República de Colombia

Libertad y Orden

AGENCIA DE DESARROLLO RURAL

Resolución Número (0409) de 2019 03 JUL. 2019

"Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural- ADR y se definen lineamientos frente al uso y manejo de la información"

LA PRESIDENTE DE LA AGENCIA DE DESARROLLO RURAL

En ejercicio de las facultades legales establecidas en el Decreto No. 1071 de 2015, Decreto Ley 2364 de 2015, Decreto 1008 de 2018, Ley 1955 de 2019 **y**

CONSIDERANDO

Que la Constitución Política de Colombia, en su artículo 15, 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 el Decreto 1078 de 2015 , modificado por 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 la seguridad de la información entre los principios de la Política de Gobierno Digital; 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

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.

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,

---

[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.

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 el Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), adoptó el Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su artículo 2.2.22.3.2 como "*... un 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 la Ley Estatutaria 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales"*, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refieren los artículos 17,15 y 20 de la Constitución Política.

Que 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*", tiene como objetivo principal regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

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 "*Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento*" (numeral 7° del artículo 3°), lo cual 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[2].

Que dicho pacto tiene como objetivo el uso y aprovechamiento y aprovechamiento de las 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[3].

Que por consiguiente, la aplicación de este pacto por el buen uso de las Tecnologias de la información y la comunicación-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

---

[2] 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".

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

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, dado lo anterior, se hace necesario adoptar mediante el presente acto administrativo, la Política General de Seguridad y Privacidad de la Información, implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), 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.

Que conforme al Decreto Ley 2364 de 2015, hace 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*" (numeral 2, artículo 11); y "*Aprobar la estrategia de la Agencia en relación con el uso de las tecnologías de la información y comunicaciones*" (numeral 24, artículo 11).

En mérito de lo expuesto,

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 de la Agencia de Desarrollo Rural - ADR, así como definir lineamientos frente al uso y manejo de la información.

ARTÍCULO SEGUNDO. ALCANCE Y APLICACIÓN: La presente política de la seguridad y privacidad de la información se dicta en cumplimiento de las 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 interesada, 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 del Agencia de Desarrollo Rural – ADR, que traten datos y generen información.

El modelo de seguridad de la información para la Agencia de Desarrollo Rural - ADR, está conformado 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 con regularidad 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.

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran integralmente a la política

ARTÍCULO TERCERO. DEFINICIONES: Para los efectos de la presente resolución, se adoptan las siguientes definiciones básicas, sin perjuicio de desarrollar su naturaleza, características, contenido y alcance en el respectivo procedimiento de seguridad y privacidad de la información de la Agencia de Desarrollo Rural- ADR, que hace parte integral de este acto administrativo.

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Antivirus: Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

Aplicaciones web: Son un tipo de software que se codifica en un lenguaje soportado por los navegadores web y cuya ejecución es llevada a cabo por el navegador en Internet o de una intranet.
Autenticación: cuando se puede garantizar la identidad de quien solicita acceso a la informática.

Autorización: Cuando la informática es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo.

Código malicioso: Es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso.

Confidencialidad: Cuando la informática es solo accesible por aquellos a los cuales se ha autorizado a tener acceso.

Controles criptográficos: Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

Correo electrónico: Es un medio de comunicación electrónico que permite el intercambio de mensajes con usuarios internos externos a través de una cuenta de correo electrónico institucional de manera segura, ágil y confiable que facilite el desarrollo de sus funciones.

Criptografía: Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

Declaración de Aplicabilidad: De la norma ISO 27001, es una relación completa de Controles de Seguridad de la Información, donde se indica si cada uno de ellos resulta de aplicación o no a la organización. Los Controles serán considerados aplicables según la actividad, la gestión interna y el entorno de la empresa. En cada caso, se deberán detallar los motivos por los que se aplica o no dicho Control, y tener información de su estado de implantación.

Declaración de Aplicabilidad: De la norma ISO 27001, es una relación completa de Controles de Seguridad de la Información, donde se indica si cada uno de ellos resulta de aplicación o no a la organización. Los Controles serán considerados aplicables según la actividad, la gestión interna y el entorno de la empresa

Disponibilidad: Cuando la informática es accesible a los usuarios autorizados en el momento de requerirla. Un ejemplo de control para garantizar la disponibilidad son los planes de contingencia.

El software malicioso: Conocido en inglés como "malware", es un software diseñado específicamente para obtener acceso a un equipo o dañarlo sin que el usuario tenga conocimiento

El spyware: Programa espía es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

El riesgo de seguridad: Es la probabilidad de que se materialice el peligro; es decir, que les genere daño a las personas, bienes o al entorno.

Extensión .BAK: Se refiere a archivos del tipo, archivos de copia de seguridad genéricos. Estos son los archivos creados por el software basado en Windows en la PC que desean almacenar la información de respaldo de la base de datos relacionada con los datos del usuario.

Extensión .EXE: Pertenece a los archivos del tipo "archivos ejecutables de Windows". Estos son uno de los tipos de archivos más comunes que se ven en el mundo de las PC hoy en día.

Extensión .PIF: Es un archivo ejecutable utilizado por el sistema MS-DOS. El documento PIF puede almacenar datos relacionados con la ruta del directorio del archivo exe y las propiedades del programa de destino.

Extensión .BAT: Contienen un conjunto de instrucciones que cuando se ejecuta este archivo, las órdenes contenidas son ejecutadas en grupo, de forma secuencial, permitiendo automatizar diversas tareas.

Extensión. PRG: Contienen un programa, una función o un código fuente del programa. Los archivos PRG son utilizados por varias aplicaciones y no están claramente definidos.

Informática: Se refiere a toda comunicación o representación de conocimiento a partir de datos, representados en diferentes formas, incluías formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio que implique almacenamiento (sistemas de informática), transmisión, ya sea por medio electrónico (correo electrónico, fax) o por medio oral (telefonía fija, móvil, correo de voz, contestadoras); medio audiovisual (prensa, radio, TV), medios masivos (publicaciones científicas, académicas y periodísticas, redes sociales), papel, entre otros.

Infraestructura: Es el conjunto de elementos o servicios que están considerados como necesarios para que una organización pueda funcionar o bien para que una actividad se desarrolle efectivamente.

Integridad: Cuando la informática es exacta y completa.

ISO27001: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

Matriz de requisitos legales: Es un documento que contiene toda la información sobre la normatividad que una empresa debe cumplir legalmente.

Matriz de requisitos legales: Matriz legal es un documento que contiene toda la información sobre la normatividad que una empresa debe cumplir legalmente

Mecanismos de control: Distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos y para fortalecer la confidencialidad, la integridad y la disponibilidad de la información tanto física como digital.

Mesa de Servicio: Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación

MIPG: El Modelo Integrado de Planeación y Gestión es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.

No repudiación: Cuando la informática involucrada en un evento corresponde a quien participa, quien no podrá evadir su intervención en este.

Página Web: Es conocida como un documento de tipo electrónico, el cual contiene información digital, la cual puede venir dada por datos visuales y sonoros, o una mezcla de ambos, a través de textos, imágenes, gráficos, audio o vídeos y otros tantos materiales dinámicos o estáticos.

Plataforma tecnológica: Es toda la base tecnológica que una empresa o institución tiene y ofrece a toda su comunidad, orientada a todo lo que es el enfoque o nivel de servicio y tecnología. En tecnología, hace referencia a lo relacionado con instalaciones de plataformas, portal de servicios web, plataformas de correos, servidores de archivos, instalaciones de servidores físicos donde se alojan todas las herramientas y recursos que se ofrecen, conectividad a internet y dentro de la entidad (cableado estructurado), acceso a todos los equipos y dispositivos, licenciamiento de antivirus a nivel organizacional, soluciones a nivel de virtualización, entre otros.

Política de navegación: El contenido en esta política de navegación web, aplica a los servicios de navegación web que brinda la Agencia de Desarrollo Rural ADR, con personal interno o externo, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos y esta publicada en el sistema de gestión de calidad de la entidad.

Portal: Es sitio Web que ofrece al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a un mismo tema. Incluye: enlaces, buscadores, foros, documentos, aplicaciones, compra electrónica, etc.

Recursos tecnológicos: Es un medio que se vale de la tecnología para cumplir con su propósito.

Red Wifi: Es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, como computadoras, tabletas, smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información.

Sensibilizar: Hacer que una persona se dé cuenta de la importancia o el valor de una cosa, o que preste atención a lo que se dice o se pide.

Sitio Web: Conjunto organizado y coherente de páginas Web que tiene como función ofrecer, informar, publicitar o vender contenidos, productos y servicios al resto del mundo.

Software: Un programa o conjunto de programas de cómputo que incluye datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.

Spam: Mensaje electrónico no deseado, no solicitado y con remitente desconocido, enviado a una gran cantidad de usuario. El contenido de un spam es normalmente publicitario con el fin de divulgar un producto o servicio de una empresa

Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Web service: Es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

ARTÍCULO CUARTO. OBJETIVOS: La Política General de Seguridad y Privacidad de la Información tendrá los siguientes objetivos:

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Gestionar los riesgos de seguridad y privacidad de la información.
3. Mitigar los incidentes de Seguridad y Privacidad de la Información 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 -ADR
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 -ADR
7. Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información
8. 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 Agencia de Desarrollo Rural -ADR a través de la Dirección de Talento Humano debe asegurar que los funcionarios, contratista y demás colaboradores adopten sus responsabilidades en relación con las políticas de la Seguridad y Privacidad de la Información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARÁGRAFO. En relación con los contratistas, la Vicepresidencia de Gestión Contractual deberá incluir en las minutas de los contratos cualquiera que sea su denominación que se le dé al mismo, las cláusulas u obligaciones correspondientes a la Seguridad de la Información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información y serán divulgadas a los contratistas a través de los supervisores.

Existen tres principios que debe respetar la gestión de la información en cualquier empresa para poder cumplir, de forma correcta, los criterios de eficiencia y eficacia. Como algo general, se entiende que mantener un sistema seguro y fiable, es garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

ARTÍCULO SEXTO. Política de Gestión de Activos. La Agencia de Desarrollo Rural -ADR a través de la Oficina de Tecnologías de la Información, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información con el objetivo de garantizar su protección, y estarán alineados a los procesos de la entidad.

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, se diseñará 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 disponga.

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, mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información física o digital, software, hardware y recurso humano).

c. **Archivos de Gestión:** La Secretaría General a través de la dependencia encargada de la gestión documental de la ADR y con el acompañamiento del líder del Sistema de Gestión Seguridad de la Información, deben implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad, con el fin de proteger y conservar la confidencialidad, la integridad y la disponibilidad de la información de la ADR.

d. **Clasificación de la Información:** La clasificación de la información de la ADR tendrá en cuenta las previsiones contenidas en la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), y lo estipulado en la Guía para Desarrollo de Inventario y Clasificación de Activos de Información de la ADR.

ARTÍCULO SÉPTIMO. Política de Control de Acceso. Los propietarios de los activos de información y teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso: a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas) 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 Agencia de Desarrollo Rural -ADR.

ARTÍCULO OCTAVO. Criptografía. La Oficina de Tecnologías de la Información brindará a solicitud 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.

ARTÍCULO NOVENO. Política de Seguridad Física y del Entorno. La Agencia de Desarrollo Rural -ADR debe 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), además para mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

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

PARÁGRAFO SEGUNDO. Los visitantes de la Agencia de Desarrollo Rural -ADR, siempre deben estar autorizados por un servidor público o contratista y se le dará un soporte de imagen impresa con los datos del visitante y el área que visita

PARÁGRAFO TERCERO. El personal de empresas contratistas, que desempeñen las funciones de forma permanente o transitoria en las instalaciones de la Agencia de Desarrollo Rural -ADR, deben estar identificados con distintivos del Contratista y portar el carné de la Administradora de Riesgos Laborales -ARL.

ARTÍCULO DECIMO. 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 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, 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 al crecimiento de la Entidad, e implementará mecanismos de contingencias y continuidad del negocio 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.

Continuación de la Resolución *"Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural- ADR y se definen lineamientos frente al uso y manejo de la información"*

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 esta, con el objetivo de recuperarla en caso de cualquier tipo de falla.

Efectuará la copia respectiva de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión, 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 en conjunto con los líderes de proceso, 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.

ARTÍCULO DECIMO PRIMERO. 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; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la Agencia de Desarrollo Rural -ADR.

La Oficina de Planeación 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 *webservice* o cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en el artículo séptimo de esta Resolución.

PARÁGRAFO. Como parte de sus términos y condiciones iniciales del contrato de prestación de servicio, todos los servidores públicos o contratistas, sin importar su nivel jerárquico, firmarán cláusula de derechos de autor y confidencialidad con una cláusula de tratamiento de datos que será elaborado por la Vicepresidencia de Gestión Contractual de la Entidad, y la autorización de tratamiento de datos personales. Dichos documentos originales serán conservados y archivados en forma segura en la historia laboral de los servidores públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

ARTÍCULO DECIMO SEGUNDO. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistema. La Oficina de Tecnologías de la Información velará porque el desarrollo interno o externo de los sistemas de información de la Agencia de Desarrollo Rural -ADR cumpla con los requerimientos de seguridad adecuados para la protección de la información.

La Oficina de Tecnologías de la Información será la única dependencia de la Agencia con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a 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 y no haya sido entregado a la Oficina de Tecnologías de la Información, no serán responsabilidad de esta, no se le brindará soporte y no se le salvaguardará la información

ARTÍCULO DECIMO TERCERO. Política de seguridad para relación con proveedores. La ADR a través de la Vicepresidencia de Gestión Contractual, establecerá mecanismos de control en la relación con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que genere, custodie, procese o se tengan acceso, supervisando el cumplimiento de lo establecido de las políticas de seguridad y privacidad de la información. Los supervisores de los contratos o

convenios tendrán la responsabilidad de divulgar y sensibilizar las políticas y procedimientos de seguridad y privacidad de la información

ARTÍCULO DECIMO CUARTO. Política de Gestión de Incidentes de Seguridad de la Información. La Agencia de Desarrollo Rural -ADR promoverá entre los servidores públicos y contratistas el reporte y seguimiento de incidentes relacionados con la seguridad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad.

PARÁGRAFO. La Oficina de tecnologías de la información conforme al rol serán los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, se debe tener en cuenta los canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

ARTÍCULO DECIMO QUINTO. Política de la Continuidad del Servicio tecnológicos. La Agencia de Desarrollo Rural -ADR 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 liderará la elaboración del Plan de Continuidad de los Servicios tecnológicos.

ARTÍCULO DECIMO SEXTO. Política de Cumplimiento. La Agencia de Desarrollo Rural -ADR 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

ARTÍCULO DECIMO SÉPTIMO. Lineamientos de las Políticas de Seguridad de la Información. Todas las políticas identificadas en este Capítulo se deberán reglamentar de manera detallada y clara en la Declaración de Aplicabilidad y en el Manual de Políticas de Seguridad de la Información.

CAPÍTULO III

RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS

ARTÍCULO DECIMO OCTAVO. Responsabilidad. Todos los servidores públicos o contratistas que hagan uso de los recursos tecnológicos de la Agencia de Desarrollo Rural -ADR, 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 de Desarrollo Rural -ADR, cuyo uso se facilitará en los siguientes términos:

   I. 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.

II. 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.

III. En cumplimiento de la iniciativa del uso racional y eficiente del papel y del principio de la Eficiencia Administrativa, se debe preferir el uso del correo electrónico para el envío de documentos físicos, siempre que la Ley lo permita.

IV. 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 legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.

V. Está prohibido el envío de correos masivos (más de 30 destinatarios) a nivel nacional tanto internos como externos, con excepción de lo que se generen desde el correo electrónico asignado por los directores. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

VI. 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.

VII. 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 -ADR

VIII. Esta expresamente prohibido el uso del correo institucional para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.

IX. Está expresamente prohibido distribuir información de la Agencia de Desarrollo Rural - ADR, que no tengan el carácter de datos abiertos, a otras entidades o ciudadanos sin la debida autorización de la Presidencia, Vicepresidencias, la Oficina de Planeación o la Oficina de Comunicaciones.

X. 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 Colombiana vigente.

XI. 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.

XII. Está expresamente prohibido distribuir, copiar, reenviar información de la Agencia de Desarrollo Rural -ADR a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.

XIII. Cuando un servidor público o contratista cesa en sus funciones o culmina la ejecución de contrato la Agencia de Desarrollo Rural -ADR, 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 de la presidencia, Secretaria

General, por orden judicial, por solicitud de la Oficina de Control Interno o de Control Disciplinario como parte de un proceso de investigación.

b. **Del uso de internet:** La Oficina de Tecnologías de la Información, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

I. 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 -ADR, y para los cuales esté formal y expresamente autorizado
II. 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.
III. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas.
IV. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
V. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

La Agencia de Desarrollo Rural -ADR, 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 -ADR, son Herramientas apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

I. Los bienes de cómputo de la ADR se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario o contratista al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o las obligaciones. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados ante la Oficina de Tecnologías de la Información mediante solicitud formal de la Presidencia, Vicepresidencias, Jefes de Oficina, Secretaría General, y Directores Técnicos Territoriales, a través de la Mesa de servicios
II. 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.
III. 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, antivirus licenciado, actualizado y solo podrá conectarse a la red de la ADR una vez esté avalado por la Oficina de Tecnologías de la Información.

IV. 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.

V. 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.

VI. No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos, en la medida que la exposición de los equipos a estos puede ocasionar daños en los mismos.

VII. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.

VIII. 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.

IX. 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.

X. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Dirección Administrativa y Financiera 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.

XI. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, el funcionario o contratista a quien se le hubiere asignado debe Informar la dependencia o sede donde se detecta la pérdida del bien a la Dirección Administrativa y Financiera de la ADR 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.

XII. La pérdida de información debe ser informada con el detalle de la información extraviada a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios para el diligenciamiento del reporte de gestión de incidente o evento de seguridad a la mayor brevedad posible para dar la solución.

XIII. 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 para el diligenciamiento del reporte de gestión de incidente o evento de seguridad a la mayor brevedad posible para dar la solución.

XIV. La Oficina de Tecnologías de la Información es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.

XV. 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.

XVI. 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.

XVII. Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina durante la noche, esto es, con el fin de proteger la seguridad y

distribuir bien los recursos de la Entidad, siempre y cuando se programe actividades vía remota 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 -ADR, son responsables de la protección de la información a la que acceden o procesan y de evitar su pérdida, alteración, destrucción o uso indebido, para lo cual se dictan los siguientes lineamientos:

I. 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.
II. Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
III. Todo funcionario y contratista es responsable de los registros o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
IV. En el caso de terminación del vínculo laboral de un funcionario de planta permanente o temporal la Dirección de Talento Humano, debe informar la novedad a la mesa de servicio con la resolución, 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.
V. En el caso de terminación de ejecución el contrato con la ADR para los contratistas cuando se realice la 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.
VI. Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato de la ADR, la información generada por funcionario o contratista será respaldada y entregada a petición de este o del jefe o Supervisor del Contrato.
VII. Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato de la ADR, el supervisor 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.
VIII. 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

REVISIÓN, VIGENCIA Y DEROGATORIA

ARTÍCULO DECIMO NOVENO. Revisión. La Política de Seguridad y Privacidad de la Información, 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 Oficial de Seguridad de la Información o quien haga sus veces.

ARTÍCULO VIGÉSIMO. Vigencia y Derogatoria. La presente resolución rige a partir de la fecha de su expedición, es de obligatorio conocimiento, aplicación y acato por todos los servidores

96

Continuación de la Resolución *"Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural- ADR y se definen lineamientos frente al uso y manejo de la información"*

públicos, contratistas y colaboradores, cualquiera sea la forma de vinculación o relación y deroga las disposiciones que le sean contrarias.

PUBLICACIÓN: Para notificación general de los destinatarios, publíquese en la página de internet de la Agencia de Desarrollo Rural - ADR, donde se facilitará el conocimiento del contenido de la política de seguridad y privacidad de la información; la cual por ser dinámica podrá actualizarse con posterioridad de acuerdo a la necesidad respectiva.

PUBLÍQUESE Y CUMPLASE

Dada en Bogotá D.C.,

CLAUDIA SOFIA ORTIZ RODRIGUEZ
PRESIDENTE

Preparó: Catherine Suárez Rodríguez – Oficina de Tecnologías de la Información
Edison Javier Bravo Mira (Apoyo Jurídico)
Revisó: Néstor Fernando Mora Téllez – Gestor T1, Grado 8.
Designado temporalmente de las funciones de la Oficina de Tecnologías de la Información
Vo.Bo.: Diego Edison Tiuzo García, Jefe Oficina Jurídica