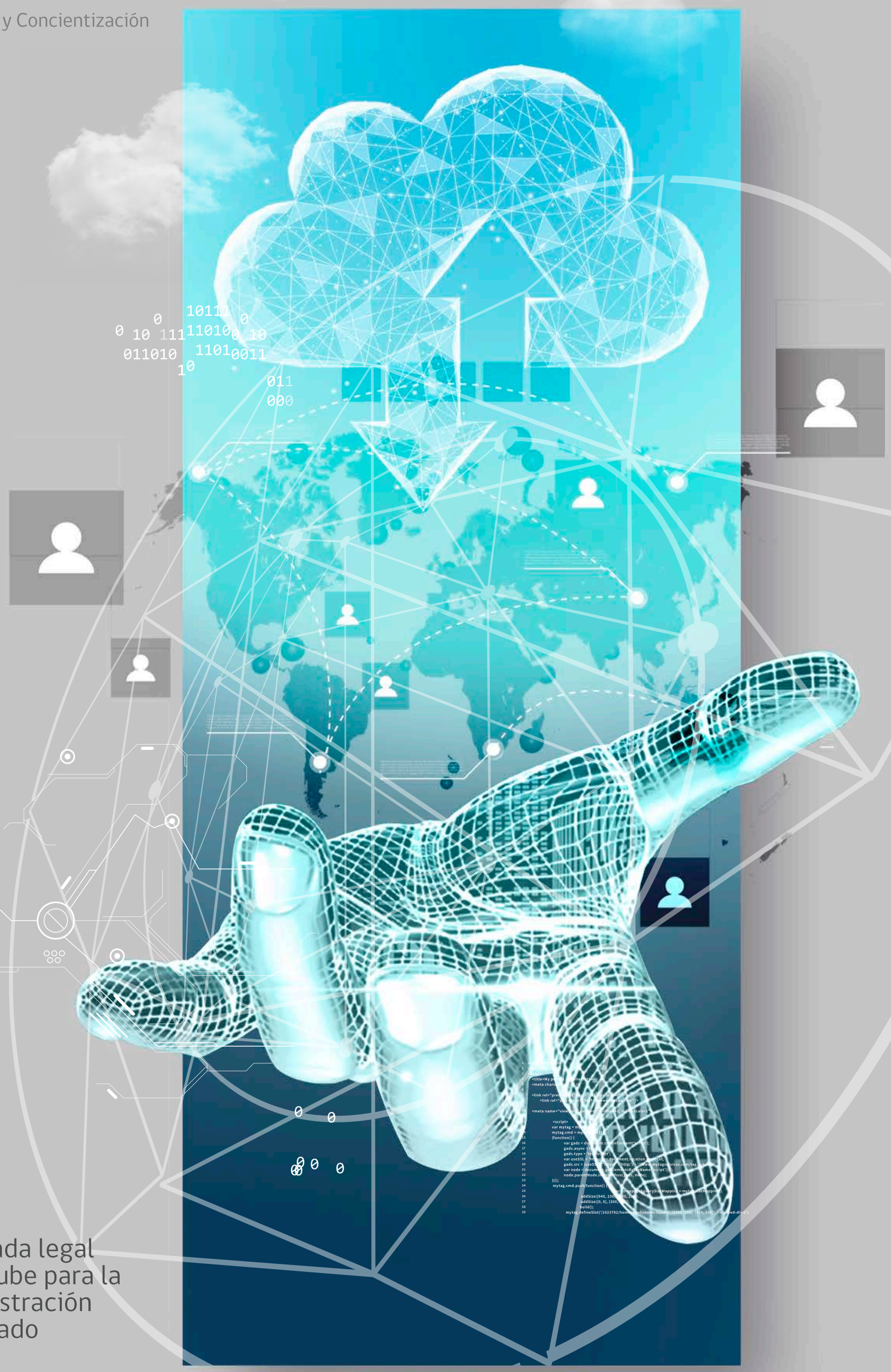
Vol. Nº 10
Mayo/2021
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización



NUESTRA VIDA EN LA NUBE

Lo que debes saber para usar servicios cloud al interior de la administración del Estado

RIESGOS DE LA NUBE

"Sin datos no hay pruebas. Sin pruebas no hay justicia"

Cooperación Internacional

Cloud Security Alliance

Tendencias

Análisis Forense en la nube

Comunidades Nacionales

CSA Las definiciones clave para saber si la nube es para nosotros

Legal

La mirada legal de la nube para la Administración del Estado

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

145 8712 7864
096 4321 5541

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

ÍNDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Ramón Rivera,
Hernán Espinoza,
Cristobal Hammersley

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Decidir si migrar o no a la nube, y de qué forma, son preguntas a las que actualmente se enfrentan las organizaciones de todo nivel, entre empresas grandes, medianas y pequeñas, e incluso más, ahora en muchos casos también debe tomarse esa decisión en distintos órganos de la administración del Estado.

Si bien como CSIRT de Gobierno nos preocupamos, además de nuestras funciones habituales de monitoreo y coordinación de la ciberseguridad a nivel país, de impulsar el desarrollo de una cloud segura, es esencial que cada uno de nosotros, y en especial los encargados de ciberseguridad de las organizaciones, tenga claro cómo resguardar la integridad de su información, para decidir cuándo vale la pena migrar a la nube, cómo elegir un proveedor de este servicio, y cuándo es mejor mantener la información en servidores físicos propios.

Por eso el presente número de CiberSucesos está dedicado a la ciberseguridad en la nube, y su tema central precisamente trata de cómo evaluar si las soluciones cloud ofrecidas por los distintos proveedores existentes cumplen con las exigencias mínimas para gestionar el riesgo de manejar los datos y programas que hoy la organización mantiene en sus servidores, "on premise".

Seguidamente, revisamos las mejores prácticas a incorporar si se quiere migrar a la nube, especialmente cuando se trata de entes de la administración del Estado. Qué factores tener en cuenta, cómo diseñar los contratos y cuándo simplemente es preferible mantener un control más directo de los datos en infraestructura física propia, son algunos de los factores que se revisan aquí.
En nuestra sección de Cooperación Internacional, hablamos con Daniele Catteddu, CTO de la Cloud Security Alliance (CSA), organización internacional dedicada a crear un ambiente más seguro en la nube, quien nos explica cómo esta alianza define nuevos estándares de seguridad en la nube. Y mientras tanto, como representante de las Comunidades Nacionales tenemos al presidente del capítulo chileno de la CSA, Ricardo Urbina, quien detalla las formas en que se promueve una nube más segura hoy en nuestro país.

Tendencias aborda el análisis forense en la nube. o sea, cómo se aplica el análisis informático posterior a un incidente de ciberseguridad, cuando no se tiene completo acceso a los servidores físicos para revisar su contenido y evitar alteraciones. Se muestra cuáles son las fases de este análisis forense cloud y algunas herramientas forenses de mucha utilidad en estos casos.
Y finalmente la sección Legal se ocupa de las particularidades que presenta la computación cloud en términos jurídicos cuando se trata de la Administración Pública.

NUESTRA VIDA **EN LA NUBE**

Lo que debes saber para usar servicios cloud al interior de la administración del Estado

La tendencia de buscar almacenamiento en la nube ha llegado también a la administración del Estado. Pero nuestro rol de custodios de los datos nos obliga a conocer los riesgos que puede llevar este tipo de almacenamiento, teniendo en cuenta también que los ciudadanos esperan que los servicios provistos por el Estado respondan a sus necesidades y estén disponibles cuándo y dónde los necesiten. Es por ello que debemos hacer una evaluación y una implementación adecuada de las soluciones cloud.

BENEFICIOS DE LAS SOLUCIONES CLOUD

Mientras las soluciones cloud se implementen bajo estándares de ciberseguridad, pueden traer utilidades como:

a. **Innovación:** La nube aporta entornos de procesamiento intensivo de datos de manera más ágil y flexible, y provee una plataforma común de colaboración entre entidades disímiles para el desarrollo de proyectos conjuntos, favoreciendo la armonización y estandarización de datos, sistemas y procesos.

b. **Economía:** Se elimina la inversión inicial en capital por servidores, almacenamiento y licencias, teniendo en su lugar costos variables que se pagan cuando y cuanto sean necesarios, ahorrando en energía, mantenimiento y reparación del equipamiento y personal técnico para la operación, entre otros.

c. **Modernización de TI:** La nube hace disponibles en forma rápida y simple servicios digitales en múltiples dispositivos, agilizar las interacciones y la colaboración entre instituciones públicas, maximizando la capacidad de respuesta a las demandas ciudadanas.

d. **Disponibilidad:** Generalmente los niveles de servicio ofrecidos por los prestadores cloud son más exigentes que los de la informática tradicional. La nube permite migrar rápidamente ambientes que presenten una falla y prevenir eventos que interrumpan los servicios, al facilitar la distribución geográfica y la redundancia de los recursos.

e. **Eficiencia:** La nube permite a las instituciones lanzar sus aplicaciones en un menor tiempo, sin cuantiosas inversiones en equipamiento, implementación y configuración, incrementando la eficiencia de sus procesos.

f. **Elasticidad, escalabilidad o pago por uso:** Se contratan los servicios sólo cuando se requieren y la cantidad de ellos que se necesita. Las instituciones añaden o eliminan servicios evitando la compra de infraestructura y licencias.

g. **Ubicuidad:** Sólo con tener internet los usuarios de las aplicaciones migradas a la nube pueden acceder desde cualquier lugar, y a través de cualquier dispositivo, según las reglas de acceso.

h. **Fácil actualización:** Habitualmente, el software en SaaS está en su última versión y es actualizado automáticamente, por lo que el usuario lo tendrá disponible la próxima vez que se conecte. Igualmente, los prestadores de cloud actualizan constantemente la infraestructura tecnológica que da soporte a sus servicios, por lo que es fácil usar siempre las últimas versiones de las plataformas tecnológicas.

i. **Capacidad:** La nube tiene capacidad “ilimitada”, ya que los prestadores cloud pueden proveer tanto almacenamiento y recursos de infraestructura como el cliente requiera en el tiempo.

j. **Respeto al medio ambiente:** El uso de la nube reduce la huella de carbono de una institución al ahorrar recursos que pasan de estar almacenados en equipos físicos a ser virtuales. Esto supone un considerable ahorro en energía, lo que beneficia al medio ambiente.

k. **Disponibilización de ambientes de contingencia:** La nube es ideal para disponer de infraestructura para algunos eventos de continuidad, puesto que se pueden conservar ambientes a menor escala que los ambientes de producción, con tal de minimizar las interrupciones, y sólo activarlos cuando sea necesario.

MODELOS DE IMPLEMENTACIÓN PARA CLOUD COMPUTING

1.– **Nube pública:** La infraestructura y recursos lógicos del entorno están disponibles para el público general a través de internet. Suele ser propiedad de un prestador que gestiona la infraestructura y los servicios que se ofrecen.

2.– **Nube privada:** La infraestructura de la nube se entrega para uso exclusivo de una única organización que comprende múltiples consumidores. Puede ser propiedad, administrado y operado por la organización, un tercero o una combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización.

3.– **Nube comunitaria:** La infraestructura en la nube es provista para uso exclusivo de una comunidad específica de instituciones.

4.– **Nube híbrida:** Implica el uso conjunto de varias infraestructuras en la nube de cualquiera de los tipos anteriores, que se mantienen como entidades separadas, pero a su vez se encuentran unidas por la tecnología estandarizada o propietaria, proporcionando portabilidad de datos y aplicaciones.

Consideraciones y cuidados
al utilizar soluciones cloud

a. Manejo y Naturaleza de los Datos

Se recomienda revisar con detenimiento que los contratos de prestación de servicios especifiquen claramente las mitigaciones a los riesgos identificados y las medidas de seguridad previstas para proteger los datos del servicio. También se debe prestar especial atención a:

1.– Propiedad de los datos a tratar, incluyendo registros y metadatos. Es importante que la propiedad de un dato no sea modificada al ser tratada en entornos cloud.

2.– Localización geográfica y jurisdicción sobre los datos a tratar.

3.– Sensibilidad de los datos a tratar, incluyendo si se trata de datos personales, datos reservados o datos referentes a la seguridad nacional, que podrían tener exigencias específicas y deben ser analizados caso a caso, pudiendo ser necesario descartar algunos modelos de servicio o implementación en la nube.

4.– Acceso y eliminación de los datos tratados, definiendo claramente los períodos mínimos y máximos de retención de datos por parte del prestador de servicios.

b. Marco legal aplicable y condiciones contractuales

Se debe definir claramente el alcance de los servicios prestados y los márgenes de crecimiento o reducción elástica del mismo, además de los Acuerdos de Nivel de Servicio (SLA) y las sanciones en caso de incumplimiento.

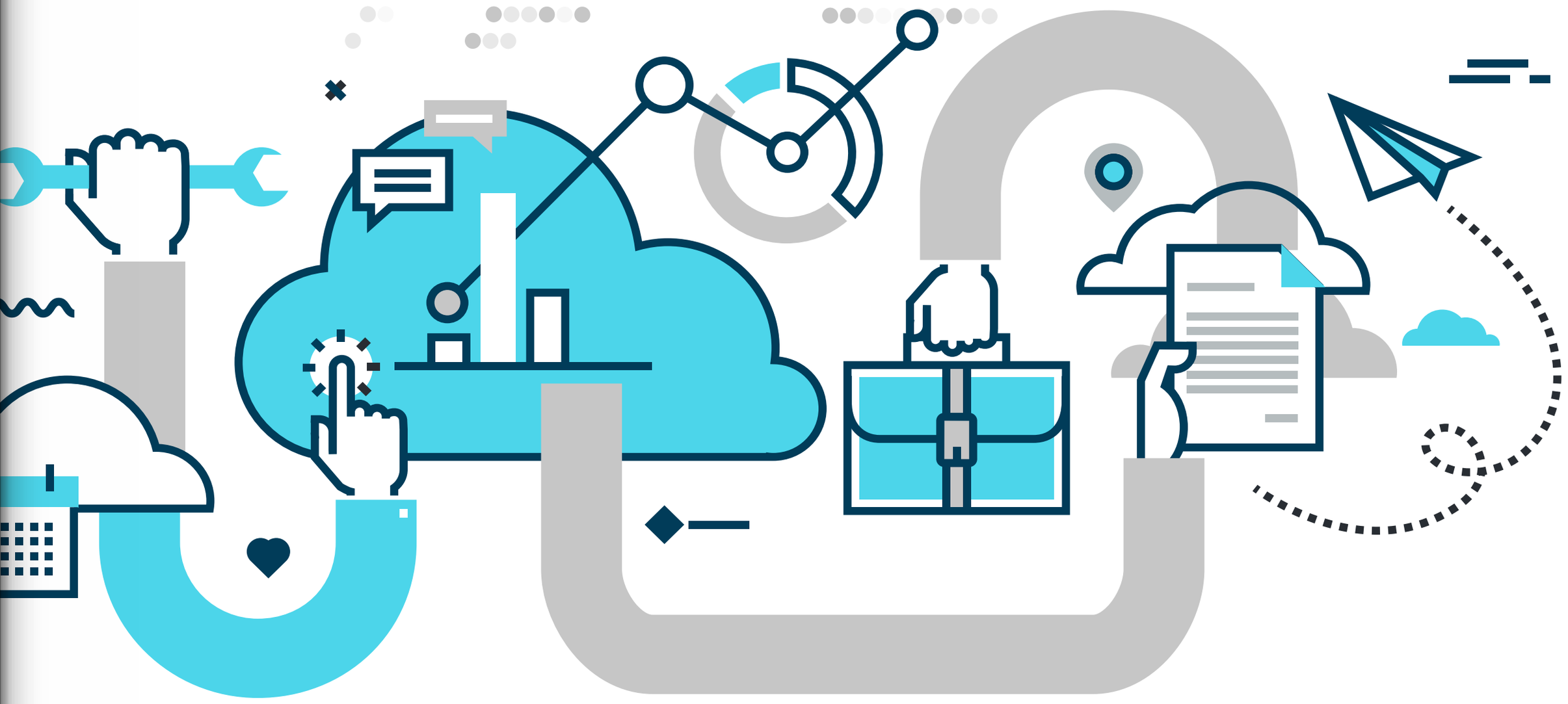
c. Evaluación estratégica de la solución

Se requiere evaluar si los servicios cloud constituyen estratégicamente una solución adecuada al problema que se desea resolver. Existen características claves para ello. Así, algunos ejemplos de cargas de trabajo idóneas para implementar en la nube son:

- Cargas de trabajo impredecibles o con potencial de crecimiento explosivo.
- Fluctuaciones de carga predecibles durante períodos de alta demanda.
- Fácil paralelización del trabajo, que permita un escalamiento horizontal más que vertical. Disponibilización de ambientes de contingencia
- Ambientes no-críticos y ambientes de baja sensibilidad.

Del mismo modo, hay características de algunos procesos que hacen que las ventajas de llevarlos a cloud no sean claras, como, por ejemplo:

- Aplicaciones que demanden muy baja latencia.
- Aplicaciones que requieran hardware especializado.
- Aplicaciones que utilicen protocolos inadecuados para la nube.
- Aplicaciones legacy que dependan de hardware no disponible en la nube.



d. Seguridad en la nube

Algunos principios de seguridad que los prestadores de servicios debieran cumplir son:

- Controles de acceso, identidad y autenticación robustos
- Protección de los activos de información y datos, tanto en tránsito como en reposo
- Seguridad operacional, del personal y proveedores
- Gestión segura de los clientes, incluyendo separación de los mismos y promoción del uso seguro del servicio
- Información de auditorías a los clientes
- Marco de gobernanza
- Reporte de incidentes de seguridad

e. Disponibilidad de auditorías y estándares

Puede ser difícil o imposible para el cliente verificar personalmente el cumplimiento de los acuerdos de servicio, forzando a depender de certificaciones y auditorías de terceros.

f. Elasticidad

Se debe tener especial consideración el riesgo presupuestario de una planificación inadecuada de la capacidad. Especialmente en infraestructuras cloud, dada su naturaleza de servicio bajo demanda, no es difícil exceder la capacidad presupuestada y, con ello el presupuesto original. Para evitarlo debemos planificar adecuadamente de la capacidad, reservar capacidad con anticipación o definir en el contrato valores de crecimiento flexibles, que no obliguen a realizar un nuevo proceso de compra.

g. Monitoreo y Cumplimiento

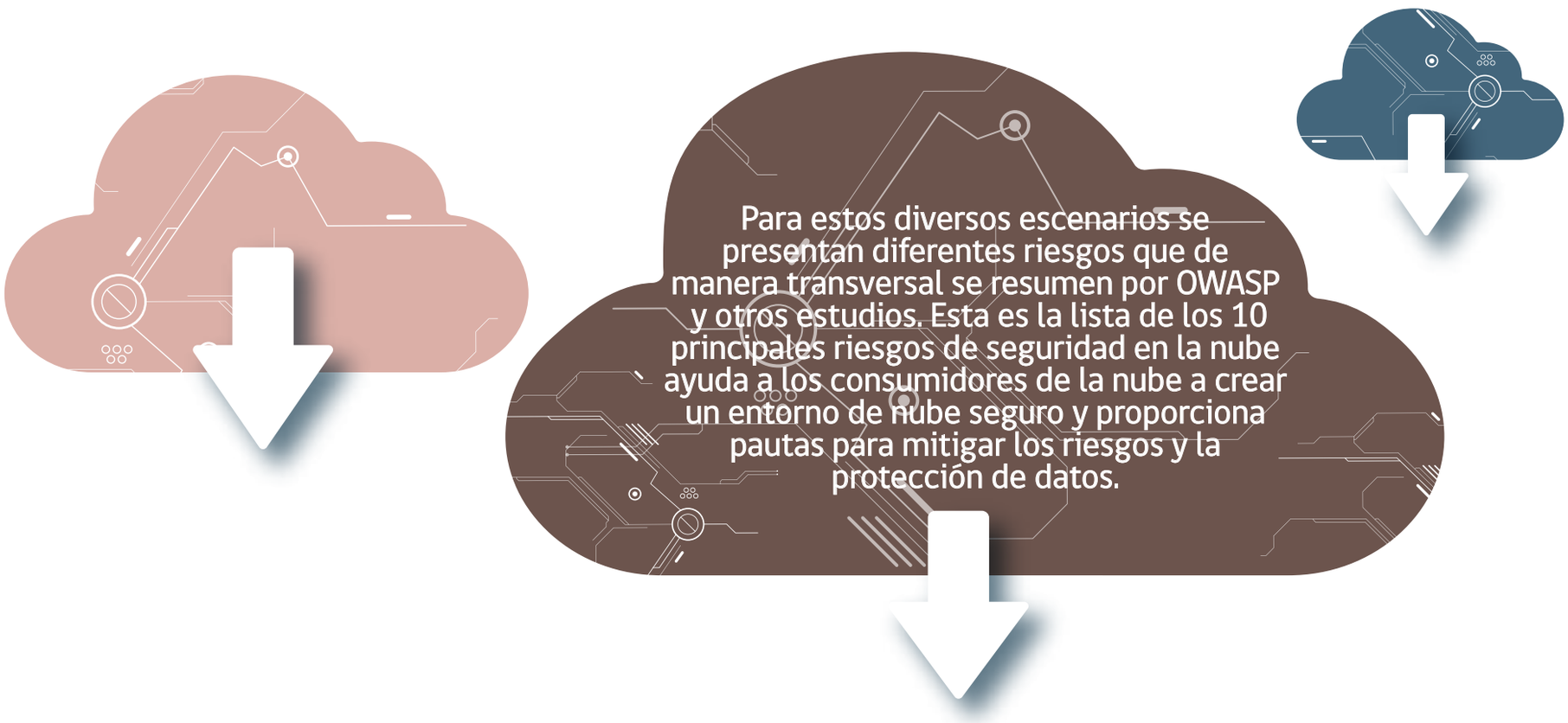
Para una correcta operación de cualquier servicio tecnológico, es fundamental contar con alguna forma de monitoreo de los servicios prestados.


Cloud
NEWS

RIESGOS DE **LA NUBE**

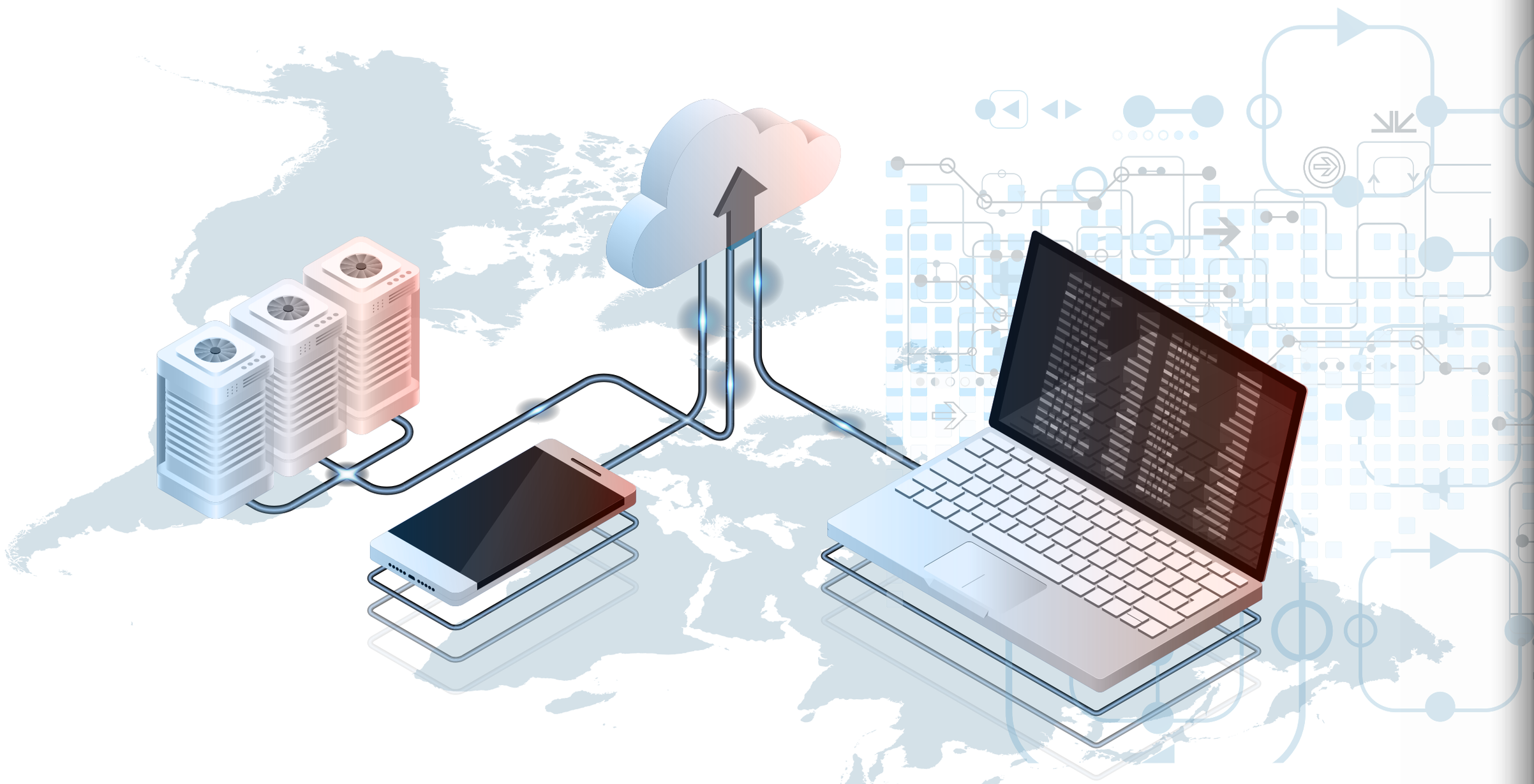
Sin datos no hay pruebas. Sin pruebas no hay justicia

El uso de estas tecnologías y plataformas de nube traen consigo múltiples y potentes beneficios para sus usuarios, pero también abren riesgos en materia de seguridad de la información que deben ser adecuadamente evaluados para abordarlos correctamente y seleccionar los modelos de servicio correctos para computación en la nube a utilizar, y la modalidad de implementación de computación en la nube, nube pública, nube privada, nube comunitaria o nube híbrida.



10 Principales riesgos de seguridad en la nube

1.- **RESPONSABILIDAD** y riesgo de datos
2.- **FEDERACIÓN** de identidad de usuario
3.- **CUMPLIMIENTO** legal y regulatorio
4.- **CONTINUIDAD** y resiliencia del negocio
5.- **PRIVACIDAD** del usuario y uso secundario de datos
6.- **INTEGRACIÓN** de datos y servicios
7.- **ARRENDAMIENTO** múltiple y seguridad física
8.- **ANÁLISIS** de incidencias y análisis forense
9.- **SEGURIDAD** de la infraestructura
10.- **EXPOSICIÓN** al entorno no productivo



R1. RESPONSABILIDAD Y RIESGO DE DATOS

En el caso del centro de datos tradicional, su seguridad está completamente en manos de la propia organización. Deben ocuparse de la seguridad de los datos, la seguridad de las aplicaciones, la seguridad de la red y la seguridad física, etc.
Sin embargo, cuando la organización decide pasar a la nube, ¿quién se encarga de la seguridad en estas capas? en el modelo de servicio en la nube se define quién será responsable de la seguridad en cada capa.
El consumidor de la nube debe cuidar la seguridad en cada capa mientras implementa sus servicios en la nube. El consumidor debe considerar cuidadosamente todos los riesgos de seguridad críticos y mitigarlos.
Los consumidores de la nube deben garantizar la garantía de recuperación de datos, ubicación de almacenamiento de datos, cifrado de datos, etc.

R2. FEDERACIÓN DE IDENTIDAD DE USUARIO

La autenticación y autorización de usuarios en las plataformas de computación en la nube son fundamentales para la seguridad de la infraestructura de una organización. En la infraestructura tradicional, las identidades de los usuarios para diferentes recursos están bajo el control de la propia organización y los usuarios pueden acceder a esos recursos dentro de la organización. Pero, en el caso de la nube, el rango de accesibilidad aumentó. Las organizaciones necesitan implementar soluciones avanzadas de administración de identidades y accesos como SAML, OAuth y 2FA.

R3. CUMPLIMIENTO LEGAL Y REGULATORIO

Sabemos que la mayoría de las regulaciones responsabilizan en última instancia al usuario del servicio de la seguridad e integridad de sus datos corporativos y de los clientes, incluso cuando están en manos del proveedor del servicio.

Los centros de datos en la nube están ubicados en áreas remotas donde la energía es barata y la conexión de fibra está disponible. El consumidor de la nube debe conocer la ubicación del centro de datos donde se almacenan sus datos porque los datos que se perciben como seguros en un país no se pueden percibir como seguros en otro país.

La visibilidad debe existir entre las organizaciones y los proveedores de la nube sobre SOX, PCI, ISO27017, ISO27018 y otras regulaciones basadas en recursos.

R4. CONTINUIDAD Y RESILIENCIA DEL NEGOCIO

La continuidad del negocio es un proceso que implementa una organización de TI para garantizar que el negocio pueda funcionar incluso en situaciones desfavorables.

¿Qué sucede si su centro de datos no funciona debido al mal tiempo u otros desastres naturales? ¿El centro de datos tiene un plan de recuperación ante desastres para que pueda volver a estar en funcionamiento lo antes posible? Asegúrese de que los proveedores de la nube estén certificados según los estándares de continuidad empresarial como ISO22301 / ISO27001.

R5. PRIVACIDAD DEL USUARIO Y USO SECUNDARIO DE DATOS

Cuando mueve sus datos a la nube, disminuye el control sobre sus datos total o parcialmente. Debe asegurarse con sus proveedores de la nube qué datos pueden o no pueden ser utilizados por ellos para fines secundarios, ya que la mayoría de los sitios sociales comparten sus datos con la menor restricción. Los consumidores de la nube también deben saber cómo se comparten sus datos y cómo se accede a ellos a través de las fronteras jurisdiccionales.

R6. INTEGRACIÓN DE DATOS Y SERVICIOS

Durante la transmisión de datos entre el consumidor de la nube y el centro de datos de la nube, estas preguntas deben responderse:

¿Qué tan seguras son las llamadas a la API REST?
¿Qué tan seguras son las bases de datos que contienen los datos?
¿Debería cifrar los datos y cómo administra todas esas claves?

Los medios de transmisión de datos inseguros pueden comprometer los datos confidenciales

R7. ARRENDAMIENTO MÚLTIPLE Y SEGURIDAD FÍSICA

El espacio proporcionado por los proveedores de la nube es compartido por varios usuarios en el entorno de la nube. Los consumidores de la nube se aseguran de que la separación lógica del espacio sea lo suficientemente segura para que ningún otro usuario pueda ver sus datos. Los proveedores de servicios en la nube deben implementar un control de acceso adecuado al espacio compartido para que, en caso de comprometerse, el recurso de un usuario no pueda afectar los datos de otros usuarios.

R8. ANÁLISIS DE INCIDENCIAS Y ANÁLISIS FORENSE

Si ocurre algún incidente de seguridad, debe conocer todos los registros de todos los recursos conectados. En caso de incidentes de seguridad, puede ser una situación difícil para los consumidores de la nube detener el ataque.

Los datos de registro a menudo incluyen información sobre otros usuarios y el acceso de auditoría puede estar restringido debido a los recursos compartidos.

R9. SEGURIDAD DE LA INFRAESTRUCTURA

Asegúrese de que su proveedor de servicios en la nube conozca todos los servicios en ejecución, puertos abiertos, políticas de contraseñas y otras configuraciones de seguridad en el entorno de la nube.

Se deben implementar mecanismos de control de acceso adecuados de acuerdo con el rol del usuario y se deben realizar evaluaciones de riesgo periódicas.

R10. EXPOSICIÓN AL ENTORNO NO PRODUCTIVO

Los entornos que no son de producción son buenos para realizar pruebas de seguridad internamente dentro de una organización. Evite el uso de datos reales o confidenciales en entornos que no sean de producción.

Asegúrese de que sus otros entornos de no producción sean tan seguros como sus entornos de producción. Asegúrese de que cualquier persona que trabaje en estos entornos tenga implementadas medidas de acceso privilegiado.

PARA TENER EN CUENTA

Las unidades comerciales y las organizaciones de TI deben evaluar los beneficios y riesgos comerciales de los productos basados en la nube. Las organizaciones deben evaluar los riesgos de la computación en la nube, identificando los controles apropiados y los casos de uso. La seguridad en la computación en la nube es una responsabilidad compartida entre el departamento de TI de una empresa y el proveedor de servicios en la nube. Por lo tanto, incluso cuando la infraestructura de TI se puede trasladar a la nube, la responsabilidad de la seguridad de la información no se puede subcontratar por completo al proveedor de servicios en la nube.

Se sugiere utilizar herramientas como la matriz de controles de la CSA v4.0 o superior, verificar los controles requeridos por:
ISO/IEC 27017 , ISO/IEC 27018 , ISO/TR 21332 y ISO/IEC 27036-4 .

Chile se encuentra en la etapa final de modernización de su ley de delitos informáticos, producto de la adhesión del país a la Convención de Budapest sobre Cibercrimen y la ley de protección de datos personales. Por esta razón resulta prudente imponer como requisito para la contratación de servicios de computación en la nube, que los países que albergarán nuestros datos y servicios cuenten con herramientas legales de igual o superior fortaleza; sin un parámetro relevante a considerar si el país depositario de nuestra confianza ha adherido a la convención internacional sobre cibercrimen.

EL TRABAJO DE LA CSA POR **UNA NUBE MÁS SEGURA**

Generar mejores prácticas, definir estándares, promover la colaboración e impulsar la concientización, con el fin de tener ambientes cloud más seguros. Esa es la misión de Cloud Security Alliance (CSA), organización internacional cuyo más alto gerente tecnológico estuvo dispuesto a conversar con CiberSucesos.

Daniele Catteddu
Chief technology officer (CTO)
de la CSA

"En los más de diez años de existencia de la CSA y nuestra experiencia apoyando la adopción segura de la computación cloud, creo que hemos suficientes datos para entender que asegurar la nube significa asegurar un ambiente que es extremadamente volátil, con muchos usuarios y organizaciones diferentes, con necesidades, recursos, mentalidades y madurez diferentes", explica Daniele Catteddu, chief technology officer (CTO) de la CSA, desde la sede de ésta en Helsinki.

La Cloud Security Alliance (CSA) es una organización internacional dedicada a crear un ambiente más seguro en la nube, explica el alto gerente.

EL PASO A PASO

Catteddu detalla que, para lograr su objetivo de una experiencia más segura en la nube, la CSA aplica distintos procesos y habilidades, los que se resumen en la creación de guías, mejores prácticas, marcos de referencia, capacitación y concientización hacia la comunidad, de forma gratuita.
Este proceso se compone de varias fases, indica el experto:

1. Crear nuevas mejores prácticas para satisfacer de mejor manera los requerimientos actuales y futuros de una audiencia más madura y con más experiencia en la nube.

2. Extender el ámbito de nuestro trabajo de a otras tendencias tecnológicas relevantes "conectadas a la nube" o "cloud relevant", como el internet de las cosas (IoT), DLT, Inteligencia Artificial (IA), computación cuántica, etc.

3. Actualizar o mejorar las mejores prácticas centrales de la CSA, como la CSA Security Guidance y CCM, para entregar bases sólidas y consistentes a cualquiera que se acerca por primera vez a la seguridad en la nube.

4. Crear material de capacitación y educación para apoyar la mejora continua del conocimiento y las habilidades de los practicantes, además de la concientización general.

5. Crear transparencia y aseguramiento basados en marcos de confianza.

6. Conectar con la comunidad y establecer redes de pares.

7. Esto solo es posible con la colaboración con varias agencias gubernamentales de los distintos países en los que opera la CSA, además de asociaciones de empresas y entes reguladores, cuerpos de estandarización internacional y la academia.

SE ACABÓ EL MITO DE UNA NUBE INSEGURA

Cattedu explica a continuación que a gracias a cuantiosos esfuerzos por parte de las firmas de servicios cloud de enfocarse en la transparencia y el aseguramiento (en conjunto con la CSA, como parte de su programa STAR), considera que ha ocurrido un cambio en la percepción de la comunidad respecto del uso de la nube, y hoy "la percepción de que el ambiente en la nube es menos seguro que una solución física en las instalaciones de la organización se terminó, y todos entienden que en la gran mayoría de los casos la nube entrega una mayor seguridad".

Por lo mismo, el problema hoy no son las percepciones erradas, sino temores legítimos de quienes se preocupan de la forma en que los proveedores de servicios cloud pueden estar tratando sus datos personales, debido a sonados casos que demuestran la complejidad del manejo de este tipo de información, su procesamiento y su transferencia.

Ahora sí, existen todavía percepciones erradas, admite el experto, siendo una muy importante la idea equivocada de muchos usuarios de que la seguridad es responsabilidad exclusiva del proveedor de la nube, sin entender sus propias responsabilidades en la seguridad, lo que se demuestra en las estadísticas, ya que la mayor parte de las brechas de seguridad se generan por malos comportamientos de los usuarios.

NOVEDADES Y PROYECCIONES

Finalmente, Catteddu delinea los próximos movimientos de la CSA para seguir haciendo más seguros los ambientes cloud a medida que estos se vuelven más comunes y complejos. "Nos movemos en varios frentes distintos, con varias iniciativas distintas pero igualmente importantes", explica. Tantos que no puede detallarlos todos por un tema de espacio y tiempo, se disculpa, pero sí describe algunos de ellos.

Por ejemplo, en el campo de la investigación, la CSA lanzó a principios de 2021 la cuarta versión (o V4) de la Cloud Control Matrix (CCM, Matriz de Control Cloud), actualización de un marco de referencia de control alineado con las mejores prácticas y "considerado un estándar de facto para la seguridad en la nube", asegura Catteddu. Los componentes de la CCM V4 son lanzados por partes a lo largo de un año, por lo que la alianza se encuentra casi lista para lanzar algunos de estos más nuevos componentes, como las Directrices de Implementación y Auditoría y el CAIQ.

"Al mismo tiempo, tenemos varios grupos trabajando en nuevos documentos sobre Key Management, DevSecOps y Top Threats, entre otros", agrega el CTO.

En materia de colaboración, Catteddu destaca el lanzamiento en marzo de un nuevo Certificado de Conocimientos de Auditoría Cloud (CCAK) en colaboración con ISACA, con lo que, señala, se cubre lo que era un gran vacío de conocimiento en un área clave: la evaluación y la auditoría.

De cara al mañana, las tendencias que el experto identifica como las más comentadas hoy por hoy en materia de cloud son DevOps, automatización, la Infraestructura como Código, el "software-defined-everything" o SDx y el compliance contínuo. Que sean los conceptos de moda no quita que efectivamente sean para donde Catteddu cree que evolucionará la computación cloud. Por ejemplo, a medida que crecen las nubes, estas requieren una mayor automatización, lo que encaja perfectamente con DevOps, que a su vez permite definir y mantener la Infraestructura como Código de una organización.

ANÁLISIS FORENSE **EN LA NUBE**

Cuando se usan los servicios de cloud computing se alcanzan grandes beneficios de eficiencia y seguridad en las diferentes modalidades IaaS, Paas, SaaS u otras combinaciones, pero eventualmente algo puede fallar o más bien puede ocurrir un ciberataque a alguno de los componentes del servicio. En estos casos puede ser necesario recurrir a un análisis forense para identificar las causas del incidente u obtener evidencias digitales para presentarlas en alguna causa judicial que se haya iniciado.

¿Qué es la **informática forense**?

La ciencia forense se define generalmente como la aplica ción de las ciencias físicas al Derecho en la búsqueda de la verdad Si pensamos en la informática como ciencia forense, podemos concluir que es una disciplina que implica la pre servación, identificación extracción, documentación e inter pretación de los medios informáticos para el análisis de las pruebas o de la causa raíz.

Debido a su relativamente nuevo campo de interés, y a la na turaleza rápidamente cambiante de la tecnología, la infor mática forense es única en el amplio campo de las especiali dades forenses. Sin embargo, hace veinte años no existía como la disciplina estructurada, metódica y reconocida que es hoy. En su lugar, las pruebas electrónicas se obtenían y procesaban por cualquier medio disponible y conocido, con poca o ninguna consideración de las características especia les que acabamos de mencionar, y asimiladas a las pruebas tradicionales.

Afortunadamente, esto ha cambiado mucho. Aunque todavía no existe una formación bien establecida y oficial para los especialistas en informática forense, hay muchos programas de formación y certificaciones reconocidos que pueden eva luar la competencia de los expertos en informática forense.

Entonces cuando se intenta obtener evidencias o las causas de un incidente en un entorno de nube lo único que estamos haciendo es aplicar la ciencia forense a una tecnología digi tal específica lo que nos permite hablar de Análisis Forense en la Nube.

FASES DEL **ANÁLISIS FORENSE**

Aunque las tareas específicas difieren de un caso a otro, en general se considera que una investigación informática forense comprende ocho pasos, que pueden agruparse en cuatro procesos de alto nivel: Identificación, Recogida y Preservación, Examen y análisis, e informe y presentación, seguidos de un último paso de decisión, cuyos detalles pueden encontrarse en el estándar internacional ISO27037

IDENTIFICACIÓN

La primera fase consiste en analizar la infraestructura de información para identificar los dispositivos clave en los que se puede encontrar información relevante.
Aquí comienzan las primeras dificultades para un análisis forense, en el sentido de que no es viable, de una manera tradicional o simple, la incautación del medio físico de los datos de interés.
Entonces el enfoque en primera instancia se centra en el rescate de los datos de interés por un mecanismo que dé garantías de confidencialidad, integridad y disponibilidad para su uso en un juicio posterior por ejemplo; todo esto sin tener que requerir el medio físico al proveedor de nube que probablemente esgrimirá que los datos están distribuido en múltiples medios y que a la vez son medios físicos compartidos con otros clientes de la nuble.

RECOGIDA Y CONSERVACIÓN

Una vez identificada la información relevante, se inicia una nueva fase que abarca su recogida y preservación. Como ya hemos mencionado, los retos técnicos que plantean los procesos de recogida obligan a poner el máximo cuidado en no alterar el contenido de las pruebas. La primera "regla de oro" para evitar la modificación accidental de pruebas es trabajar, siempre que sea posible, con copias de la información original. Por ello, la práctica habitual exige que se realice una copia forense del contenido del soporte de almacenamiento original y que éste sea custodiado por las autoridades oficiales. La expresión copia forense significa que se garantiza que la copia es idéntica al original y que el proceso de obtención no ha alterado el dispositivo original.
Por tanto, para el enfoque sobre la nuble, resulta más relevante finalmente obtener acceso al dato y proveer las garantías de que este es fiel copia del original, más que el medio físico en sí.

EXAMEN Y ANÁLISIS

Durante esta fase, se identifican y analizan todos los artefactos contenidos en los repositorios de datos recopilados con el fin de extraer información relevante para el caso. La mayoría de las tareas que se realizan son de carácter muy técnico y requieren mucho tiempo, debido a la mano de obra y la capacidad de procesamiento necesarias para analizar el enorme volumen de datos que se suelen recoger. De nuevo, en esta fase se utilizan soluciones de software especializadas, que proporcionan al investigador las herramientas que necesita y preservan la integridad de la información. Algunos conjuntos de herramientas forenses ampliamente utilizadas en entornos tradicionales y que han sido exitosamente aplicadas a los entonos cloud son:

- Encase de Guidance
- Fastdump
- Memoryze
- Volume Block copy
- Agent injection
- AWS Export

INFORME Y PRESENTACIÓN

La última etapa consiste en presentar los resultados de la investigación, normalmente un informe pericial, a la persona responsable del expediente para que lo revise y, si es necesario, testifique ante el tribunal.

¿Qué dificultades particulares representa **hacer análisis forense en la nube**?

La ciencia forense digital para la computación en nube plantea nuevos retos técnicos y jurídicos. La computación en nube hace que la investigación forense sea diferente, sobre todo por la naturaleza remota de las pruebas, la falta de acceso físico y la confianza que se requiere en la integri dad y la autenticidad. Aunque los objetivos del examinador forense son los mismos que antes, los problemas difíciles no convencionales incluyen la adquisición forense de datos remotos, los grandes volúmenes de datos, los datos distri buidos y elásticos, la cadena de custodia y la propiedad de los datos.

La incautación y adquisición de artefactos digitales son los pasos iniciales del proceso forense. Existen dos escenarios posibles: los investigadores remotos podrían recoger las pruebas forenses ellos mismos desde la fuente, o los pro veedores podrían entregarlas. Cada escenario requiere un grado diferente de confianza en los datos devueltos.
Ya hay estudios que han logrado verificar las herramientas tradicionalmente utilizadas en esta disciplina son técnica mente capaces de obtener información desde entornos cloud quedando si aún pendientes por resolver aspectos de fiabilidad de los datos, en atención a las múltiples capas de confianza que son necesarias.

Aún quedan desafíos por resolver y la convención de Buda pest sobre cibercrimen, a través del “Cloud Evidence Group”, el “Transborder Group”, entre otros, están trabajando en la modernización de la cooperación y divulgación de las evi dencias electrónicas en los nuevos escenarios tecnológicos, donde uno de ellos es la nube.

Por el momento las dificultades para acceder a los medios físicos de estos entornos nube hacen pensar que la solución ha de pasar por que el análisis esté centrado en los datos y las cadenas de confianza para obtenerlos y resguardarlos tanto las copias de los datos como los originales mientras duren los proceso judiciales, necesitándose que los provee dores evolucionen en esta dimensión de la seguridad para apoyar estos requerimientos cuando sean necesarios.

CSA Chile Chapter

LAS DEFINICIONES CLAVE PARA SABER SI LA **NUBE ES PARA NOSOTROS**

Al momento de saber si como organización debemos pasarnos a un entorno cloud, es esencial evitar las generalidades. La nube no sirve para todos, ni tampoco el migrar a lo cloud requiere necesariamente que se haga de una vez y para todos nuestros sistemas. Todo dependerá de las necesidades de nuestra empresa, de los riesgos que estamos dispuestos a soportar, y de la regulación, entre otros factores.

Al momento de saber si como organización debemos pasar nos a un entorno cloud, es esencial evitar las generalidades. La nube no sirve para todos, ni tampoco el migrar a lo cloud requiere necesariamente que se haga de una vez y para todos nuestros sistemas. Todo dependerá de las necesidades de nuestra empresa, de los riesgos que estamos dispuestos a soportar, y de la regulación, entre otros factores.

Mucho se habla hoy en día de moverse a la nube como si fuera una obligación para las empresas. Pero antes de tomar esa decisión, es necesario analizar concretamente las nece sidades y riesgos que enfrenta la organización para el logro de sus objetivos.
Así lo explica Ricardo Urbina, presidente del capítulo chileno de la Cloud Security Alliance (CSA), quien nos define las prin cipales consideraciones que debe tener la adopción de en tornos cloud en el contexto de nuestro país.
Por eso, continúa el también CISO de Elecmetal, el análisis sobre la conveniencia de pasar a la nube puede hacerse solo después de que la organización tenga claras las amenazas y requerimientos de sus funciones, en base, por ejemplo, al tipo de datos que maneja y las leyes y regulaciones que rigen en la industria de la que forma parte, además de las obliga-ciones que debe cumplir con sus trabajadores, clientes y pro-veedores.

Y es que la nube no es una solución ideal para cualquier situación. "Al revisar las historias de fracaso en la nube, pode-mos verificar que no se realizó una evaluación en detalle de las exigencias de cada organización, para saber si son com-patibles con lo que los servicios de nube ofrecen", explica Urbina.

Del mismo modo, incluso cuando la empresa decide que la nube puede ser útil para ella, eso no significa que se deba llevar todo al entorno cloud. "La evaluación puede ser par-cial", indica el presidente de CSA en Chile, para funciones como las siguientes, por ejemplo:

Ricardo Urbina
Presidente del capítulo chileno de la CSA

CSA | Chile Chapter

1.- Aplicar niveles de seguridad sin tener que adquirir equipos y el conocimiento para operarlos.

2.- Permitir el respaldo de datos fuera de mi instalación para protegerlos de un posible ataque de ransomware.

3.- Mover las páginas web para poder ges tionar períodos de mayor demanda y poder fácilmente crecer en servidores para atender ese tráfico.

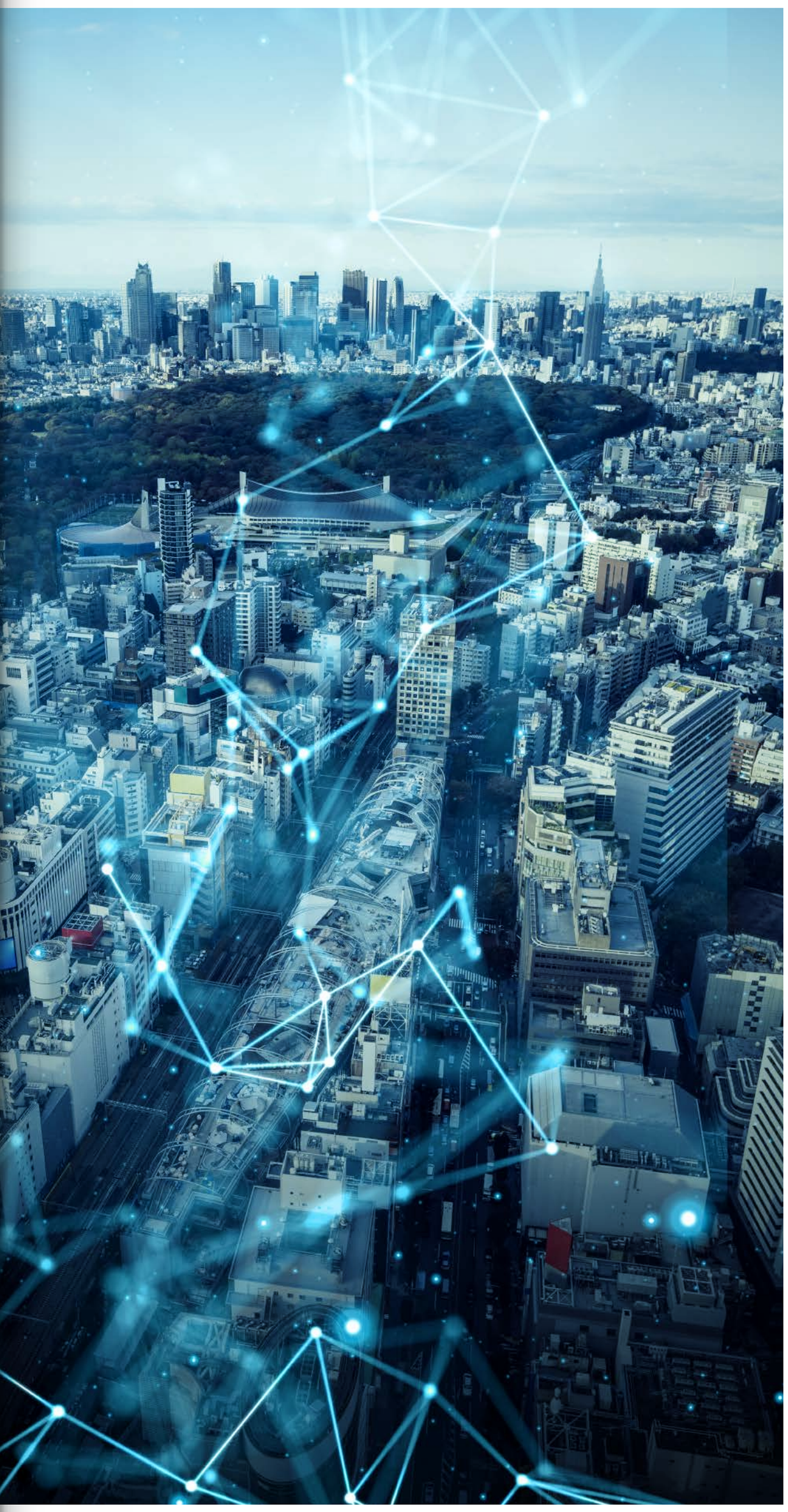
4.- Habilitar la alta disponibilidad de datos y de red y disponer de servicios de au-tenticación centralizados entre distin-tas aplicaciones.

TENER CONCIENCIA **DE LOS RIESGOS**

Lógicamente, una de las razones que más detiene a muchas compañías al momento de analizar la conveniencia de migrar a la nube son los potenciales peligros que podría suponer. Al respecto, Urbina explica que "usar servicios en la nube tiene riesgos, al igual que los servicios almacenados de forma local", pero que "la gran diferencia es que los proveedores de servicios en la nube cumplen con muchas normativas y certificaciones que avalan el uso de las mejores prácticas, y por lo tanto una gestión controlada de los riesgos. Difícilmente en los servicios locales se cumplen tantas certificaciones, por lo que la idea de una mayor seguridad es una ilusión".

Además de la evaluación de las propias necesidades y los riesgos, agrega el experto, el paso siguiente es evaluar lo que ofrecen los distintos proveedores de nube, en términos de certificaciones, diferentes modelos de servicio y su reputación, incluyendo en el análisis los potenciales controles extra necesarios debido a que se estén llevando parte de los datos de la empresa a un tercero, como es el proveedor.

"Desde Cloud Security Alliance ofrecemos guías para evaluar a los proveedores de nube. De igual modo, certificamos a los profesionales que manejan el proceso de evaluación, así como también aportamos una norma certificable por los proveedores", explica Urbina, agregando que "hoy en día, todos los proveedores grandes cloud tienen algún nivel en nuestro modelo de nuestra certificación".



LAS ACTIVIDADES EN **CHILE**

El ejecutivo asimismo define las tareas que cumple el capítulo chileno de la CSA, siendo la fundamental el difundir las mejores prácticas que define la misma organización a nivel internacional. Para ello, se han realizado recientemente algunas de las siguientes acciones:

- Firma de convenio de colaboración con el Ministerio del Interior y Seguridad Pública.
- Firma de convenio de colaboración con la Universidad Mayor.
- Participación en el Comité Académico de CyberSEC de la Usach.
- Participación en eventos de Segdata, Convid, Escuela Sochisi, Owasp, ISACA, ISSA, ISC2, Inacap, LOL Tech Connect.
- Realización de presentaciones a instituciones de la banca y el comercio minorista.
- Aparición en medios como TrendTIC, Revista Gerencia y Radio Demente.
- Concientización a través de Linkedin (Cloud Security Alliance, Chile Chapter) y Twitter (@CloudSA_cl)

Muy importante además es la capacitación de profesionales a través del Certificate of Cloud Security Knowledge (CCSK), que valida los conocimientos que tienen los profesionales de seguridad en la nube, explica Urbina. Esto incluye cursos en la Universidad Mayor que apoyan a los alumnos que están optando a dicha certificación.

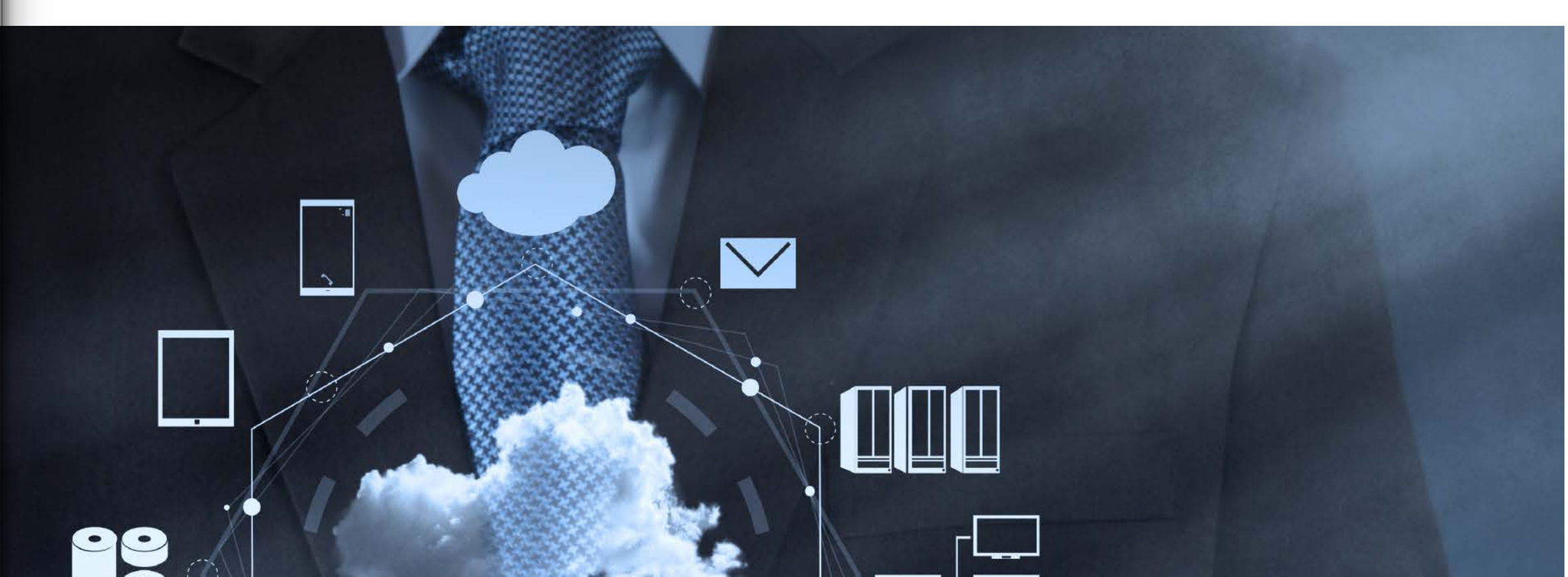
Finalmente, y también como invitación, el líder de la CSA en Chile menciona tres eventos que vienen en los próximos meses: Convid-2021 el 19 de junio, Cloud Security Day con Sochisi el 20 de agosto y un evento que harán para hablar en detalle sobre la Cloud Control Matrix (CCM).

LA MIRADA LEGAL DE LA NUBE PARA **LA ADMINISTRACIÓN DEL ESTADO**

En ediciones anteriores de esta revista hemos abordado el tema de la transformación digital y como el Estado se ha comprometido con ella a través de la publicación de la Ley 21.180, la cual impulsa la digitalización de la administración pública. Hemos hablado de sus ventajas y también de los riesgos asociados a la misma, pero no hemos hablado sobre la infraestructura que permitiría aquello.

Tanto es así, que la adopción de la nube ha ido en aumento desde hace décadas y ahora ha llegado a un nivel en el que no vemos ningún entorno de TI "sin nube".

Teniendo en cuenta este tremendo aumento, no es exagerado decir que todos los sectores podrían estar utilizando una u otra forma de procesos de computación en la nube para sus actividades habituales.



¿Pero qué es lo que impulsa a los gobiernos a adoptar esta tecnología?

La respuesta está en la capacidad de la nube para prestar servicios de forma eficiente a través de la red, a bajo costo y de manera escalable.

Así, podría decirse que las mayores ventajas de la computación en nube para el sector público en general son el aumento de los niveles de eficiencia y la reducción de costos. Ello porque no hay necesidad de adquirir un costoso hardware local, ni incurrir en costos de mantenimiento, más allá de los computadores de escritorio o portátiles. Esto libera a una organización de grandes costos, así como de los ciclos de vida del hardware. En el entorno de la nube, la mayoría de los costos son operativos, mientras que la escalabilidad es casi infinita. Esto es especialmente útil para los aumentos estacionales de la demanda de servicios o para aquellos casos en que se requiera de una rápida migración a la nube.

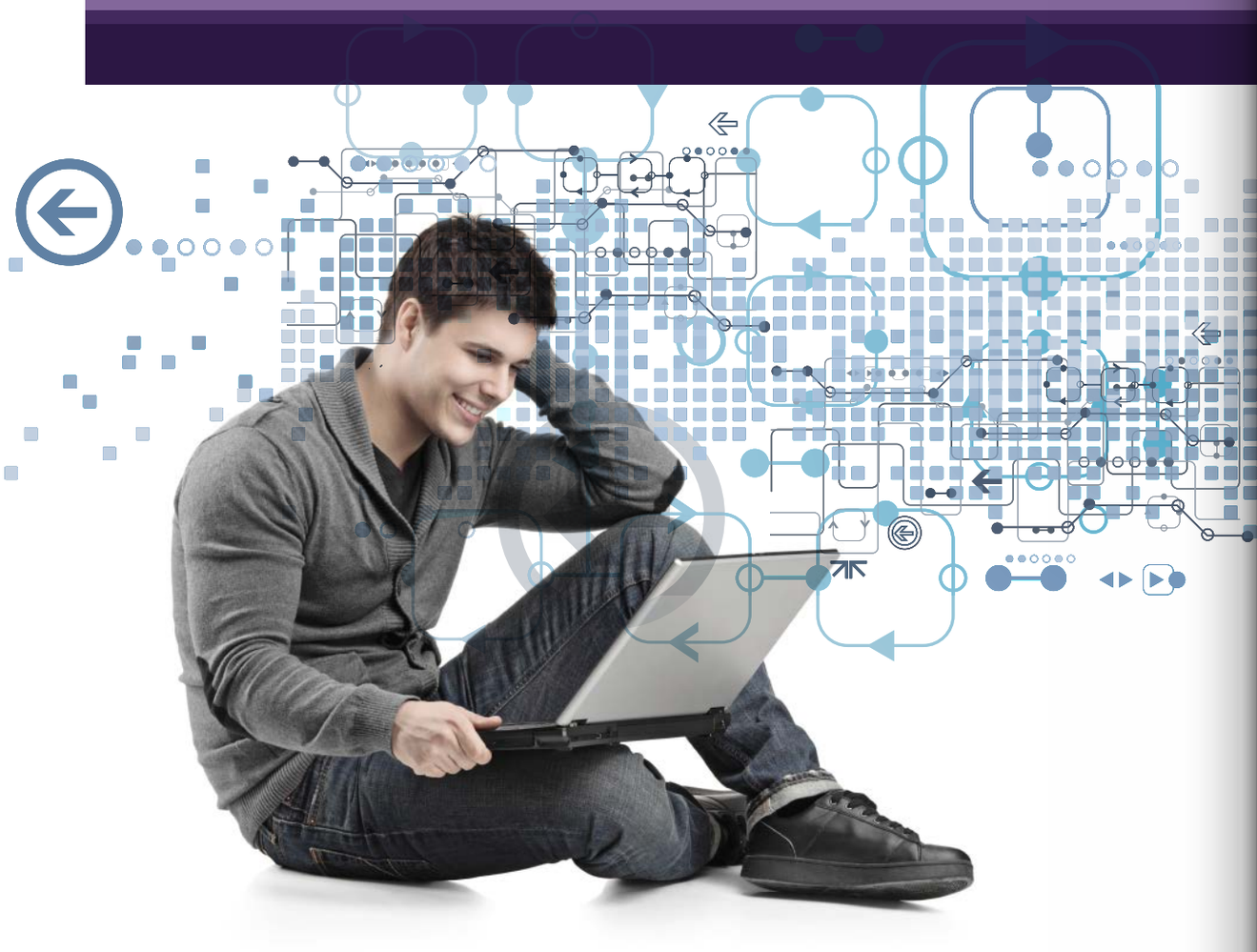
Retos de la computación en nube para el sector público

A pesar de todos los beneficios que presenta esta tecnología, también existen riesgos que deben ser gestionados para su correcta implementación.
De los riesgos que ya se mencionaron en el artículo central, el relativo a los aspectos legales sobre los datos en la "nube" resulta ser una cuestión sumamente compleja, debido a la aterritorialidad de la misma versus la territorialidad del derecho inherente a todo ordenamiento jurídico. Esta cuestión es fundamental para determinar la legislación aplicable a los datos almacenados en terceros países, los cuales pueden consistir en datos personales e incluso de información crítica para la seguridad nacional.
Hace algunos años, con los servicios de data centers para Housing que no se encontraban en la nube el problema recién planteado se resolvía fácilmente, ya que el tema central jurídicamente era localizarlos territorialmente a fin de intentar aplicarles normas jurídicas específicas, y hacer efectiva la posible "responsabilidad" derivada de algún delito o incumplimiento. Al día de hoy, efectuar dicho ejercicio resulta prácticamente imposible porque los servidores son enlazados, distribuidos y ubicados en diversos países.
El hecho de que existan normas extranjeras como el CLOUD ACT de USA que autoriza a las autoridades a acceder bajo ciertas circunstancias a la información almacenada por las empresas prestadoras de este tipo de servicios hacen esta situación aún más compleja.
En ese contexto es de suma relevancia que las instituciones gubernamentales que contraten servicios en la nube adopten medidas preventivas desde el Derecho para garantizar la seguridad de la información.

Así, desde el punto de vista del Derecho, este no se opone a la "nube" sino que le exige control:

a. Para la seguridad de las personas: mediante el control de acceso y sesiones, que busca determinar la responsabilidad de los agentes que intervienen los documentos y datos contenidos en el sistema; el control sobre los usuarios y los recursos utilizados con el fin de permitir identificar responsabilidades laborales de los empleados y la segregación de funciones.

b. Para la seguridad de los bienes y activos de la información: mediante el control de los sistemas, lo que permite identificar la responsabilidad por acciones maliciosas sobre estos; mediante el control sobre datos y procesos y sus modificaciones, lo que permite construir las pruebas necesarias para su presentación y eficacia en juicio como también el determinar las responsabilidades por el uso de datos personales.



Para lograr este control y así garantizar la seguridad de la información, la principal herramienta a utilizar es el contrato, el que es una ley para las partes. Por ello es importante que el contrato contenga los elementos esenciales para resguardar los controles que el derecho le solicita para resguardar la seguridad jurídica y eficacia de los derechos y obligaciones que emanan de él.

Así si se contrata infraestructura de nube como servicio con capacidades de procesamiento y almacenamiento, el contrato debiera a lo menos señalar las certificaciones que se solicitará al proveedor, el SLA del servicio y las multas asociadas al incumplimiento, la responsabilidad en la migración de los datos, la propiedad intelectual, la confidencialidad de la información entre otros.

Para determinar las exigencias a plasmar en el contrato de servicios en la nube, es fundamental que las instituciones públicas se hagan las siguientes preguntas respecto de la información y servicio:

¿La información almacenada es sensible para la Seguridad Nacional?, ¿Es dicha información pública o es reservada de conformidad a lo dispuesto en la Ley N° 20.285?, ¿Cuán importante es para la organización mantener en reserva la información que se subirá? ¿Cuáles son las consecuencias en caso de que esta información se filtrara?, ¿Se comprenden bases de datos de personas naturales?, ¿Son estos datos sensibles?, ¿En las bases de datos se contiene información comercial sensible o perteneciente a empresas que no han autorizado la divulgación de dicha información?

Es en base a estas preguntas que el servicio público debiera determinar el servicio a contratar y las exigencias contractuales del mismo. Como podría serlo la contratación de una nube privada con datacenters que tengan presencia nacional para garantizar una mejor protección de los datos y la aplicación de la legislación Chilena.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl