

La seguridad en los sistemas CLOUD



Subvenciona

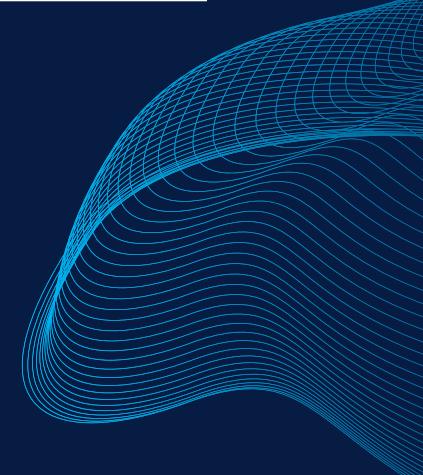


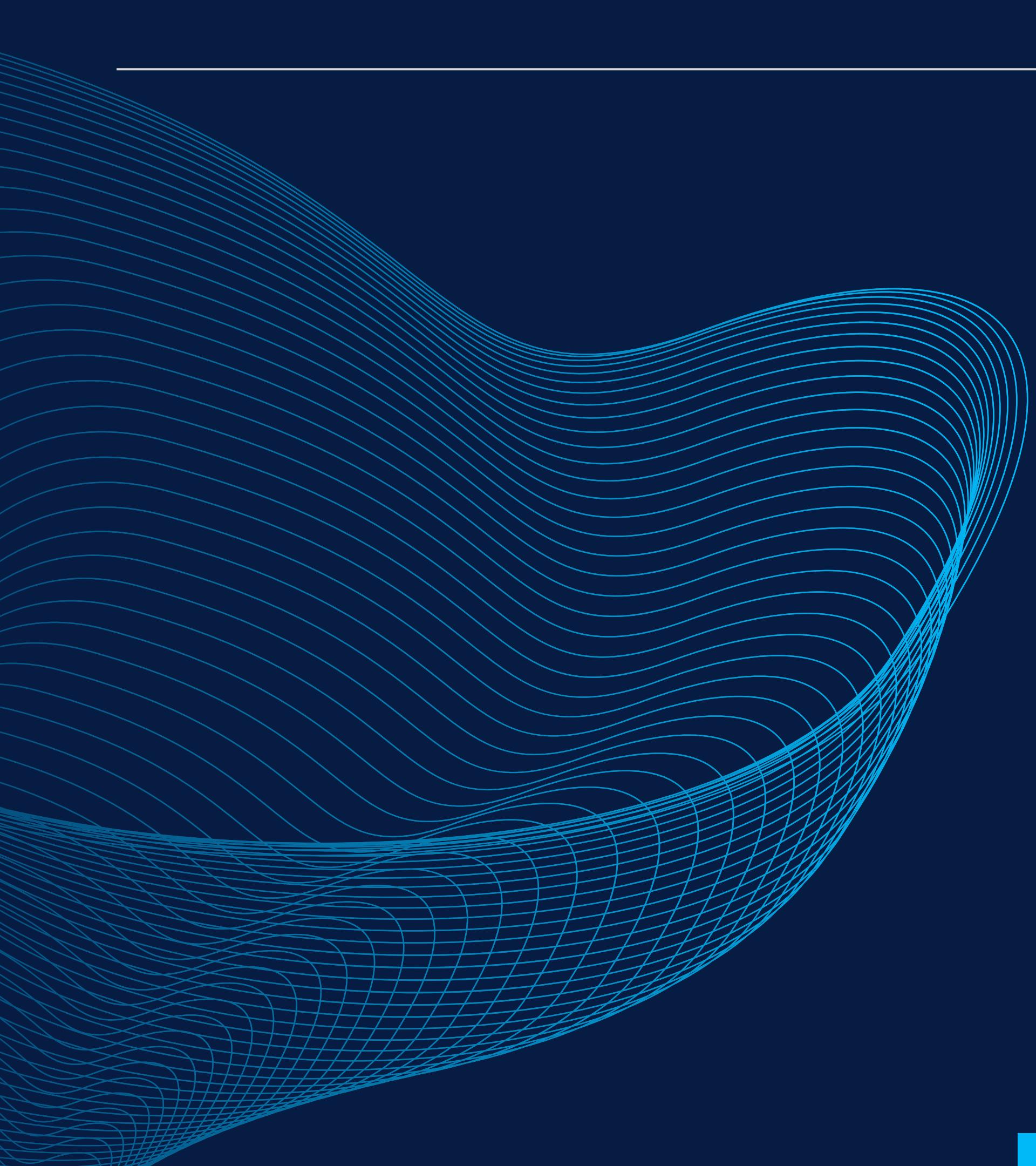
COORDINACIÓN
Y DESARROLLO ESTRÁTÉGICO,
PRODUCTIVO Y SOCIAL

Desarrolla



índice

- 
- 1. Introducción**
 - 2. Definición de Seguridad en la Nube**
 - 3. ¿Cómo funciona la Seguridad en la Nube?**
 - 4. ¿Qué hace que la Seguridad en la Nube sea diferente?**
 - 5. Riesgos de Seguridad en la Nube**
 - 6. ¿Por qué es importante la Seguridad en la Nube?**
 - 7. ¿Cómo asegurar la Nube?**
 - 8. Soluciones de Seguridad en la Nube para Personas Trabajadoras Autónomas y/o Personas Emprendedoras**
 - 9. Normas ISO de Ciberseguridad**
 - 10. Bibliografía**

A large, abstract graphic on the left side of the slide features a series of thin, light blue lines that curve and overlap to create a sense of depth and motion, resembling waves or a grid that has been twisted.

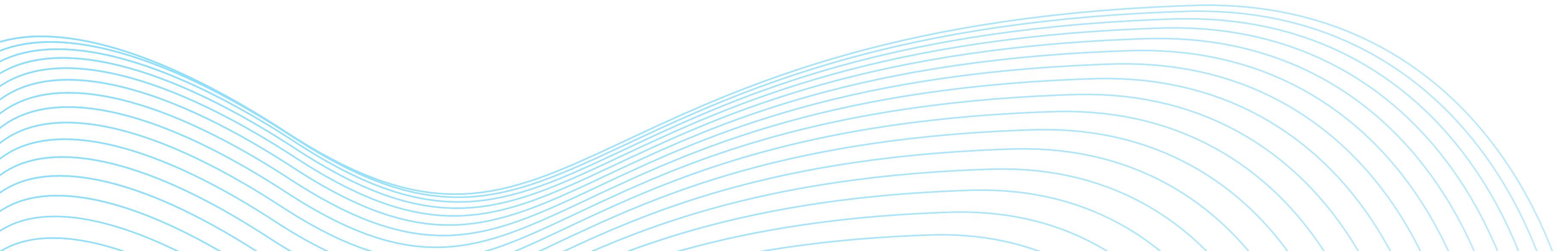
Introducción

Cuando alguien dice que sus datos están en la nube (cloud), o que puede trabajar en la nube (cloudcomputing), lo que dice en realidad es que sus datos están almacenados en alguna parte de Internet (o en muchas partes), y que hay una red de servidores que encuentra lo que necesita cuando lo necesita, y se lo entrega.

Los términos **cloud** y **cloudcomputing** se vienen utilizando, indistintamente, para referirse a lo mismo. Pero si queremos ser más exactos, podríamos decir que cloud es el Internet en general, mientras que cuando hablamos de cloudcomputing nos referimos al conjunto de productos, aplicaciones, y servicios que trabajan en la nube y a los cuales accedemos a través de Internet.

Teniendo en cuenta las definiciones anteriores, una gestión documental en la nube (Cloud Document Management) es un sistema de gestión documental (DMS) en el que los documentos (y muy posiblemente también la aplicación) están en la nube se accede a través de una conexión a Internet, desde cualquier parte y a través de diversos dispositivos.

Se ha indicado que, "muy posiblemente también la aplicación" porque algunos empresas proveedoras de un cloud DMS necesitan instalar, al menos, parte de la lógica de la aplicación en los ordenadores locales, mientras que otros son entregados como un servicio SaaS (Software as a Service) sin necesidad de instalar nada en los ordenadores locales.



El procesamiento en cloud se traduce en grandes ahorros para las personas trabajadoras autónomas y/o personas emprendedoras. Por ejemplo:

- ° **Coste por factura:** Un procesamiento en la nube cuesta aproximadamente un 20 % menos que una solución local.
- ° **Procesamiento directo:** Las soluciones en la nube ofrecen una mejora del 18 % del proceso, aproximadamente, que respalde su actuación.
- ° **Pagos puntuales:** Con gestión documental basada en cloudcomputing se mejora la gestión de pagos puntuales en un 9 %, aproximadamente.

En general, con una gestión documental basada en la nube, las pymes trabajan de manera más inteligente y rápida, y son capaces de concentrarse en tareas más importantes, lo cual repercute directamente en sus resultados de forma positiva.

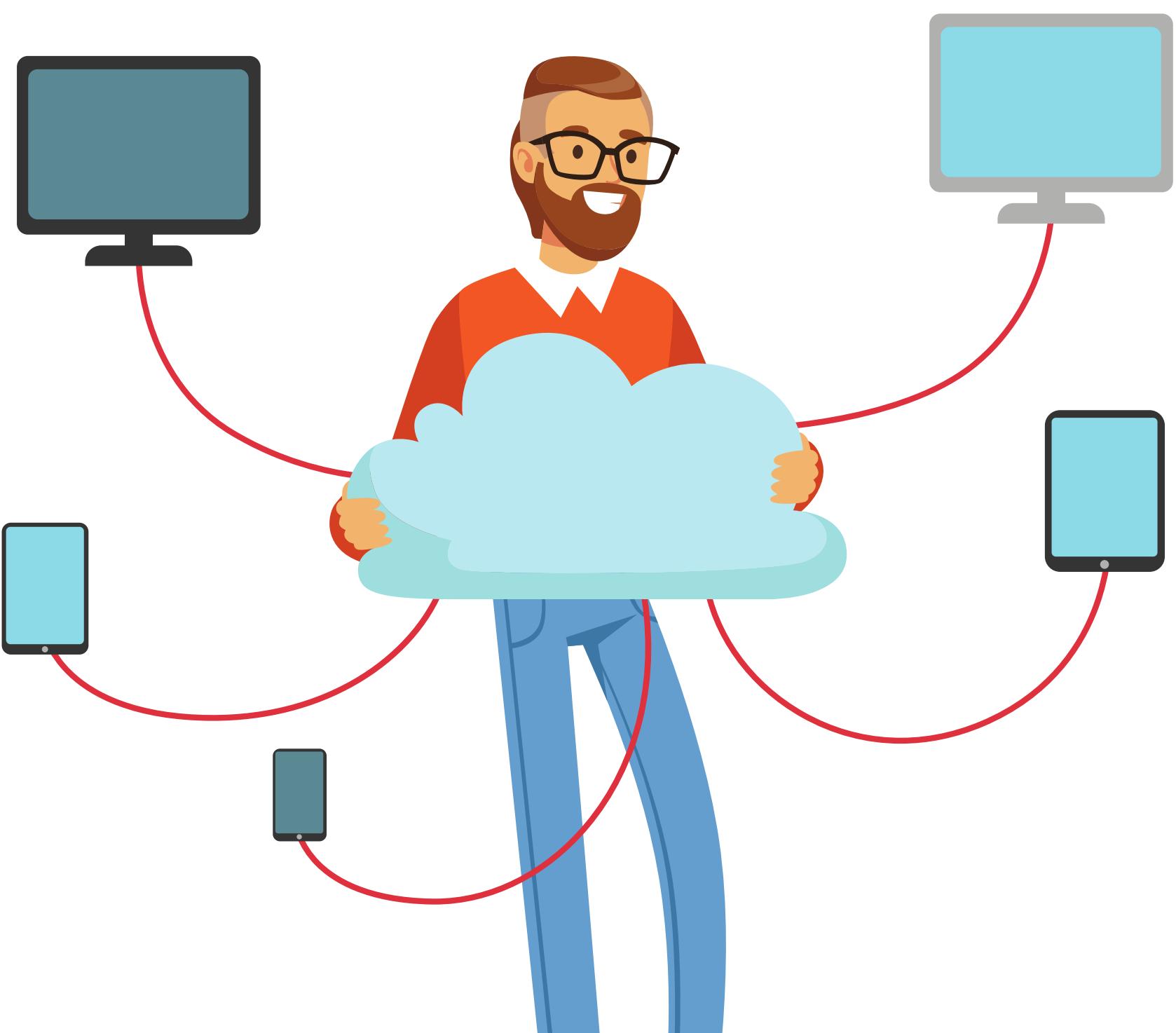


De esta manera, la protección de la información es un tema de gran relevancia en la era digital y el uso seguro de servicios en la nube se ha convertido en un importante desafío. Continuamente, se levantan voces que advierten de que los datos almacenados en la nube no pueden estar seguros bajo ninguna circunstancia, lo que provoca que, a menudo, las personas usuarias más precavidas eviten este tipo de soluciones online.

No obstante, no es el ámbito privado el único que se preocupa por la seguridad en la nube, pues en el sector empresarial también se utilizan estos servicios para guardar un gran volumen de datos de carácter privado, así como información confidencial relativa a la empresa.

A pesar de los rumores sobre los riesgos de seguridad que conlleva almacenar información en la nube, el volumen de datos que se depositan en ella, va aumentando continuamente, pues se suele recurrir a estos sistemas con bastante frecuencia.

Por un lado, las personas usuarias los utilizan por la comodidad que supone poder acceder a todos datos guardados desde cualquier lugar e incluso crean copias de seguridad de sus discos duros y las guardan en estos sistemas online.



Por otro lado, las empresas encuentran en la nube una herramienta de gran ayuda para poder mantener una mejor conexión entre el personal y, de este modo, aumentar la eficiencia de los procesos de trabajo. Además, su uso reduce costes, dado que con el cloud hosting se pueden ir aumentando los recursos según se requiera, necesitando una infraestructura in situ menor.

La variante más común es la conocida como **nube pública (public cloud)**, en la que empresas proveedoras de servicios en la nube como Google Drive o Box ofrecen un espacio de almacenamiento en la nube listo para usar, aunque a cambio establecen sus propias medidas de seguridad. No obstante, quien prefiera tener un mayor control sobre sus datos suele decantarse bien por una nube privada (privatecloud) o por una nube híbrida (hybrid cloud), que se configuran respectivamente con completa o parcial independencia de las entidades proveedoras públicas.

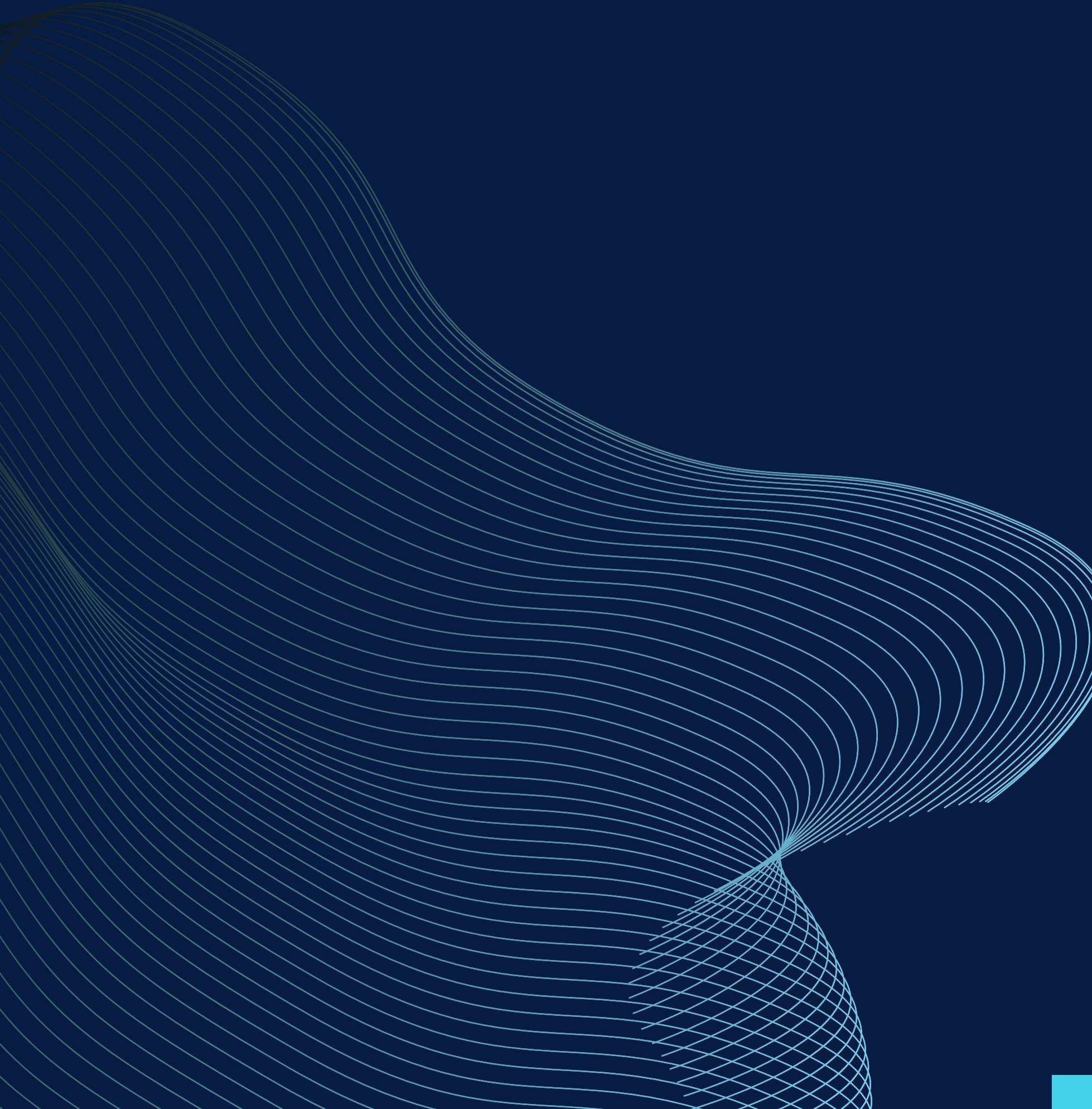
De este modo, las personas usuarias disponen de un mayor control sobre las medidas de seguridad, aunque al mismo tiempo se les exige un mayor esfuerzo técnico.

Principalmente, son las empresas las que, por motivos de protección de datos y seguridad, optan por estas soluciones, aunque con un software con ownCloud, las personas usuarias también pueden crear una nube gestionada por ellos mismos.

Dado que cada vez es mayor la información que circula por los servicios en la nube, surgen inevitablemente con más frecuencia cuestiones relativas a la seguridad. **¿Cuál es la mejor forma de protección de la información en la nube tanto para empresas como para particulares?**

A lo largo de esta Guía Didáctica, se explican los riesgos a los que se puede exponer la información con objeto de aclarar los aspectos a los que hay que prestar especial atención. Asimismo, se presentan diferentes métodos para poder usar todos los tipos de servicios en la nube de forma segura.



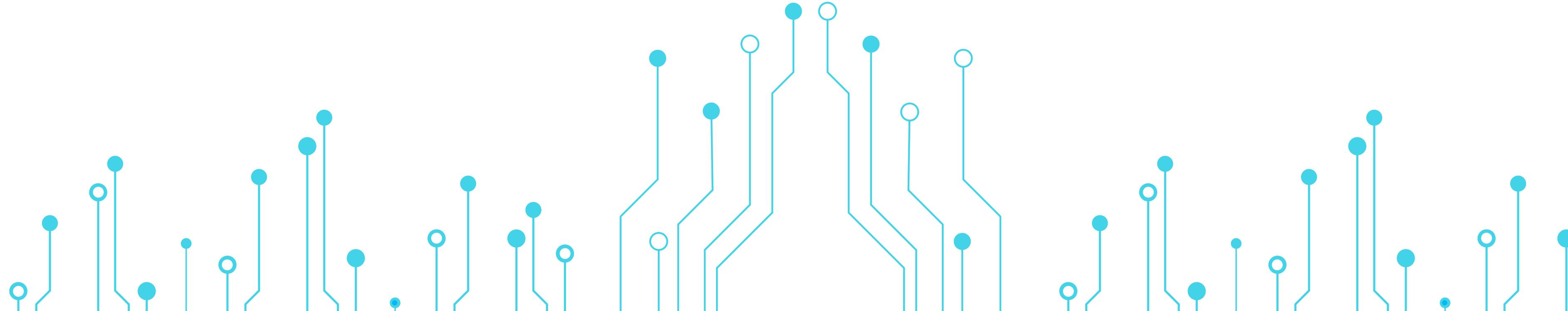


Definición de Seguridad en la Nube

La nube ya no es una nueva tecnología, sino un nuevo modelo de suministro de información y servicios que utilizan, hoy en día, las tecnologías existentes que utiliza la infraestructura de Internet para permitir la comunicación entre los servicios y aplicaciones del lado de la clientela y del lado del servidor

De este modo, la nube proporciona una capa de abstracción entre los recursos informáticos y la arquitectura de bajo nivel implicada. Las personas autónomas trabajadoras y/o personas emprendedoras, no son propietarias de la infraestructura física real, sino que se limitan a pagar una cuota de suscripción y la empresa proveedora de servicios en la nube les da acceso a los recursos y la infraestructura de la nube. Un concepto clave es que las personas usuarias pueden reducir el gasto en hosting.

Así, la nube se ha convertido en una tendencia entre los servicios más utilizados, por lo que es primordial reconocer cuáles son los desafíos de seguridad. Junto a la nube, los términos "transformación digital" y "migración hacia la nube", se han utilizado regularmente en entornos empresariales durante los últimos años. Si bien ambas frases pueden significar cosas diferentes, cada una está impulsada por un denominador común: **la necesidad de cambio**.



A medida que las empresas adoptan estos conceptos y avanzan hacia la optimización de su enfoque operativo, nuevos desafíos aparecen al tratar de equilibrar los niveles de productividad y seguridad.

Si bien las tecnologías más modernas ayudan a las empresas a desarrollar capacidades fuera de los límites de la infraestructura local, la transición principalmente hacia entornos basados en la nube puede tener varias implicaciones si no se realiza de manera segura.

Lograr el equilibrio adecuado requiere comprender cómo las empresas y, en especial, las personas trabajadoras autónomas y/o personas emprendedoras, pueden beneficiarse del uso de tecnologías de nube interconectadas mientras implementan las mejores prácticas de seguridad.

La seguridad en la nube es una disciplina de la ciberseguridad dedicada a asegurar los sistemas informáticos en la nube. Incluye mantener los datos privados y seguros a través de la infraestructura, las aplicaciones y las plataformas en línea. Asegurar estos sistemas implica los esfuerzos de las empresas proveedoras de la nube y de las personas trabajadoras autónomas que los utilizan, bien se trate de una persona física o jurídica, una pequeña o mediana empresa o una organización.





Las empresas proveedoras de servicios en la nube alojan los servicios en sus servidores a través de conexiones de Internet siempre activas. Debido a que su negocio depende de la confianza de la clientela, se utilizan métodos de seguridad en la nube para que los datos se mantengan privados y almacenados de forma segura. No obstante, la seguridad en la nube también está parcialmente en manos de las personas trabajadoras autónomas. Comprender ambas facetas es fundamental para una solución saludable de seguridad en la nube.

En su núcleo, la seguridad en la nube se compone de las siguientes categorías:

- ▪ Seguridad los datos.
- ▪ Gestión de identidades y accesos (IAM, por sus siglas en inglés).
- ▪ Gobernanza (políticas de prevención, detección y mitigación de amenazas).
- ▪ Planificación de la retención de datos (DR) y la continuidad del negocio (BC).
- ▪ Cumplimiento legal.

La seguridad en la nube puede parecer como la seguridad informática heredada, pero esta plataforma exige en realidad un enfoque diferente. Antes de profundizar en el tema, se procede a definir qué es la seguridad en la nube.

Definición de Seguridad en la Nube

La seguridad en la nube es toda la tecnología, los protocolos y las buenas prácticas que protegen los entornos informáticos en la nube, las aplicaciones que se ejecutan en la nube y los datos almacenados en ella.

La seguridad de los servicios en la nube comienza por comprender qué se está asegurando exactamente, así como los aspectos del sistema que se deben administrar. A modo de resumen, el desarrollo del soporte contra las vulnerabilidades de seguridad está en gran medida en manos de las empresas proveedoras de servicios en la nube.

A parte de elegir una empresa proveedora consciente de la seguridad, las personas trabajadoras autónomas deben centrarse sobre todo en la configuración adecuada del servicio y en los hábitos de uso seguro. Además, deben asegurarse de que el hardware y las redes de las personas usuarias finales estén debidamente asegurados.



El alcance total de la seguridad en la nube está diseñado para proteger lo siguiente, independientemente de sus responsabilidades:

Redes físicas Enrutadores, energía eléctrica, cableado, controles de clima, etc.	Almacenamiento de datos Discos duros, NAS, etc.	Servidores de datos Hardware y software informáticos de la red central.	Plataformas de virtualización de equipos informáticos Software de máquinas virtuales, máquinas anfitrionas y máquinas invitadas.	Sistemas operativos (OS) Software que soporta todas las funciones informáticas.
Middleware Gestión de la interfaz de programación de aplicaciones (API).	Entornos de ejecución Ejecución y mantenimiento de un programa en ejecución.	Datos Toda la información almacenada, modificada y a la que se ha accedido.	Aplicaciones Servicios tradicionales de software (correo electrónico, software de impuestos, paquetes de productividad, etc.).	Hardware de usuario final Ordenadores, dispositivos móviles, dispositivos de Internet de las cosas (IoT), etc.

Con la informática en la nube, la propiedad de estos componentes puede variar ampliamente. Esto puede hacer que no esté claro el alcance de las responsabilidades de seguridad de la persona trabajadora autónoma y/o persona emprendedora. Dado que, asegurar la nube puede parecer diferente, en función de quién tiene autoridad sobre cada componente, es importante entender cómo se suelen agrupar.

Para simplificar, los componentes informáticos en la nube están asegurados desde dos puntos de vista principales:



Los tipos de servicios en la nube son servicios ofrecidos por empresas proveedoras externas como módulos utilizados para crear el entorno de la nube.

Dependiendo del tipo de servicio, se puede gestionar un grado diferente de los componentes dentro del servicio:



El núcleo de cualquier servicio de la nube implica que la empresa proveedora administre la red física, el almacenamiento de datos, los servidores de datos y las plataformas de virtualización de los ordenadores. El servicio se almacena en los servidores de la empresa proveedora y se virtualiza a través de su red administrada internamente para entregarse a la clientela para su acceso remoto. Esto transfiere los costes de hardware y otras infraestructuras para proporcionar a la clientela acceso a sus necesidades informáticas desde cualquier lugar a través de su conexión a Internet.





Los servicios en la nube de software como servicio (SaaS) proporcionan acceso a aplicaciones que están puramente alojadas y se ejecutan en los servidores de la empresa proveedora. Éstas administran las aplicaciones, los datos, el tiempo de ejecución, el middleware y el sistema operativo. Las personas trabajadoras autónomas y/o personas emprendedoras, solamente se encargan de obtener y utilizar las aplicaciones. Algunos ejemplos de SaaS incluyen Google Drive, Slack, Salesforce, Microsoft 365, Cisco WebEx y Evernote.



Los servicios en la nube de plataforma como servicio proporcionan un host para el desarrollo de sus propias aplicaciones, que se ejecutan dentro del propio espacio “sandbox” de la clientela en los servidores de la empresa proveedora, quiénes administran el tiempo de ejecución, el middleware y el sistema operativo. Las personas trabajadoras autónomas se encargan de gestionar sus aplicaciones, datos, acceso de usuarios, dispositivos de personas usuarias finales y redes. Algunos ejemplos de PaaS incluyen Google App Engine y Windows Azure.





Los servicios en la nube de infraestructura como servicio (IaaS) ofrecen hardware y plataformas de conectividad remota para alojar la mayor parte de sus tareas informáticas, incluido el sistema operativo. Las empresas proveedoras solo administran los servicios básicos en la nube. Las personas trabajadoras autónomas se encargan de asegurar todo lo que se apila en un sistema operativo, incluidas las aplicaciones, los datos, los tiempos de ejecución, el middleware y el propio sistema operativo. Además, deben gestionar el acceso de las personas usuarias, su dispositivos finales y las redes. Algunos ejemplos de IaaS incluyen Microsoft Azure, Google Compute Engine (GCE) y Amazon Web Services (AWS).



2

Los entornos de la nube son modelos de implementación en los que uno o más servicios en la nube crean un sistema para las personas usuarias finales y las empresas.

Estos segmentan las responsabilidades de gestión, incluida la seguridad, entre las personas trabajadoras autónomas y las empresas proveedoras.

Los entornos de la nube que se utilizan, en la actualidad, son:



Entornos de nubes públicas, compuestos por servicios en la nube de varias personas usuarias en los que se comparte los servidores con otras personas, empresas y/o proyectos, como un edificio de oficinas o un espacio de trabajo. Se trata de servicios dirigidos por la empresa proveedora para dar acceso a través de la web.



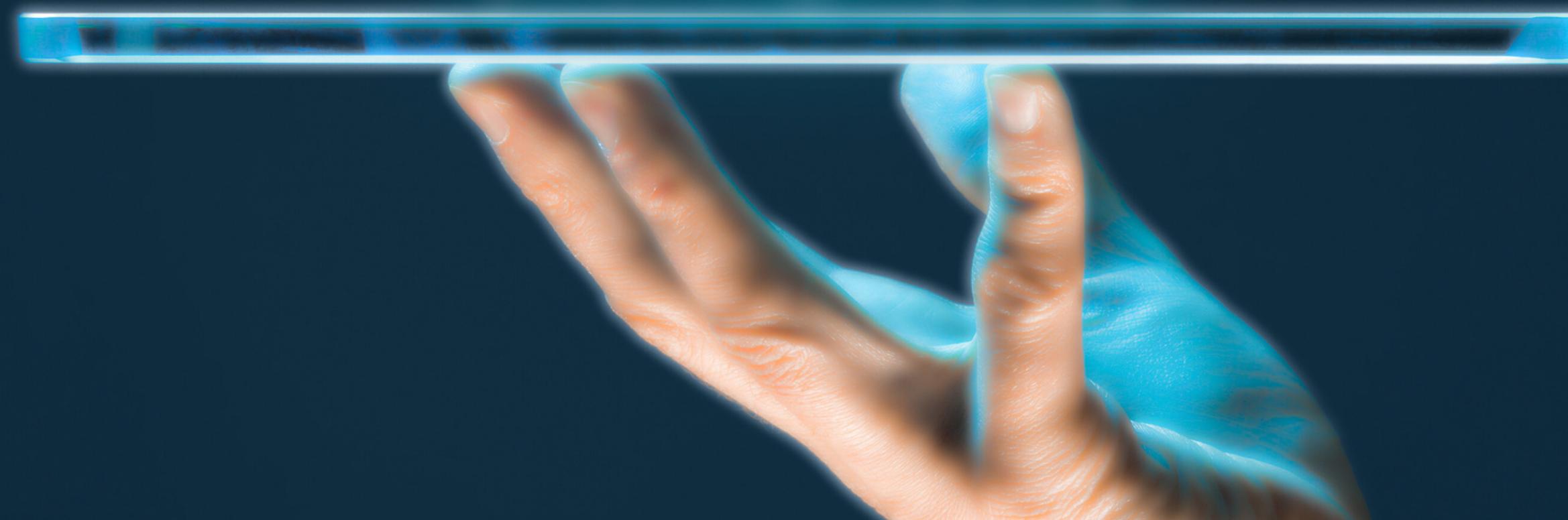
Entornos de nubes privadas, que se basan en el uso de un servicio en la nube que proporciona el uso exclusivo de su propia nube. Estos entornos de una sola persona usuaria normalmente son propiedad de una empresa proveedora externa, y se administran y operan fuera del sitio.



Entornos de nubes híbridas, que consisten en el uso de una combinación de nube privada o centro de datos de nubes privadas in situ con una o más nubes públicas.



Al enfocarlo desde esta perspectiva, se entiende que la seguridad basada en la nube puede ser un poco diferente según el tipo de espacio de nubes en el que trabajan las personas usuarias. No obstante, los efectos se sienten en las empresas.





**¿Cómo funciona
la Seguridad
en la Nube?**



Existe una variedad de tecnologías, políticas y procesos que la empresa proveedora de la nube debe utilizar para garantizar la seguridad de los datos en la nube. La persona autónoma trabajadora debe considerar aquellos que basan su política y procedimientos de seguridad en estándares de seguridad internacionales universalmente aceptados, como ISO 27001 y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), y considere los requisitos de los marcos normativos locales relacionados, tales como el Reglamento General de Protección de Datos de Europa (GDPR, por sus siglas en inglés) y la HIPAA.

Recomendaciones de otras tecnologías y procedimientos que las pymes deben seguir y/o buscar en una empresa proveedora en la nube son:



Cifrado de archivos.

Debe cifrar sus datos, incluso antes de enviarlos a la nube, con un cifrado sólido AES-256 aprobado por el gobierno. Su empresa configura el cifrado y sólo las personas usuarias autorizadas pueden acceder a él. La empresa proveedora de la nube no debería poder ver los datos porque los datos están almacenados en un almacenamiento cifrado en la nube.



Comunicaciones seguras.

Los metadatos deben estar encriptados y todas las comunicaciones de administración entre los sistemas y la nube de la empresa proveedora deben ejecutarse a través de canales seguros con encriptación SSL. Esto significa que, en cualquier momento, todos los aspectos de sus datos están seguros.



Firewall de aplicaciones web.

La empresa proveedora debe usar un Firewall de Aplicaciones Web (WAF, por sus siglas en inglés), que incluye protección instantánea contra inyección SQL, secuencias de comandos entre sitios, acceso no autorizado a recursos, inclusión de archivos remotos y otras amenazas de Seguridad de Aplicaciones Web Abiertas (OWASP, por sus siglas en inglés).





Disponibilidad del centro de datos.

La infraestructura de la empresa proveedora de la nube debe cumplir con los SLA de alta disponibilidad, manteniendo una infraestructura redundante para minimizar el tiempo de inactividad y eliminar los puntos únicos de fallo.



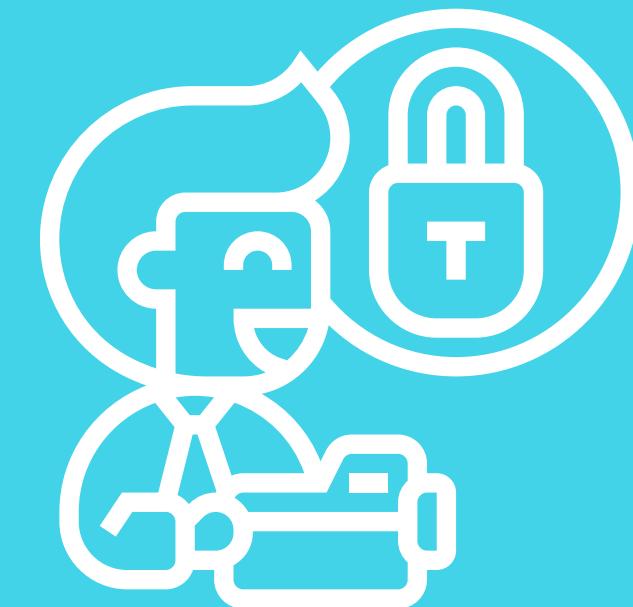
Copias de seguridad periódicas.

La empresa proveedora de la nube debe ejecutar copias de seguridad en un horario acordado, regularmente, para asegurarse que sus datos estén protegidos debido a una interrupción importante.



Mejores prácticas profesionales.

La empresa proveedora también debe haber implementado políticas estrictas de confidencialidad, ética comercial y código de conducta para todas las personas de la empresa, incluidas verificaciones de antecedentes cuando corresponda, acuerdos de no divulgación y principios de segregación de deberes, necesidad de saber y acceso con privilegios mínimos para proteger contra actos maliciosos o inadvertidamente peligrosos por parte de personas con información privilegiada. Los estrictos controles de acceso, la autenticación de múltiples factores y el registro de actividad ubicuo garantizan solo el acceso adecuado a los sistemas sensibles.





**¿Qué hace que la
Seguridad en la Nube
sea diferente?**

La seguridad informática tradicional ha experimentado una inmensa evolución debido al cambio a la informática basada en la nube. Si bien los modelos de la nube permiten una mayor comodidad, la conectividad siempre activa requiere nuevas consideraciones para mantenerlas seguras. La seguridad en la nube, como una solución de ciberseguridad modernizada, se distingue de los modelos informáticos heredados en algunos aspectos.

Almacenamiento de datos

La mayor distinción es que los modelos antiguos de IT dependían en gran medida del almacenamiento de datos in situ. Las personas trabajadoras autónomas han descubierto, desde hace mucho tiempo, que la creación de todas las plataformas informáticas internas para los controles de seguridad detallados y personalizados es costosa y rígida. Las plataformas basadas en la nube han ayudado a transferir los costes de desarrollo y mantenimiento de los sistemas, pero también a eliminar cierto control de las personas usuarias.



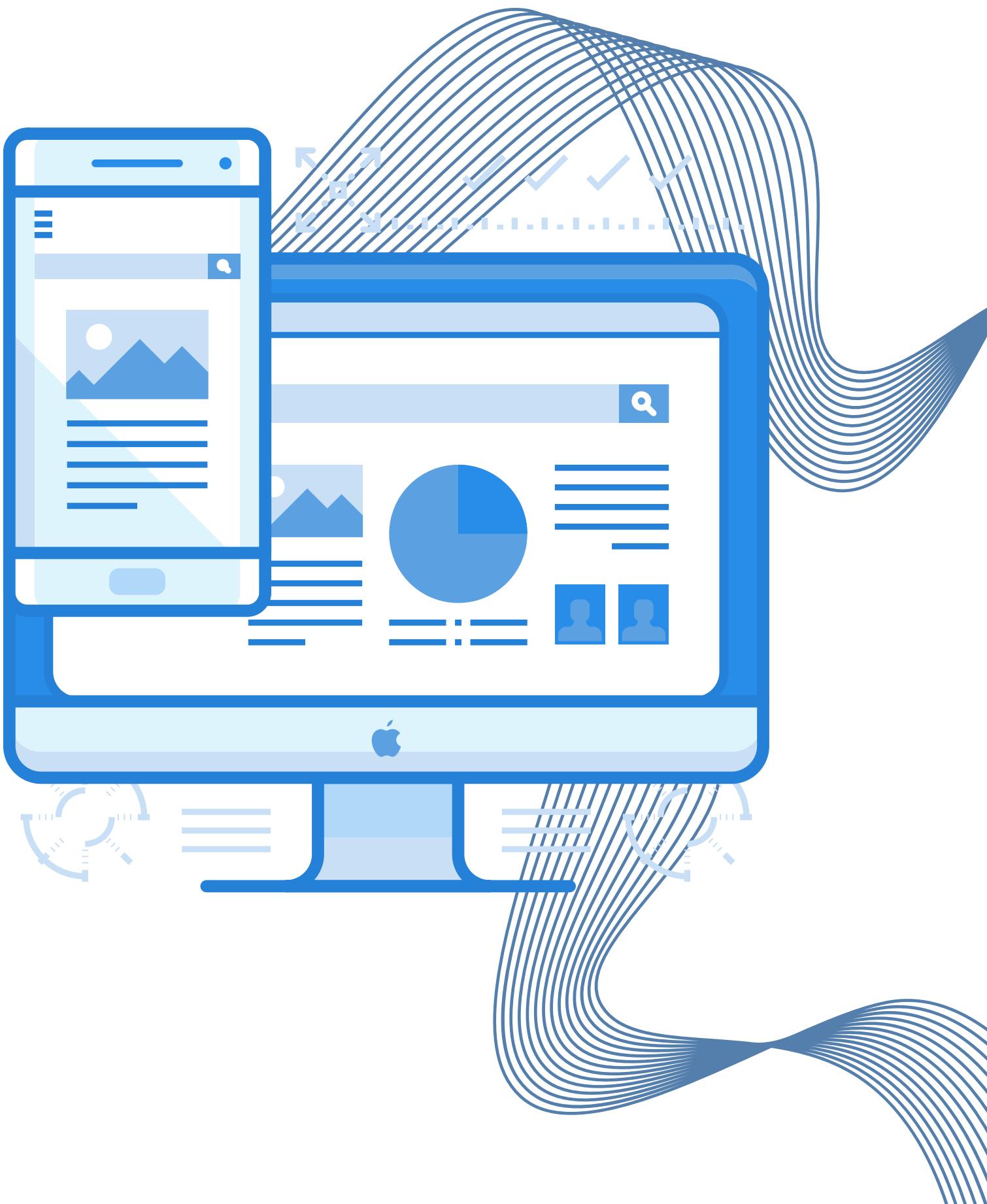
Velocidad de escalada

De manera similar, la seguridad en la nube exige una atención única al escalar los sistemas de IT de la empresa. La infraestructura y las aplicaciones centradas en la nube se movilizan rápidamente. Si bien esta capacidad mantiene los sistemas uniformemente ajustados a los cambios empresariales, también plantea problemas cuando la necesidad de mejoras y comodidad supera su capacidad para mantenerse al día en materia de seguridad.



Interfaz del sistema de personas usuarias finales

Tanto para las empresas como para las personas usuarias individuales, los sistemas de nubes también se conectan con muchos otros sistemas y servicios que se deben asegurar. Los permisos de acceso deben mantenerse desde el nivel de dispositivo hasta el nivel de software e incluso el nivel de red. Además, tanto empresas proveedoras como personas usuarias deben estar atentos a las vulnerabilidades que pueden causar a través de comportamientos de configuración y acceso al sistema inseguros.



Proximidad a otros datos y sistemas en red

Dado que los sistemas en la nube son una conexión persistente entre las empresas proveedoras de la nube y todas las personas usuarias, esta importante red puede comprometer incluso a la propia empresa proveedora. En los entornos de redes, un solo dispositivo o componente débil se puede explotar para infectar al resto. Las empresas proveedoras de la nube se exponen a las amenazas de muchas personas usuarias finales con los que interactúan, bien sea que estén proporcionando almacenamiento de datos u otros servicios. Las responsabilidades adicionales en materia de seguridad de la red recaen en las empresas proveedoras cuyos productos entregados de otro modo se basarán, exclusivamente, en los sistemas de los usuarios finales y no en los propios.

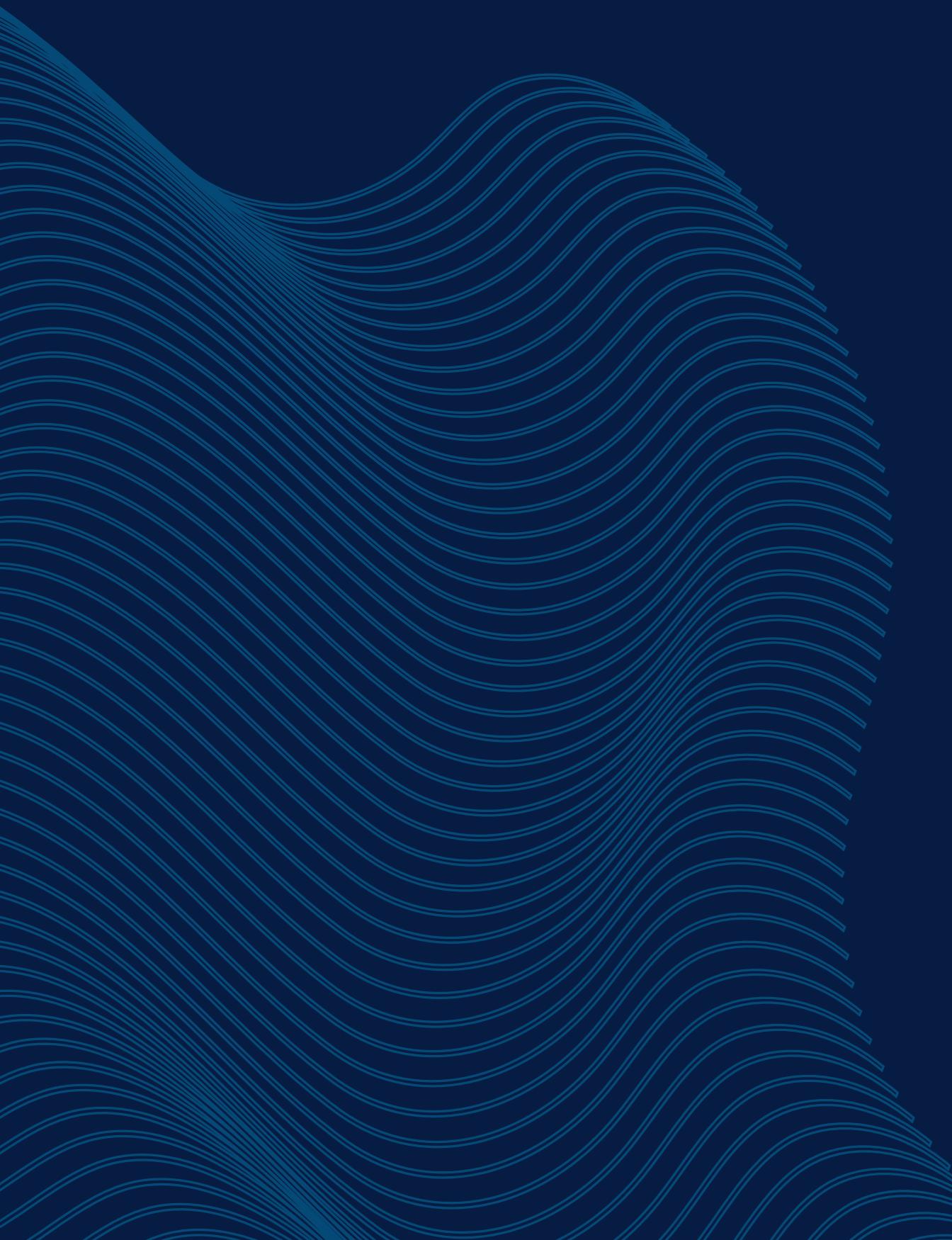


Resolver la mayoría de los problemas de seguridad en la nube

Esto significa que, tanto las personas usuarias como las empresas proveedoras de la nube, tanto en entornos personales como en empresariales, deben ser proactivos en cuanto a sus propias funciones en la ciberseguridad. Este doble enfoque significa que ambas partes deben abordar lo siguiente:

- Configuración y mantenimiento seguros del sistema.
- Educación sobre seguridad de la persona usuaria, tanto a nivel de comportamiento como a nivel técnico.
- Las empresas proveedoras y las personas usuarias de la nube deben tener transparencia y responsabilidad para garantizar que ambas partes estén seguras.





Riesgos de Seguridad en la Nube



El Cloud computing continúa transformando la forma en que las pymes utilizan, almacenan y comparten datos, aplicaciones y cargas de trabajo, pero también conlleva nuevas amenazas y desafíos de seguridad. Con tantos datos entrando en la nube y en los servicios de nube pública en particular, estos recursos se convierten en objetivos para actos malintencionados.

El volumen de utilización de la nube pública está creciendo rápidamente, por lo que inevitablemente conduce a un mayor cuerpo de cosas sensibles que potencialmente están en riesgo.

Contrariamente a lo que muchas personas podrían pensar, la principal responsabilidad de proteger los datos corporativos en la nube no recae en la empresa proveedora de servicios, sino en quien utiliza la nube, la persona autónoma trabajadora. Estamos en un período de transición de seguridad en la nube en el que el enfoque está cambiando. Para identificar las principales preocupaciones, expertos de la industria consideran que los principales problemas de seguridad en la nube, clasificados en orden de gravedad son:

1. Violaciones de datos.

Las infracciones pueden causar un gran daño financiero y en la reputación. Pueden resultar potencialmente, en pérdidas de propiedad intelectual y responsabilidades jurídicas significativas. Las principales amenazas de violación de datos incluyen:



El objetivo principal de un ciberataque se centra en el robo de datos, por lo que las personas trabajadoras autónomas y/o personas emprendedoras, deben definir el valor de sus datos y el impacto de su pérdida.

¿Quién tiene acceso a los datos?, es una pregunta clave para resolverlos.

Los datos accesibles a Internet son los más vulnerables a la mala configuración o explotación.

El cifrado puede proteger los datos, pero con una compensación en el rendimiento y la experiencia del usuario.

Las personas trabajadoras autónomas necesitan planes de respuesta a incidentes robustos y probados que tomen en cuenta a las empresas proveedoras de servicios en la nube.

2. Configuración incorrecta y control inadecuado de cambios.

Esta es una amenaza que no sorprende al ser muchas las empresas que exponen datos accidentalmente a través de la nube. No es sólo la pérdida de datos de los que las empresas tienen que preocuparse, sino la eliminación o modificación de recursos hechos con la intención de interrumpir el negocio. Las malas prácticas de control de cambios y los errores de configuración incorrecta son algunas de las causas.

La configuración incorrecta y el control inadecuado de cambios incluyen:



- La complejidad de los recursos basados en la nube los hace difíciles de configurar.
- No esperar a que los controles tradicionales y los enfoques de administración de cambios sean eficaces en la nube.
- Utilizar la automatización y las tecnologías que analizan continuamente en busca de recursos mal configurados.

3. Falta de arquitectura y estrategia de seguridad en la nube.

Este problema es tan antiguo como la nube. El deseo de minimizar el tiempo necesario para migrar sistemas y datos a la nube suele tener prioridad sobre la seguridad.

La falta de arquitectura y estrategia de seguridad en la nube incluyen:

- La arquitectura de seguridad debe alinearse con los objetivos y objetivos empresariales.
- Desarrollar e implementar un marco de arquitectura de seguridad.
- Mantener los modelos de amenazas actualizados.
- Implementar la capacidad de supervisión continua.



4. Identidad insuficiente, credencial, acceso y gestión de claves.

Otra amenaza es la gestión y el control inadecuados del acceso en torno a datos, sistemas y recursos físicos, como salas de servidores y edificios. La nube requiere que las personas trabajadoras autónomas cambien prácticas relacionadas con la administración de identidades y accesos (IAM). Las consecuencias de no hacerlo, podrían dar lugar a incidencias de seguridad y violaciones causadas por:

- Credenciales insuficientemente protegidas.
- Falta de rotación automatizada de claves criptográficas, contraseñas y certificados.
- Falta de escalabilidad.
- Falta de uso de la autenticación multifactor.
- Falta de uso de contraseñas seguras.

La identidad insuficiente, la credencial, el acceso y la administración de claves incluyen:

- Cuentas seguras, incluido el uso de la autenticación de dos factores.
- Utilizar controles estrictos de identidad y acceso para personas usuarias e identidades en la nube.
- Segregar y segmentar cuentas, nubes privadas virtuales y grupos de identidades en función de las necesidades y el principio de privilegios mínimos.
- Adoptar un enfoque programático y centralizado para la rotación de claves.
- Quitar las credenciales no utilizadas y los privilegios de acceso.

5. Secuestro de cuentas.

El secuestro de cuentas sigue siendo la quinta mayor amenaza en la nube. A medida que los intentos de phishing se vuelven más eficaces y dirigidos, el riesgo de una persona atacante obtenga acceso a cuentas con privilegios elevados es significativo. El phishing no es la única manera en que un ciberataque puede obtener credenciales. También pueden adquirirlos comprometiendo el propio servicio en la nube a robarlos a través de otros medios.



Una vez que se produzca un ataque y consiga entrar en el sistema utilizando una cuenta legítima, puede causar una gran cantidad de interrupción, incluyendo robo o destrucción de datos importantes, detener la prestación de servicios o fraude financiero.

Con respecto al secuestro de cuentas incluyen:

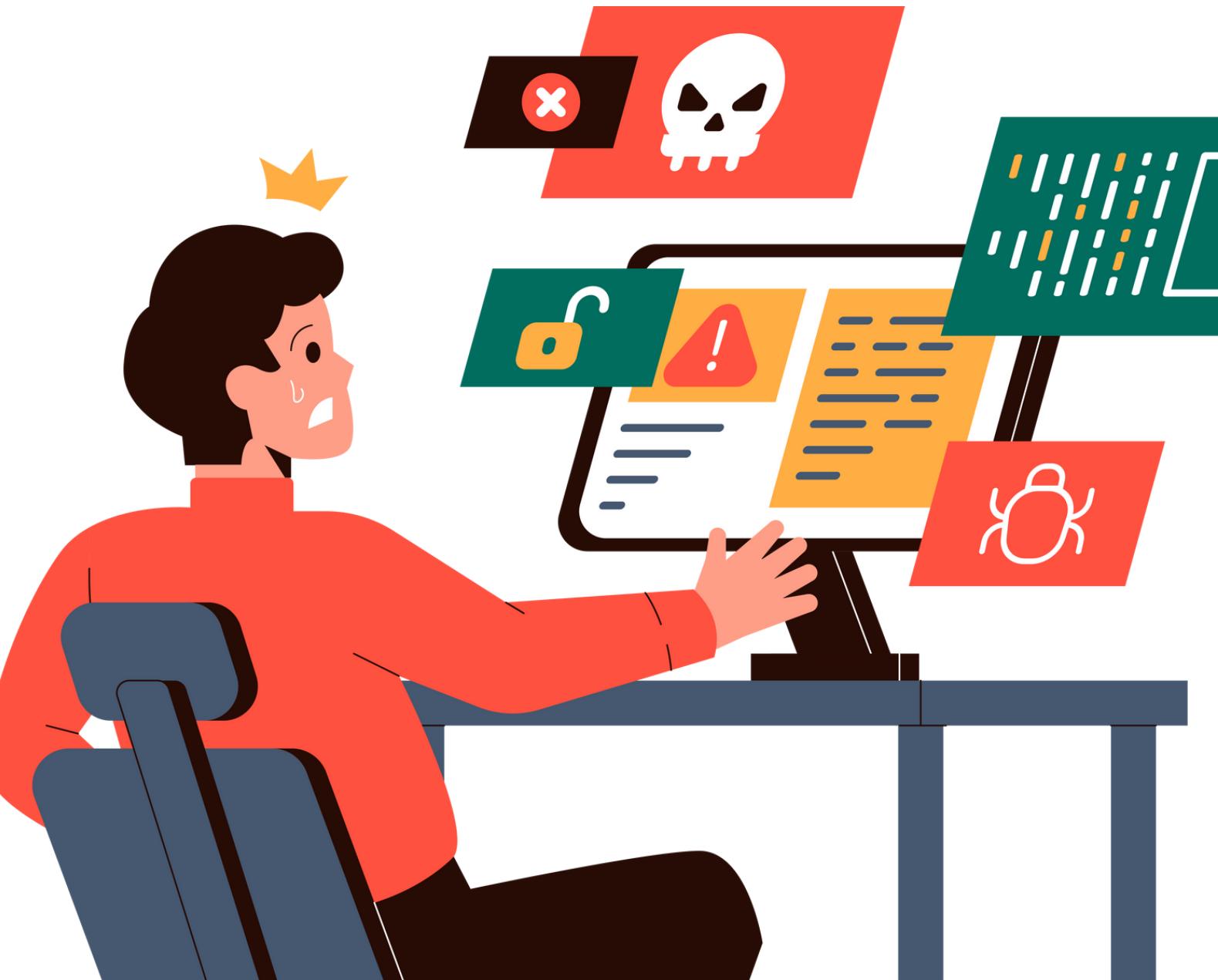
- No solo se realiza un restablecimiento de contraseña cuando se roban las credenciales de la cuenta.
- Un enfoque de defensa en profundidad y controles de control de acceso fuertes son la mejor defensa.

6. Amenazas internas.

Las amenazas son tan graves en la nube como con los sistemas locales. Quien realice el ataque pueden ser parte del personal actual y/o anterior, contratistas o alguien de confianza y/o cualquier persona que no tenga que romper las defensas de una empresa para acceder al sistema.

Las principales conclusiones con respecto a las amenazas internas incluyen:

- Llevar a cabo la capacitación y la formación de las personas trabajadoras autónomas y/o personas emprendedoras sobre las prácticas adecuadas para proteger los datos y los sistemas. Hacer de la formación un proceso continuo.
- Auditarse y corregir regularmente servidores en la nube mal configurados.
- Restringir el acceso a sistemas críticos.



7. Interfaces y API inseguras.



Las interfaces inseguras y las API son un vector de ataque común. Especialmente, cuando se asocia con interfaces, las vulnerabilidades de API pueden dar a quien ataque una ruta clara para robar credenciales de acceso.

Las principales conclusiones con respecto a las interfaces y API inseguras incluyen:

- Emplear buenas prácticas de API, como la supervisión de artículos como inventario, pruebas, auditorías y protecciones anormales de la actividad.
- Proteger las claves de API y evitar la reutilización.
- Considerar la posibilidad de un marco de API abierto, como la interfaz de computación en la nube abierta (OCCI) o la interfaz de administración de infraestructura en la nube (CIMI).

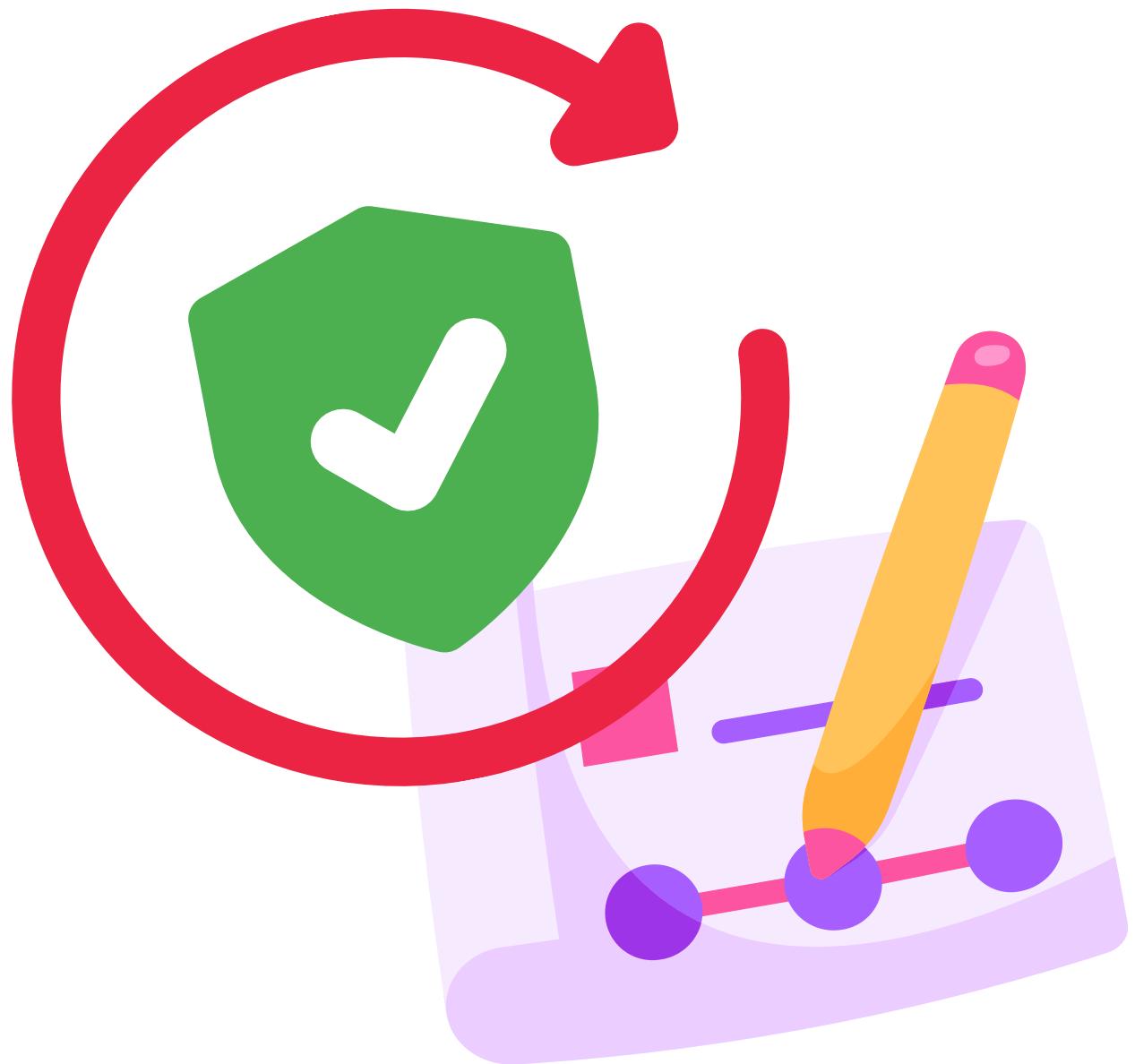
8. Plano de control débil.

Un plan de control abarca los procesos de duplicación de datos, migración y almacenamiento. El plano de control es débil si la persona a cargo de estos procesos, no tiene control total sobre la lógica, la seguridad y la verificación de la infraestructura de datos.

Estas personas encargadas de su control, deben comprender la configuración de seguridad, cómo fluyen los datos y las cegueras arquitectónicas detectan brechas de seguridad o debilidades. Si no se realiza, podría producirse una filtración de datos, la indisponibilidad de los datos o la corrupción de datos.

Las principales conclusiones con respecto a un plan de control débil incluyen:

- Asegurar que la empresa proveedora de servicios en la nube ofrezca los controles de seguridad necesarios para cumplir con las obligaciones legales y legales.
- Realizar la debida diligencia para garantizar que la empresa proveedora de servicios en la nube posea un plan de control adecuado.



9. Fallos en la metaestructura y la estructura de aplicaciones.

La metaestructura de una empresa proveedora de servicios en la nube contiene información de seguridad sobre cómo protege los sistemas y divulga esa información a través de llamadas a la API. Las API ayudan a detectar el acceso no autorizado, pero también contienen información muy sensible, como registros o datos del sistema de auditoría.

Esta línea también es un punto potencial de fallo que podría dar a quienes ataquen el acceso a los datos. La implementación deficiente de la API suele ser la causa de una vulnerabilidad. Por otro lado, es posible que no entiendan cómo implementar correctamente las aplicaciones en la nube. Esto es particularmente cierto cuando conectan aplicaciones que no estaban diseñadas para entornos en la nube.

Las principales conclusiones con respecto a los fallos de metaestructura y aplicación incluyen:

- Asegurar que la empresa proveedora de servicios en la nube ofrezca visibilidad.
- Implementar las características y controles adecuados en diseños originarios de la nube.
- Asegurar que la empresa proveedora de servicios en la nube realice pruebas y proporcione hallazgos a las empresas.



10. Visibilidad limitada del uso de la nube.

Una queja común es que un entorno en la nube los hace ciegos a gran parte de los datos que necesitan para detectar y prevenir actividades maliciosas. Este desafío limitado de visibilidad de uso se divide en dos categorías: uso de aplicaciones no autorizadas y uso indebido de aplicaciones sancionadas.



Las aplicaciones no autorizadas son esencialmente shadow IT: Las personas responsables usan aplicaciones sin permiso ni soporte de departamento IT.. Cualquier aplicación que no cumpla con las directrices corporativas de seguridad representa un riesgo que el equipo de seguridad podría desconocer.



El uso indebido de la aplicación sancionada podría ser una persona autorizada que usa una aplicación aprobada con credenciales robadas. Los equipos de seguridad deben ser capaces de distinguir entre personas usuarias válidas e inválidas mediante la detección de comportamientos fuera de norma.

Las principales ventajas con respecto a la visibilidad limitada del uso de la nube incluyen:

Desarrollar un esfuerzo de visibilidad de la nube desde arriba hacia abajo que se vincule a las personas trabajadoras autónomas, los procesos y la tecnología.

Pedir a la persona responsable de seguridad en la nube o al personal de gestión de riesgos que evite todos los servicios en la nube no aprobados.

Implementar un firewall de aplicaciones web para analizar las conexiones entrantes.

Llevar a cabo una capacitación obligatoria en toda la empresa sobre las políticas de uso de la nube aceptadas y la aplicación de la aplicación.

Implementar seguridad de acceso a la nube (CASB) o puertas de enlace definidas por software (SDG) para analizar las actividades de salida.

Implementar un modelo de confianza cero en toda la organización.

11. Abuso y mal uso de los servicios en la nube.

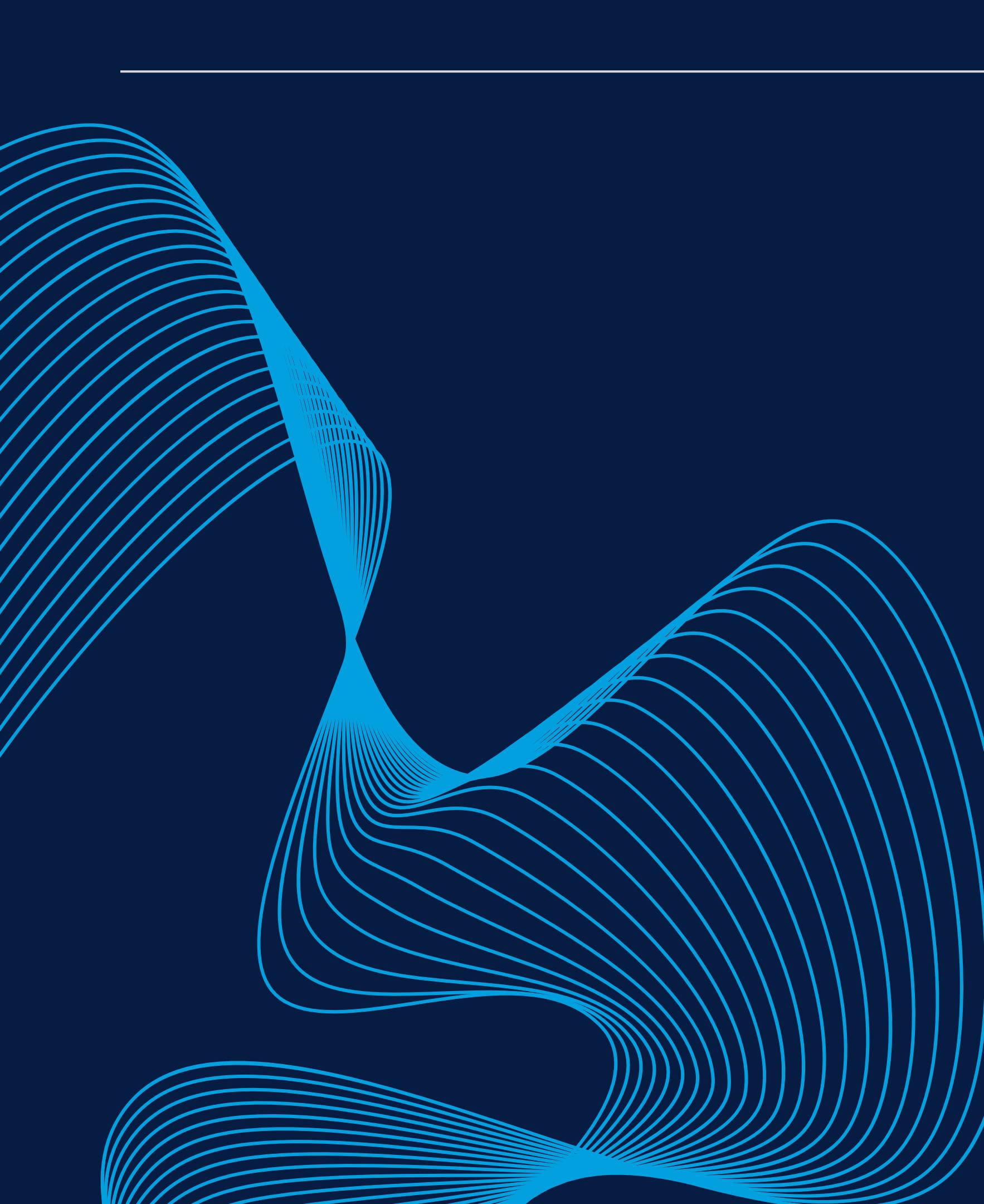
Quienes atacan utilizan cada vez más servicios legítimos en la nube para apoyar sus actividades. Por ello, las empresas proveedoras de servicios en la nube, deben tener detectores para prevenir e identificar abusos como fraude de instrumentos de pago o mal uso de los servicios en la nube.

También es importante que estas empresas proveedoras tengan un marco de respuesta a incidentes para responder al uso indebido y permitir que la clientela denuncie el uso indebido.

Las principales conclusiones con respecto al abuso y el uso indebido de los servicios en la nube incluyen:

- Supervisar el uso de la nube de las personas empleadas con accesos para detectar abusos.
- Emplear soluciones de prevención de pérdida de datos en la nube (DLP) para supervisar y detener la exfiltración de datos.



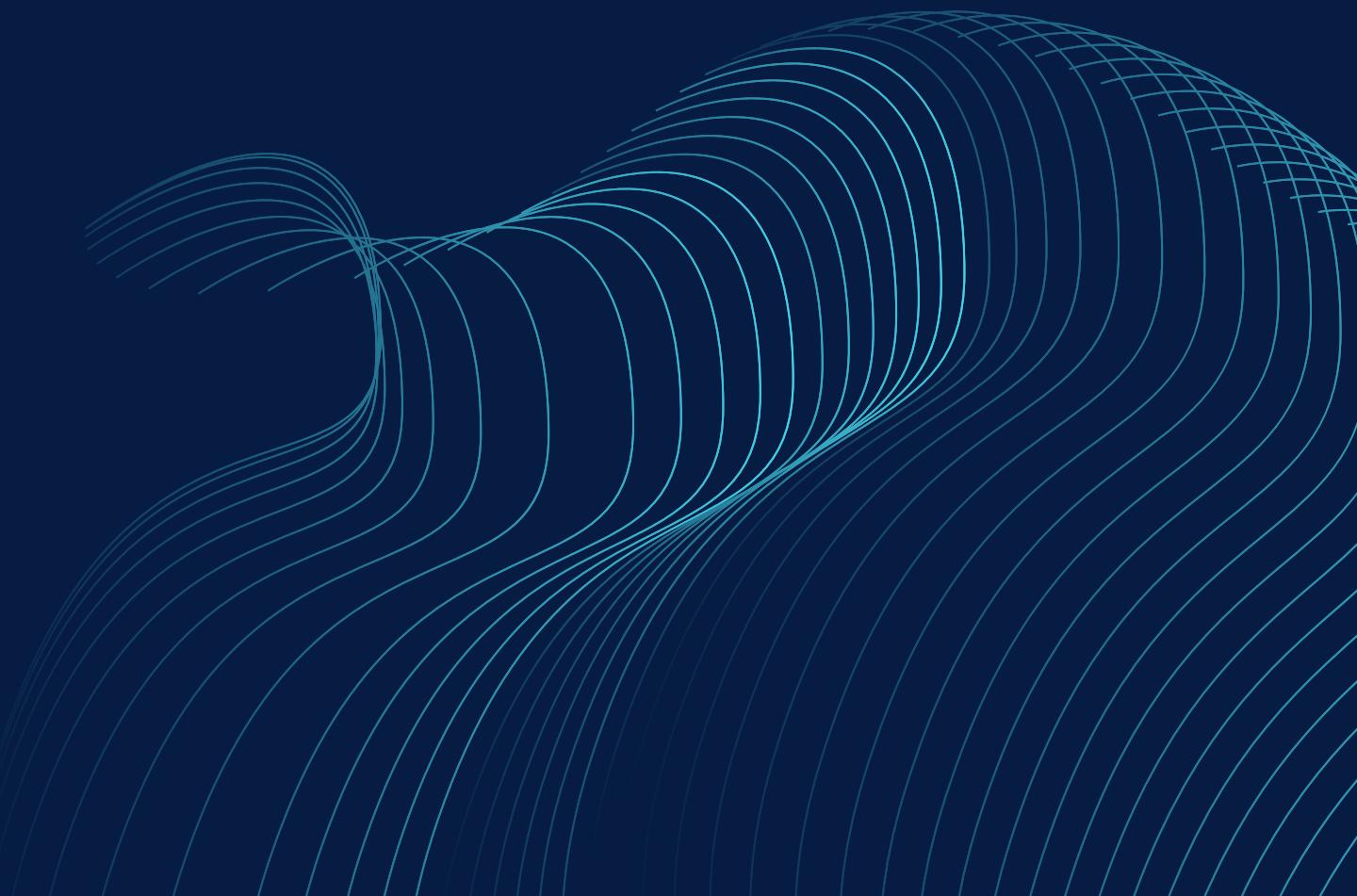


**¿Por qué es
importante la
Seguridad
en la Nube?**

Al igual que, con cualquier tipo de estrategia a considerar en un negocio, el uso de la nube para cualquier persona trabajadora autónoma conlleva riesgos. Aunque, operar en la nube se considera normalmente más segura que la tradicional, hay numerosos casos de hackeos de alto perfil.

La seguridad en la nube ha avanzado enormemente, pero los riesgos persisten a medida que las personas ciberdelincuentes desarrollan nuevas formas de ataque a la red. Las violaciones de datos no siempre son el resultado de una actividad delictiva. También pueden producirse por negligencia o error humano.

Los datos de cualquier negocio o proyecto empresarial también son accesibles sólo a través de la empresa proveedora de servicios en la nube. Si la empresa proveedora tiene problemas con la conectividad a Internet, es posible que no pueda acceder a sus archivos cuando los necesite. Además, con poca o ninguna consideración a la seguridad de los datos en la nube y sin una estrategia de salida para cuando quieras cambiar de CSP, la persona emprendedora se arriesga a la pérdida temporal o permanente de los datos.





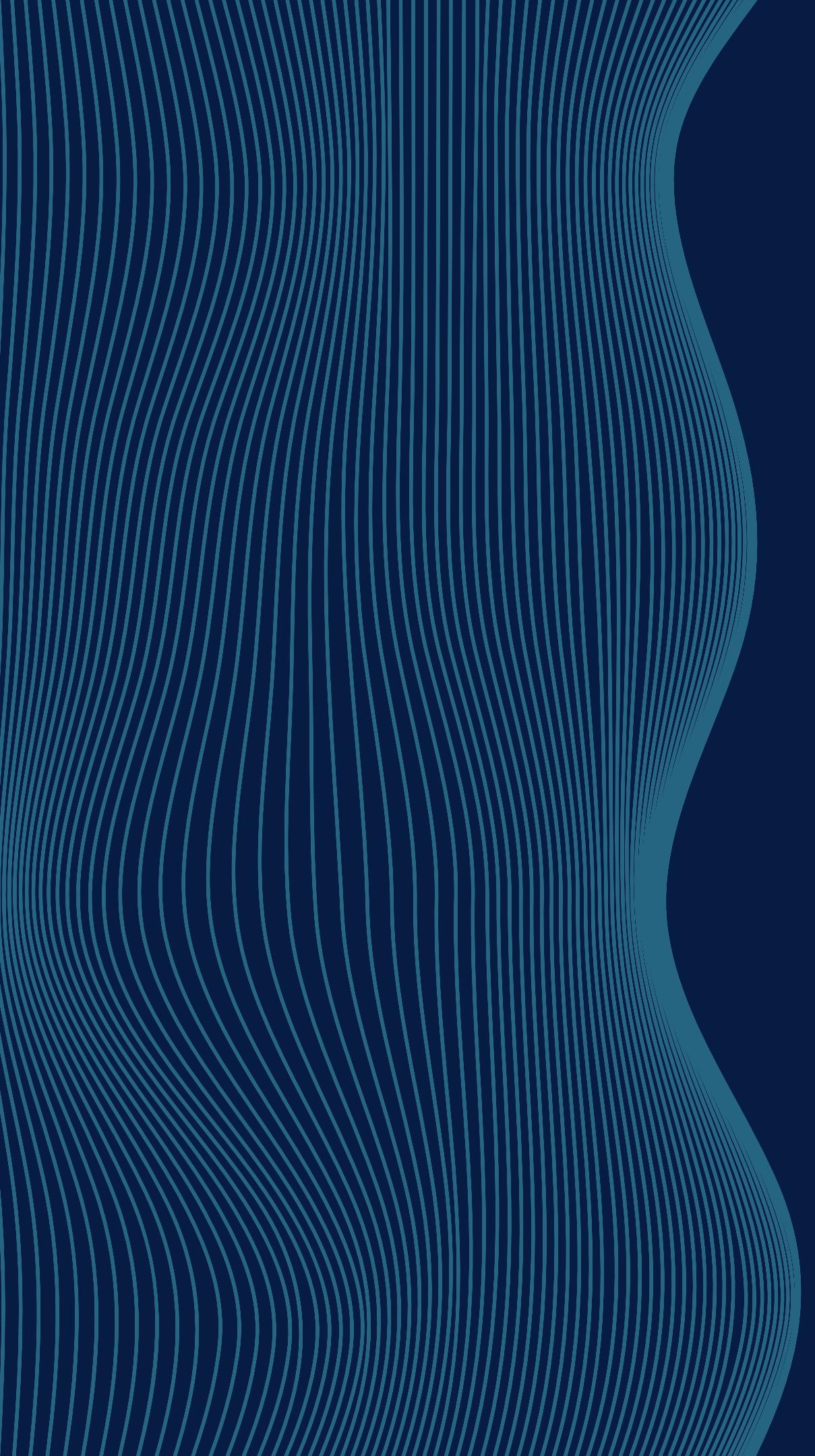
Por estas razones, la importancia de la seguridad en la nube es una de las características más relevantes al momento de decidir migrar los recursos informáticos a este servicio.

La seguridad de la información debe representar una prioridad para la persona trabajadora autónoma, además de la capacidad de almacenar grandes volúmenes de datos de manera integral y confiable. Es por ello, que los servicios ofrecidos en la nube, proveen cada vez mejores garantías en cuanto a la confidencialidad y resistencia a posibles problemas.

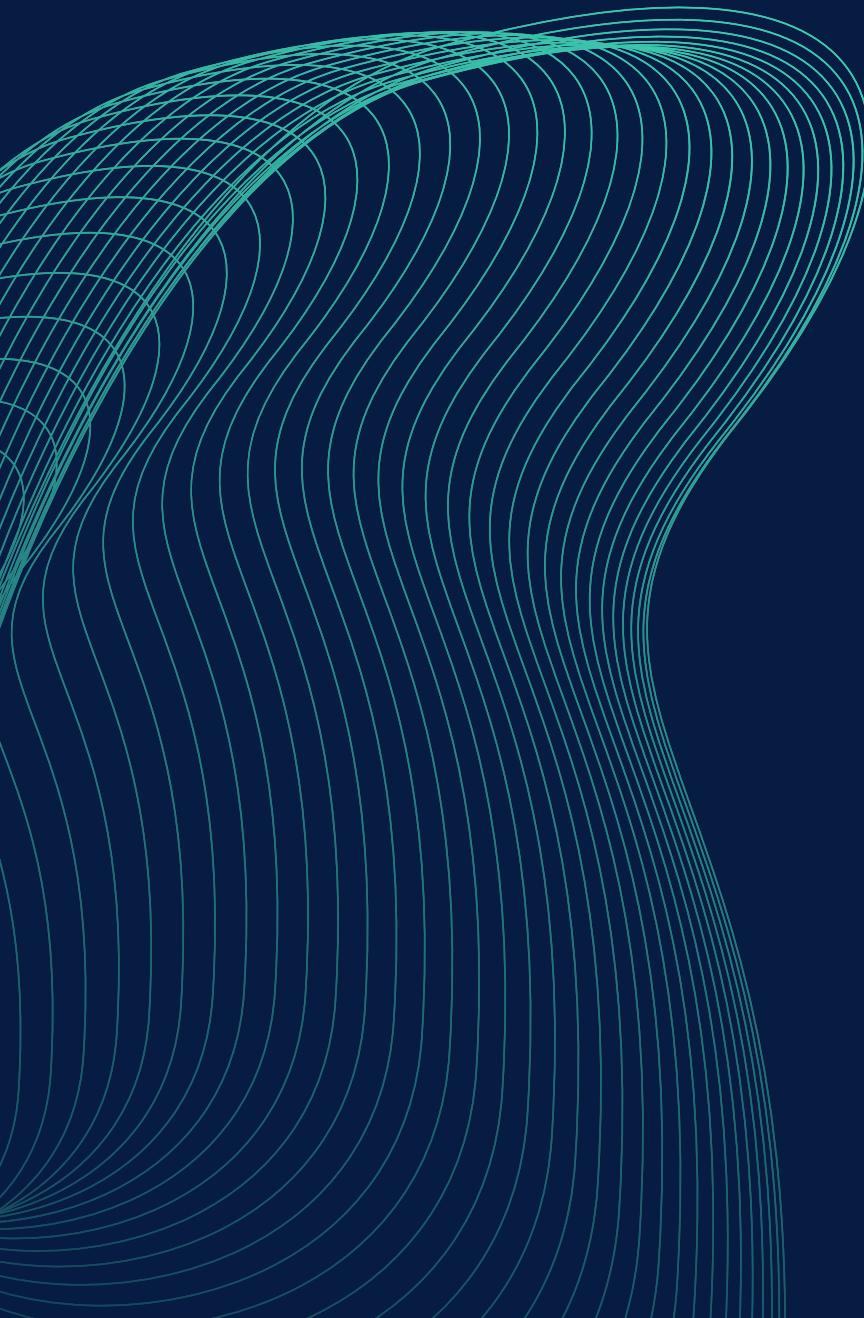
Además de la importancia de la seguridad en la nube, el rendimiento de este servicio resulta de gran relevancia. Una de las mayores ventajas y atractivo del uso de la nube, es el acceso a la información desde diferentes puntos, además de ofrecer soluciones rápidas y fáciles.

Implementar sistemas con una seguridad fuerte, permite potenciar la sostenibilidad y éxito de distintos proyectos empresariales. Su importancia radica en que, estos servicios promueven la resiliencia de las empresas. De esta manera, un correcto uso de la nube, garantiza la rápida adaptación de los negocios a diversos entornos y realidades.

En general, la desconfianza hacia la seguridad de la nube es una de las principales barreras que encuentran las personas autónomas trabajadoras para emplear este servicio. Sin embargo, el empleo de configuraciones adecuadas, así como el correcto uso general del sistema, se convierten en aceleradores del éxito en diversos procesos empresariales.



¿Cómo
asegurar
la Nube?



Con el aumento de los datos que se trasladan a la nube, garantizar la seguridad en la nube es más importante que nunca. La nube, aunque es más segura en general que en sus inicios, sigue siendo un objetivo lucrativo para las personas ciberdelicuentes que buscan propiedad intelectual, secretos comerciales e información personal.

Es importante saber que la seguridad en la nube es una responsabilidad compartida entre la empresa proveedora de la nube y las personas trabajadoras autónomas y/o personas emprendedoras. La elección de las herramientas de apoyo adecuadas, ayuda a mantener la seguridad de los datos en la nube, al igual que el seguimiento de las mejores prácticas. Si se implementan en los negocios algunas medidas inteligentes y se asocia con las empresas proveedoras de soluciones adecuados, la persona trabajadora autónoma puede estar tranquila sabiendo que los datos en la nube están seguros.

¿Hasta qué punto son seguros los archivos que se almacenan a cientos o miles de kilómetros de distancia, en el hardware de otra empresa? Debido a estas preocupaciones, existen multitud de debates sobre la protección de los datos en la nube, las amenazas a la seguridad, las interrupciones y las posibles violaciones de los datos en la nube.

Por suerte, existen muchas opciones para proteger los propios datos en la nube. El método más conocido es el cifrado.



El cifrado es una de las mejores maneras de proteger sus sistemas de informática en la nube.

Existen diversas maneras de usar el cifrado, y puede ofrecerlas la empresa proveedora de servicios en la nube o una empresa proveedora de soluciones de seguridad en la nube independiente:

- Cifrado de las comunicaciones con la nube, en su totalidad.
- Cifrado de datos especialmente confidenciales, como las credenciales de las cuentas.
- Cifrado de extremo a extremo de todos los datos que se suben a la nube.

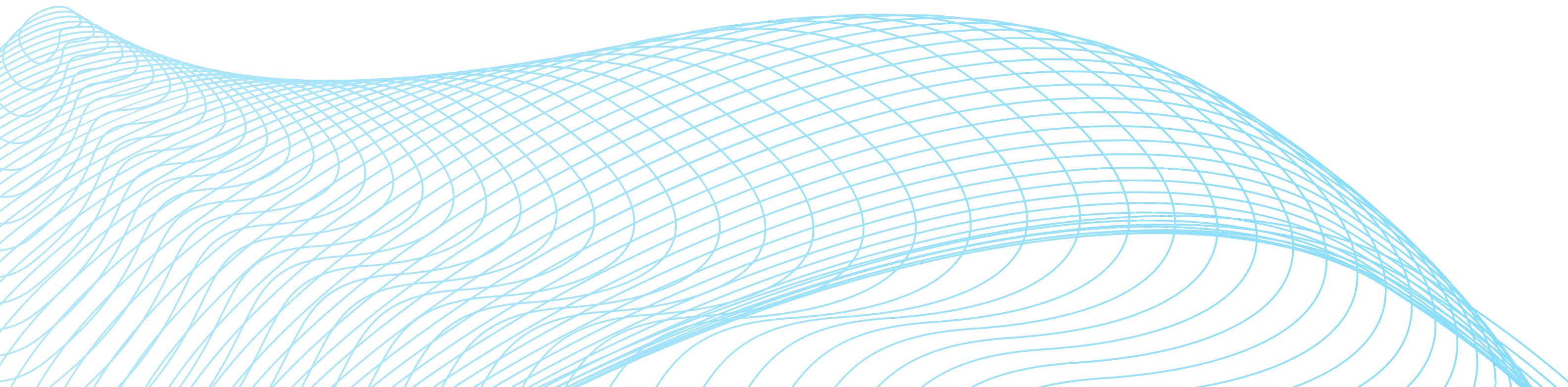
En la nube, los datos corren más riesgo de ser interceptados cuando están en movimiento. Cuando se están trasladando entre dos ubicaciones de almacenamiento o cuando se transmiten a su aplicación local, los datos son más vulnerables.

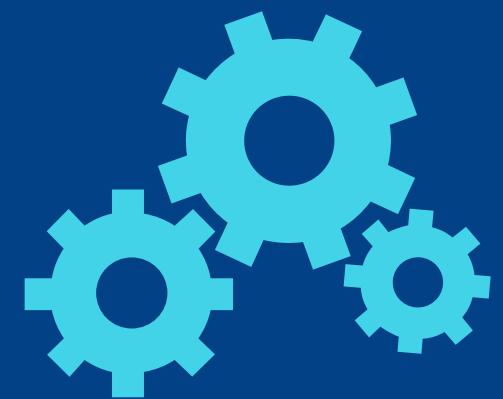
Por este motivo, el cifrado de extremo a extremo es la mejor solución de seguridad en la nube para los datos esenciales. Con el cifrado de extremo a extremo, en ningún momento, la comunicación se pone a disposición de personas que no dispongan de la clave de cifrado.

Puede cifrar los datos la misma persona trabajadora autónoma antes de guardarlos en la nube o usar una empresa proveedora de servicios en la nube que los cifre como parte de los servicios que le ofrece. Sin embargo, si solamente se utiliza la nube para almacenar datos no sensibles, el cifrado de extremo a extremo podría ser excesivo. Por otro lado, en el caso de la información financiera, confidencial o comercialmente sensible, este tipo de cifrado es vital.

Si se utiliza cifrado, es fundamental manejar de manera segura la clave de cifrado. Guardar una copia de seguridad de la clave y, si es posible, no situar en la nube. Asimismo, puede que sea de utilidad cambiar las claves de cifrado de manera periódica para que, si alguien consigue acceder a ellas, quede desconectado del sistema cuando realice el cambio. La configuración es otra herramienta de enorme utilidad en la seguridad en la nube. Muchas infracciones de datos en la nube se deben a vulnerabilidades básicas, tales como errores de configuración. Al prevenirlas, está disminuyendo enormemente el riesgo de seguridad en la nube.

A continuación, le indicamos algunos de los principios que puede seguir:





Nunca dejar sin modificar la configuración predeterminada

Utilizar la configuración predeterminada permite a la persona atacante entrar por la puerta principal.



Nunca dejar un sector de almacenamiento en la nube abierto

Mediante un ciberataque, se podría ver el contenido con solo abrir la URL del sector de almacenamiento.



Si la empresa proveedora de servicios en la nube le proporciona controles de seguridad que puede activar, utilizarlos.

No seleccionar las opciones de seguridad correctas podría poner en riesgo la empresa.

Los consejos básicos de ciberseguridad también se deben incorporar en cualquier implementación de la nube. Si utiliza la nube, conviene que no pase por alto las prácticas estándar de ciberseguridad. Entre los consejos más recomendables a seguir, se encuentran:

Utilizar contraseñas seguras. Combinar letras, números y caracteres especiales hace que resulte más difícil descifrar una contraseña. Cuanto más aleatoria sea la secuencia de una contraseña, mejor.

Hacer una copia de seguridad de los datos periódicamente para que, en caso de producirse un apagón en la nube o una pérdida de datos de la empresa proveedora de servicios en la nube, pueda restaurarse completamente.

Evitar acceder a sus datos a través de una Wi-Fi pública, sobre todo, si no está protegida por una autenticación segura.

Utilizar un sistema seguro de gestión de contraseñas. De este modo, podrá asignar a cada aplicación, base de datos y servicio que utilice una contraseña propia, sin necesidad de recordarlas todas.

Modificar los permisos para evitar que ningún dispositivo o persona acceda a todos sus datos a menos que sea necesario.

Utilizar una red privada virtual (VPN) para proteger su acceso a la nube.

Proteger todos los dispositivos para acceder a los datos en la nube. Si se tienen los datos sincronizados en varios dispositivos, cualquiera de ellos podría ser un eslabón débil que ponga toda la huella digital en riesgo.

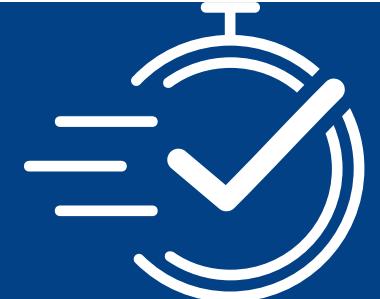
Proteger con un buen software antivirus y antimalware. Las personas atacantes podrán acceder fácilmente a la cuenta si un malware se abre camino en su sistema.



¿Qué características tiene la seguridad en la nube?



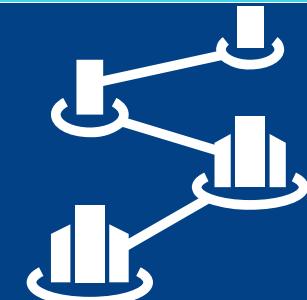
Rapidez: La seguridad en la nube usa aceleradores nativos de la empresa proveedora de servicio en la nube que permiten optimizar las capacidades y controles de seguridad en cuestión de minutos, mejorando así la gestión de recursos.



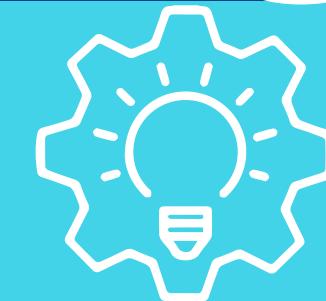
Sin fricciones: Se refiere a la protección en todas las soluciones, en cualquier proceso de gestión y en equipos operativos.



Escalabilidad: Los procesos de automatización y recuperación automática de la nube consiguen alejar a un segundo plano las tareas manuales, permitiendo a las empresas escalar mejorando el modelo de recursos.



Proactividad: Este sistema establece controles de prevención que ayudan a evitar incidentes y posibles ataques maliciosos.



Rentabilidad: Este servicio es rentable desde el minuto 0, evitando costes adicionales que suelen ocurrir en ocasiones donde hay que repetir el trabajo ya hecho.



Ventajas de tener el sistema en la nube

- Proteger a la persona trabajadora autónoma, conservando sus datos y haciendo que el trabajo realizado con la información de cada persona sea confidencial y esté guardado de forma segura.
- Mejorar su reputación o generar mejores comentarios sobre su marca gracias a la seguridad que aportan.
- Lograr el cumplimiento de todas las normativas legales de forma actualizada, en especial el Reglamento General de Protección de Datos (RGPD).
- Ofrecer las máximas garantías de protección informática con una seguridad de última generación, que proteja al máximo todos los datos personales y documentos almacenados.

Aunque los datos de Eurostat posicionan a las empresas españolas por debajo de la media en adopción del cloud, cada vez son más los negocios que muestran su interés por la nube. Se avanza a buen ritmo, pero no es suficiente. Las personas expertas insisten en la importancia de que la nube sea vista como una prioridad estratégica tanto para el sector público como para el privado, con especial incidencia, para las pymes.





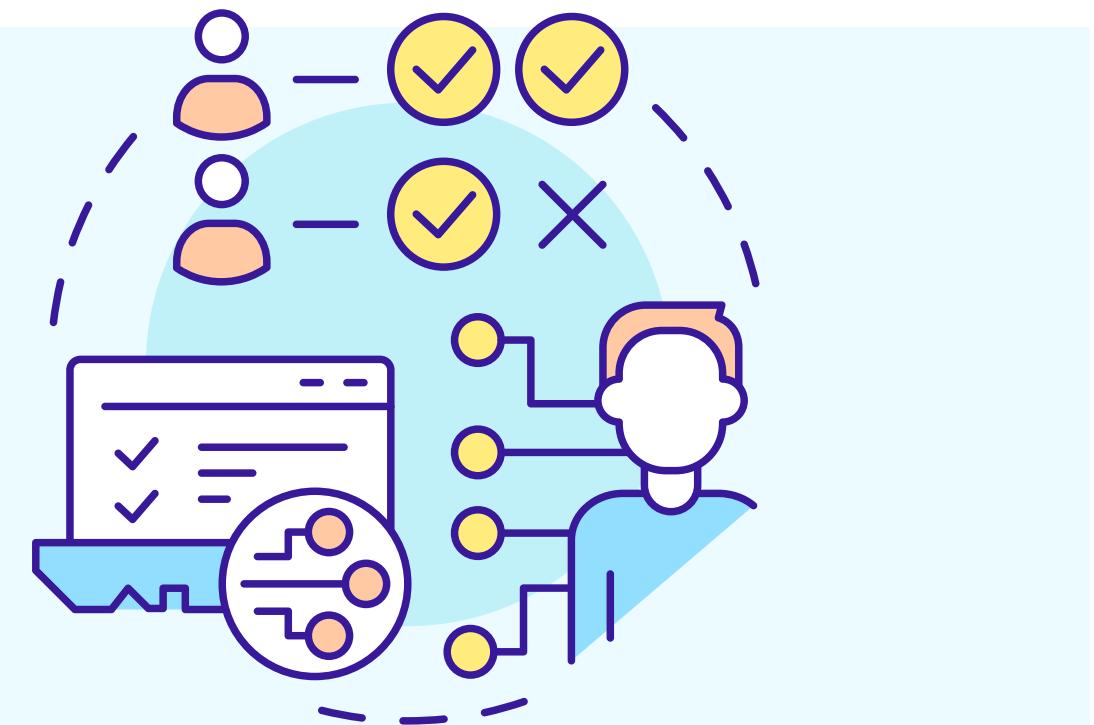
Soluciones de Seguridad en la Nube para Personas Trabajadoras Autónomas y/o Personas Emprendedoras

En las aplicaciones de las pequeñas y medianas empresas, la seguridad en la nube reside en gran medida en las empresas proveedoras públicas que utiliza. Sin embargo, hay medidas para mantenerse a salvo:



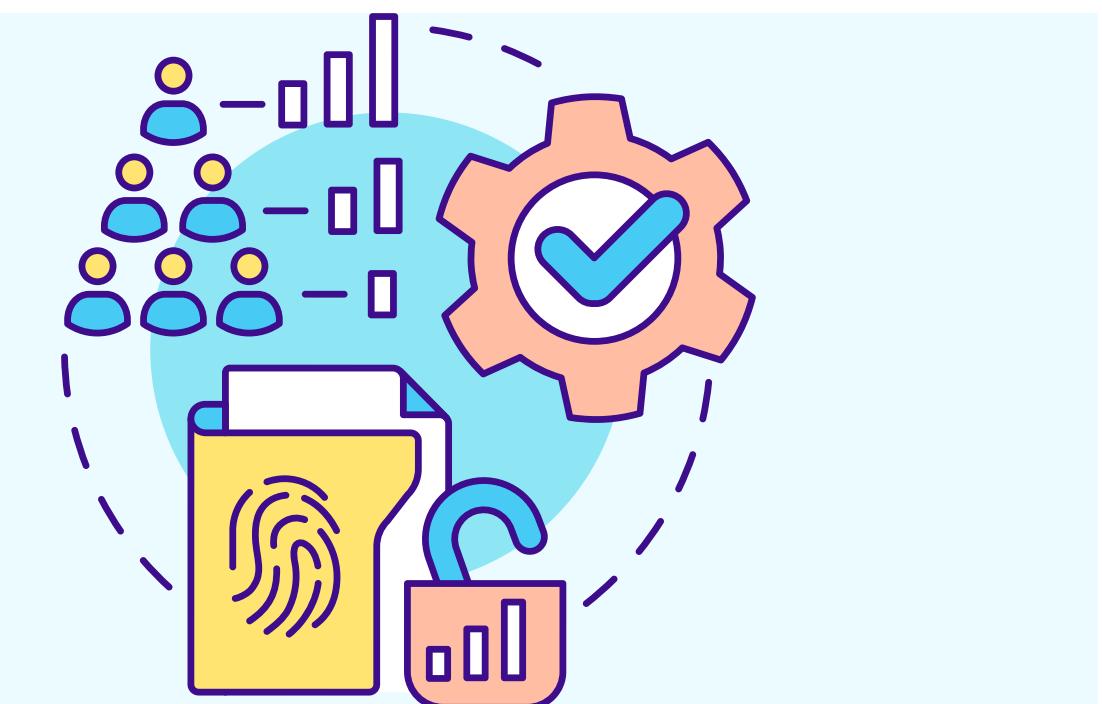
Segmentación de datos de varias personas usuarias.

Las personas trabajadoras autónomas deben asegurarse de que, ninguna otra empresa y/o persona trabajadora autónoma con la que comparta recursos en su sistema cloud (nube pública o híbrida), pueda acceder a sus datos. Bien sea que estén alojados en servidores segmentados o cuidadosamente codificados, se recomienda que se apliquen correctamente las medidas de segmentación adecuadas.



Controles de acceso de las personas usuarias.

Los permisos de control pueden significar que, el acceso de las personas usuarias se reduzca a un nivel que resulte incómodo. Sin embargo, ser restrictivo y trabajar de forma segura para encontrar un equilibrio puede ser mucho más seguro que permitir que los permisos sin asignar se filtre en su red.





Cumplimiento legal de los datos.

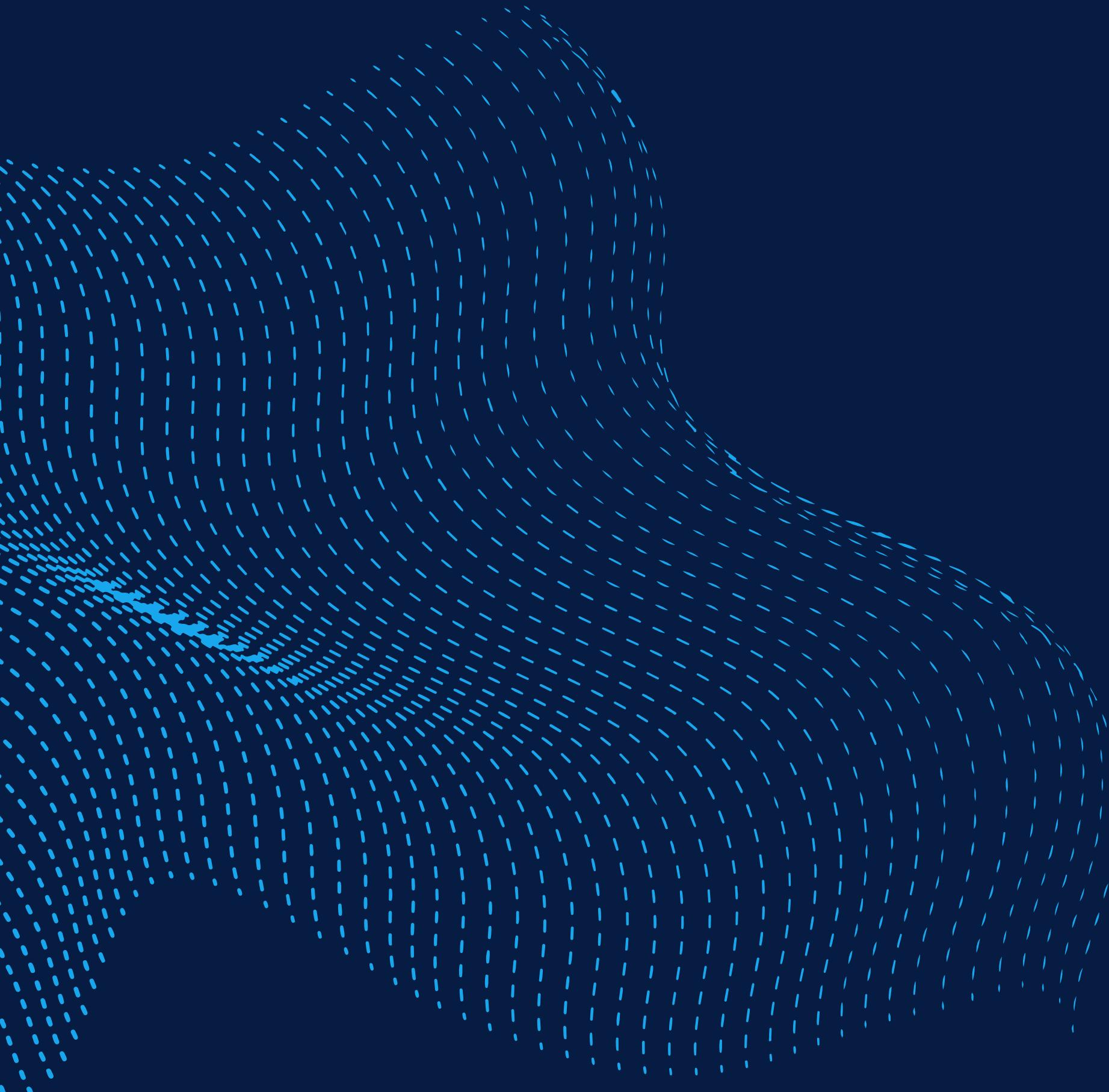
Mantener los datos de conformidad con los reglamentos internacionales como el RGPD, es crítico para evitar importantes sanciones y daños a la reputación. Es clave el establecimiento de medidas, como el enmascaramiento de datos y la clasificación de datos confidenciales, para que sean una prioridad dentro de la cultura empresarial.



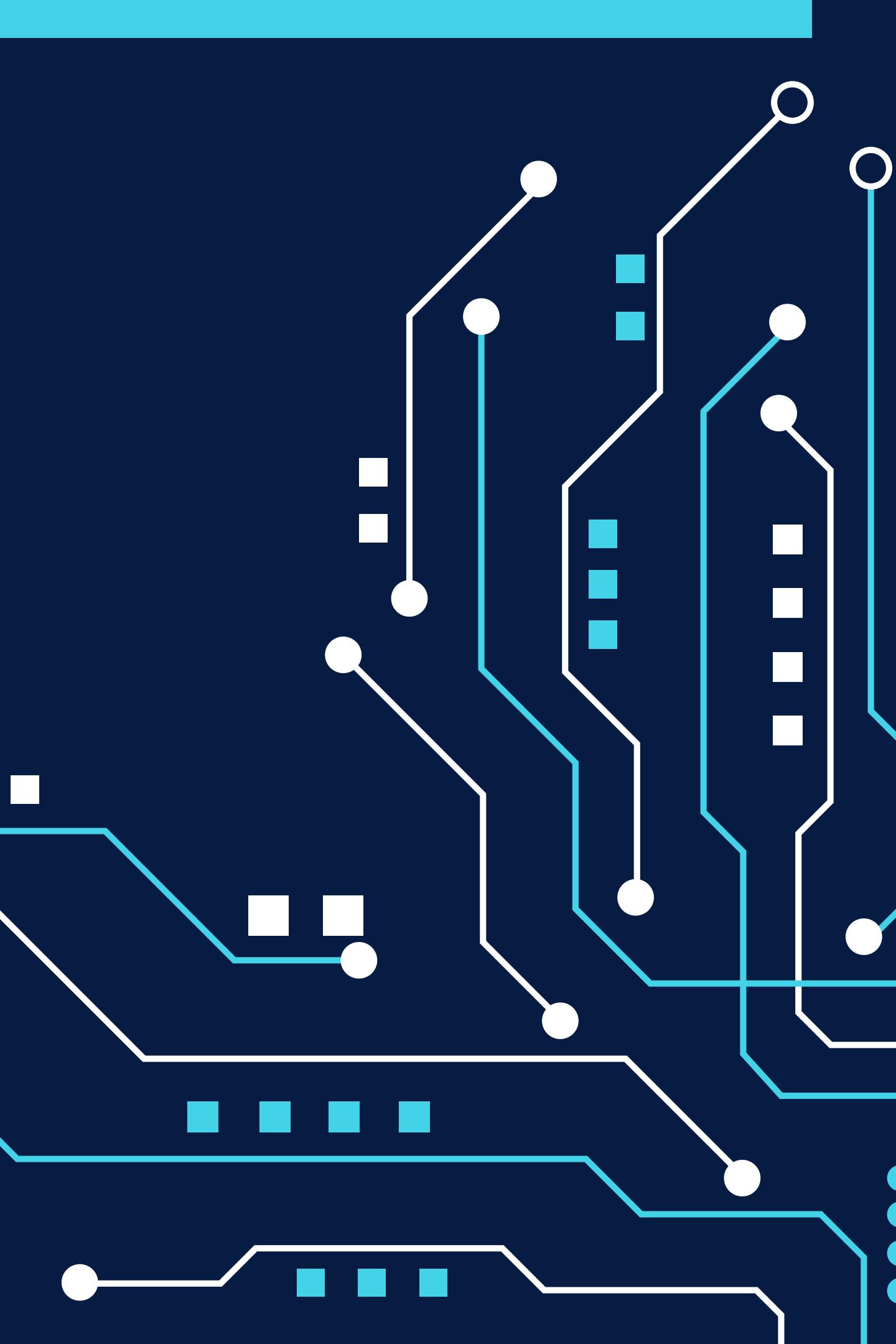
Escalada cuidadosa de los sistemas de la nube.

Con la rápida implementación de los sistemas de la nube, es imprescindible la inversión en tiempo necesario para revisar los sistemas de la empresa con objeto de obtener seguridad por encima de la comodidad.





Normas ISO de Ciberseguridad



A la hora de trabajar con información en la nube, las empresas proveedoras deben garantizar la integridad de los datos de las personas trabajadoras autónomas y/o personas emprendedoras. Para ello, existen las normas ISO 27017 ,27001 y 27018, las que apuntan a fortalecer la ciberseguridad en servicios cloud.

Contar con una certificación ISO es uno de los parámetros más importantes a la hora de elegir una empresa proveedora de servicios en la nube. Dicha certificación garantiza altos estándares en la seguridad de la información, uno de los activos más valiosos para las empresas que prestan servicios DBaaS (Data Base as a Service, o Base de Datos como Servicio), al igual que aquellas cuyo modelo es el SaaS (Software as a Service).

Al respecto, las normas ISO 27017 ,27001 y 27018 constituyen algunos de los principales estándares para resguardar la ciberseguridad y garantizar la integridad de la información alojada en la nube, servicio ofrecido por empresas como Amazon Web Services (AWS), Google Cloud o Microsoft Azure.

1. ISO 27001

A grandes rasgos, la norma ISO 27001 es un estándar generado por la Organización Internacional de Normalización (ISO, por sus siglas en inglés) que describe la manera correcta de gestionar la seguridad de la información al interior de una empresa.

Se trata de la principal norma de seguridad, a nivel global, para el manejo de la información. Su eje central es el Sistema de Gestión de la Seguridad de la Información (SGSI), el cual debe realizarse a través de un "un proceso sistemático, documentado y conocido por toda la organización", tal como lo establece el propio organismo.

Es prácticamente imposible garantizar la total seguridad de la información pues, la norma ISO 27001 apunta a que las organizaciones conozcan los riesgos asociados al manejo de información, asumiéndolos, minimizándolos y gestionándolos por medio de un proceso documentado, sistemático, estructurado, eficiente, repetible y adaptable a los eventuales cambios que pudieran presentar los riesgos, el entorno y la tecnología.



Para obtener una certificación ISO 27001, las personas trabajadoras autónomas en sus negocios deben cumplir con ciertos pasos:

Etapa previa

Aquí, deben implementar una serie de pasos básicos para iniciar su proceso hacia la certificación. Entre los principales, están la utilización de una metodología de gestión de proyectos, contar con el apoyo de toda la dirección en el proceso de implementación, definir el alcance del sistema de seguridad, determinar una política de evaluación de riesgos, implementación de controles y medidas correctivas.

Auditoría de revisión

Personal externo revisará que lo anterior se cumpla para dar curso al proceso de certificación.

Auditoría principal

Una empresa auditora verificará que las medidas anteriores cumplan con sus objetivos. De estar todo en orden, la empresa puede ser certificada.

Revisões periódicas

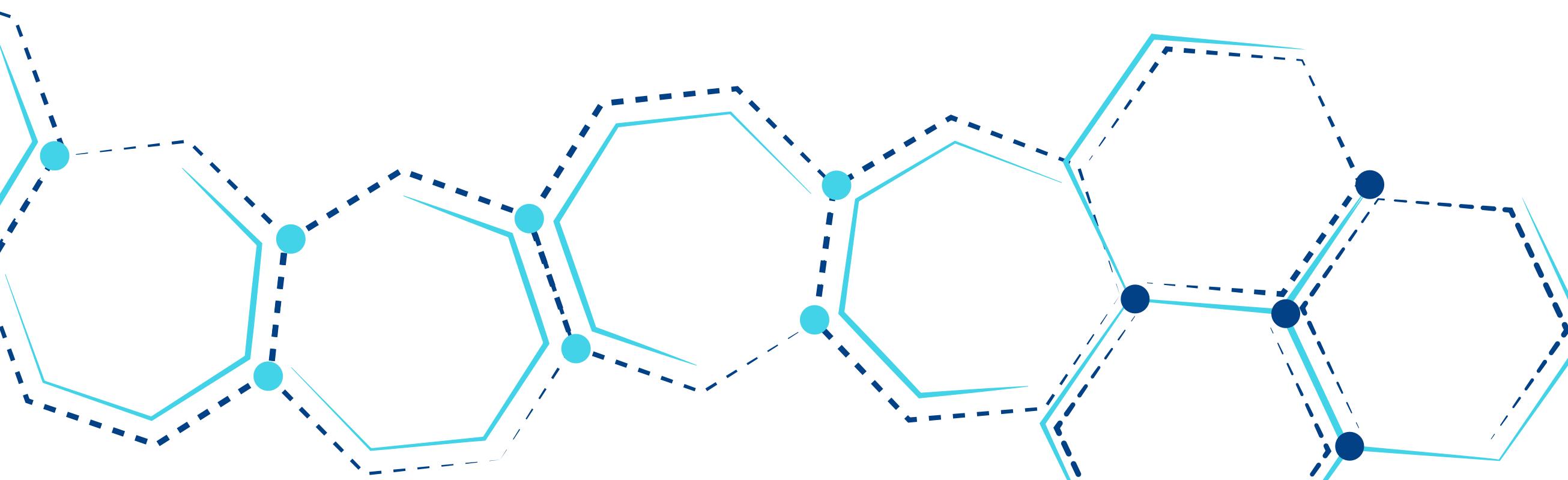
Una vez aprobada la certificación, el organismo monitorea dicha empresa durante 3 años para garantizar que cumpla con los esfuerzos de protección de datos.

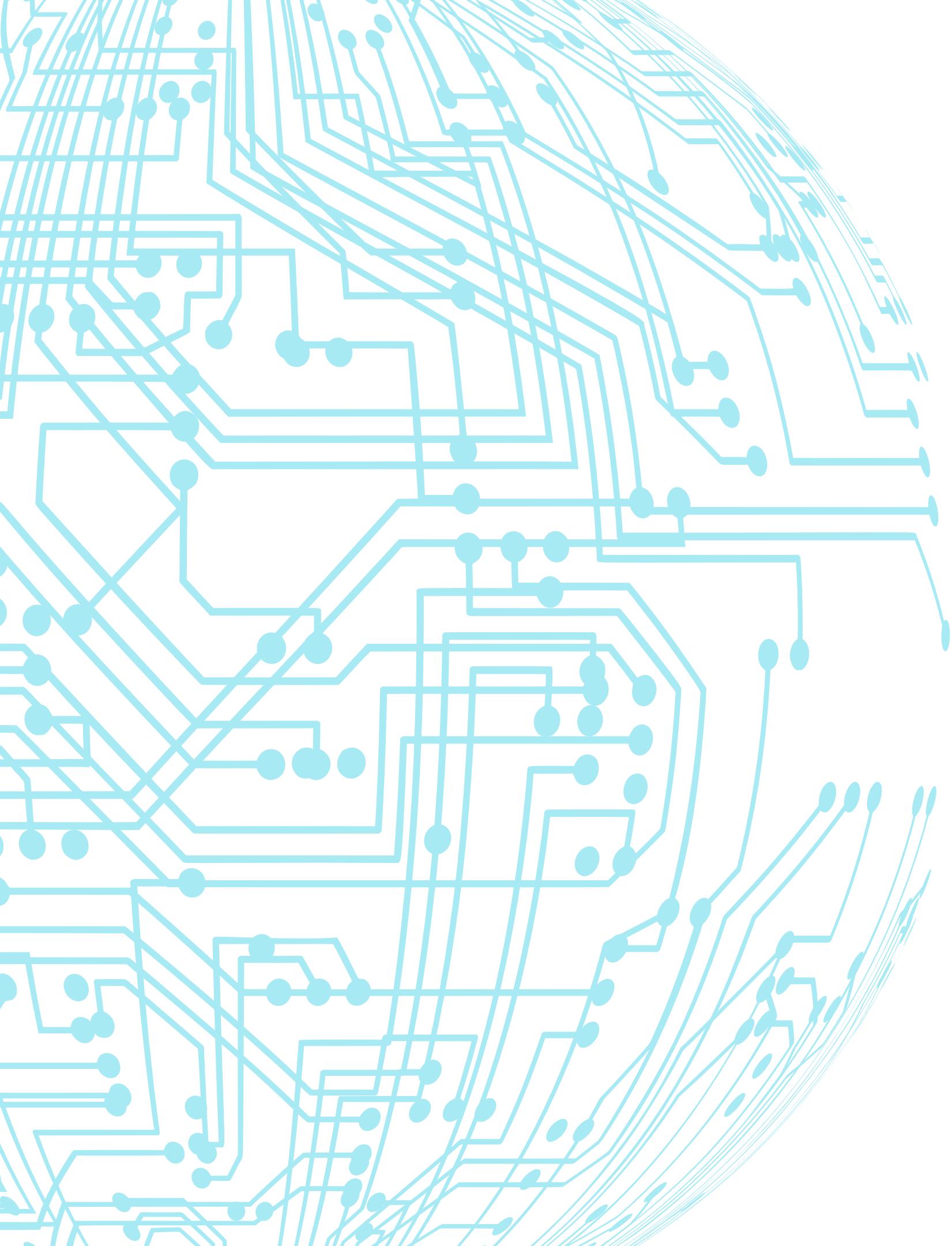
2. ISO 27017

La norma ISO 27017 es un estándar de seguridad que proporciona controles, tanto para clientela como para empresas proveedoras de servicios en la nube. Su importancia radica en la precisión con la que establece las relaciones entre las personas trabajadoras autónomas y las empresas proveedoras de servicios en la nube, determinando qué pueden exigir como clientela y qué información deben proporcionarle a la empresa proveedora.

El cumplimiento de esta guía permite fortalecer la ciberseguridad y la gestión del servicio referente a arquitectura, medidas de seguridad, funcionalidades disponibles, tecnología de cifrado y localización geográfica de los datos.

Esta norma contempla 37 controles en la nube -basados en la ISO -27002, junto a 7 adicionales que permiten fortalecer la seguridad de los servicios cloud.





3. ISO 27018

Finalmente, la norma ISO 27018 constituye un compendio de buenas prácticas -referentes a controles de protección de datos- para servicios cloud, enfocada específicamente en las empresas proveedoras.

Su objetivo central es delimitar las normas, procedimientos y controles que las empresas proveedoras, en su calidad de "procesadoras de datos", deben aplicar.

Además, garantiza el cumplimiento de la normativa legal en cuanto al manejo de datos personales.

Bibliografía



Publicaciones



- “Computación en Nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. European Network and Information Security Agency. ENISA. 2009.
- “Introducción a la Seguridad en Cloud Computing”. Caparrós Ramírez, Joan; Cubero Luque, Lorenzo; Guijarro Olivares, Jordi. Universitat Oberta de Catalunya.
- “La función de la seguridad en cloud computing de confianza”. White paper de RSA. RSA Security Inc. 2009.
- “Cloud Computing. Una guía de aproximación para el empresario”. Instituto Nacional de Ciberseguridad. INCIBE. 2017.
- “La seguridad y utilidad del cloud como tema clave para la empresa”. Basque Cibersecurity Centre y Grupo SPI Taldea. 2020.
- “La seguridad de los sistemas cloud y la gestión del talento”. Libro Blanco Cornerstone. 2015.
- “Guía para empresas: seguridad y privacidad del cloud computing”. Instituto Nacional de Tecnologías de la Información. Ministerio de Industria, Turismo y Comercio. 2011.
- “Protección del Cloud Computing en seguridad y privacidad. Areitio, Javier. Universidad de Deusto. 2010.
- “Guía de Seguridad de las TIC (CCN-STIC-823). Utilización de servicios en la nube”. Esquema Nacional de Seguridad. Ministerio de Hacienda y Administraciones Públicas. 2014.

Webs



- www.kaspersky.es
- www.ibm.com
- www.zscaler.es
- www.kinsta.com
- www.redhat.com
- www.google.com
- www.cyberark.com
- www.proofpoint.com
- www.blog.beservices.es
- www.kyoceradocumentsolutions.es
- www.intel.es
- www.trendmicro.com
- www.nutanix.com
- www.enisa.europa.eu
- www.vmware.com

Este proyecto está financiado por el Área de Coordinación y Desarrollo Estratégico, Productivo y Social de la Diputación de Cádiz, y surge del Plan Dipuactiva 2023 entre la Diputación Provincial de Cádiz y la Asociación Profesional de Trabajadores Autónomos (ATA) de Andalucía.

Proyecto: "Seguriza tu actividad. Aprende a utilizar servicios y programas para trabajar de forma segura en la red".

Datos de contacto: www.ata.es | ata@ataandalucia.com. 900 100 060 / 956 329 518

Dirección: ATA Jerez (Cádiz) C/ Larga nº 14, 4^a Planta.

Subvenciona



COORDINACIÓN
Y DESARROLLO ESTRÁTÉGICO,
PRODUCTIVO Y SOCIAL

Desarrolla

