República de Colombia

Libertad y Orden

AGENCIA DE DESARROLLO RURAL

RESOLUCIÓN NÚMERO (___ 0 8 1 ___) DE 2021

2 1 ABR. 2021

"Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural - ADR"

LA PRESIDENTE DE LA AGENCIA DE DESARROLLO RURAL

En ejercicio de las facultades constitucionales y legales establecidas en los artículos 209 y 269 de la Constitución Política, la Ley 489 de 1998, la Ley Estatutaria 1581 de 2012, la Ley 1712 de 2014, el Decreto No. 1071 de 2015, el Decreto 1083 de 2015, el Decreto Ley 2364 de 2015, el Decreto 1008 de 2018, el Decreto 2106 de 2019, la Ley 1955 de 2019 y,

CONSIDERANDO

Que en el artículo 15 de la Constitución Política de Colombia se consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

Que los artículos 209 y 269 de la Constitución Política han señalado que la administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley. Por ello, las autoridades de las entidades públicas están en la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Que el artículo 17 de la Ley Estatutaria 1581 de 2012 *"Régimen General de Protección de Datos Personales"*, y el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015 *"Decreto Único Reglamentario del Sector Comercio Industria y Turismo"*, consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para el ejercicio de este derecho.

Que la Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho, junto con lo dispuesto en el Decreto 1080 de 2015, *"Por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura"*, establecen las directrices para la calificación de información pública, y se establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

Que el Decreto 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"* modificado mediante el Decreto 1008 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, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*, en el artículo 2.2.9.1.1.3. incluye dentro de los principios de la Política de Gobierno Digital la seguridad de la información, de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y

habilitadores transversales[1] y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que las disposiciones de este Decreto representan la evaluación de la estrategia de *"Gobierno en Línea"* a la política pública de *"Gobierno Digital"*, cuyo objetivo es incentivar el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones - TIC, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Que las entidades que conforman la Administración Pública, en los términos del artículo 39 de la Ley 489 de 1998, como es el caso de la Agencia de Desarrollo Rural, están obligados a adoptar la Política de Gobierno Digital siguiendo los lineamientos del Manual de Gobierno Digital, que define procedimientos, estándares y acciones a ejecutar por parte de las entidades, de conformidad con lo establecido en el artículo 2.2.2.35.6 del Decreto 1083 del 2015.

Que la adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una entidad pública como es la Agencia de Desarrollo Rural, están influenciados por las necesidades y objetivos de la Entidad, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.

Que mediante el artículo 1 del Decreto 1499 de 2017, se sustituyó el Título 22 de la Parte 2 del Libro2 del Decreto 1083 de 2015. El nuevo artículo 2.2.22.1.1 del Decreto 1083 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"*, señala que el Sistema de Gestión *"que integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, es el conjunto de entidades y organismos del Estado, políticas, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad"*.

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de *"11. Gobierno Digital, antes Gobierno en Línea"* y *"12. Seguridad Digital"*.

Que en el artículo 2.2.22.3.2. del Decreto 1083 de 2015, se definió el Modelo Integrado de Planeación y Gestión (MIPG), como el *"Marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio"*.

Que el Documento CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Que, a su vez, el parágrafo del artículo 16 del Decreto 2106 de 2019, *"Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"* establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

---

[1] Entiéndase por habilitadores transversales de la Política de Gobierno Digital: Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales, como elementos de base que permiten el desarrollo de los componentes de la política.

Que la Ley 1955 de 2019 *"Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 – 'Pacto por Colombia, Pacto por la Equidad'"*, establece que el Plan Nacional de Desarrollo está compuesto por objetivos de política pública denominados pactos, concepto que refleja la importancia del aporte de todas las facetas de la sociedad en la construcción de una Colombia equitativa; dichos pactos contienen estrategias transversales como el contenido en el numeral 7 del artículo 3 de la mencionada ley, denominado "*Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento*" (numeral 7° del artículo 3°).

Que lo anterior es coherente con los objetivos generales y específicos del Ministerio de Ciencia, Tecnología e Innovación, en relación con el desarrollo del conocimiento científico, tecnológico y de innovación, en aras de la modernización del Estado, según lo establecido en el artículo 126 de la Ley 1955 de 2019, que modificó parcialmente el artículo 2 de la Ley 1951 de 2019, "*Por la cual crea el Ministerio de Ciencia, Tecnología e Innovación, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación y se dictan otras disposiciones*".

Que dicho pacto tiene como objetivo el uso y aprovechamiento de las Tecnologías de la Información y de las Comunicaciones - TIC para mejorar la provisión de servicios digitales de confianza, el desarrollo de procesos internos eficientes, la toma de decisiones basadas en datos confiables y actualizados, el empoderamiento de los ciudadanos y el impulso en el desarrollo de territorios y ciudades inteligentes, logrados a partir de la consolidación de un Estado y ciudadanos competitivos, proactivos, e innovadores, que generan valor público en un entorno de confianza digital[2].

Que por consiguiente, la aplicación de este pacto por el buen uso de las TIC, permitirá a las entidades públicas mejorar su funcionamiento y su relación con otras entidades, con los ciudadanos y agentes del sector, fortaleciendo la relación con el Estado en un entorno confiable, que permita la apertura y aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, la participación en el diseño de servicios y programas, así como la identificación de soluciones a problemáticas de interés común, todo esto en el marco de la eficiencia en la prestación del servicio público.

Que de conformidad con lo establecido en los numerales 2 y 24 del artículo 11 del Decreto Ley 2364 de 2015, hacen parte de las funciones del Presidente de la Agencia de Desarrollo Rural, "*Dirigir las actividades administrativas, financieras y presupuestales, y establecer las normas y procedimientos internos necesarios para el funcionamiento y prestación de los servicios de la Agencia*" y "*Aprobar la estrategia de la Agencia en relación con el uso de las tecnologías de la información y comunicaciones*".

Que, en mérito de lo expuesto, es necesario actualizar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, así como definir los lineamientos frente al uso y manejo de la información en la Agencia de Desarrollo Rural, armonizando los postulados y objetivos del pacto por la transformación digital, como estrategia transversal establecida por el Plan Nacional de Desarrollo,

RESUELVE

CAPITULO I
DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. Objeto. La presente Resolución tiene como objeto adoptar la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural.

ARTÍCULO SEGUNDO. Alcance y Aplicación: La presente política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, se adopta en cumplimiento de las

[2] Manual de Gobierno Digital, consultado en https://mintic.gov.co/portal/604/articles-61775_recurso_2.pdf

disposiciones legales vigentes y basada en la norma ISO27001:2013, con el ánimo de gestionar adecuadamente la seguridad de la información en los procesos, en los activos, en sistemas informáticos y lógicos, partes interesadas, la infraestructura de red de la organización, instalaciones físicas y el entorno.

Esta política aplica a los procesos y procedimientos de la Entidad y está dirigido a todos los usuarios internos, externos, servidores, funcionarios en todas las vinculaciones, y a la ciudadanía en general, que sean usuarios de los servicios informáticos y manuales de la ADR que traten datos y generen información. De igual manera, esta política aplica a toda la información creada, procesada o utilizada por la Agencia de Desarrollo Rural. sin importar el medio, formato, presentación o lugar en el cual se encuentre y deberán adherirse integralmente a la política.

El modelo de seguridad de la información para la Agencia de Desarrollo Rural se conformará por políticas, estándares, procedimientos y mecanismos de seguridad, basados en el modelo Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC. Son fundamentos de la seguridad de la información: confidencialidad, integridad, disponibilidad, según la norma ISO 27001.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad informática, de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en la Entidad; este proceso será liderado de manera permanente por el Oficina de Tecnologías de la Información.

Esta política será revisada anualmente como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

ARTÍCULO TERCERO. Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios de la Agencia de Desarrollo Rural La Agencia de Desarrollo Rural, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño Controles en Entidades Públicas, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de procesos de la Entidad, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño, promoviendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones.

ARTÍCULO CUARTO. Objetivos: La política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación tendrá los siguientes objetivos:

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios.
3. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital de forma efectiva, eficaz y eficiente.
4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la Agencia de Desarrollo Rural.
5. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
6. Fortalecer la cultura de seguridad y privacidad de la información en los usuarios, proveedores, visitantes, tercerizados, contratistas y funcionarios de la Agencia de Desarrollo Rural.
7. Generar conciencia para el cambio organizacional requerido para la apropiación de la seguridad y privacidad de la información.

8. Definir, operar y mantener el Plan de Continuidad de los servicios de la ADR.
9. Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

CAPÍTULO II
POLÍTICAS ESPECIFÍCAS DE MANEJO DE INFORMACIÓN

ARTÍCULO QUINTO. Política de seguridad de los Recursos Humanos. La Dirección de Talento Humano a cargo de la Secretaría General de la Agencia de Desarrollo Rural debe desplegar esfuerzos con el apoyo de la Oficina de Tecnologias de la Información para generar conciencia y apropiación en los servidores públicos y contratistas de la Entidad, sobre sus responsabilidades en el marco de la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, para que actúen de manera consistente frente a las mismas, con el fin de reducir los riesgos de hurto y/o fraude, el mal uso de las instalaciones físicas y medios tecnológicos, asegurando la confidencialidad, disponibilidad e integridad de la información.

ARTÍCULO SEXTO . Obligación de cumplimiento. En relación con los contratistas, proveedores y aquellas personas o terceros que en razón del cumplimiento de sus obligaciones y las de la Agencia de Desarrollo Rural, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, la Vicepresidencia de Gestión Contractual deberán incluir en los documentos contractuales, cualquiera que sea su naturaleza o modalidad, obligaciones correspondientes al cumplimiento de la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, de las cuales deberá ser garante el supervisor del contrato.

ARTÍCULO SÉPTIMO. Política de Gestión de Activos. La Dirección Administrativa a cargo de la Secretaría General, con el acompañamiento permanente de la Oficina de Tecnologías de la Información, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información con el objetivo de garantizar su protección que estarán alineados con los procesos y procedimientos de la Entidad. Dichos lineamientos se impartirán teniendo en cuenta los siguiente literales, que serán consolidados y publicados en el proceso de apoyo "Gestión Documental" de la Dirección Administrativa.

a. **Inventario de Activos:** Los activos de la ADR deben ser identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección y recuperación ante desastres. Por tal motivo, la Dirección Administrativa con el apoyo de la Oficina de Tecnologías de la Información diseñarán una metodología con los lineamientos necesarios para llevar el inventario de los activos de información de su propiedad, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la Entidad defina.
b. **Protección:** Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Oficina de Tecnologías de la Información.
c. **Archivos de Gestión:** La Dirección Administrativa a cargo de la Secretaría General, debe implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental, con el fin de proteger y conservar la confidencialidad, la integridad y la disponibilidad de la información física de la ADR.
d. **Clasificación de la Información**: La Dirección Administrativa a cargo de la Secretaría General deberá establecer una metodología para la clasificación y rotulado de la información de la Agencia, para lo que tendrá en cuenta las previsiones contenidas en la en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014, reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y el Decreto 1080 de 2015 y demás normativa que reglamente la clasificación de información de las entidades públicas del país. Así mismo, la Dirección Administrativa deberá contar con mecanismos para rotular la información física.

ARTÍCULO OCTAVO. Política de Control de Acceso. Los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deberán adoptar las medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías, estructura física e instalaciones, con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de la ADR.

ARTÍCULO NOVENO. Política de Criptografía. La Oficina de Tecnologías de la Información dispondrá de herramientas que permitan el cifrado para proteger la confidencialidad, integridad y disponibilidad. de la información clasificada y reservada, en sistemas de información, mecanismos de transferencia de información internas o externas. El cifrado de la información se realizará por solicitud de los usuarios o de manera general cuando así se requiera.

ARTÍCULO DÉCIMO. Política de Seguridad Física y del Entorno. La ADR deberá adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones) con el fin de mitigar los riesgos y amenazas externas y ambientales, y evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

PARÁGRAFO PRIMERO. La Secretaria General implementará en el marco de sus competencias acciones para la protección de los datos, semiprivados, privados y sensibles recolectados de los servidores públicos, contratistas y visitantes, en lo que refiere a la aplicación de la política de tratamiento de datos personales y establecer mecanismos alternativos para quienes no autorizan el tratamiento de sus datos.

PARÁGRAFO SEGUNDO Para el ingreso, los visitantes de la Agencia de Desarrollo Rural siempre deben estar autorizados por un servidor público o contratista.

PARÁGRAFO TERCERO. Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas de la Agencia de Desarrollo Rural, deben estar debidamente identificados, con un carné, documento o distintivo que acredite su tipo de vinculación y dicho documento se debe portar en un lugar visible.

PARÁGRAFO CUARTO. El personal de empresas contratistas que desempeñen labores de forma permanente o transitoria en las instalaciones de la ADR, deben estar identificados con distintivos de la empresa y contar el carné de la Administradora de Riesgos Laborales - ARL.

ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad de las Operaciones. La Oficina de Tecnologías de la Información de la ADR será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información y contará con los mecanismos necesarios para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados.

De igual manera, se proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Entidad e implementará mecanismos de contingencias, y recuperación ante desastres, con el fin de propender por la disponibilidad de los servicios de tecnologías de la información en el marco de la operación de la ADR.

La Oficina de Tecnologías de la Información deberá realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que ésta sea reportada por el responsable de dicha información, con el objetivo de recuperarla en caso de cualquier tipo de falla. La Oficina de Tecnologías de la Información efectuará la copia respectiva de acuerdo con el esquema definido previamente en un

procedimiento que enmarque la gestión de copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la Entidad.

El diseño de este procedimiento se hará bajo la dirección de la Oficina de Tecnologías de la Información, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la Entidad, con el fin de determinar la información a respaldar y la periodicidad del respaldo, los tiempos de recuperación y restauración, y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

PARÁGRAFO. En el evento que se haga uso de una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales de la ADR, se deberá cumplir con lo establecido en la presente política.

ARTÍCULO DÉCIMO SEGUNDO. Política de Seguridad de las Comunicaciones. La Oficina de Tecnologías de la Información establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas. Asimismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la ADR.

La Oficina de Planeación con el apoyo de la Oficina de Tecnología de la Información, establecerá mecanismos para que el intercambio de información con las partes interesadas internas o externas, se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicio de web o cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en esta Resolución y será coordinado por la Oficina de Tecnologías de la Información con los mecanismos establecidos para tal fin.

PARÁGRAFO. Todos los contratistas o servidores de la ADR, sin importar su nivel jerárquico, deberán dentro de sus obligaciones o funciones cumplir con las normas relacionadas con los derechos de autor y confidencialidad de la información, así como del tratamiento y protección de datos personales dando cumplimiento a lo dispuesto en la Ley 1581 de 2012 y de conformidad con lo señalado en el Decreto 1377 de 2013. Cualquier documentación generada será conservada y archivada en forma segura en la historia laboral de los servidores públicos y en el archivo de los procesos contractuales para el caso de los contratistas.

ARTÍCULO DÉCIMO TERCERO. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas. La Oficina de Tecnologías de la Información garantizará que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información de la ADR, para lo cual establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Oficina de Tecnologías de la Información es la única dependencia de la Agencia con la capacidad de adquirir, desarrollar e implementar soluciones tecnológicas para la ADR, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme con los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la ADR.

En consecuencia, cualquier software que opere en la ADR deberá contar con la autorización de la Oficina de Tecnologías de la Información y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuéstales de dicha oficina, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro y en el evento que no haya sido entregado a la Oficina de Tecnologías de la Información, no será responsabilidad de ésta.

PARÁGRAFO. En caso de que alguna dependencia requiera desarrollo para sistemas de información dentro del desarrollo misional u operacional en la Agencia de Desarrollo Rural, se debe contar con el

apoyo y aprobación de la Oficina de Tecnologías de la Información, adicional deberá cumplir con lo establecido en la presente política.

ARTÍCULO DÉCIMO CUARTO. Política de seguridad para la relación con contratistas. La Vicepresidencia de Gestión Contractual establecerá mecanismos necesarios para asegurar que la información que generen custodie, procesen o a la que se tengan acceso los contratistas con ocasión de la ejecución de sus actividades, se utilice dentro del marco de la seguridad y privacidad de la información. En el mismo sentido, y a través del seguimiento a la ejecución, se garantizará se apliquen las políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, los cuales deberán ser comunicados a los contratistas con el apoyo de la Oficina de Comunicaciones.

PARÁGRAFO. Tratándose de relaciones contractuales de la ADR, estas disposiciones deberán ser incorporadas en los documentos contractuales con los que se relacionen con los contratistas, a efectos de garantizar su implementación.

ARTÍCULO DÉCIMO QUINTO. ***Política de Gestión de Incidentes de Seguridad de la Información.*** La Oficina de Tecnologías de la Información promoverá entre los servidores públicos y contratistas de la Entidad, el reporte y seguimiento de incidentes relacionados con la seguridad de la información y sus medios y asignará responsables de la mencionada oficina, para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados.

La Oficina de Tecnologías de la Información es el único autorizado al interior de la ADR, para reportar incidentes de seguridad ante las autoridades correspondientes,

ARTÍCULO DÉCIMO SEXTO. P*olítica de la Continuidad de la Operación del Servicio.* La Agencia de Desarrollo Rural dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. La Oficina de Tecnologías de la Información, la Oficina de Planeación y la Dirección Administrativa liderarán conjuntamente la elaboración la elaboración del Análisis de Impacto del Negocio (BIA) y del Plan de Continuidad de la Operación de los Servicios.

ARTÍCULO DECIMO SÉPTIMO. ***Política de Cumplimiento.*** La Agencia de Desarrollo Rural a través de la Oficina de Tecnologías de la Información velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.

CAPÍTULO III
RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS

ARTÍCULO DÉCIMO OCTAVO POLÍTICA DE SEGURIDAD DIGITAL. Todos los servidores públicos o contratistas que hagan uso de los recursos tecnológicos de la Agencia de Desarrollo Rural tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y por ende, el cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

a. **Del uso del correo electrónico.** El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los servidores públicos y contratistas de la Agencia, cuyo uso se facilitará en los siguientes términos:
   1. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la Entidad es el asignado por la Oficina de Tecnologías de la Información, que cuenta con el dominio @adr.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

2. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la Agencia.
3. En cumplimiento de la iniciativa institucional del uso racional y eficiente del papel, se debe preferir el uso del correo electrónico para el envío de documentos físicos, siempre que la ley lo permita.
4. Los mensajes de correo electrónico tendrán en cuenta las previsiones contenidas en la Ley 527 de 1999 "*Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones*", normativa que establece la validez de los mensajes de datos.
5. Está prohibido el envío de correos masivos (más de 30 destinatarios) tanto internos como externos, con excepción de los que se generen desde el despacho del Presidente, de los Vicepresidentes, de la Secretaría General, de los Directores de las Unidades Técnicas Territoriales, de la Oficina de Comunicaciones, y Oficina de Tecnologías de la Información, en caso de ventana de mantenimientos de los servicios a cargo. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.
6. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Oficina de Tecnologías de la Información a través de la herramienta de la Mesa de Servicios como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.
7. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o a cualquier otra instancia ajena a los fines o a la misionalidad de la Agencia de Desarrollo Rural.
8. Está expresamente prohibido el uso del correo institucional para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
9. Está expresamente prohibido distribuir información de la Agencia que no tenga el carácter de datos abiertos, a otras entidades o ciudadanos sin la debida autorización de la Presidencia, Vicepresidencias, la Secretaría General, Oficina de Planeación o la Oficina de Comunicaciones, previa revisión de la Oficina de Planeación en caso de cifras oficiales y de la Oficina de Comunicaciones en caso de comunicados oficiales.
10. El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.
11. Todos los correos electrónicos institucionales en sus mensajes deben contener una nota de confidencialidad, que será diseñada por la Oficina de Tecnologías de la Información y debe reflejarse en todos los buzones con dominio @adr.gov.co.
12. Está expresamente prohibido distribuir, copiar, reenviar información de la Agencia de Desarrollo Rural a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
13. Cuando culmina la vinculación con la Entidad de un servidor público o contratista, la Agencia de Desarrollo Rural en cabeza de la Oficina de Tecnologías de la Información deshabilitará el correo electrónico y no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa del despacho de Presidencia, Secretaria General, por solicitud de la Oficina de Control Interno o de Control Disciplinario, o por orden judicial, como parte de un proceso en curso.
14. La Agencia de Desarrollo Rural a través de la Oficina de Tecnologías de la Información se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la misma, previa solicitud expresa del supervisor del contrato, Presidente, Vicepresidentes, Secretario General, de los Directores de las Unidades Técnicas Territoriales a la Oficina de Tecnologías de la Información.

b. **Del uso de internet:** La Oficina de Tecnologías de la Información establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones u obligaciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

1. El uso del servicio de Internet está limitado exclusivamente para propósitos laborales y los servicios a los que un determinado usuario pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario en la Agencia de Desarrollo Rural y para los cuales esté formal y expresamente autorizado
2. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
3. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas.
4. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
5. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

La Agencia de Desarrollo Rural a través de la Oficina de Tecnologías de la Información se reserva el derecho de controlar los accesos a los sitios web, navegados desde la Red Interna hacia la Internet Pública, con el fin de evitar fuga de información y accesos a sitios que pongan en riesgo la integridad de la red institucional, así como, el parque computacional y demás infraestructura tecnológica y por tanto el uso del servicio de internet de todos sus funcionarios o contratistas, puede limitar el acceso a determinadas páginas de Internet, los horarios de conexión, el acceso a los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

c. **Del Uso de los Recursos Tecnológicos:** Los recursos tecnológicos de la Agencia de Desarrollo Rural, son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

1. Los bienes de cómputo de la ADR se emplearán de manera exclusiva y bajo la completa responsabilidad del el funcionario o contratista al cual han sido asignados, únicamente para el correcto desempeño de las funciones o las obligaciones contractuales pactadas. Por tanto, estos no pueden ser utilizados con fines personales o por terceros a excepción de aquellos autorizados ante la Oficina de Tecnologías de la Información, previa solicitud formal enviada por la Presidencia, Vicepresidencias, Jefes de Oficina, Secretaría General y Directores de la Unidades Técnicas Territoriales, a través de la Mesa de servicios.
2. Sólo está permitido el uso de software licenciado por la ADR o aquel que, sin requerir licencia, sea expresamente autorizado por la Oficina de Tecnologías de la Información. Las aplicaciones generadas o adquiridas por la Entidad, en desarrollo de su operación institucional, deben ser reportadas a la Oficina de Tecnologías de la Información para su administración. Adicionalmente es la única dependencia autorizada para la administración del software de la ADR, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.

3. En caso de que el servidor público o contratista deba hacer uso de equipos ajenos a la ADR, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo antivirus licenciado y actualizado y solo podrá conectarse a la red de la ADR una vez esté avalado por la Oficina de Tecnologías de la Información.
4. Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas a la ADR en custodia al finalizar la vinculación con la Entidad.
5. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mimos.
6. No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos o información física que pueda estar expuesta a daño parcial y por ende, a la pérdida de la integridad de ésta.

7. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos y la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
8. Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son los designados por la Oficina de Tecnologías de la Información para tal labor.
9. La Oficina de Tecnologías de la Información realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información, en la medida que la exposición de los equipos represente riesgos de daños en los mismos.
10. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Dirección Administrativa de la ADR, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de dicha dependencia.
11. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada por el funcionario o contratista a quien se le hubiere asignado a la Dirección Administrativa para realizar el procedimiento establecido para este tipo de siniestro, así como también a la Oficina de Tecnologías de la Información con el fin de reportar evento o incidente se seguridad de la información, sin perjuicio de las acciones penales y disciplinarias que se requiera adelantar según el caso.
12. La pérdida de información debe ser informada con detalle a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios.
13. Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios, siguiendo el procedimiento establecido.
14. Todo acceso a la red de la ADR, mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Oficina de Tecnologías de la Información.
15. La conexión a la red wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Oficina de Tecnologías de la Información, quien implantará políticas para la seguridad de la información.
16. Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina o durante la noche, esto con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando no se programen actividades vía remota que deben ser autorizadas por la Oficina de Tecnologías de la Información.

d. **Del Uso de los Sistemas o Herramientas de Información:** Todos los funcionarios y contratistas de la Agencia de Desarrollo Rural son responsables de la protección de la información a la que acceden o procesan, así como de evitar su pérdida, alteración, destrucción o uso indebido, para lo cual se dictan los siguientes lineamientos:

1. Las credenciales de acceso a la red o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible, los funcionarios y contratistas no deben revelar éstas a terceros, ni utilizar claves ajenas.
2. Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos.
3. Todo funcionario y contratista es responsable de los registros o modificaciones de información que se hagan a nombre de su cuenta de usuario.
4. En el caso de terminación del vínculo laboral de un funcionario, la Dirección de Talento Humano debe informar la novedad a la mesa de servicio remitiendo la resolución de desvinculación para la inactivación de los servicios tecnológicos correspondientes con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad.
5. En el caso de terminación de un contrato con la ADR, para los contratistas, cuando se realice la certificación de paz y salvo, la mesa de servicio hará la inactivación de los servicios tecnológicos correspondientes con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad.

6. Cuando un funcionario o contratista finaliza su vínculo laboral o contractual con la ADR, la información generada será respaldada y entregada a petición de este o del jefe o supervisor del Contrato o jefe inmediato.
7. Cuando un funcionario o contratista finaliza su vínculo laboral o contractual con la ADR, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente.
8. Cuando un funcionario o contratista finaliza su vínculo laboral o contractual con la ADR, el supervisor del contrato o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo con la normativa vigente.
9. Todos los funcionarios y contratistas de la Agencia deben respetar lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

CAPITULO IV
LINEAMIENTOS, REVISIÓN, VIGENCIA Y DEROGATORIA

ARTÍCULO DÉCIMO NOVENO. Lineamientos *de las Políticas de Seguridad de* la Información. Todas las políticas identificadas en este acto administrativo se deberán desarrollar de manera detallada y clara en la Declaración de Aplicabilidad y en el Manual de Políticas de Seguridad y Privacidad de la Información.

ARTÍCULO VIGÉSIMO. Revisión. La Política de Seguridad y Privacidad de la Información de la ADR, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por el Jefe de la Oficina de Tecnologías de la Información o quien este delegue.

ARTÍCULO VIGÉSIMO PRIMERO. Vigencia y Derogatoria. La presente resolución rige a partir de la fecha de su publicación y deroga la Resolución 409 de 2019.

Dada en Bogotá D.C., 21 ABR. 2021

PUBLÍQUESE Y CUMPLASE

ANA CRISTINA MORENO PALACIOS
2021.04.21 11:11:59 -05'00'

ANA CRISTINA MORENO PALACIOS
PRESIDENTE

Proyectó: Catherine Suárez Rodríguez – Contratista Oficina de Tecnologías de la Información
Revisó: Nhazly Marcela Correa Bustos – Contratista Oficina Jurídica
Marisol Orozco Giraldo – Jefe la Oficina Jurídica
Yinna Mora Cardozo – Contratista Presidencia
Andrea Juliana Ortiz Bohórquez-Contratista Secretaria Genera
Aprobó.: Víctor Manuel Mondragón Maca- Jefe Oficina de Tecnologías de la Información
Cesar Augusto Castaño Jaramillo – Secretario General