización de los recursos, tanto financieros como tecnológicos, para maximizar el valor y la rentabilidad de las inversiones. Apenas un 5,9% de los encuestados considera que reducir costes es la prioridad principal. Esto muestra que, pese a la importancia manifiesta de garantizar un adecuado equilibrio en las inversiones realizadas, tratando de encontrar formas de ahorrar costes y optimizar nuestra eficiencia económica, no se plantean comprometer la calidad en la arquitectura y soluciones tecnológicas.

1.3 – Explotación de Datos, Infraestructura y Ciberseguridad

La **explotación de datos** (2,67), la **infraestructura tecnológica en la nube** (2,44) y la **ciberseguridad y cumplimiento normativo** (2,39) son considerados como los retos principales por parte de las organizaciones, considerando los valores más próximos a 1 como aquellos en los que la prioridad es máxima.

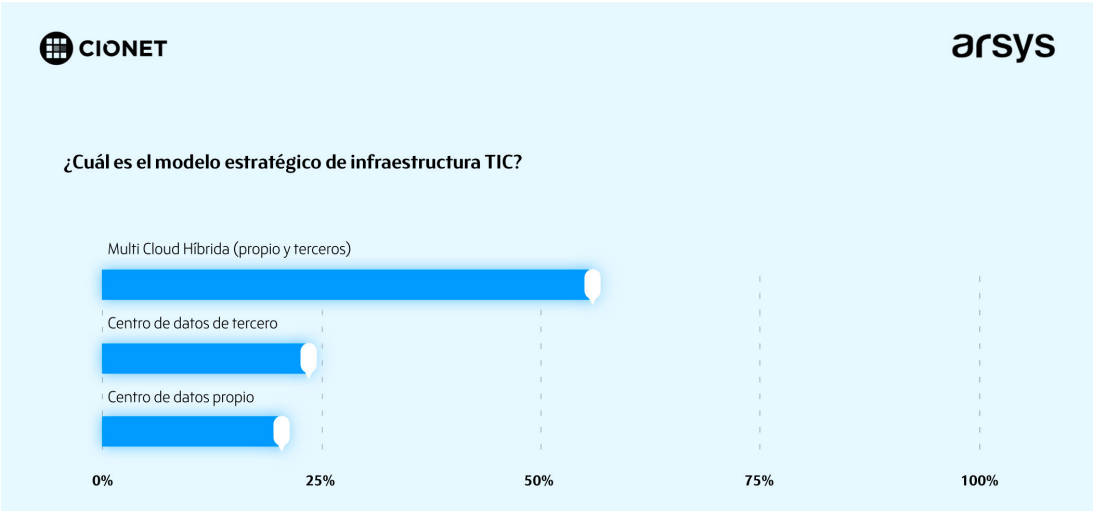
No es de extrañar que la mejora de la experiencia del cliente y los procesos se consideren como los aspectos de negocio más relevantes, con una puntuación de 2.94. De esta forma, las organizaciones están enfocadas en mejorar la interacción con los clientes y optimizar los procesos internos para ofrecer un mejor servicio y aumentar la eficiencia operativa.

- Ciberseguridad y cumplimiento
- Infraestructura TI en cloud
- Explotación de los datos
- Customer Experience & Procesos
- Otros proyectos de Innovación (IA, IoT, Blockchain, Kubernetes, etc.).

Según la puntuación proporcionada, los proyectos de innovación como AI, IoT, Blockchain y Kubernetes se consideran los menos relevantes en términos de prioridad, con una puntuación de 4.56. Esto sugiere que, aunque estos proyectos pueden ser importantes y prometedores en términos de innovación tecnológica, actualmente no se les asigna la máxima prioridad en relación con los otros retos mencionados.

1.4 – Modelo utilizado para la estrategia de infraestructura

La infraestructura tecnológica desempeña un papel fundamental en el soporte de las operaciones empresariales y la implementación de estrategias digitales. En el estudio se evalúa si el modelo utilizado para la estrategia de infraestructura, centrando el análisis en la utilización de una multi nube híbrida, nube pública y/o centros de datos de terceros o nube privada y/o centro de datos propio.



De acuerdo con los resultados del estudio, el **55.9% de los participantes indicó que utilizan un modelo de multi nube híbrida**, que combina recursos de infraestructura propios y servicios de proveedores externos. Este enfoque permite aprovechar lo mejor de ambos mundos, al utilizar los recursos internos para cargas de trabajo críticas o sensibles y

aprovechar la nube pública para lograr escalabilidad y flexibilidad. La multi nube híbrida brinda a las organizaciones la capacidad de adaptarse rápidamente a demandas cambiantes y optimizar costes al seleccionar los servicios y proveedores más adecuados para cada caso.

Por otro lado, el **23.5% de los participantes indicó que utilizan un modelo basado en nube pública y centros de datos de terceros**. Este enfoque implica confiar en proveedores externos para alojar y gestionar la infraestructura tecnológica. La nube pública ofrece escalabilidad, acceso a servicios avanzados y la capacidad de consumir y pagar solo por los recursos utilizados. Al utilizar centros de datos de terceros, las organizaciones se benefician de la experiencia y la infraestructura robusta proporcionada por sus proveedores de confianza. Sin embargo, es importante tener en cuenta las consideraciones de seguridad y Soberanía Digital al utilizar este modelo, con los datos y servicios alojados en infraestructuras controladas por terceros.

El **20.6% de los participantes indicó que utilizan un modelo de nube privada y centro de datos propio**. Este enfoque implica la construcción y operación de una infraestructura interna para satisfacer las necesidades tecnológicas de la organización. La nube privada puede llegar a ofrecer un mayor control y seguridad en la medida en la que las inversiones y esfuerzos en seguridad sean también elevados, ya que los datos y servicios se mantienen en las instalaciones propias. Esto puede ser especialmente relevante para organizaciones con requisitos de seguridad o cumplimiento rigurosos. Sin embargo, es importante considerar los costes y la capacidad de escalabilidad al utilizar este modelo, ya que puede requerir inversiones significativas en infraestructura y recursos internos.

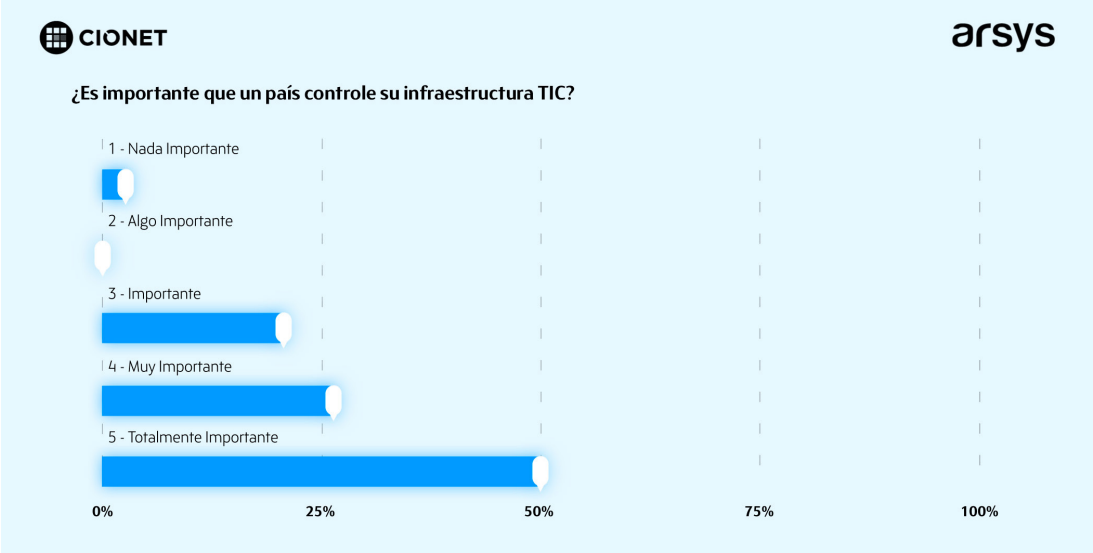
1.5 – Incidencia de la infraestructura tecnológica en la Soberanía Digital

Los modelos de infraestructura, como hemos anticipado, están claramente relacionados con la soberanía tecnológica siendo uno de los aspectos fundamentales en este ámbito el control de la infraestructura tecnológica por parte de un país y las organizaciones localizadas en su territorio. En este estudio, hemos evaluado la opinión de los participantes sobre la importancia de que un país tenga control sobre su infraestructura tecnológica, utilizando una escala de puntuación del 1 al 5.

De acuerdo con los resultados de nuestro estudio, la mitad de los participantes asignó una puntuación máxima a la *"afirmación de que es importante que un país tenga el control sobre su infraestructura tecnológica"*. Este resultado destaca la conciencia dentro de las organizaciones de que **tener el control sobre la infraestructura tecnológica es crucial para salvaguardar la Soberanía Digital** de un país. Así, la independencia y el control de la infraestructura tecnológica son fundamentales para proteger los intereses y la seguridad del país en un entorno digital.

Por otro lado, el 26.5% de los participantes asignó una puntuación de 4, lo que indica un acuerdo considerable con la afirmación. Estos participantes también reconocen la importancia del control de la infraestructura tecnológica, aunque con un grado menor de intensidad. En conjunto, el 76.5% de los participantes asignó una puntuación de 4 o 5, lo que indica un **consenso generalizado sobre la importancia del control de la infraestructura tecnológica en la Soberanía Digital**.

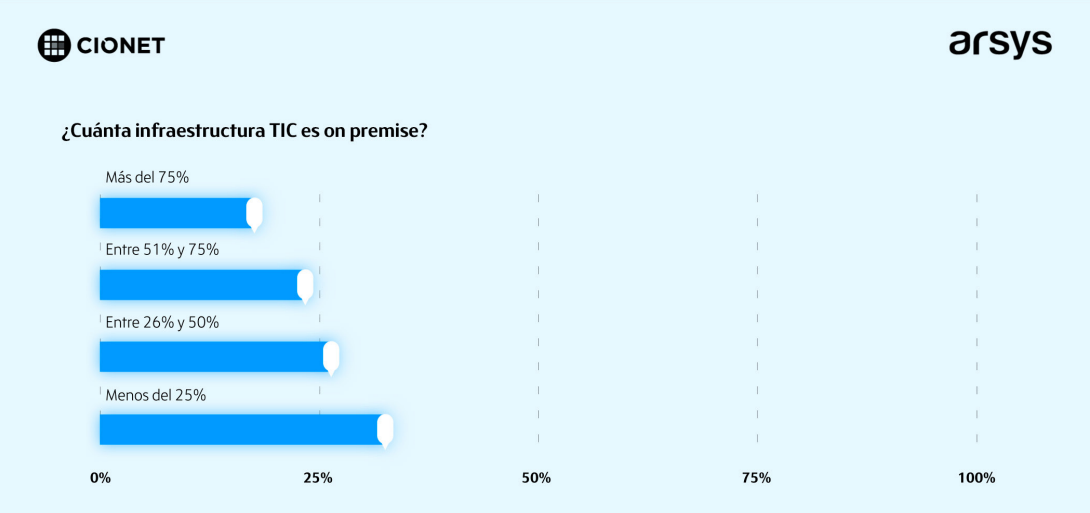
Un 20.6%, con una puntuación de 3, manifestó una opinión más neutral o ambigua sobre la importancia del control de la infraestructura tecnológica lo que configura que se pueden tener diferentes perspectivas sobre el equilibrio entre el control y la colaboración con actores externos en términos de infraestructura tecnológica.



De esta forma, los resultados del estudio muestran que en las organizaciones existe una valoración significativa de la **importancia de que un país tenga control sobre su infraestructura tecnológica en el contexto de la Soberanía Digital**. La mayoría de los participantes está de acuerdo en que el control de la infraestructura tecnológica es fundamental para garantizar la independencia, la seguridad y la protección de los intereses nacionales en el ámbito digital. Estos resultados respaldan la necesidad de implementar medidas y políticas que fomenten la Soberanía Digital y aseguren un control adecuado sobre la infraestructura tecnológica. Al mismo tiempo, es importante considerar las perspectivas de aquellos participantes que asignaron puntuaciones más bajas, ya que pueden aportar ideas valiosas y enriquecer el debate sobre este tema crítico.

1.6 – Infraestructura on premise

La infraestructura tecnológica como componente esencial del entorno corporativo, y la forma en que se distribuye y administra puede tener un impacto significativo en la Soberanía Digital. Con las organizaciones participantes en el estudio hemos evaluado el porcentaje aproximado de infraestructura actual que se encuentra on premise, es decir, en las instalaciones propias de la empresa. Así, **uno de cada tres participantes indicó que entre el 26% y el 50% de la infraestructura actual se encuentra on premise**. Esto indica que una proporción significativa de la infraestructura tecnológica está alojada en las instalaciones propias, lo que puede brindar un mayor control y seguridad en términos de Soberanía Digital con un enfoque de ejercer un mayor control sobre sus datos y servicios.



Por otro lado, otro **1 de cada 4 participantes manifiesta que menos del 25% de su infraestructura se encuentra on premise**. Estas organizaciones han optado por externalizar la mayoría de su infraestructura tecnológica, confiando en proveedores de servicios en la nube u otras soluciones externas. Si bien esta opción puede proporcionar flexibilidad y escalabilidad, también puede presentar desafíos en términos de Soberanía Digital y dependencia de terceros.

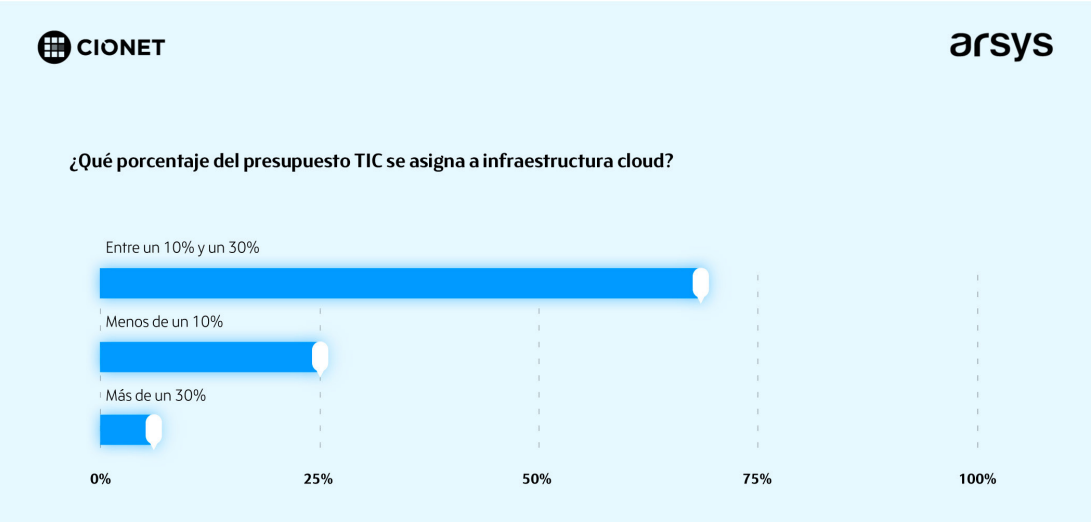
El **23.5% de los participantes indicó que entre el 51% y el 75% de su infraestructura se encuentra on premise**, optando por mantener una parte considerable de su infraestructura en sus propias instalaciones, lo que les permite tener un mayor control y autonomía en términos de Soberanía Digital. Al mantener una parte significativa de la infraestructura internamente, pueden mitigar algunos riesgos asociados con la dependencia de terceros y salvaguardar mejor la seguridad de sus datos y servicios.

Finalmente, el **17.6% de los participantes indicó que más del 75% de su infraestructura está on premise**. Estos participantes han optado por mantener la gran mayoría de su infraestructura tecnológica en sus propias instalaciones, lo que les brinda un control total y una Soberanía Digital máxima. Esta elección puede estar respaldada por consideraciones de seguridad, regulaciones específicas o necesidades específicas de la organización.

Los resultados del estudio muestran que en nuestra organización existe una variedad de enfoques en términos de infraestructura on premise. Si bien una parte significativa de los participantes ha externalizado parte de su infraestructura, aún hay una proporción considerable que ha optado por mantenerla en sus propias instalaciones. Esta diversidad de enfoques refleja **la necesidad de encontrar el equilibrio adecuado entre la flexibilidad y los beneficios de la nube**, y la autonomía y el control que ofrece la infraestructura on premise en el contexto de la Soberanía Digital. Cada enfoque tiene sus ventajas y desafíos, y es importante evaluar cuidadosamente las necesidades y objetivos de la organización al determinar el porcentaje de infraestructura.

1.7 – Inversión en tecnología cloud

Según los resultados obtenidos, **tres de cada cuatro de los encuestados asigna entre un 10% y un 30% del total de su presupuesto de tecnología en infraestructura y tecnología cloud** para este 2023, manifestando la importancia de invertir una cantidad significativa de recursos en este ámbito para mejorar y optimizar su infraestructura tecnológica.

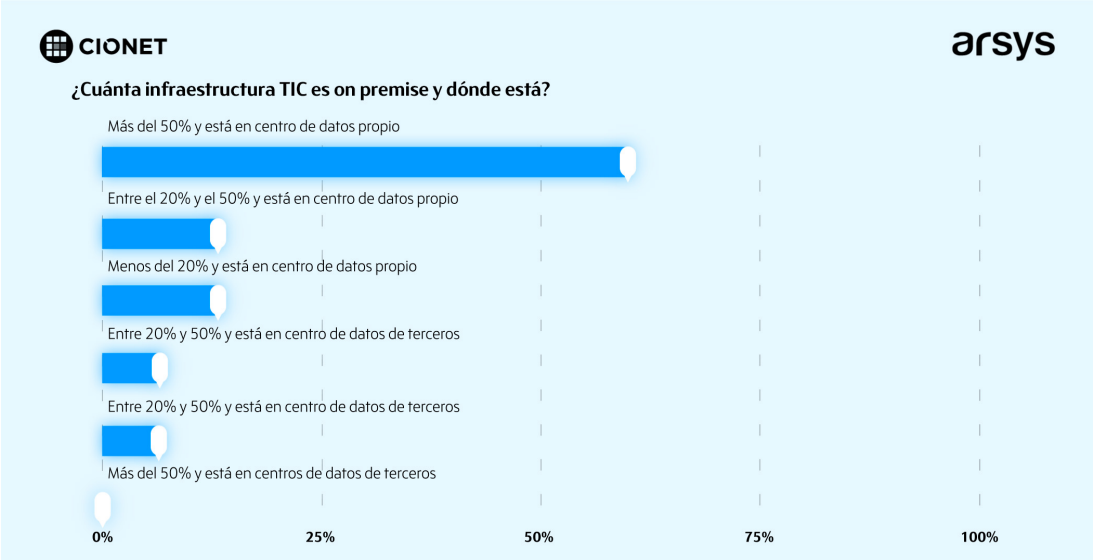


Por el contrario, uno de cada cuatro encuestados indica que asignará menos del 10% del presupuesto total a este objetivo. Esto puede sugerir que, aunque la empresa considera importante la evolución de la infraestructura de TI en la nube, por diversas razones, se ha asignado una menor proporción de recursos financieros en comparación con otros retos tecnológicos.

No se menciona específicamente en la encuesta si más del 30% del presupuesto se destinará a la infraestructura de TI en la nube. Por lo tanto, se puede inferir que no se ha asignado una proporción tan alta de recursos para este objetivo en particular, ya que no se refleja en las opciones proporcionadas.

1.8 – El viaje hacia la nube

Según las respuestas proporcionadas, el 60% de la infraestructura actual en la empresa se encuentra en un centro de datos propio y constituye más del 50% del total. Esto indica que las organizaciones mantienen **una parte significativa de su infraestructura en sus propias instalaciones**, lo que implica una mayor inversión y control directo sobre la gestión de los recursos tecnológicos.



Para el 13,3% de los encuestados se encuentra en centros de datos propios y representa entre el 20% y el 50% del total. Esto sugiere que una parte considerable de la infraestructura se encuentra en instalaciones internas, pero en menor medida en comparación con el primer grupo mencionado. Para otro 13,3% de los participantes, la infraestructura se encuentra en centros de datos propios, pero representa menos del 20% del total. Esto indica que una pequeña parte de los recursos tecnológicos se mantiene internamente en las instalaciones de la empresa, pero en una proporción menor.

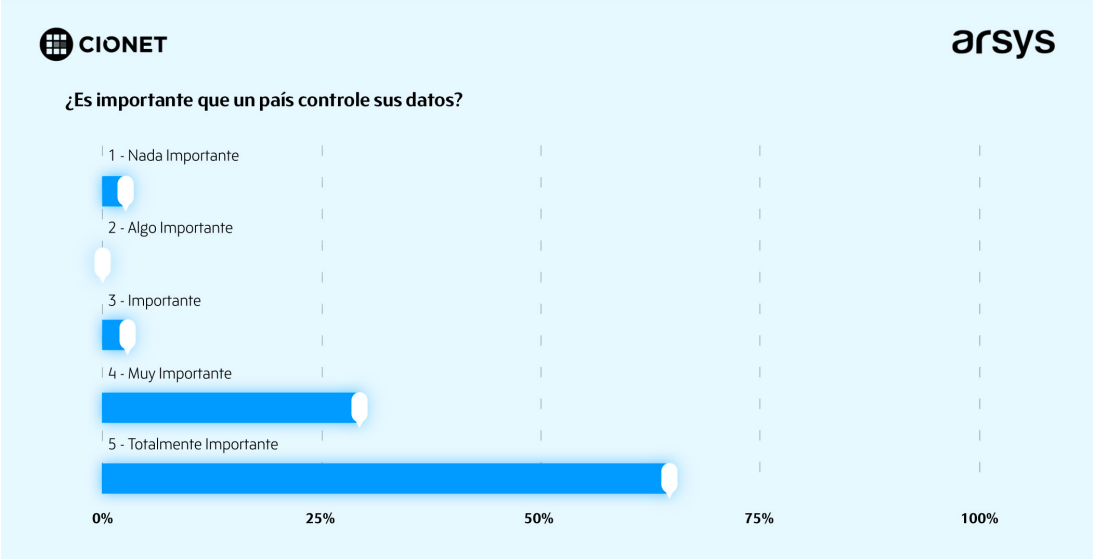
Para el 6,7% de los encuestados, la infraestructura se encuentra en centros de datos de terceros, y representa entre el 20% y el 50% del total. Esto implica que la empresa ha externalizado parte de su infraestructura tecnológica, confiando en proveedores externos para el alojamiento y la gestión de esos recursos. Finalmente, también se identificó que el 6,7% de la infraestructura está en centros de datos de terceros, pero representa más del 50% del total. Esto indica que una parte significativa de la infraestructura se ha externalizado a proveedores de servicios de centros de datos.

En resumen, según los resultados de la encuesta, la mayoría de la infraestructura actual en la empresa se encuentra en centros de datos propios, ya sea representando más del 50% del total o entre el 20% y el 50%. Sin embargo, también existe una proporción significativa de infraestructura alojada en centros de datos de terceros, tanto en una proporción mayor como en una menor.

2 – Soberanía de los Datos

2.1 – La importancia del control de los datos

La Soberanía Digital es un tema relevante en la tecnología y, cada vez más, en el negocio. Una de las principales áreas de discusión en este ámbito es el control de los datos y en qué medida es importante que un país tenga el control sobre ellos. En CIONET en colaboración con Arsys, hemos evaluado la opinión de los participantes en el estudio en relación con esta afirmación, utilizando una escala de puntuación del 1 al 5.



De acuerdo con los resultados obtenidos, el 64.7% de los participantes asignó una puntuación de 5, indicando un **alto nivel de acuerdo con la afirmación de que es importante que un país tenga el control de sus datos**. Este resultado resalta la conciencia de la importancia del control de datos en la Soberanía Digital dentro de las organizaciones al considerar que el control de datos es un aspecto crucial para la independencia y la seguridad digital de un país.

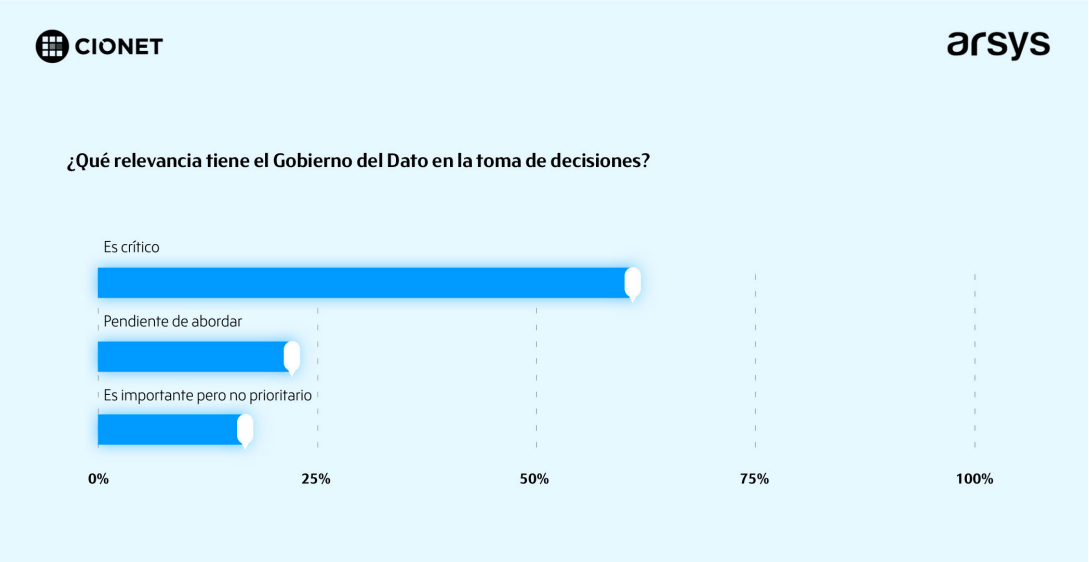
Por otro lado, el 29.4% de los participantes asignó una puntuación de 4, lo que indica un acuerdo considerable con la afirmación. Estos participantes también reconocen la importancia del control de datos, aunque con un grado menor de intensidad. Juntos, el 94.1% de los participantes asignó una puntuación de 4 o 5, lo que indica un **consenso generalizado sobre la importancia del control de datos en la Soberanía Digital**. Estos resultados respaldan la necesidad de adoptar medidas y políticas que promuevan la Soberanía Digital y protejan los datos sensibles de un país.

Pese a ello, escasamente el 2.9% de los participantes asignó una puntuación de 1 o 3, lo que indica un nivel de desacuerdo o neutralidad con la afirmación. Estos participantes podrían tener diferentes perspectivas sobre el control de datos en relación con la Soberanía Digital. Sin embargo, siendo el total de respuestas tan reducidas en este aspecto podríamos considerarlo dentro del rango de error del estudio cuya incidencia no es significativa.

2.2 – Criticidad del Gobierno del Dato

En las organizaciones, se considera el Gobierno del Dato como un aspecto crítico en la toma de decisiones. Así, el 61,6% de los encuestados compartió esta opinión, lo que indica que **reconocemos la importancia de tener una política de datos bien definida** que regule cómo se recopilan, almacenan, procesan y eliminan los datos en las organizaciones.

El Gobierno del Dato implica establecer procesos y controles claros para garantizar la calidad, integridad, privacidad y seguridad de los mismos. Al tener una política sólida, podemos asegurar la confidencialidad de la información, cumplir con las regulaciones y normativas pertinentes, y tomar decisiones basadas en datos confiables y precisos.



Sin embargo, también se identificó que el 22,2% de los encuestados considera que el Gobierno del Dato está en un estado pendiente de abordar en sus organizaciones, lo que sugiere que aún existe margen de mejora en términos de establecer y aplicar una política de datos efectiva. Es necesario evaluar y desarrollar los procesos y procedimientos necesarios para gestionar de manera adecuada estos datos y maximizar su valor.

Además, el 16,7% de los encuestados opinó que el Gobierno del Dato es importante, pero no es una prioridad inmediata. Esto indica que se reconoce su relevancia, pero que actualmente la prioridad son otros desafíos o proyectos que tienen una mayor relevancia en su estrategia empresarial.

De esta forma, se considera el Gobierno del Dato como un aspecto crítico en nuestra toma de decisiones, aunque también reconocemos que existen áreas de mejora y que aún no han sido completamente abordadas en sus empresas. Por tanto, será un objetivo establecer y seguir una política de datos sólida que regule cómo se maneja la información, con el fin de garantizar la calidad, seguridad y cumplimiento normativo en todas nuestras actividades.

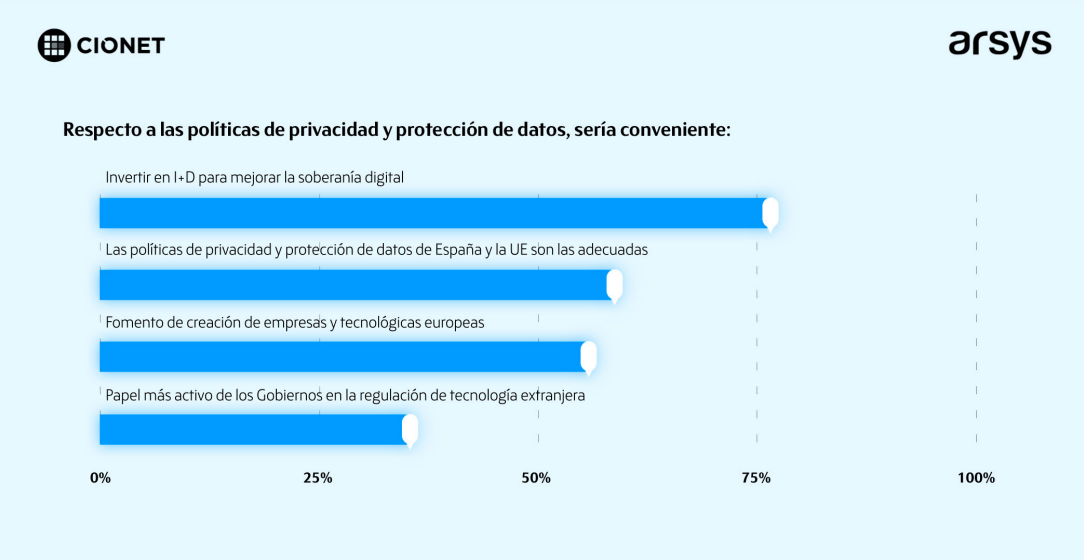
2.3 – Políticas de privacidad y protección de datos

Las políticas de privacidad y protección de datos desempeñan un papel fundamental en la Soberanía Digital, siendo elementos clave para salvaguardar la seguridad y proteger los intereses de un país en el entorno digital. En el estudio se ha evaluado la opinión de los participantes sobre una serie de políticas relacionadas con la privacidad y la protección de datos.

De acuerdo con los resultados obtenidos, el 76.5% de los participantes considera **adecuado que los estados inviertan en investigación y desarrollo de tecnología para mejorar la Soberanía Digital**. Estos participantes reconocen la importancia de que los estados destinen recursos a la investigación y desarrollo de tecnologías que fortalezcan la Soberanía Digital, lo que incluye la protección de datos y la garantía de la seguridad en el ámbito digital.

En cuanto a las políticas de privacidad y protección de datos de España y la Unión Europea (UE), el 58.8% de los participantes considera que son adecuadas. Esto indica que existe una confianza significativa en las políticas existentes en estos ámbitos. Los participantes valoran el marco legal y regulatorio establecido por España y la UE para proteger la privacidad y los datos personales como adecuado, y consideran que estas políticas son un paso en la dirección correcta hacia la Soberanía Digital.

Al mismo tiempo, el 55.9% de los participantes está de acuerdo en que los países de la UE deberían **fomentar la creación de empresas tecnológicas nacionales** para reducir la dependencia de las empresas extranjeras. Esta opinión refleja la importancia de fomentar la innovación y el desarrollo local en el ámbito tecnológico, con el objetivo de disminuir la dependencia externa y fortalecer la Soberanía Digital de los países de la UE. Y, en paralelo, el 35.3% de los participantes considera que los **gobiernos y administraciones públicas deberían tener un papel más activo en regular a las empresas de tecnología extranjeras**. Estos participantes abogan por una mayor regulación y supervisión de las actividades de las empresas tecnológicas extranjeras, con el fin de proteger los intereses nacionales y garantizar la Soberanía Digital.



3 – Soberanía Digital y el rol del CIO

3.1 – ¿Qué es la Soberanía Digital?

La Soberanía Digital se refiere a la **capacidad de un país para ejercer control sobre su infraestructura digital, datos y actividades digitales con el fin de proteger su seguridad, economía y valores**. Para Europa, la Soberanía Digital implica reducir la dependencia de las empresas tecnológicas extranjeras, garantizar que los datos se almacenen y procesen dentro de la UE y desarrollar tecnologías y estándares digitales europeos, lo que obliga a crear un marco regulatorio que permita a la UE dar forma al mercado digital y fomentar la innovación, al mismo tiempo que se protege la privacidad de los ciudadanos y se promueve un entorno digital libre y abierto.

3.2 – Europa, la Suiza de los datos

En el marco de CIOFEST 2023, con el liderazgo de Arsys en las actividades realizadas en España, se llevó a cabo otro estudio con 20 *Chief Information Officers (CIO)* de toda Europa que reveló que la **estrategia de Soberanía Digital está impulsada principalmente por el deseo de asegurar el valor de los datos y facilitar su intercambio**. Y dado que la mayoría de las empresas ya utilizan intensivamente la nube pública, se preocupan por la Soberanía Digital tan pronto como se refiere a datos críticos o sensibles para el negocio. En este contexto, es bastante sorprendente observar que solo unos pocos CIOs indicaron que realizaron evaluaciones en profundidad de las nuevas legislaciones europeas relacionadas con los datos.

La investigación mostró que las principales preocupaciones de los CIOs con respecto a la (falta de) Soberanía Digital están relacionadas con su falta de control sobre un complejo panorama digital, el temor a perder oportunidades comerciales debido a la falta de alcance global de las ofertas de nube e intercambio de datos más pequeñas (europeas) y los efectos de bloqueo de las infraestructuras digitales existentes. Los CIOs expresaron su pesar de que no haya alternativas europeas a gran escala para el uso de los servicios de los gigantes de la tecnología e indicaron un camino a seguir con el objetivo de desarrollar la tecnología necesaria, estándares y construir un marco legislativo líder. Entre estos caminos, tanto para los CIOs como para los responsables de políticas, se debe poner el foco en la **creación de estrategias de Soberanía Digital**, gestión de la complejidad y una estrategia equilibrada de la nube resaltando las oportunidades de las nuevas legislaciones europeas. Fortalecer la Soberanía Digital por parte de los responsables de políticas es un acto de equilibrio, ya que también se debe tener en cuenta la economía abierta. Esto podría ser una oportunidad para que Europa se convierta en "la Suiza de los datos".

El CIO tiene una nueva misión en la economía actual de los datos, donde es crucial tratar los datos como un activo, como un valor clave para la empresa. Seis aspectos siguen siendo importantes en este contexto: 1) la velocidad de acceso a los datos, 2) la fluidez de los datos (aspecto de localización), 3) la agilidad (opción de escalar), 4) la seguridad, 5) la calidad de los datos y, finalmente, 6) la sostenibilidad. Hoy en día, la Soberanía Digital es un ámbito crítico, porque el mundo está cambiando rápidamente en términos de evoluciones tecnológicas, presiones geopolíticas, creciente conciencia de los consumidores y el ritmo de las iniciativas legislativas. Estamos presenciando una batalla de IA, comprometiéndonos en el frente de la seguridad y modelando nuevas legislaciones en consecuencia.

3.3 – El 92% de los datos de Europa se almacenan fuera de Europa

Sin embargo, no debemos dejar de lado las principales limitaciones que enfrenta el CIO para cumplir su nueva misión, como se describió anteriormente. Entre estos obstáculos se encuentra la falta de control de los datos. **El 92% de los datos de Europa se almacenan fuera de Europa, principalmente en Estados Unidos**. Unos pocos gigantes tecnológicos globales dominan el panorama digital. No existe un campo de juego equitativo mientras ellos posean la mayor parte de la infraestructura. La Soberanía Digital sigue siendo una cuestión de alta complejidad y muchas incertidumbres, ya que los países legislan de manera independiente y el Tribunal de la UE se pronuncia sobre casos de protección de datos como Schrems II. Los riesgos provienen de la falta de transparencia en el procesamiento de datos, la falta de estándares de interoperabilidad entre los actores actuales y las crecientes amenazas cibernéticas.

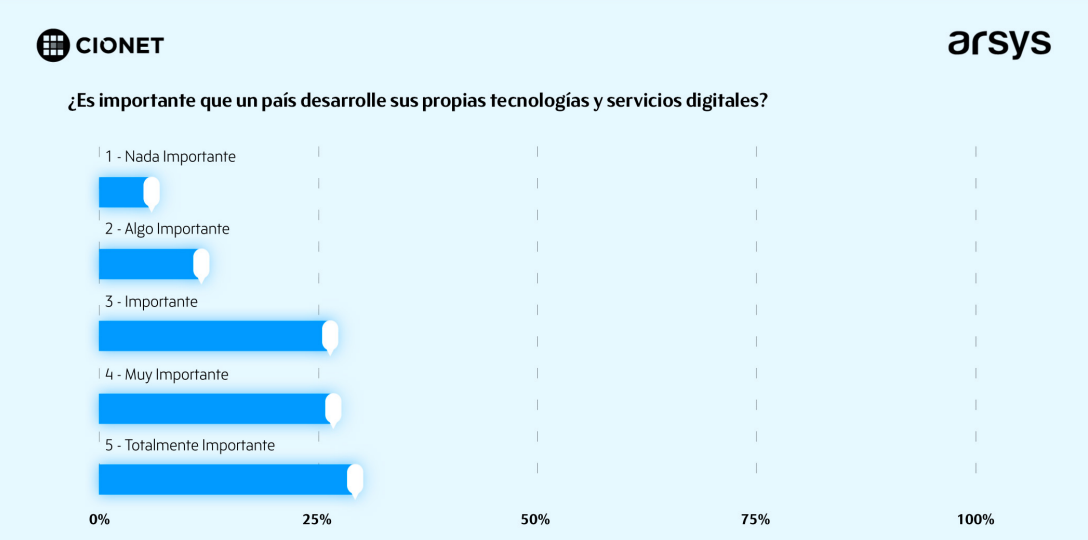
Europa siempre ha tenido una economía muy abierta, lo cual es óptimo siempre y cuando todos los socios comerciales jueguen con las mismas reglas. La UE está creando legislaciones comunes para establecer o aclarar las reglas (Pierre Chastanet de la Comisión Europea). El Reglamento de Gobernanza de Datos y el Reglamento de Datos establecen un marco para el intercambio y uso de datos por parte de empresas y gobiernos en toda la UE. El enfoque de los legisladores se centra en la interoperabilidad y la seguridad. Además, la Comisión Europea ha destinado casi el 70% de sus fondos en los programas de recuperación posterior a la pandemia a la transformación digital. Las inversiones se destinarán, entre otras cosas, a iniciativas como la Nube de Datos Industriales y los Espacios de Datos, creando así el entorno adecuado para que Europa se convierta incluso en un ejemplo a seguir para el mundo.

Establecer estándares puede impulsar un mercado como por el ejemplo con la utilización del estándar tecnológico GSM. Una vez que se estableció el estándar europeo, Nokia y Ericsson conquistaron el mercado y dieron ejemplo al resto del mundo. Pierre Chastanet (Comisión Europea) agregó que la estandarización no construye barreras alrededor de Europa,

sino que fomenta la cooperación e invita a la inversión en áreas nuevas, lo que abre la posibilidad de incorporar a la discusión alternativas de código abierto. La comunidad de código abierto sigue siendo un elemento constituyente crucial de la solución, pero no necesariamente la solución en sí misma. Así, la forma deseada de avanzar hacia la Soberanía Digital estará muy vinculada a la filosofía de código abierto: se basará en la competencia abierta entre muchos actores y posibilidades de federación de componentes y soluciones disponibles libremente para todos.

3.4 – Consenso respecto al desarrollo propio en Soberanía Digital

En el estudio de CIONET y Arsys se ha evaluado la opinión de los participantes sobre la *"importancia de que un país desarrolle sus propias tecnologías y servicios digitales, en contraposición a depender de compañías extranjeras"*. El 29.4% de los participantes asignó una puntuación de 5, lo que indica un **alto nivel de acuerdo con la afirmación de que un país debería desarrollar sus propias tecnologías y servicios digitales en lugar de depender de compañías extranjeras**. Estos participantes consideran que el desarrollo propio es esencial para asegurar la independencia y la Soberanía Digital de un país. Valorar la capacidad de crear y controlar las tecnologías y servicios digitales permite mantener la seguridad, proteger los intereses nacionales y fomentar la innovación local.

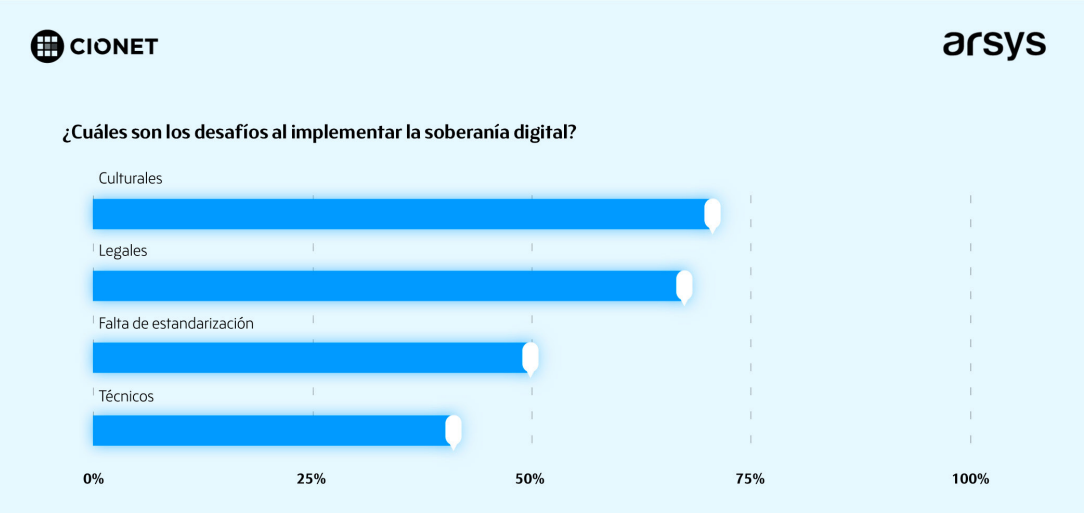


Por otro lado, el 26.5% de los participantes asignó una puntuación de 4, lo que indica un acuerdo considerable con la afirmación. Estos participantes reconocen la importancia del desarrollo propio de tecnologías y servicios digitales, aunque con un grado menor de intensidad. En conjunto, el 55.9% de los participantes asignó una puntuación de 4 o 5, lo que indica un **consenso generalizado sobre la relevancia del desarrollo propio en la Soberanía Digital**.

Un 26.5% de los participantes asignó una puntuación de 3, lo que indica una opinión más neutral o ambigua sobre la importancia del desarrollo propio. Estos participantes pueden tener diferentes perspectivas sobre la colaboración con compañías extranjeras y el equilibrio entre el desarrollo propio y la adquisición de tecnologías y servicios externos.

3.5 – Desafíos culturales y legales en la estrategia de Soberanía Digital

Implementar una estrategia de Soberanía Digital presenta desafíos significativos que deben abordarse para garantizar su éxito. El **70.6%** de los participantes considera que los **desafíos culturales son uno de los principales obstáculos para implementar una estrategia de Soberanía Digital**. Esto implica la necesidad de fomentar un cambio cultural en la organización, donde se valore la importancia de proteger la privacidad y los datos, así como la necesidad de confiar en soluciones y servicios digitales desarrollados internamente o provenientes de proveedores nacionales. Superar los obstáculos culturales requiere concienciación, educación y promoción de una mentalidad de seguridad y Soberanía Digital en todos los niveles de la organización.



El 67.6% de los participantes considera los desafíos legales como una barrera significativa en la implementación de una estrategia de Soberanía Digital. Las leyes y regulaciones pueden variar entre países y regiones, lo que puede dificultar la aplicación coherente de políticas de protección de datos y Soberanía Digital. Es fundamental contar con marcos legales claros que protejan los derechos y la privacidad de los ciudadanos y que proporcionen pautas para la gestión de datos y la seguridad cibernética. Además, la armonización de las leyes y regulaciones a nivel internacional puede facilitar el intercambio seguro y regulado de datos entre países.

La falta de estandarización también se identificó como un desafío importante por el 50% de los participantes. La ausencia de estándares comunes puede dificultar la interoperabilidad y la integración de sistemas, especialmente en entornos multinacionales. La falta de estandarización puede afectar la seguridad, la transferencia de datos y la compatibilidad de las soluciones tecnológicas. Es crucial promover la adopción de estándares abiertos y desarrollar marcos comunes que permitan la compatibilidad y la cooperación en un entorno digital global.

En cuanto a los desafíos técnicos, el 41.2% de los participantes los considera relevantes en la implementación de una estrategia de Soberanía Digital. Estos desafíos pueden incluir la infraestructura tecnológica necesaria para respaldar una estrategia de Soberanía Digital, como sistemas de almacenamiento, redes seguras y sistemas de protección cibernética. Además, la adquisición y el desarrollo de tecnologías y servicios digitales propios pueden requerir inversiones significativas en recursos y capacidades técnicas.

Metodología y agradecimientos

Este paper, realizado con el apoyo técnico de Arsys con foco en las estrategias se adopción de infraestructura y tecnología cloud en las organizaciones, así como la priorización y estrategias en la utilización de los datos y su relación con la Soberanía Digital se realizó con la información proporcionada por 54 representantes de marcado perfil técnico (CIOs, Directores de Arquitectura e Infraestructura, entre otros) de compañías participantes en en dos sesiones de trabajo de CIONET (Cloud Quest del 22 de febrero de 2023 y CIOFEST del 15 de marzo de 2023).

Entre otras organizaciones representadas en el estudio:

- Agencia para la Digitalización de la Comunidad de Madrid
- Allianz Technology
- AON
- ArcelorMittal
- Eulen
- Exolum
- FCC
- Food Delivery Brands
- García Carrión
- General Dynamics
- Grupo Envera
- Logitravel Group
- Mercedes-Benz Group Services
- Ministerio de Asuntos Económicos y Transición Digital
- Nestlé
- Pago Next | Grupo Santander
- Pepsico
- Prosegur
- Sociedad Estatal de Infraestructuras del Transporte Terrestre
- Telefónica
- TEVA Farmacia
- The Phone House
- Top Doctors
- Vodafone

Sobre CIONET

CIONET es la comunidad líder de altos ejecutivos de TI en todo el mundo. Con una membresía de CIO, CDO, CTO y líderes de TI de las principales empresas del mundo, CIONET tiene la experiencia y la visión pionera para resolver o abordar cualquier desafío de gestión digital o de TI.

CIONET desarrolla, administra y modera una comunidad y una plataforma de conocimiento con una variedad integrada de herramientas y servicios tanto online como presenciales diseñados para proporcionar soporte en tiempo real a los ejecutivos en sus decisiones sobre tecnología.

Sobre Arsys

Con más de 25 años en el mercado de servicios TI, Arsys es un proveedor especializado en soluciones de infraestructura cloud flexibles y personalizadas (cloud público, privado o híbrido, escritorios virtuales, almacenamiento, backup...), que acompaña a las empresas en su transformación digital con las mejores garantías de disponibilidad, rendimiento y seguridad.

Con oficinas en Logroño, Madrid, Barcelona, Sevilla, Bilbao y Valencia, Arsys forma parte de la compañía cotizada en bolsa IONOS Group SE (ISIN DE000A3E00M1), que cuenta con una red global de datacenters (España, Estados Unidos, Francia, Reino Unido y Alemania) para facilitar la última tecnología cloud a los proyectos internacionales.