



MINISTERIO DE DEFENSA NACIONAL

RESOLUCIÓN NÚMERO 0463 DE 2022
(09 FEB 2022)

Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones

EL MINISTRO DE DEFENSA NACIONAL

En ejercicio de las facultades legales, especialmente las que le confiere el artículo 9 y 60 de la Ley 489 de 1998, el artículo 2 del Decreto 4890 de 2011, y

CONSIDERANDO:

Que la Ley 1341 del 30 de julio de 2009 "*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional de espectro y se dictan otras disposiciones*" consagra en el artículo 2 numeral 6 dentro de los principios rectores de las Tecnologías de la Información y las Comunicaciones (TIC) la neutralidad tecnológica, así: "*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*". Sea preciso señalar que mencionado principio también se encuentra contemplado en el Decreto 1087 del 26 de mayo de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*", en el artículo 2.2.9.1.1.4.

Que el Documento CONPES 3650 del 15 de marzo de 2010 establece la "*Importancia Estratégica de la Estrategia de Gobierno en Línea*" y su justificación en términos generales radica en que "*La adopción y aprovechamiento de nuevas tecnologías por parte de las entidades del Estado redundan en beneficios, tanto del Gobierno como de los ciudadanos, empresas, academia y otras organizaciones relacionadas. El desarrollo de la estrategia de Gobierno en Línea ha procurado incrementar la eficiencia del Estado, permitiendo la integración de los diferentes servicios, la racionalización de recursos y la disponibilidad de información al interior de las entidades. De la misma manera, incrementa la transparencia del Estado y la participación ciudadana, utilizando nuevos canales de comunicación, tanto desde el Gobierno a los ciudadanos como en sentido inverso.*".

Que el Documento CONPES 3701 del 14 de julio de 2011 señala los "*Lineamientos de política para ciberseguridad y ciberdefensa*", la cual tiene como objetivo central "*(...) fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio.*". Para tal efecto, concentra los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética.

Que el Documento CONPES 3854 del 11 de abril de 2016 trata sobre la "*Política Nacional de Seguridad Digital*", que constituye la "*(...) hoja de ruta para que el Gobierno, las organizaciones públicas y privadas, la fuerza pública, la academia y los ciudadanos en general, cuenten con un entorno digital confiable y seguro.*", el cual estipula dentro de los objetivos específicos: 5.2.4. "*Fortalecer la defensa*

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos", y a su vez E4.1. "Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital" y E4.5. "Fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital".

Que el Decreto 415 del 07 de marzo de 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones", establece en el artículo 2.2.35.3 dentro de los objetivos del fortalecimiento institucional, numeral 3 "Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia".

Que el Decreto 1008 del 14 de junio de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015", transformó la "Estrategia de Gobierno en Línea" en la "Política de Gobierno Digital", la cual forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores, que "(...) busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano, a través de la participación y la prestación de servicios de calidad.". También incentiva 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 en su versión dos (02), expedido por el Ministerio de las Tecnologías de la Información y las Comunicaciones, plantea que el Estado no debe privilegiar tecnologías, ni proveedores y, por 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 dentro del Modelo de Arquitectura Empresarial (MAE), en el dominio de arquitectura de infraestructura TI, el lineamiento de acceso a servicios en la nube - MAE.LI.AIT.03, estableciendo el deber de evaluar como primera opción la posibilidad de prestar o adquirir los bienes y servicios asociados a la infraestructura tecnológica haciendo uso de la nube (pública, privada o híbrida), para atender las necesidades de las entidades (Mm TIC, 2019)1.

Que la Resolución 4240 del 15 de junio de 2018 "Por la cual se adopta el Modelo Integrado de Planeación y Gestión, se integra el Modelo Estándar de Control Interno en el Sector Defensa, se crea el Comité de Gestión y Desempeño para el Sector Defensa", consagra en el artículo 5 dentro de las dimensiones de gestión y desempeño institucional: "Gestión con Valores para Resultados" e "Información y Comunicación"; las cuales se desarrollan por medio de las siguientes políticas de gestión y desempeño institucional: "Transparencia, acceso a la información pública y lucha contra la corrupción", "Gobierno Digital" y "Seguridad Digital".

Que mediante la Resolución 5563 del 02 de agosto de 2018 "Por la cual se formula el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018-2022 y se emiten otros lineamientos relacionados con las Tecnologías de la Información y las Comunicaciones en el Sector Defensa", se establece en el artículo 8 la estrategia sectorial para la gestión de tecnologías de la información y las comunicaciones del Ministerio de Defensa Nacional, el cual fija el alcance del elemento de la estrategia "Infraestructura" - enfoque "Nube Sectorial" así: "desarrollar y ejecutar los estándares y la estrategia para contar con una solución de nube sectorial bajo un ambiente seguro".

Que mediante la Directiva Presidencial 03 del 15 de marzo de 2021, Por la cual se expiden "Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos", en su numeral 1 Uso de servicios de nube precisa directrices para la adopción de esta Tecnología en las Entidades Públicas.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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 mismo, 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* 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 Resolución, 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.

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 o recursos de computación en la medida en que las requiera sin necesidad de interacción humana por parte del proveedor del servicio. Aprovisionar corresponde a la posibilidad de contratar, abastecer o asignar recursos computacionales en el periodo que sea requerido.
- 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 con todas las medidas de seguridad 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 en la nube automáticamente controlan y optimizan el uso de los recursos dotándose de capacidades para medir su rendimiento en un nivel de abstracción suficiente para la naturaleza del servicio proporcionado. Además, dicho control debe permitir ser monitoreado y reportado de manera transparente tanto al proveedor del servicio como al consumidor de este.

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

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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 principios:

- 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 Sectorial:** 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 cualquier momento o desde cualquier lugar, sin requerir de inversiones elevadas en hardware ni software, manteniendo los Acuerdos de Nivel de Servicio (ANS) o Service Level Agreement (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. Así mismo, deben permitir 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 y sobre la base de una aproximación basada en el riesgo, deberán establecerse medidas de mitigación y control acordes con el nivel de riesgo. De igual manera, deberán 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.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

- 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.

PARÁGRAFO: Es responsabilidad de cada Entidad evaluar el tipo de información que podrá ser gestionada en cada uno de los modelos de despliegue de tecnologías en la nube, señalados en el presente artículo, teniendo en cuenta lo dispuesto en el artículo 2.1.1.4.2.1 del Decreto 1081 de 2015, "Por el cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República", en especial lo referente a la información considerada como PÚBLICA RESERVADA, conforme a lo cual la Entidad podrá contratar el modelo de despliegue de tecnología en la nube que se considere más adecuado, de acuerdo a lo definido en el literal e del artículo 11 de la presente resolución.

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

CAPÍTULO II

POLÍTICA DE TECNOLOGÍAS EN LA NUBE

ARTÍCULO 6. 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 7. 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,

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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 8. 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 normatividad y regulación vigente aplicable, incluyendo lo relacionado con el manejo de bases de datos personales e información sensible, particularmente lo establecido por las Leyes 1266 de 2008, Ley 1581 de 2012, Ley 1621 de 2013 y Ley 1712 de 2014.

ARTÍCULO 9. 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. 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 de la Dirección de Tecnologías de la Información y las Comunicaciones – TICS del Ministerio de Defensa Nacional, 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 10. 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 toda la normatividad y regulación vigente de privacidad, confidencialidad y disponibilidad aplicables a nivel nacional, sectorial e institucional. En caso de tratamiento de datos personales, se debe aplicar lo referido en la sección 3.2 del Título V de la Circular Única de la SIC.

Las unidades ejecutoras o dependencias 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, confidencialidad y disponibilidad de la información 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

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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, por ser considerada PÚBLICA RESERVADA de acuerdo a establecido en el artículo 2.1.1.4.2.1 del decreto 1081 de 2015, podrá ser almacenada o contratada en servicios en la nube pública o híbrida, salvo que sea nube pública con infraestructura dedicada. 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, con información clasificada como PÚBLICA RESERVADA, podrán implementarse o migrarse totalmente, incluyendo la infraestructura que los soporta in situ, a soluciones basadas en servicios de nube privada, incluso fuera del territorio colombiano, siempre y cuando el fabricante disponga de infraestructura física exclusiva y garantice la soberanía de los datos.

Cuando el proveedor se trate de un tercero diferente al fabricante, 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 en este caso particular el concepto de "multi-tenant". En ambos casos, debe prevalecer la salvaguarda de la información de seguridad y defensa nacional".

- 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 riesgo 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 de la información.
- 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. Se deberán establecer pólizas de responsabilidad en caso de que se presenten pérdidas de la información que generen afectación de la imagen institucional.

PARÁGRAFO: Cuando se requiera hacer uso de analítica de datos o procesos que requieran la implementación de proyectos de inteligencia artificial, se podrá almacenar o contratar servicios de nube pública.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

ARTÍCULO 11. 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 particulares de seguridad de cada solución, las pruebas específicas y la periodicidad para las siguientes consideraciones mínimas:

- 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 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), la Oficina de Respuesta a Incidentes Cibernéticos – CSIRT, en coordinación con la respectiva unidad de Ciberdefensa o la que haga sus veces.
- 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 12. 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 física y lógica, gestión de operaciones, servicios de operación y administración, copias de seguridad de la información con una determinada periodicidad, servicios de administración y monitoreo, y reportes

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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 alternativo ubicado en Colombia, 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 lógico y físico de acuerdo a los estándares internacionales (DoD, NATO, RCMP, TSSIT, Gutmann, NIST SP 800-88), para que sea ejecutado junto con personal calificado de cada una de las Fuerzas e Instituciones luego de la entrega al finalizar los servicios para corroborar la ejecución del proceso.
- 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 este 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, de que trata el literal f del Artículo 10 de esta resolución.
- 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

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

(Controles de Seguridad para Servicios Cloud), ISO/IEC 22301 (Continuidad del Negocio) e ISO 31000 (Gestión del Riesgo), en sus versiones vigentes.

ARTÍCULO 13. 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 consideraciones 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 (Uptime Institute, BICSI, EIA), 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.
- 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 14. 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.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

PARÁGRAFO. Sin perjuicio de lo anterior, se podrá 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 15. 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.
- 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 16. 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 de Servicios y Tecnología en la Nube, priorizando y estableciendo el impacto de las soluciones a migrar. Este plan se elaborará para cada aplicación o solución, existente o nueva, en sitio o con Tecnologías en la Nube, que se pretenda migrar, adoptar o reubicar, posterior a la expedición de la presente Resolución.

ARTÍCULO 17. MODELO DE PLAN DE MIGRACIÓN. La elaboración del Plan de Migración 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 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:

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

- 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, basados en los estándares proporcionados por Uptime Institute, BICSI y EIA.
- 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.

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 18. 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, previendo que el centro de datos alterno del proveedor debe ser activo-activo, 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 19. SOLUCIONES EXISTENTES. Las dependencias de tecnología, o las que hagan sus veces, de 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

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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.

PARÁGRAFO. La Dirección de Tecnologías de la Información y las Comunicaciones - TICS establecerá el método, las herramientas y los medios para realizar el seguimiento al cumplimiento de la Política de Nube.

CAPÍTULO III

PROTECCIÓN DE DATOS PERSONALES EN SERVICIOS Y SOLUCIONES CON TECNOLOGÍAS EN LA NUBE

ARTÍCULO 20. 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.

ARTÍCULO 21. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES. Las unidades ejecutoras y dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa, en su calidad de contratantes de los servicios o soluciones con Tecnologías en la Nube, serán las Responsables del Tratamiento de Datos; es decir que, por sí mismas o en asocio con otros, decidirán 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 22. ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES. 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 23. 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 24. 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 25. 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

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

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.
- k. Gestionar los incidentes de seguridad que pueden afectar la confidencialidad, disponibilidad e integridad de la información personal tratada por el proveedor.
- l. Establecer los requisitos que debe acreditar el proveedor de servicios de tecnologías en la nube basados en evaluaciones de impacto relativas a la protección de los datos personales que administren o estén bajo su custodia.
- m. Garantizar servicios de conectividad a través de un canal dedicado con redundancia permitiendo la alta disponibilidad de las comunicaciones, entre el datacenter y la nube, con el fin de asegurar la latencia y seguridad en la transmisión de la información.

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

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.

ARTÍCULO 26. GARANTÍAS OFRECIDAS POR EL PROVEEDOR. Las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberán recurrir únicamente a proveedores que ofrezcan suficientes garantías para cumplir el Régimen General de Protección de Datos Personales, en cuanto al tratamiento y seguridad.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

CAPÍTULO IV

DISPOSICIONES FINALES

ARTÍCULO 27. ENFOQUE DE GASTOS ASOCIADOS A TECNOLOGÍA. El Sector Defensa, en cabeza del Viceministerio para la Estrategia y Planeación, realizará los estudios necesarios para enfocar la estrategia de gastos basada en soluciones tecnológicas en sitio a una inversión centrada en 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 en la nube 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, en consecuencia, inajenable, inembargable e imprescriptible.

PARÁGRAFO. 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 someterse a la ley y jurisdicción colombiana. Así mismo, los datos e información son propiedad del Estado y, en consecuencia, inajenable, inembargable e imprescriptible.

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; y por la Oficina de Telemática de la Policía Nacional, para el caso de las direcciones o dependencias de la Policía Nacional. En lo que corresponde a las entidades adscritas y vinculadas al Sector Defensa, el Viceministerio de Veteranos y del Grupo Social Empresarial del Sector Defensa- GSED propondrá y coordinará, en los temas relacionados con soluciones con Tecnologías en la Nube, la definición de sinergias, alianzas estratégicas, negociaciones conjuntas y unificación de procesos entre las entidades representadas en el Grupo Social y Empresarial del Sector Defensa "GSED". En todos los casos 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 Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Sector Defensa deberán, además de cumplir con la normatividad vigente y aplicable:

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.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

- 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 por parte del proveedor, 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.
- 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.
- j. Realizar evaluaciones constantes de seguridad y de impacto relativas al tratamiento de datos personales por parte de un proveedor de servicios de tecnologías en la nube, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento con el fin de monitorear los riesgos y aplicar medidas para mitigarlos, evitando que el tratamiento infrinja lo dispuesto en el Régimen de Protección de Datos Personales.

Continuación de la Resolución. "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones."

ARTÍCULO 31. DELEGACIÓN. Se delega a la Dirección de Tecnologías de la Información y Comunicaciones 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 y deroga la resolución 0413 del 01 de marzo de 2021.

PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, D. C., a los

09 FEB 2022

EL MINISTRO DE DEFENSA NACIONAL,


DIEGO ANDRES MOLANO APONTE 