



1

estos problemas según la configuración. Cuando las soluciones se implementan para satisfacer necesidades relacionadas con la misión, pueden proporcionar beneficios o mejoras en lo siguiente:¹



Soporte más amplio: Las organizaciones pueden elegir entre una amplia gama de proveedores de nube.



Flexibilidad en el diseño: Los servicios en la nube ofrecen funciones administradas como almacenamiento de documentos, almacenamiento de bases de datos con replicación e interfaces de aplicaciones para la automatización.



Rendimiento escalable: Los servicios en la nube admiten un amplio rango de escalabilidad horizontal.²



Disponibilidad: Los servicios en la nube pueden gestionar fallas de la infraestructura subyacente de la organización y mover el código en ejecución con una interrupción mínima.



Costo: Los servicios en la nube pueden aumentar la eficiencia y al mismo tiempo permitir que las organizaciones dirijan recursos financieros hacia tareas fundamentales para la misión.



Recuperación ante desastres y continuidad comercial: Las organizaciones con datos e infraestructura en la nube fuera de las instalaciones pueden estar mejor posicionadas para gestionar eventos adversos en las oficinas locales (por ejemplo, desastres naturales) y recuperarse de estos.



Ciberseguridad: Los servicios en la nube suelen ofrecer opciones para diferentes aspectos de la seguridad, por lo que las organizaciones individuales no tienen que crear soporte para sí mismas; sin embargo, es fundamental que las organizaciones conozcan las opciones e implementen y configuren las que sean adecuadas para ellas.

Consideraciones para la adopción de la nube en el sector de la seguridad pública

Para aprovechar los beneficios potenciales de las soluciones basadas en la nube, las organizaciones de seguridad pública pueden elegir entre varias estrategias de adopción de la nube para adaptarse a sus necesidades. Las estrategias ejemplares popularizadas por la industria de la nube incluyen reubicar, refactorizar o rearquitectar, revisar o replataformar, reconstruir y reemplazar.³ Sin embargo, independientemente del modelo, la estrategia o el proveedor, se recomienda a las organizaciones que revisen las siguientes consideraciones para garantizar que la adopción de la nube sea la solución adecuada. Además, se recomienda que las organizaciones revisen las guías y los materiales sobre seguridad en la nube para evitar posibles problemas en la implementación basada en la nube.⁴

¹ Cybersecurity and Infrastructure Security Agency (CISA), "Cloud Security Technical Reference Architecture Version 2.0," Junio de 2022. <https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf>.

² La capacidad de agregar más máquinas al grupo de recursos de una organización.

³ CISA, ibid, 17.

⁴ Por ejemplo, la Agencia de Seguridad Cibernética y de Infraestructura (CISA) recomienda revisar el documento [Arquitectura de referencia técnica de seguridad en la nube \(Cloud Security Technical Reference Architecture\)](#), monitorear la base teórica Tácticas, técnicas y conocimientos comunes de adversarios de MITRE (ATT&CK®) para conocer la taxonomía del comportamiento de los adversarios cibernéticos y revisar conceptos esenciales como [gestión de identidad, credenciales y acceso](#) (ICAM, por sus siglas en inglés) y los servicios de seguridad de puntos finales.

Consideración n.º 1: Necesidades y alcance

En primer lugar, hay que determinar las necesidades organizativas y operativas que deben abordarse, ya que no todas las necesidades propias de la seguridad pública podrían satisfacerse fácilmente con soluciones basadas en la nube. Además, las regulaciones federales, estatales, locales, tribales y territoriales (FSLTT, por sus siglas en inglés) pueden imponer requisitos para conservar determinados datos e infraestructura en las instalaciones con fines de seguridad, redundancia y continuidad de las operaciones.

LOS SIGUIENTES SON ALGUNOS EJEMPLOS DE PREGUNTAS QUE SE PUEDEN CONSIDERAR:



¿La adopción de la computación en la nube⁵ es apropiada para la organización, el sistema o la aplicación?



¿Qué modelo de computación en la nube satisface mejor las necesidades organizativas (por ejemplo, modelos de nube privada versus nube híbrida)?



¿Las redes y sistemas existentes pueden soportar la migración hacia la nube?



¿La organización ya posee u opera sus propios servidores, hardware y centros de datos? ¿De qué manera la adopción de la nube podría afectar estas operaciones?



¿Hay personal calificado disponible para implementar, gestionar y respaldar la adopción de la nube?



¿Qué proveedor de servicios en la nube (CSP, por sus siglas en inglés) podría satisfacer las necesidades de la organización?



¿Qué requisitos FSLTT deben cumplir contractualmente las organizaciones si migran a la nube? Por ejemplo, ¿existen leyes que restringen el almacenamiento de datos confidenciales y el proveedor de servicios en la nube (CSP) puede cubrir esta necesidad?



¿Quiénes son los socios y las partes interesadas que deberían participar en la toma de decisiones, tanto al inicio como a medida que se mantienen los servicios en la nube?



¿De qué manera la adopción por parte de una organización afectaría su operación e interoperabilidad con socios jurisdiccionales?

Además de las consideraciones generales, los costos operativos y de almacenamiento son factores importantes a la hora de migrar a la nube. Como los servidores físicos y los centros de datos están ubicados fuera de las instalaciones y son administrados por el proveedor de servicios en la nube (CSP), las organizaciones pueden redirigir recursos hacia otras misiones o beneficiarse de una reducción en los costos operativos. La implementación de la nube puede reducir la necesidad de espacio físico, los gastos de capital o los gastos operativos. Además, los proveedores de servicios en la nube (CSP) podrían ofrecer diferentes niveles de apoyo para aliviar las preocupaciones relacionadas con el personal de las organizaciones.

LOS SIGUIENTES SON EJEMPLOS DE PREGUNTAS SOBRE LA OPTIMIZACIÓN DE COSTOS Y LA DOTACIÓN DE PERSONAL:



¿Cuál es la relación costo-beneficio?



¿El presupuesto actual permite realizar investigaciones iniciales y recopilar información?

⁵ El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) define la computación en la nube en NIST SP 800-145. [Según la definición del NIST, la computación en la nube](#) es “un modelo que permite el acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios)

que se puede aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios”.



Luego de la adopción, ¿de qué manera la organización mantendrá los servicios?



¿De qué manera la organización debe documentar y evaluar los gastos en compras o adquisiciones de nube?



¿Los proveedores de servicios en la nube (CSP) requerirán capacitación y certificación anual u otra capacitación regular para mantener niveles de competencia adecuados?



¿Existen puestos en la organización que podrían delegarse o externalizarse a los proveedores de servicios en la nube (CSP)? ¿El personal necesitará capacitación para gestionar la nueva cartera o será necesario modificar las descripciones de los puestos? ¿Será necesario contratar personal adicional?



Si no es factible comenzar a adoptar la nube en el corto plazo, ¿cómo deberían trabajar las organizaciones con sus líderes para determinar la necesidad y asignar recursos en el futuro?

Consideración n.º 2: Requisitos

Después de llegar a un consenso para adoptar servicios en la nube, las organizaciones deben investigar y documentar los requisitos en su solicitud de propuesta (RFP, por sus siglas en inglés) y su acuerdo de nivel de servicio (SLA, por sus siglas en inglés). Es imperativo describir de forma clara y completa las necesidades organizativas para garantizar un proceso de adopción exitoso. Además, las organizaciones deben consultar a sus equipos legales, de Tecnologías de la Información (IT, por sus siglas

⁶ "La infraestructura de la nube es una composición de dos o más infraestructuras de nube distintas que siguen siendo entidades únicas, pero están unidas por tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones". *NIST SP 800-154, La definición de computación en la nube del NIST.*

⁷ Algunos ejemplos de criterios son infraestructura, certificaciones, características del servicio, seguridad de datos y sistemas, y control de costos.

en inglés) y financieros para asegurarse de que los acuerdos contractuales sean claros y de que se cumplan los requisitos legales. Por ejemplo, es común que las organizaciones consideren una solución de múltiples nubes⁶. Aun así, esta solución requiere un enfoque de ciberseguridad diferente para optimizar los entornos y al mismo tiempo gestionar el conocimiento de la situación con cada proveedor de servicios en la nube (CSP) respectivo.

Los siguientes son otros temas que las organizaciones pueden considerar:



¿Cuáles son los requisitos técnicos, de seguridad y de precios?
¿Cuáles son los criterios de calificación propuestos para los proveedores de servicios en la nube (CSP)?⁷



¿Cuáles son los riesgos de seguridad que implican los servicios basados en la nube? ¿De qué manera las organizaciones abordarían estos problemas? ¿Cómo los abordarían los proveedores de servicios en la nube (CSP)?



¿Qué responsabilidades manejará el proveedor de servicios en la nube (CSP)? ¿De qué aspectos de la nube será responsable la organización?⁸



¿Cómo podrían las soluciones en la nube cumplir con los estándares de seguridad específicos de la seguridad pública?⁹



¿Cómo podrían las organizaciones mantener la autoridad sobre sus datos? ¿Cuáles son las distinciones entre los diferentes modelos de propiedad de datos en la nube (por ejemplo, datos creados antes de la migración a la nube versus datos producidos en la nube)?

⁸ Las organizaciones deben hacer referencia a las matrices de responsabilidad del cliente del proveedor de servicios en la nube (CSP) que definen las responsabilidades de seguridad y actualización del proveedor y del cliente.

⁹ Entre los estándares o requisitos de ejemplo se incluyen la [Política de seguridad de los Servicios de información de justicia penal \(CJIS, por sus siglas en inglés\) de la Oficina Federal de Investigación \(FBI, por sus siglas en inglés\)](#), el [Programa federal de gestión de riesgos y autorizaciones \(FedRAMP, por sus siglas en inglés\)](#), la [Ley de Portabilidad y Responsabilidad del Seguro Médico \(HIPPA, por sus siglas en inglés\)](#) y otras regulaciones federales, estatales, locales, tribales y territoriales (FSLTT, por sus siglas en inglés).



¿Cuáles son los requisitos para garantizar que las organizaciones mantengan una cadena de custodia¹⁰ de sus datos mientras utilizan servicios en la nube? ¿Cuáles son los requisitos de evidencia de datos en la nube que deben cumplir las organizaciones?



¿Cómo se gestionarán los incidentes de ciberseguridad y cuáles son las responsabilidades de las organizaciones y los proveedores de servicios en la nube (CSP)?



¿Será necesario instalar una herramienta de gestión de dispositivos en todos los dispositivos vinculados a la nube?



¿De qué manera los servicios en la nube mejorarán el acceso seguro?



¿Cómo apoyarán los proveedores de servicios en la nube (CSP) los servicios de auditoría?



¿Qué requisitos jurisdiccionales o locales pueden influir en la propiedad, la retención, el almacenamiento y la privacidad de los datos?

LAS SIGUIENTES SON ALGUNAS SOLICITUDES DE EJEMPLO:



- Una descripción general de la empresa, incluidas referencias y testimonios específicos en relación con la seguridad pública.
 - o ¿Qué pólizas de seguro tiene vigente la empresa? ¿Cumplen los requisitos de misión? ¿Cómo afectará la política a los clientes? ¿Hay otros clientes de seguridad pública que puedan ser contactados como referencias?



- Indicación de la capacidad del proveedor de servicios en la nube (CSP) para cumplir los requisitos
 - o ¿Cómo se puede personalizar la oferta estandarizada para las necesidades de la misión? ¿Qué cubre(n) el(los) Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés) estándar?
 - o ¿Existe una matriz de responsabilidad que describa las cadenas de mando y las tareas requeridas para la organización y el proveedor de servicios en la nube (CSP)?
 - o ¿Cuándo y cómo se proveen las actualizaciones y mejoras a la organización?



La tasa de retención de la empresa y la duración media de la relación con el cliente.



Diferenciadores de otros proveedores de servicios en la nube (CSP) centrados en la seguridad pública.



Soluciones alternativas más adecuadas a las necesidades de la organización.



Modelo de precios y estimación en función del alcance y los requisitos descritos.

Consideración n.º 3: Cuestionario para solicitar información

Las organizaciones podrían considerar la elaboración de un cuestionario para interactuar mejor con proveedores potenciales y ver si los proveedores de servicios en la nube (CSP) podrían cumplir con los requisitos específicos de la organización.

¹⁰ "La cadena de custodia es un proceso utilizado para rastrear el movimiento y el control de un activo a lo largo de su ciclo de vida mediante la documentación de cada persona y organización que maneja el activo,

la fecha y hora en que se lo recogió o transfirió, y la finalidad de la transferencia". [Cadena de custodia y sistemas de infraestructura crítica de la Agencia de Seguridad Cibernética y de Infraestructura \(CISA\)](#)

Conclusión

Gracias a la capacidad de la computación en la nube de escalar rápidamente para satisfacer las fluctuaciones en el poder de cómputo, los sistemas de misión crítica pueden evitar tiempos de inactividad y dificultades técnicas que se presentan en momentos de alta demanda. Las organizaciones de seguridad pública podrían aprovechar la multitud de beneficios que ofrece la computación en la nube. Como se destaca en este documento, existen varias áreas de consideración clave para determinar si una solución o arquitectura en la nube es adecuada y cómo trabajar con los proveedores de servicios en la nube (CSP) para administrar y mantener el servicio. Si bien no todas las consideraciones sugeridas pueden aplicarse a circunstancias individuales, estimulan el pensamiento y permiten iniciar la conversación con líderes y responsables de la toma de decisiones. La transición a la nube puede parecer intimidante para organizaciones de todos los tamaños y contextos. Al revisar las consideraciones de este documento y consultar orientación adicional pertinente, las organizaciones de seguridad pública podrían determinar si la adopción de soluciones basadas en la nube es adecuada y qué vías de adopción de la nube pueden adaptarse a sus estructuras y satisfacer las necesidades fundamentales para su misión.