



MINISTERIO DE DEFENSA NACIONAL

RESOLUCIÓN NÚMERO

DE 2019

()

Por la cual se emite la Política de Tecnologías en la Nube del Sector Defensa y Seguridad y se dictan otras disposiciones.

EL MINISTRO DE DEFENSA NACIONAL

En ejercicio de las facultades constitucionales y legales, especialmente las que le confiere el artículo 208 de la Constitución Política y los artículos 58, 59 y 61 de la Ley 489 de 1998 y los numerales 2, 3 y 5 del artículo 2 del Decreto 4890 de 2011, y

CONSIDERANDO

Que, de acuerdo a lo señalado en el artículo 208 de la Constitución Política, corresponde a los Ministros formular políticas atinentes a su despacho, dirigir la actividad administrativa y ejecutar la ley.

Que el literal c) del artículo 61 de la Ley 489 de 1998, señala como función de los Ministros, dirigir y orientar la función de planeación del sector administrativo a su cargo.

Que la Ley 1341 del 30 de julio de 2009 consagra como uno de los principios rectores de las Tecnologías de la Información y las Comunicaciones (TIC) la neutralidad tecnológica, principio ratificado en el artículo 2.2.9.1.1.1 del Decreto 1078 de 2017 en el que se establece que *"el Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible"*.

Que los numerales 2, 3 y 5 del artículo 2 del Decreto 4890 de 2011, señalan como funciones del Ministro de Defensa Nacional la formulación de políticas generales y la estrategia para el desarrollo de los planes y programas en materia de defensa y seguridad, así como su divulgación, y las de orientar, controlar y evaluar el ejercicio de las funciones de los organismos y entidades que conforman el Sector Defensa.

Que el numeral 7 del artículo 16 del Decreto 4890 de 2011 establece como función del Despacho del Viceministro para la Estrategia y Planeación la de formular el Plan Estratégico Sectorial en Tecnologías de Información y Comunicaciones.

Que el numeral 9 del artículo 16 del Decreto 4890 de 2011 establece como función del Despacho del Viceministro para la Estrategia y Planeación la de dirigir la elaboración de propuestas que apunten a una adecuada gerencia de lo público en el Sector Defensa.

Que el numeral 2 del artículo 20 del Decreto 4890 de 2011 establece como función del Director de Logística la de proponer el Plan Estratégico Sectorial en Tecnologías de Información y Comunicaciones.

Que el título 35 del Decreto 415 de 2016 determina los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones (TIC), estableciendo, dentro de los objetivos del fortalecimiento institucional, el desarrollo de los lineamientos en materia tecnológica necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

entidad y/o sector, en beneficio de la prestación efectiva de sus servicios, que, a su vez, faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones (TIC).

Que, mediante la Resolución 5563 de 2018, se formuló el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad (PETI) 2018-2022, el cual plantea, dentro de la estrategia sectorial de TI, el enfoque de Nube Sectorial, para lo cual se deben desarrollar y ejecutar los estándares para contar con una solución de nube sectorial bajo un ambiente seguro.

Que el Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital para Colombia", establece el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Que el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, expedido en el año 2014 por el Ministerio de las Tecnologías de la Información y las Comunicaciones, plantea que el Estado no debe privilegiar tecnologías, ni proveedores y, por lo tanto, las entidades del Estado deben hacer una evaluación de las alternativas de inversión, aplicando criterios y evaluando todas las posibilidades para obtener una buena relación costo/beneficio. Así mismo, este marco de referencia define el lineamiento de acceso a servicios en la Nube - LI.ST.04, que establece el deber de evaluar la posibilidad de prestar los Servicios Tecnológicos, haciendo uso de la Nube para atender las necesidades de los grupos de interés.

Que, con el propósito de dar cumplimiento al artículo 5 de la Resolución 4240 de 2018, mediante la cual se define que el Modelo Integrado de Planeación y Gestión (MIPG) del Sector Defensa, en el desarrollo de las dimensiones (iii) Gestión con Valores para Resultados y (v) Información y Comunicación, y de las políticas de gestión y desempeño institucional, en las dimensiones 6) Transparencia, acceso a la información pública y lucha contra la corrupción, 11) Gobierno Digital y 12) Seguridad Digital, se requiere formular el marco regulatorio sectorial para habilitar el Uso de Servicios de Tecnologías en la Nube en el Sector Defensa.

Que, en virtud de lo anterior, es necesario definir los lineamientos generales y mínimos que habiliten el uso de Servicios de Tecnologías en la Nube para el Sector Defensa, con un enfoque de generación de valor público, que habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo del Sector Defensa y la eficiencia y transparencia del Estado.

RESUELVE

CAPÍTULO I

GENERALIDADES Y CONCEPTOS

ARTÍCULO 1. DEFINICIÓN DE TECNOLOGÍAS EN LA NUBE - SECTOR DEFENSA: El Ministerio de Defensa Nacional, en coherencia con la definición del Ministerio de las Tecnologías de la Información y las Comunicaciones, adopta la definición de *Cloud Computing*¹ del Instituto Nacional de Estándares y Tecnología (NIST, por su nombre en inglés) del Gobierno de Estados Unidos, el cual establece que el uso de tecnologías en la Nube *"es un modelo para habilitar el acceso conveniente por demanda (según sea solicitado) a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios"*.

PARÁGRAFO. Para los efectos de esta Política, se adopta la definición del NIST para *Cloud Computing*. El término a utilizar por las Unidades Ejecutoras y Dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las Entidades Adscritas y Vinculadas del Sector Defensa es **Tecnologías en la Nube**.

¹ Tomado de Ministerio TIC: <https://www.mintic.gov.co/portal/604/w3-propertyvalue-34317.html> y The NIST Definition of Cloud Computing. NIST, National Institute for Standards and Technology, 2011.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> Consultado el 7 de mayo de 2019.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

ARTÍCULO 2. CARACTERÍSTICAS ESENCIALES DE LOS SERVICIOS DE TECNOLOGÍAS EN LA NUBE. Las soluciones basadas en Tecnologías en la Nube a implementar por las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deben garantizar que cuentan con las siguientes cinco (5) características esenciales:

- 1) Auto-servicio por demanda:** Los servicios de Tecnologías en la Nube deben aprovisionar, de manera unilateral, capacidades de cómputo, en la medida en que las requiera sin necesidad de interacción humana por parte del proveedor del servicio.
- 2) Acceso amplio a la red:** Las capacidades de los servicios de Tecnologías en la Nube deben estar disponibles sobre la red y deben accederse a través de mecanismos estándares.
- 3) Conjunto común de recursos:** Los recursos computacionales del proveedor de servicios de Tecnologías en la Nube, tanto físicos como virtuales, se deben habilitar de acuerdo con los requerimientos del Sector Defensa.
- 4) Elasticidad y Rápida Escalabilidad:** Las capacidades de los servicios de Tecnologías en la Nube deben ser escalados y aprovisionados rápida y elásticamente, además, en los casos más sensibles, deben ser automáticos. La elasticidad debe permitir una provisión de servicios que puede parecer ilimitada o a la medida en cualquier cantidad y momento.
- 5) Servicio medible:** Los sistemas y soluciones basados en Tecnologías en la Nube deben ser monitoreados, controlados y reportados, proporcionando transparencia, tanto para el proveedor como para el consumidor, por el servicio utilizado.

ARTÍCULO 3. PRINCIPIOS DE LOS SERVICIOS BASADOS EN TECNOLOGÍAS EN LA NUBE EN EL SECTOR DEFENSA. La adopción de servicios basados en Tecnologías en la Nube por parte de las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, estará orientado a cumplir con las buenas prácticas y estándares aprobados y adoptados, principalmente por asociaciones internacionales reconocidas por el desarrollo de metodologías, estándares y certificaciones para la realización de actividades de auditoría y control en tecnologías y sistemas de información. Por esta razón se adoptan los siguientes principios²:

- a. Enfoque Estratégico:** Planificar las Tecnologías en la Nube como un habilitador estratégico más que como un simple acuerdo de tercerización o como una plataforma tecnológica. La adopción y uso de Tecnologías en la Nube debe ser tratada como una decisión estratégica de alto impacto en el cumplimiento de la misión institucional.
- b. Costo - Beneficio:** Evaluar los beneficios del uso de Tecnologías en la Nube a partir de una comprensión completa de sus costos asociados, comparados con otras soluciones tecnológicas, incluyendo los asociados a sostenibilidad y mantenimiento. La adopción de soluciones basadas en Tecnología en la Nube debe impactar, de manera directa, en la reducción de la inversión en tecnologías, al tiempo que debe garantizar el fácil acceso a los recursos tecnológicos y a los sistemas de información.
- c. Riesgo empresarial:** Adoptar una perspectiva de gestión de riesgo sectorial para dirigir la adopción y el uso de la Nube. Las soluciones de infraestructura en la Nube deben, además de mitigar los riesgos asociados a factores naturales, al hacer uso de centros de datos fuera de las instalaciones de la institución o entidad, también garantizar la seguridad de la información, mediante los más estrictos niveles de acceso físico y digital, así como verificar la disponibilidad y preservación de datos clave en caso de siniestros o daños causados por fenómenos naturales.
- d. Capacidad:** Integrar todas las capacidades que los proveedores de Tecnologías en la Nube ofrezcan, con los recursos propios, para ofrecer una solución técnica integral. Al implementar o desarrollar soluciones basadas en Tecnologías en la Nube, se debe garantizar su acceso en

² Principios adaptados de Guiding Principles for Cloud Computing Adoption and Use, ISACA, 2012. <http://www.eurogeography.eu/SoC/sofia-workshop/SoC-implementation/ISACA-Guiding-Principles.pdf> Consultado en 11/Dic/2018

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

cualquier momento o desde cualquier lugar, sin requerir de inversiones elevadas en hardware ni software, manteniendo los acuerdos de nivel de servicio (SLA).

- e. Responsabilidad:** Gestionar la responsabilidad, mediante una definición clara de lo que corresponde al proveedor y al usuario, en este caso, el Sector Defensa. Las soluciones de Tecnologías en la Nube deben facilitar el soporte y el monitoreo, tanto por el contenido como por el tipo de aplicaciones. Así mismo, deben permitir la verificación del estado de la Nube, la generación de estadísticas y la realización de auditorías internas y externas.
- f. Confianza:** Hacer de la confianza un elemento esencial de las soluciones de Tecnologías en la Nube, incorporándola en todos los procesos misionales que dependen de la Nube.
- g. Seguridad:** Los servicios de Tecnologías en la Nube deben aplicar las medidas de seguridad necesarias para garantizar la integridad, disponibilidad y confidencialidad de la información de la institución, así como cumplir con los requisitos establecidos en la normatividad vigente y con los niveles de seguridad adecuados para los servicios que presta cada unidad ejecutora o dependencia del Ministerio de Defensa Nacional, la Policía Nacional y demás entidades adscritas y vinculadas al Sector Defensa.

ARTÍCULO 4. MODELOS DE DESPLIEGUE DE TECNOLOGÍAS EN LA NUBE. Las definiciones de los modelos de despliegue de Tecnologías en la Nube que pueden ser objeto de estudio para contratación o adquisición como solución en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Ministerio de Defensa Nacional, son los siguientes:

- a. Nube Privada:** La infraestructura de la Nube es operada únicamente para una organización. Puede ser administrada por la organización o por un tercero y puede existir tanto en las instalaciones de la organización como fuera de ellas.
- b. Nube de Comunidad:** La infraestructura de la Nube es compartida por varias organizaciones y soporta una comunidad específica que tiene preocupaciones compartidas (por ejemplo, misión, requisitos de seguridad, política y consideraciones de cumplimiento). Puede ser administrado por las organizaciones o un tercero y puede existir tanto en las instalaciones de las organizaciones como fuera de ellas.
- c. Nube Pública:** La infraestructura de la Nube se pone a disposición del público en general o de un gran grupo industrial y es propiedad de una organización que vende servicios en la Nube.
- d. Nube Híbrida:** La infraestructura de la Nube es una composición de dos o más nubes (privadas, comunitarias o públicas) que siguen siendo entidades únicas, pero están unidas entre sí por una tecnología normalizada o propietaria que permite la portabilidad de datos y aplicaciones.

ARTÍCULO 5. MODELOS DE SERVICIO EN LA NUBE. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa podrán optar por cualquiera de los siguientes modelos de servicio en la Nube:

- a. Infraestructura como Servicio (IaaS).** La capacidad proporcionada al consumidor es proveer procesamiento, almacenamiento, redes y otros recursos de computación fundamentales, en el cual el consumidor tiene control sobre los sistemas operativos, el almacenamiento, las aplicaciones implementadas y, posiblemente, el control limitado de determinados componentes de red.
- b. Plataforma como Servicio (PaaS).** La capacidad proporcionada al consumidor es la capacidad de desplegar en la infraestructura de nube aplicaciones creadas por el propio consumidor, o adquiridas, utilizando lenguajes de programación y herramientas soportadas por el proveedor, tiene control sobre las aplicaciones implementadas y, de manera limitada, sobre las configuraciones del entorno de hospedaje de aplicaciones.
- c. Software como Servicio (SaaS).** La capacidad proporcionada al consumidor es utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Las aplicaciones son

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero como un navegador web.

ARTÍCULO 6. MODELOS DE IMPLEMENTACIÓN DE INFORMÁTICA DE TECNOLOGÍAS EN LA NUBE: Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, podrán optar por cualquiera de los siguientes modelos de implementación de Tecnologías en la Nube:

- a. Nube:** Una aplicación basada en la nube se encuentra implementada totalmente en la nube, de modo que todas las partes de la aplicación se ejecutan en ésta. Las aplicaciones en la nube se han creado directamente en la nube o se han transferido de la infraestructura existente para aprovechar los beneficios de la informática en la nube. Las aplicaciones basadas en la nube se pueden construir en partes de infraestructura de bajo nivel o pueden utilizar servicios de nivel superior que proporcionan abstracción de los requisitos de administración, arquitectura y escalado de la infraestructura principal.
- b. Solución híbrida:** Una implementación híbrida es una manera de conectar los recursos existentes situados fuera de la nube y la infraestructura y las aplicaciones basados en la nube. El método más común de implementación híbrida consiste en conectar la nube y la infraestructura existente local para ampliar e incrementar la infraestructura de la empresa en la nube al mismo tiempo que se conectan estos recursos en la nube con el sistema interno.
- c. Implementación local:** La implementación local de recursos mediante herramientas de administración de recursos y virtualización se denomina a veces "nube privada". La implementación local no aporta muchos de los beneficios de la informática en la nube, pero se utiliza por su capacidad de ofrecer recursos dedicados. En la mayoría de los casos, este modelo de implementación es idéntico al de la infraestructura de TI antigua, mientras que utiliza tecnologías de virtualización y administración de aplicaciones para intentar incrementar el uso de los recursos.

CAPÍTULO II

POLÍTICA DE TECNOLOGÍAS EN LA NUBE

ARTÍCULO 7. OBJETIVO DE LA POLÍTICA DE TECNOLOGÍAS EN LA NUBE DEL SECTOR DEFENSA. Establecer los lineamientos mínimos necesarios para habilitar el uso de los servicios de Tecnologías en la Nube en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, con el fin de reducir costos, aumentar la productividad y desarrollar mejores servicios en apoyo a la misión institucional, facilitando la interoperabilidad en el Sector Defensa y garantizando un máximo aprovechamiento de los recursos TIC disponibles.

ARTÍCULO 8. ALCANCE. La Política de Tecnologías en la Nube es aplicable a cualquier adquisición o contratación de Tecnologías en la Nube, para implementación y/o migración de soluciones nuevas o existentes, que realicen las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas del Sector Defensa, para proveer servicios institucionales y/o sectoriales a través de un proveedor externo.

ARTÍCULO 9. CUMPLIMIENTO DE LA LEGISLACIÓN VIGENTE. Independientemente del tipo de solución de Tecnologías en la Nube elegida, las unidades ejecutoras, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deben demostrar el cumplimiento de toda la legislación nacional vigente aplicable.

ARTÍCULO 10. DECISIÓN SOBRE SOLUCIONES DE TECNOLOGÍAS EN LA NUBE. Las soluciones basadas en Tecnologías en la Nube en todas las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa obedecerán a los principios, características y modelos establecidos en la presente resolución y se considerarán, junto con las soluciones tradicionales de Infraestructura y Servicios Tecnológicos en Centros de Datos propios, como una respuesta válida y adecuada a las necesidades existentes.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

Exceptuando lo descrito en el literal e del artículo 11 de la presente resolución, si una solución basada en la nube satisface las necesidades de cumplimiento de la misión institucional, demostrando su seguridad, viabilidad técnica y financiera, así como su sostenibilidad, se preferirá ésta a una solución propia tradicional.

PARÁGRAFO. Sin perjuicio de lo descrito en la presente resolución, el Sector Defensa, en cabeza del Viceministerio para la Estrategia y Planeación, enfocará sus esfuerzos y realizará los estudios necesarios que permitan establecer la viabilidad de contar con un modelo sectorial de nube privada o de comunidad, de manera tal que se brinden servicios basados en Tecnologías en la Nube de manera conjunta a las unidades ejecutoras, dependencias, instituciones y entidades que conforman el Sector Defensa, en cualquier escenario de unificación y consolidación de infraestructura, servicios tecnológicos y centros de datos.

ARTÍCULO 11. ASPECTOS FUNDAMENTALES EN SOLUCIONES DE TECNOLOGÍAS EN LA NUBE. Como parte del proceso de decisión sobre la adopción e implementación de una solución basada en Tecnologías en la Nube, las unidades ejecutoras del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas del Sector Defensa, deben aplicar sin excepción lo siguiente:

- a. Las soluciones ofrecidas, basadas en Tecnologías en la Nube, se evaluarán caso por caso en función de las políticas, los principios, los lineamientos y las normas nacionales, sectoriales e institucionales.
- b. Las soluciones basadas en Tecnologías en la Nube deberán ofrecer los mismos o mejores niveles de servicio (SLA) que una solución propia interna en sitio (*on-premise*) para garantizar la continuidad del negocio, en línea con los requisitos del servicio que se está entregando.
- c. Las soluciones basadas en Tecnologías en la Nube deberán cumplir con todas las leyes y reglamentos vigentes de privacidad y confidencialidad aplicables a nivel nacional, sectorial e institucional. La unidad ejecutora o dependencia del Ministerio de Defensa Nacional, la Policía Nacional o las entidades adscritas y vinculadas al Sector Defensa que adquieran servicios de Tecnologías en la Nube serán responsables de asegurar los roles y las responsabilidades relacionadas con el manejo de datos. Así mismo, serán responsables de que la privacidad y confidencialidad de los mismos esté clara y adecuadamente definida en los respectivos acuerdos de servicios del proveedor de Tecnologías en la Nube.
- d. La información almacenada en los diferentes sistemas tecnológicos deberá ser clasificada conforme a lo establecido en la Ley 1712 de 2014, *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*. De igual manera, se deberá efectuar el inventario de Activos Sensibles. Conforme a lo definido en la Ley 1712 de 2014, sólo la información clasificada como PÚBLICA RESERVADA deberá contar con estudio y justificación que permita almacenarla en una solución o servicio basado en Tecnologías en Nube pública.
- e. Ninguna información o sistema de información, de inteligencia o de carácter operacional, de las Fuerzas Militares o de la Policía Nacional, podrá ser almacenada o contratada en servicios en la nube pública o híbrida. Para este efecto, deberán considerarse exclusivamente servicios de nube privada, mediante la garantía del proveedor que se destinará infraestructura física ubicada dentro del territorio colombiano y de manera exclusiva, descartando el concepto de *"multi-tenant"*.
- f. Para sistemas de información empresariales como CRM, ERP o SCM, propios de un fabricante, podrán implementarse o migrarse totalmente, incluyendo la infraestructura que los soporta en sitio, a soluciones basadas en servicios de nube privada, propia del mismo fabricante, incluso fuera del territorio colombiano, siempre y cuando el fabricante disponga de infraestructura física exclusiva y garantice la soberanía de los datos. Cuando se trate de un tercero, éste deberá estar habilitado y contar con certificación vigente, emitida por la casa matriz del fabricante, garantizando que se realizará bajo el modelo de nube privada y que se destinará infraestructura física ubicada dentro del territorio colombiano y de manera exclusiva, descartando el concepto de *"multi-tenant"*.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

- g. Al tratarse de un servicio totalmente dependiente de una conexión a internet, se deben realizar los estudios necesarios que permitan establecer la necesidad de contratación de un mayor ancho de banda e implementación de políticas de calidad de servicio o conexiones alternas, para evitar problemas de cuellos de botella en el acceso a las aplicaciones o para prevenir accesibilidad lenta que puedan poner en juego el desempeño de las aplicaciones. Adicionalmente, se deberá actualizar los planes de capacidad sobre los servicios de TI, así como revisar y ajustar las condiciones técnicas, como el ancho de banda, la latencia del servicio, la pérdida de paquetes, los *delays* (retraso) y las tecnologías a utilizar.
- h. Establecer los impactos que tendría la implementación de la solución sobre la estabilidad operacional o el rendimiento de los sistemas centrales de la respectiva unidad ejecutora o dependencia del Ministerio de Defensa Nacional, la Policía Nacional o las entidades adscritas y vinculadas del Sector Defensa.
- i. Establecer los mecanismos que permitan mantener y dar cumplimiento a los requerimientos de seguridad, confiabilidad, integridad y disponibilidad.
- j. Establecer y documentar los mecanismos de portabilidad de la información y el proceso de migración entre plataformas que garanticen la disponibilidad de datos y los servicios prestados, en caso de tomar la decisión de trasladar, desde la nube originalmente contratada a otra nube distinta, la información existente, garantizando así la integridad de la información y evitando los costos adicionales.
- k. Las soluciones de computación en la nube tendrán los procesos y controles de entrega que son utilizados para cualquier otra solución de tecnología en el Sector Defensa.

ARTÍCULO 12. SEGURIDAD EN LAS SOLUCIONES CON TECNOLOGÍAS EN LA NUBE. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa tendrán la responsabilidad de asegurar que la adopción, implementación o migración de una solución basada en Tecnologías en la Nube sea confiable y segura, teniendo en cuenta la disponibilidad para proporcionar, de manera prospectiva, los servicios de TI. Así mismo, deberán establecer las necesidades de seguridad de cada solución, considerando como mínimo:

- a. **Características de los datos** para evaluar las protecciones fundamentales que el conjunto de datos de una aplicación requiere.
- b. **Privacidad y confidencialidad** para proteger contra el acceso accidental y catastrófico a la información.
- c. **Integridad** para asegurar que los datos estén autorizados, sean completos y precisos, protegiéndolos de modificaciones no autorizadas.
- d. **Controles de datos y políticas de acceso** para determinar dónde se pueden almacenar los datos y quién puede acceder a ubicaciones físicas.
- e. **Gobernabilidad** para asegurar que los proveedores de servicios de nube sean suficientemente transparentes, tengan controles de seguridad y de administración adecuados y proporcionen la información necesaria para que las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, evalúen y monitoreen, adecuadamente e independientemente, la eficacia de esos controles.
- f. **Pruebas de penetración y pruebas de intrusión** para evaluar la vulnerabilidad de la infraestructura y de los equipos asignados para la operación de los servicios de Tecnologías en la Nube.
- g. **Control de acceso** para facilitar el acceso suficiente y necesario, local o remoto, a cada unidad ejecutora, dependencia, institución o entidad del Sector Defensa y a los proveedores autorizados, para proceder con la instalación o actualización de los sistemas. De igual manera, se deberán

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

documentar los procedimientos que se usan para otorgar dicho acceso, así como el mecanismo de trazabilidad y revisión del historial de cambio y las modificaciones efectuadas.

- h. Ethical Hacking** para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web y bases de datos. Esto podrá ser realizado por, o con el apoyo, del Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares, el Centro Cibernético Policial (CCP) y el Grupo ColCERT de la Dirección de Seguridad Pública e Infraestructura.
- i. Correlación de eventos** que permitan relacionar diferentes eventos con patrones identificables que amenacen la seguridad de la información y prever las acciones a tomar para prevenir las amenazas.

ARTÍCULO 13. ASPECTOS TÉCNICOS EXIGIBLES A LOS PROVEEDORES DE TECNOLOGÍAS EN LA NUBE. Las propuestas de solución dadas por proveedores externos para la adquisición y/o implementación de servicios de Tecnologías en la Nube en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberán cumplir con los requisitos técnicos mínimos, adicionales cuando aplique, a los establecidos en los Acuerdos Marco de Precios, como se señala a continuación:

- a. Condiciones del servicio:** Se debe garantizar el cumplimiento de las condiciones transversales a todos los niveles de servicio respecto a conectividad, gestión de red, seguridad, gestión de operaciones, servicios de operación y administración, servicios de administración y monitoreo, y reportes del servicio, garantizando así el cumplimiento de los requerimientos de flexibilidad, elasticidad y acuerdos de niveles de servicio.
- b. Continuidad y recuperación ante desastres:** Se debe describir los mecanismos, procedimientos e infraestructura que tiene el proveedor para ofrecer continuidad del servicio de acuerdo con la norma ISO22301 (Continuidad del Negocio). Para ello, se debe contar como mínimo con un centro alterno, enmarcado en las especificaciones establecidas en la norma ISO27001 (Seguridad de la Información). Durante la ejecución del contrato, se debe solicitar imágenes de máquinas virtuales, las cuales el proveedor deberá entregar dentro del servicio de entrega de medios.
- c. Entrega al finalizar los servicios:** Al término del contrato, se debe entregar la documentación de configuraciones y parámetros de los servicios contratados, así como los procedimientos o tareas específicas realizadas sobre los servicios, imágenes de máquinas virtuales, y toda la información necesaria para que la unidad ejecutora, dependencia, institución o entidad del Sector Defensa pueda configurar sus servicios con otro proveedor en el tiempo pactado.
- d. Borrado Seguro:** El proveedor de servicios debe contar con un procedimiento normalizado de borrado seguro, de acuerdo a los estándares internacionales, para que sea ejecutado luego de la entrega al finalizar los servicios.
- e. Cambio, actualización o modificación de componentes:** Durante la operación del servicio, el proveedor debe recibir solicitudes para cambio, actualización o modificación de componentes o configuraciones sobre el Hardware y Software; para mejorar el ambiente de operación, e incluso la conformación de nuevos ambientes basados en el aprovisionamiento de elementos adicionales. El proveedor debe aprovisionar el nuevo requerimiento en el tiempo definido por los acuerdos de niveles de servicio y en los costos acordados. El cambio, por daño o mal funcionamiento en la infraestructura, hace parte del servicio integral prestado por el proveedor y debe remplazarse con cargo a éste último.
- f. Infraestructura física en Colombia:** Se debe garantizar que la infraestructura tecnológica del Centro de Datos principal que soporta la prestación de los Servicios de Nube Privada esté ubicada físicamente en Colombia. Se exceptúa de esta consideración técnica a los servicios de Nube Pública, así como a los servicios de Nube Privada, propia de un fabricante, de que trata el literal f del Artículo 11 de esta resolución.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

- g. Auditoría:** Las unidades ejecutoras, dependencias, instituciones y entidades del Sector Defensa, a modo propio o por interpuesta persona, deberán estar en la capacidad de comprobar los procesos de gestión de cambios, controles de seguridad, análisis de riesgos, gestión del servicio y mejora continua respecto a la gestión de tecnología, seguridad de la información y continuidad del negocio, con el fin de garantizar que se está dando cumplimiento a las condiciones contractuales. Esta comprobación podrá soportarse sobre informes de evaluaciones y/o certificaciones de terceros, a las que se hayan sometido los procesos del proveedor.
- h. Pruebas de Latencia:** En coordinación con el proveedor de Servicios de Nube, se debe realizar un monitoreo de red, verificando las pruebas de latencia para el respectivo análisis con respecto a la distancia hasta el Centro de Datos principal que soporta la infraestructura tecnológica en la nube.
- i. Ancho de Banda:** Se debe garantizar un ancho de banda (internet) en la solución de tecnología de la nube (si es requerido).
- j. Ancho de Banda Local:** Se debe contar con un reporte del ancho de banda local (red interna) a garantizar, basado en los análisis de velocidades y el uso en horas pico.
- k. Normas Técnicas:** El Proveedor de Servicios de Nube debe garantizar la calidad del servicio a la entidad contratante mediante la aplicación de lo establecido en las normas ISO/IEC 27017 (Controles de Seguridad para Servicios Cloud), ISO/IEC 22301 (Continuidad del Negocio) e ISO 31000 (Gestión del Riesgo), en sus versiones vigentes.

ARTÍCULO 14. ASPECTOS DE SEGURIDAD EXIGIBLES A LOS PROVEEDORES DE TECNOLOGÍAS EN LA NUBE. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa necesitan garantías de que los riesgos asociados, al almacenamiento de sus datos y ejecución de sus aplicaciones en estos ambientes, son comprendidos y gestionados adecuadamente. Por lo anterior, las consideraciones³ mínimas de seguridad que los Prestadores de Servicios deben cumplir son:

- a. Controles de acceso, identidad y autenticación robustos:** El acceso a todas las interfaces de servicio debe restringirse a personas autenticadas y autorizadas, con el fin de prevenir cambios no autorizados en el servicio del consumidor, robo o modificación de datos o la denegación de servicio.
- b. Protección de los activos de información y datos, tanto en tránsito como en reposo:** Los centros de datos deben estar contruidos bajo estándares reconocidos de seguridad, para que los datos, activos y redes estén adecuadamente protegidos contra la manipulación, espionaje, pérdida, daño o incautación. Deben existir criterios claros sobre el uso de controles criptográficos sobre los datos. Así mismo, debe existir una política clara de retención de datos y plazos específicos para su posterior eliminación.
- c. Seguridad Operacional, del Personal y Proveedores:** El Prestador de Servicios debe tener procesos y procedimientos establecidos para garantizar la seguridad en la operación del servicio, incluyendo la gestión de su personal y proveedores.
- d. Gestión segura de los clientes, incluyendo separación de los mismos y promoción del uso seguro del servicio:** El Prestador de Servicios debe promover el uso seguro de sus servicios por parte de sus clientes, transmitiendo, de forma clara, las responsabilidades de cada parte cuando se use un servicio en la nube, para que el uso permanezca seguro y para que los datos de sus clientes estén adecuadamente protegidos. Parte de las responsabilidades del Prestador de Servicios en este ámbito es tomar las medidas adecuadas para garantizar la separación lógica o física de los clientes, según corresponda.

³ Adaptado de la "Guía de Computación en la Nube", MinTIC (2017) [Online] Disponible en: https://mintic.gov.co/portal/604/articles-58727_recurso_2.pdf y del documento de "Buenas Prácticas para el uso de Servicios Cloud Computing al interior de la Administración del Estado". Versión 2, 19 de febrero de 2018. División de Gobierno Digital. Gobierno de Chile (2018) [Online] Disponible en: <https://cdn.digital.gob.cl/Guia+Cloud+v2.pdf> Consultado en 19 de diciembre de 2018.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

- e. Proveer información de auditorías a los clientes:** Se debe proporcionar a los consumidores los registros de auditoría necesarios para controlar el acceso a su servicio y los datos contenidos en él, puesto que, en algunos casos, podría ser poco práctico o imposible para el cliente verificar personalmente el correcto cumplimiento de los contratos o acuerdos de servicio, lo que podría forzar a depender de certificaciones y auditorías de terceros. Este acceso debe ser razonable y debe respetar las políticas de confidencialidad.
- f. Marco de gobernanza:** El Prestador de Servicios debe tener un marco de gobernanza de seguridad que entregue suficiente coordinación y dirija su enfoque hacia la gestión del servicio y la información que contiene el servicio.
- g. Reporte de incidentes de seguridad:** El Prestador de Servicios debe entregar al cliente información detallada y oportuna sobre los incidentes de seguridad que afecten el servicio contratado o a la información que contiene el servicio, así como adoptar medidas para mitigar los posibles daños resultantes.

ARTÍCULO 15. SUSCRIPCIÓN O DERECHO DE USO PERIÓDICO POR SERVICIOS DE TECNOLOGÍAS EN LA NUBE. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, al igual que las escuelas de formación y capacitación de la Fuerza Pública, podrán contratar soluciones de Software como Servicio – SaaS, basados en la modalidad de suscripción o derecho de uso periódico, analizando sus necesidades particulares y adoptando esquemas de almacenamiento acordes a la información que manejan.

PARÁGRAFO. Sin perjuicio de lo anterior, se deberá buscar la realización de negociaciones sectoriales con los proveedores de esta modalidad que permitan armonizar las soluciones a adquirir, garantizar las mismas condiciones contractuales y de servicios, y generar economías de escala.

ARTICULO 16. MANEJO Y NATURALEZA DE LOS DATOS. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deben revisar, con detenimiento, los contratos de prestación de servicios, garantizando que en éstos se especifique las mitigaciones a los riesgos identificados y las medidas de seguridad utilizadas para proteger los datos del servicio. Así mismo, deben prestar especial atención a la jurisdicción aplicable a los servicios contratados, considerando temas como la naturaleza de los datos tratados (en particular si se trata de datos de seguridad nacional o de datos personales), propiedad de los activos, así como leyes y regulaciones normativas aplicables, responsabilidades contractuales, interoperabilidad de los sistemas, utilización de formatos abiertos, etc. Adicionalmente, deben considerar aspectos relevantes al tratamiento de los datos, incluyendo registros y metadatos, a la gestión de salida; es decir, en el proceso de terminación de un contrato o acuerdo de prestación de servicios.

PARÁGRAFO. Para abordar los aspectos del manejo de datos, las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deben considerar aspectos claves para determinar la naturaleza de los datos a utilizar en ambientes de nube y las medidas apropiadas que se deben tomar para proteger esos datos, entre las que se incluyen las siguientes:

- a. 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 de nube.
- b. Localización geográfica y jurisdicción sobre los datos a tratar.** Esto incluye cuando un Prestador de Servicios esté sometido a normas extranjeras que permitan la solicitud de información por parte de agencias estatales de otros países.
- c. 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 que deben ser analizadas caso a caso, pudiendo ser necesario descartar algunos modelos de servicio o implementación en la nube.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

d. Acceso y eliminación de los datos tratados, definiendo claramente los períodos mínimos y máximos de retención de datos por parte del Prestador de Servicios.

ARTÍCULO 17. PLAN DE MIGRACIÓN. Cada una de las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberá contar con su respectivo Plan de Migración **Inicial** de Servicios y Tecnología en la Nube, priorizando y estableciendo el impacto de las soluciones a migrar. Para el caso de las soluciones sectoriales, el Plan de Migración inicial será liderado por la Oficina Asesora de Sistemas de la Unidad de Gestión General del Ministerio de Defensa Nacional, presentado ante el Comité de Integración de Tecnologías de Información y Comunicaciones del Sector Defensa, o el que haga sus veces, y deberá ser aprobado por el señor Ministro de Defensa Nacional, Comandante General de las Fuerzas Militares, Comandantes de Fuerza y Director de la Policía Nacional, según corresponda.

PARAGRAFO 1. Al término de los doce (12) meses siguientes a la fecha de expedición de la presente Resolución cada una de las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, deberá contar con el Plan de Migración Inicial en las fases de Análisis, Planeación y Diseño, descritas en el Artículo 18, debidamente aprobado por su institución o entidad y por el Comité de Integración de Tecnologías de la Información y las Comunicaciones del Sector Defensa, o el que haga sus veces. No obstante lo anterior, este plan deberá contener y describir de manera proyectada las actividades y tiempos estimados de las fases de ejecución y monitoreo, las cuales deberán dar inicio antes de que se cumplan veinticuatro (24) meses posteriores a la fecha de expedición de la presente Resolución.

PARÁGRAFO 2. Se establece la obligatoriedad de elaborar un Plan de Migración para cada aplicación o solución, existente o nueva, en sitio o con Tecnologías en la Nube, que se pretenda migrar, adoptar o reubicar, posterior al Plan de Migración Inicial.

ARTÍCULO 18. MODELO DE PLAN DE MIGRACIÓN. La elaboración del Plan de Migración⁴ deberá incluir las siguientes etapas:

a. Análisis: En esta etapa se deberá:

- Determinar la manera en que la solución con Tecnologías en la Nube aportará para el logro de los objetivos estratégicos y la generación de valor.
- Socializar y recibir las autorizaciones correspondientes de la alta dirección, comandantes, gerente, presidente, o el que haga sus veces.
- Entrenar al personal de TI en el modelo de nube.
- Contar con la evaluación y el análisis financiero correspondiente.

b. Planeación: En esta etapa se deberá:

- Revisar la infraestructura de hardware y software del centro de datos.
- Realizar el análisis de conectividad correspondiente.
- Seleccionar las aplicaciones o soluciones para el despliegue en nube, según el nivel de criticidad.
- Elaborar la estrategia de migración.
- Elegir el modelo de servicio a utilizar.
- Seleccionar el modelo de despliegue a usar.

c. Diseño: En esta etapa se deberá:

- Especificar las características requeridas para el centro de datos.
- Establecer los Acuerdos de Niveles de Servicio requeridos.
- Diseñar el cronograma de migración.
- Diseñar la red de datos y la conectividad propuesta.
- Diseñar el entorno de virtualización (cuando aplique) y los recursos requeridos en el centro de datos.

⁴ Consultado en: "Guía de Computación en la Nube", MinTIC (2017), [Online] Disponible: https://mintic.gov.co/portal/604/articles-58727_recurso_2.pdf y Adaptado de: C.A. Gutiérrez, R. Almeida., y W. Romero, "Diseño de un modelo de migración a cloud computing parantidades públicas", Investigación e Innovación en Ingenierías, vol. 6, n°. 1, pp. 10 - 26., 2018. DOI: <https://10.17081/invinno.6.1.2772> Consultado en 10/Dic/2018.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

d. Ejecución: En esta etapa se deberá:

- Adecuar la red de datos y la conectividad.
- Migrar las aplicaciones según la estrategia de migración.

e. Monitoreo: En esta etapa se deberá:

- Realizar las pruebas de eficiencia.
- Gestión y medición del servicio recibido.

ARTÍCULO 19. APLICACIÓN DE TECNOLOGÍAS EN LA NUBE EN EL SECTOR DEFENSA. La adopción, implementación o migración de Tecnologías en la Nube en el Sector Defensa, se realizará para las siguientes soluciones que se corresponden con cada uno de los modelos de servicio en la nube descritos en el artículo 5 de la presente resolución, así:

a. Infraestructura como Servicio (IaaS). Servidores virtuales, capacidad de cómputo habilitadas por APIs, aprovisionamiento, discos lógicos, APIs para integración de servicios IaaS, almacenamiento, copias de seguridad, balanceadores de carga, redes, dispositivos de red y recuperación, gestión de servicios, computación por lotes.

b. Plataforma como Servicio (PaaS). Ambientes de aplicación (J2EE, RoR, .Net), plataformas de configuración y motores de scripting, entornos de desarrollo y pruebas de aplicaciones, capacidades de infraestructura de aplicaciones, bases de datos, almacenes de datos, APIs para integraciones PaaS, servidores web (lógicos), inteligencia de negocios – BI, implementación de aplicaciones.

c. Software como Servicio (SaaS). Sitios web, herramientas de colaboración, correo electrónico, productividad de oficina, ofimática, escritorios virtuales, comunicaciones, sistemas de gestión y manejo de relaciones con clientes - CRM, sistemas de planificación de recursos empresariales - ERP, sistemas de administración de la fuerza de ventas - SFA, sistemas de administración de la cadena de suministro - SCM, aplicaciones / interfaces de gestión, APIs para integración de servicios, aplicaciones de gestión de contenidos, herramientas de gestión de documentos.

ARTÍCULO 20. SOLUCIONES EXISTENTES. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa que a la fecha de entrada en vigencia de la presente resolución tengan implementadas soluciones con Tecnologías en la Nube deberán, en el término de seis (6) meses, realizar una evaluación integral que permita establecer que la solución existente cumpla con lo establecido en la presente resolución.

PARAGRAFO. El Grupo de Tecnologías de la Información y las Comunicaciones establecerá el método, las herramientas y los medios para realizar el seguimiento de la Política de Nube.

CAPÍTULO III

PROTECCIÓN DE DATOS PERSONALES EN SERVICIOS / SOLUCIONES CON TECNOLOGÍAS EN LA NUBE ⁵

ARTÍCULO 21. CONSIDERACIONES GENERALES SOBRE EL USO DE DATOS PERSONALES.

Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberán revisar si el servicio a contratar implica la consulta, tratamiento y/o tráfico de información, en particular de datos personales. De ser así, su decisión debe involucrar también consideraciones relacionadas con la protección de datos personales y la seguridad de la información. En este sentido, deben tener claridad sobre las garantías que ofrecen los proveedores, en cuanto al cumplimiento de los principios de disponibilidad, confidencialidad e integridad de la información, así como las acciones previstas para responder por la continuidad del negocio y la recuperación de desastres y por la accesibilidad a la información durante los tiempos de ventanas de mantenimiento programadas y no programadas.

⁵ Adaptado del documento "Protección de los datos personales en los servicios de computación en la nube (Cloud Computing)" - SIC (2015), [Online] Disponible en: http://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

ARTÍCULO 22. RESPONSABLE DEL TRATAMIENTO. Como contratantes de los servicios o soluciones con Tecnologías en la Nube, las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa serán las **Responsables del Tratamiento de Datos**, es decir que, por sí misma o en asocio con otros, decidirá sobre la base datos y/o el tratamiento de datos. En tal sentido, serán las que determinen el objetivo último del tratamiento, decidirán sobre la externalización y delegarán parte o todo el tratamiento a un tercero.

ARTÍCULO 23. ENCARGADO DEL TRATAMIENTO. El proveedor que preste los servicios de computación en la nube, bien sea, suministrando los medios y/o la plataforma, de acuerdo con el régimen general de protección de datos personales, será el **Encargado del Tratamiento**, esto es, la persona natural o jurídica, pública o privada que, por sí misma o en asocio con otros, realizará el tratamiento de datos personales por cuenta del Responsable.

ARTÍCULO 24. SUBCONTRATACIÓN DE LOS SERVICIOS O SOLUCIONES CON TECNOLOGÍAS EN LA NUBE. En los casos en que el proveedor de servicios o soluciones con Tecnologías en la Nube subcontrate el servicio o parte de éste, los subcontratistas adquieren la calidad de **Encargados del Tratamiento**. Esta situación debe ser transparente para las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, a quienes el proveedor de servicios deberá informar las características y condiciones de esa subcontratación, garantizando la protección de la información personal a la que tendrán acceso los Encargados, por cuenta del tratamiento que realizan para los fines únicos señalados por el Responsable.

ARTÍCULO 25. IDENTIFICACIÓN DE DATOS. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberán identificar qué tipo de datos serán objeto del tratamiento en la nube, bien sea, públicos, semiprivados, privados, sensibles o datos de niños, niñas y adolescentes, y tomará la decisión de conservar el control respecto de algunos o de todos.

ARTÍCULO 26. CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, dentro de los términos y condiciones del contrato de servicios de computación en la nube, deberán establecer las garantías que cumplirá el proveedor respecto al cumplimiento de las normas sobre protección de datos personales. Especialmente, el contrato deberá contemplar los aspectos relacionados con la protección de datos personales, así:

- a. Limitar la finalidad del tratamiento que realizará el Proveedor, de acuerdo con lo que defina el cliente.
- b. Imponer cargas al Proveedor para reportar los incidentes de seguridad al cliente y a los titulares, dependiendo del tipo de tratamiento que realice el Encargado.
- c. Establecer la manera como el Proveedor apoyará al cliente frente al ejercicio de los derechos de los titulares.
- d. Disponer claramente si subcontratarán servicios y, de ser así, las condiciones que regirán esos contratos.
- e. Estipular el principio de confidencialidad para el Proveedor, sus empleados y subcontratistas.
- f. Prever el uso de medidas necesarias para dar seguridad al tratamiento de los datos personales y durante el tránsito desde su origen hasta el final.
- g. Incluir la obligación del proveedor de actualizar y rectificar la información, de acuerdo con lo que le indique el cliente.
- h. Establecer el formato en el que se almacenarán los datos para evitar inconvenientes con la portabilidad de esa información.
- i. Acordar cómo se llevará a cabo la devolución y/o destrucción de la información e incluir el procedimiento que se llevará a cabo con los subcontratistas.
- j. Consagrar acuerdos sobre el nivel de servicio y las sanciones por su incumplimiento.

PARÁGRAFO 1. Se debe establecer la localización de los servidores utilizados por el proveedor y el manejo de los requerimientos de acceso, por parte del proveedor, que realicen entidades competentes, cuando éstos se encuentren ubicados fuera de Colombia.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

PARÁGRAFO 2. Siempre que el tratamiento de datos se realice fuera del territorio colombiano, es importante que el contrato de servicios de computación en la nube se adecúe a lo establecido en el Decreto Único 1074 de 2015, Capítulo 25, Sección 5, numeral 2.2.2.25.5.2, de manera que el control y responsabilidad sobre el tratamiento de datos esté siempre en cabeza del Responsable del Tratamiento.

PARÁGRAFO 3. Cuando el contrato incluya la transmisión de datos, el Encargado se compromete a cumplir con las políticas de tratamiento del Responsable y además se obliga a: 1) Cumplir con los principios de tratamiento de datos personales, 2) Salvaguardar la seguridad de la base de datos y, 3) Guardar la confidencialidad sobre los datos personales a que tenga acceso.

CAPÍTULO IV

DISPOSICIONES FINALES

ARTÍCULO 27. ENFOQUE DE GASTOS ASOCIADOS A TECNOLOGÍA. Las soluciones basadas en Tecnologías en la Nube deben permitir que los sistemas de TI sean escalables y flexibles. En este sentido, el Sector Defensa, en cabeza del Viceministerio para la Estrategia y Planeación, realizará los estudios necesarios para enfocar la estrategia de gastos basada en aplicaciones, capacidad y licenciamiento a una inversión centrada en el gasto por servicios consumidos, determinando la favorabilidad de la relación costo - beneficio. En la aplicación de lo anterior, se debe considerar el establecimiento de acuerdos sectoriales con uno o más proveedores de servicios de manera que permita al sector Defensa contar más de una opción de Tecnologías en la Nube garantizando la continuidad de los servicios tecnológicos.

ARTICULO 28. SOBERANÍA DE LOS DATOS. Los datos e información de carácter estratégico y operacional de la Fuerza Pública constituyen un recurso indispensable que debe ser resguardado con el objetivo de defender la soberanía nacional en materia de información. Por lo anterior, sólo podrán ser almacenados físicamente dentro del territorio colombiano y estarán sometidos únicamente a su ley y jurisdicción. Así mismo, los datos e información son propiedad del Estado y, por consecuencia, inajenable, inembargable e imprescriptible.

PARÁGRAFO. Cuando se trate de datos personales, la transferencia de los datos deberá realizarse únicamente a los países autorizados en la Circular Externa 002 de 2018 de la Superintendencia de Industria y Comercio (o la vigente en la materia) dando cumplimiento con todo lo allí establecido. En este caso, la soberanía de los datos se regirá, además, por las normas de protección de datos personales del país de destino final (no de tránsito) que, en todo caso, son de un nivel igual o superior a las establecidas en Colombia.

ARTICULO 29. APROBACIONES. Todas las necesidades e iniciativas de implementación de soluciones con Tecnologías en la Nube deberán ser aprobadas por el Departamento Conjunto de Comunicaciones del Comando General de las Fuerzas Militares, para el caso de las Fuerzas Militares, por la Oficina de Telemática de la Policía Nacional, para el caso de las direcciones o dependencias de la Policía Nacional, por el Viceministerio del GSED y Bienestar, para el caso de las entidades adscritas y vinculadas al Sector Defensa. En todos los casos, el Grupo de Tecnologías de la Información y las Comunicaciones de la Dirección de Logística del Ministerio de Defensa Nacional, verificará la viabilidad y cumplimiento de los lineamientos y políticas establecidas, las cuales deberán contar con la aprobación definitiva del Comité de Integración de Tecnología de Información y Comunicaciones del Sector Defensa, o el que haga sus veces.

ARTÍCULO 30. RESPONSABILIDADES DE LAS UNIDADES EJECUTORAS O DEPENDENCIAS DEL MINISTERIO DE DEFENSA NACIONAL, LA POLICÍA NACIONAL Y LAS ENTIDADES ADSCRITAS Y VINCULADAS AL SECTOR DEFENSA. En todos los casos, para contratar servicios basados en Tecnologías en la Nube, las unidades ejecutoras o dependencias del Ministerio de Defensa

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberán, además de cumplir con la normatividad vigente y aplicable⁶:

a. Determinar la justificación para utilizar un modelo de Tecnologías en la Nube, incluyendo:

- Mayor eficiencia o efectividad en la provisión del servicio tecnológico.
- Requerimiento puntual de un atributo específico de Tecnologías en la Nube (ej., elasticidad, escalabilidad, modelo basado en utilización).
- Necesidad de implantar un servicio tecnológico en un corto período de tiempo.
- Necesidad de implantar nuevos o mejores mecanismos de contingencia, recuperación de desastres o estrategias para garantizar la continuidad del negocio.
- Necesidad de contar con una estrategia para establecer ambientes de desarrollo, pruebas, control de calidad o cualquier requerido definido para mejores prácticas en el ciclo de desarrollo de software.

b. Cuantificar todos los costos asociados con el ciclo de vida de la solución de Tecnologías en la Nube, entendido esto como su sostenibilidad y mantenimiento, no solamente su implantación, con un enfoque de evaluación costo beneficio.

c. Considerar maneras de estructurar las soluciones y acuerdos de servicios o contratos de forma que faciliten la adopción de Tecnologías en la Nube, en otros programas, unidades ejecutoras, dependencias, instituciones o entidades del Sector Defensa.

d. Establecer, como mínimo, los siguientes elementos relacionados con incidentes:

- Los procedimientos para el manejo de incidentes, informar y obtener respuesta por parte del proveedor y otras funciones de seguridad, en colaboración con el proveedor de Tecnologías en la Nube.
- Las medidas respectivas relacionadas con recuperación de desastres y para garantizar la continuidad de los servicios de Tecnologías en la Nube. Así mismo, se deben integrar a los planes de continuidad y recuperación del contratante con los planes de continuidad del negocio y recuperación del proveedor.
- Los acuerdos de niveles de servicio – SLA, en los que se establezcan los niveles de respuesta de los proveedores ante cualquier incidente. Adicionalmente, que se cuente con notificaciones que indiquen el estado de la capacidad o servicio contratado, de manera que permita conocer cuando se está a punto de superar lo contratado y poder establecer nuevos parámetros.
- Los procesos de respaldo, custodia y tiempos de retención entre otros.

e. Documentar los roles y responsabilidades de las partes involucradas, relacionadas con la implantación, operación y apoyo a la solución de Tecnologías en la Nube, así como los usuarios que realizarán el aprovisionamiento automático o por demanda de las capacidades de cómputo, toda vez que se debe tener un control específico sobre los servicios creados.

f. Establecer un Plan de Migración, en caso de que haya que cambiar de proveedor de solución de Tecnologías en la Nube o se desee traer la solución a la infraestructura tecnológica de la respectiva unidad ejecutora o dependencia del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, con el fin de disminuir y evitar el riesgo de estar atado a un único proveedor o tipo de tecnología, garantizando la entrada y salida de la nube.

g. Incluir, en todos los contratos, una cláusula en donde se manifieste de forma explícita que los datos y su uso son propiedad exclusiva de la respectiva unidad ejecutora o dependencia del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa. Conforme a lo anterior, se debe establecer el proceso de entrega y la disposición final de la información, de eliminación de toda la información almacenada en el tiempo de la vigencia del contrato, así como la eliminación de los respaldos realizados durante el mismo.

⁶ Basado en la Guía de Computación en la Nube, MinTIC (2017) [Online] Disponible en: https://mintic.gov.co/portal/604/articles-58727_recurso_2.pdf y adaptado con información de "PolíticaTIG-017: Tecnologías en la Nube (Cloud Computing) – Oficina del Principal Ejecutivo de Información – Estado Libre Asociado de Puerto Rico (2013). [Online] Disponible: <https://www2.pr.gov/GobiernoAGobierno/Documents/Guia%20TIG-017%20-Tecnolog%C3%ADas%20en%20la%20Nube%20%E2%80%99CCloud%20Computing%E2%80%99D.pdf> Consultado el 26 de septiembre de 2018.

Continuación de la Resolución "Por la cual se emite la Política de Tecnologías en la Nube para el Sector Defensa y Seguridad y se dictan otras disposiciones"

- h. Establecer la aplicabilidad de las políticas vigentes y relacionadas, tanto sectoriales como institucionales, y verificar el cumplimiento por parte del proveedor de servicios de Tecnologías en la Nube.
- i. Adoptar un marco de referencia de gestión de riesgos para la monitorización, medición y control del riesgo empresarial introducido por las Tecnologías en la Nube.

ARTÍCULO 31. DELEGACIÓN. Se delega en el Viceministro para la Estrategia y Planeación la competencia para expedir los formatos, guías técnicas y actos administrativos requeridos para la implementación de lo dispuesto en la presente resolución en las unidades ejecutoras o dependencias del Ministerio de Defensa, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa.

ARTÍCULO 32. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación.

Publíquese y cúmplase.

Dada en Bogotá, D. C.,

EL MINISTRO DE DEFENSA NACIONAL

GUILLERMO BOTERO NIETO