COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Luis Guillermo Agudelo Ramírez
Gerente

Luis Ernesto Salazar Jiménez
Subgerente Administrativo y Financiero

Humberto Tobón
Subgerente de Planeación Estratégica y Prospectiva

Henry Andrés García Martínez
Jefe Oficina Asesora de Comunicaciones Internas y Externas

José David Pascuas
Jefe Oficina Asesora Jurídica

Lina Marcela Hurtado Acevedo
Tesorero General

Equipo de Apoyo

Jose Fernando Rodriguez Bernal
Profesional Especializado -Contratista

Alciber Francisco Salas Gómez
Profesional Especializado - Contratista

CONTENIDO

INDICE TABLAS

1. INTRODUCCIÓN

LA RAP Región Administrativa y de Planificación del Eje Cafetero, identifica la información como un activo importante que permite el desarrollo continuo de la misión y su cumplimiento facilitando las labores de los funcionarios, contratistas y demás integrantes en el uso de las herramientas tecnológicas. Por lo cual se observa la necesidad de estipular reglas y normas que permita proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de la vida de la información, por consiguiente se establece las políticas de seguridad informáticas, así mismo definir el sistema de gestión de seguridad de la información (SGSI) a través del análisis, diseño e implementación de los objetivos, requisitos de seguridad, procesos, procedimientos, planes y políticas las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que prestan sus servicios o tengan algún tipo de relación; estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia de gobierno digital del ministerio de las tecnologías de la información y las comunicaciones según lo establecido en el Decreto 1078 de 2015. La seguridad de la información es para la empresa, una labor prioritaria que exhorta a todos por velar por el cumplimiento de las normas establecidas.

2. ASPECTOS GENERALES

2.1 OBJETIVOS GENERAL

Disponer de una guía sobre las políticas de seguridad informática de la Región Administrativa de Planificación Eje Cafetero para indicar a los funcionarios, profesionales, contratistas o terceros sobre la información obtenida, en especial enuncia los principios lineamientos y buenas prácticas en aspectos de seguridad y privacidad de la información, con sistemas que apoyan la gestión de la organización, servicios informáticos, equipos de cómputo, redes de datos, seguridad informática entre otros.

2.2 OBJETIVOS ESPECÍFICOS

- Determinar las políticas de seguridad y privacidad de la información de la RAP
- disponer lineamientos para la implementación y verificación del cumplimiento de las Políticas de seguridad y privacidad de la información de la entidad
- Definir los roles y responsabilidades para la administración de la seguridad y privacidad de la información
- Contar con un sistema de políticas, procedimientos y estándares actualizados con el fin de mantener su vigencia y eficacia para minimizar los riesgos que puedan afectar los activos de la empresa
- Interiorizar una cultura de seguridad y privacidad de la información en funcionarios, contratistas y usuarios que hacen parte de la entidad
- Definir una estrategia de continuidad de los procesos de la empresa cuando se presente un riesgo de seguridad de la información

2.3 ALCANCE

Las directivas que se enuncian en el presente documento aplican al Sistema de Gestión y Tecnologías de la información y va dirigido a directivos y funcionarios en general que se benefician con la infraestructura Tecnológica de la Región Administrativa y de Planificación, incluyendo contratistas y terceros que laboran en las instalaciones.

2.4 DEFINICIONES

Para generar claridad en el uso de los conceptos manejados en el presente documento se transcribe las siguientes definiciones que hacen parte de la Norma [ISO 27000:2013]:

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos estratégicos del Ministerio

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Impacto al Negocio: Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos). Ciberactivo crítico: Ciberactivo que es crítico para la operación de un activo crítico.

Ciberactivo: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.

Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Ministerio, destinado a apoyar el cumplimiento de las normas, procesos y procedimientos de seguridad de la información.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Dispositivos móviles: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

DMZ: Sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet de VPN.

Equipos activos de red: Son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.

Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.

Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.

Medio removible: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.

Mesa de Servicios: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Tecnologías de la Información recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

Paneles de conexión (patch panel): Elemento encargado para la organización de conexiones en la red.

Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las

operaciones a los niveles pre-definidos después de un incidente que afecte la continuidad de las operaciones.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Propietario del riesgo: Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.

Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

Oficial de Seguridad de la información: Es la persona que cumple la función de supervisar el cumplimiento de la Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del Ministerio.

Tecnologías de la Información: Las tecnologías de la información y las Comunicaciones -TIC, Nuevas Tecnologías de la Información y de la Comunicación -NTIC, agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.

Test de penetración: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.

VPN: Red virtual privada por sus siglas en ingles Virtual PrivateNetwork.

Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (Ministro, Viceministros, Secretaria General y Direcciones).

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control Correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control Detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control Disuasorio: Control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.

Control Preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).

Dato Personal Público: Toda información personal que es de conocimiento libre y abierto para el público en general.

Dato Personal Privado: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.

Dato Semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.

Datos Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evento de Seguridad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de

seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Fiabilidad: Se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura o velocidad).

Impacto: Resultado de un incidente de seguridad de la información.

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Privacidad de la información: El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

Teletrabajo: Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación –TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

3. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La REGIÓN ADMINISTRATIVA DE PLANIFICACIÓN EJE CAFETERO, mediante la adaptación e implementación de los lineamientos del modelo de seguridad y privacidad de la información orientado a la gestión de sus buenas prácticas el cual conserva, administra y vigila la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información mediante la gestión de controles en la entidad. Previniendo acontecimientos cumplimiento las obligaciones reglamentarias encaminados a la protección de los Sistemas de Gestión de Seguridad de la Información controlando el acceso, uso y manejo adecuado de los sistemas informáticos a través de políticas y programas, para mejorar las actividades de los funcionarios.

El comité Institucional de gestión y desempeño debe aprobar las políticas de seguridad y privacidad de la información, demostrando así su compromiso con la seguridad de la información en la entidad. Una vez aprobada dichas políticas, la alta dirección entra a revisar periódicamente la aplicabilidad y vigencia de las siguientes políticas específicas de seguridad informática y ejecutar los ajustes necesarios sobre ellas para que sean funcional y se puede seguir exigiendo su cumplimiento por parte de todos los funcionarios y personal suministrado por terceras partes que proveen los servicios.

3.1 CONDICIONES GENERALES

- El Ingeniero de sistemas con el apoyo de las demás dependencias que hacen parte de la entidad, serán los responsables de hacer cumplir las políticas enunciadas de acuerdo con las indicaciones y lineamientos establecidos.
- La Región Administrativa y de Planificación Eje Cafetero hará responsable al usuario del conocimiento de la presente política y las consecuencias que se derivan del incumplimiento. Así mismo, el usuario deberá conocer las políticas desde su ingreso a la organización.
- La Región Administrativa y de Planificación Eje Cafetero se reserva el derecho a evaluar periódicamente el incumplimiento de esta (Tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos por la entidad y en estricto acato de las estipulaciones legales vigentes.
- En materia de Irregularidades o incumplimiento en el uso del software, el usuario que no cumpla la política será directamente responsable de las sanciones legales (que, por responsabilidad laboral, penal Y/o civil se incurra) derivadas de sus propios actos.

3.2 GESTIÓN DE ACTIVOS

La Región Administrativa y de Planificación EJE CAFETERO tiene definida las responsabilidades y deberes con respecto a la seguridad de la información, y asegurar la concientización de funcionarios y terceros respecto a la importancia y el cumplimiento de la normatividad definida.

Los Terceros que efectúen el tratamiento de la información propia de la entidad o sobre la cual sea responsable, deben cumplir con la política de seguridad de la información

- Una vez al año se deben revisar, verificar y actualizar los activos de información para definir deberes, obligaciones, responsabilidades y posibles fallas que se requieran mejorar
- Implementar una gestión de riesgos en los activos de información teniendo clara las herramientas a usar de acuerdo con el Manual de riesgos sugerido por el MINTIC
- Solo él personal del área de TI está autorizado para realizar descargas, instalaciones, modificaciones o cambios en los equipos de cómputo, periféricos, software y redes en las instalaciones de la entidad.
- Cualquier cambio o modificación que se necesite hacer, se debe informar por escrito al área de gestión de TI
- Se debe promover el buen uso de los activos de información, conservando el derecho a la intimidad, privacidad, el habeas data, y la protección de los datos y de sus propietarios.
- Una vez Cese la relación laboral con la entidad todo funcionario o contratista debe entregar los activos de información a su cargo con el jefe directo o supervisor de cada área.
- La entidad se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente.
- Los controles serán diseñados para proveer un nivel de protección de la información apropiado y consistente dentro de la empresa, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.
- Todos los activos de información están inventariados y/o identificados por la Subgerencia Administrativa y Financiera, Su responsabilidad será entregada a cada usuario durante su tiempo de uso.
- El usuario que tiene bajo su custodia los recursos tecnológicos debe velar por los mismos, acatando las normas del uso adecuado para evitar daños.
- La Subgerencia Administrativa y Financiera con apoyo del subproceso de Gestión de Sistemas de las tecnologías de la información, administra los recursos TI de la Entidad y fijará las indicaciones para la modernización tecnológica de la entidad, en función de la mejora continua para la optimización de los servicios prestados a los usuarios internos y externos.
- En caso de requerir soporte técnico, el usuario debe hacer la solicitud al Subproceso de Gestión TI.
- En caso de detectar alguna violación a las políticas y lineamientos de TI mencionadas, reportar a soporte técnico y/o por la herramienta de Gestión de Recursos de TI de la entidad
- Las aplicaciones, los computadores y cuentas inscritas que son entregadas a los Usuarios para facilitar su trabajo. no tienen privacidad en relación con la información manejada el cual pertenece a la Entidad.

- Toda información, aplicaciones o contenido encontrado en los equipos tecnológicos de la Entidad, que no cumpla requerimientos laborales, será borrada y se reportara el usuario para las sanciones
- El subproceso de Gestión de TI mantendrá actualizado las hojas de vida de los equipos tecnológicos e informará de los ajustes pertinentes a la Subgerencia Administrativa y Financiera, Control Interno y demás dependencias que lo requieran.
- Los usuarios deben tener copias de respaldo de la información relevante de su labor en el servidor de almacenamiento en el área de trabajo.
- verificar que los equipos de la entidad utilizan usuario y contraseña
- Conservar al día todas las solicitudes relacionadas con los equipos tecnológicos (sistemas de información, redes, servidores, conectividad, especificaciones técnicas y aplicaciones)
- Toda modificación no autorizada de información de la Entidad almacenada en medios físicos removibles, como USB, Cd, DVD, entre otros están prohibidas
- Está Prohibido el uso de software no licenciado en los equipos de la entidad.
- Está prohibido copiar el software licenciado de la entidad en los equipos personales sin previa autorización del Subproceso de Gestión de sistemas de información
- El uso de la red de la entidad para los equipos que no hacen parte de esta sólo es permitido por el wifi

3.3 SEGURIDAD EN EL RECURSO HUMANO

Capacitar en seguridad de la información y de los procedimientos de gestión de incidentes de seguridad a funcionarios y contratistas para reconocer la normatividad relacionada con la seguridad de la información en la empresa ya que el desconocimiento de esta no los exonerará de los procesos disciplinarios definido ante violaciones de las políticas de seguridad

3.4 SEGURIDAD FÍSICA

- Disponer de áreas seguras para la gestión, almacenamiento y procesamiento de información de la RAP. Las áreas deben contar con protecciones físicas y ambientales acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, incluyendo la definición de perímetros de seguridad, controles de acceso físicos, seguridad para protección de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales adecuadas de operación y sistemas de contención, detección y extinción de incendios.
- El ingreso de terceros al centro de datos y cableado debe estar debidamente registrado por el personal de vigilancia.
- Los privilegios de acceso físico a los centros de datos deben ser actualizados en caso de terminación o cambio del contrato del personal encargado
- El centro de Datos debe contar con mecanismos de control de Acceso tales como puertas de seguridad, sistemas de alarmas o controles biométricos; sistemas de detección y extinción automáticas de incendios, control de

inundación y alarmas en caso de detectarse condiciones inapropiadas, estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.
    - Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.
    - Los funcionarios o terceros que presten sus servicios a la RAP no deben intentar ingresar a áreas a las cuales no tenga la debida autorización
    - La seguridad de los equipos de cómputo fuera de las instalaciones será responsabilidad de cada funcionario y contratista asignado, junto con una autorización del jefe inmediato.
    - Los accesos a áreas seguras deberán tener un control de acceso físico, y no se debe permitir ingresar equipos fotográficos, de filmación, grabación de audio u otras formas de registro salvo con autorización especial del responsable del área segura.
    - Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.
- Es responsabilidad del usuario mantener el área del equipo libre de alimentos, bebidas u otro cualquier elemento que pueda dañar sus componentes.

3.5 GESTIÓN DE COMUNICACIONES Y OPERACIONES

- A efectos de proteger la integridad y confidencialidad de los activos de información es imprescindible que se cuente con protecciones contra el software malicioso, mantenimiento de los equipos de cómputo, administración de red y bloqueo de puertos de red de telecomunicaciones
    - La oficina de gestión de sistemas de información debe garantizar los recursos necesarios que aseguren la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios que ejecutan dichas labores
    - Todos los usuarios de activos de información tecnológicos y recursos informáticos que requieran la adición o modificación de funcionalidades de estos, deben solicitar el cambio por medio del procedimiento vigente para dicha acción.
    - Toda adquisición, mantenimiento y eliminación de medios de almacenamiento deberá ser realizada por el Subproceso de Gestión de Sistemas de Información, de manera que se garantice seguridad en estos activos de información

3.6 USO DEL CORREO ELECTRÓNICO

- Los servicios de mensajería electrónica son de uso exclusivo para actividades relacionadas con la entidad, por lo tanto, queda prohibida el uso para fines personales.
- Está restringido el envío de mensajes con archivos de música, videos, imágenes pornográficas y/o programas, ya que este tipo de archivos facilitan la propagación de virus e incrementa el ingreso de correos no solicitados. Al

igual que él envió de correos que no hacen parte del desarrollo normal de la entidad.

- Se prohíbe el correo masivo de correos
- Se prohíbe él envió de copias con información confidencial sin el consentimiento del remitente original
- Se prohíbe a los usuarios suscribirse a las listas de correo electrónico o participar en grupo de noticias que divulguen información o mensajes ajenas a las funciones y labores de la RAP EJE CAFETERO
- Todo usuario del correo electrónico deberá leer y responder oportunamente los mensajes y citaciones que se envíen por este medio: con el fin de aprovechar el mayor beneficio que ofrece el correo electrónico que es la rapidez y efectividad de las comunicaciones
- No enviar correo spam como son cadenas, pornografía. Chistes, videos o cualquier otro similar
- Depurar la información del correo eliminando lo que no utilice y guardando los contenidos importantes para la entidad
- Todo correo enviado debe tener un TITULO y ASUNTO que refleje el contenido del mensaje
- No abrir correos cuyo remitente le sea desconocido o cuyo asunto le resulte sospechoso, por lo general estos contenidos vienen con virus
- El usuario del correo electrónico tiene derecho a manejar su información en forma confidencial, asumiendo toda responsabilidad por dicho uso.

3.7 CONTROL DE ACCESO

El compromiso de la entidad es realizar control de acceso a la información, sistemas y de red, así como a monitorear el ingreso, de tal forma que este sea seguro, sin importar si los mismos son electrónicos o físicos. De igual forma se protege la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos, así como el riesgo que se genera de los accesos otorgados a terceros como son proveedores y contratistas, son igualmente supervisados y controlados por la entidad.

- Deben establecerse medidas de control de acceso al sistema operativo, para garantizar la autenticación de los funcionarios.
- Los funcionarios no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical. La longitud mínima de las contraseñas será igual o superior a 8 caracteres y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Se debe permitirse identificar de manera inequívoca cada usuario, dejar registro de las actividades que realiza.
- Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo de la empresa, la interfaz del sistema operativo debe estar configurada de tal forma q tengas solo privilegios de invitado. todas las

labores deben ser estrictamente realizadas por el proceso de gestión de sistemas de información.

- Todos los usuarios con acceso a un sistema de información o a la red informática de la RAP EJE CAFETERO dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que ha sido asignado.
- el acceso a la información de la RAP EJE CAFETERO deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad
- El Sistema Operativo de los equipos de los funcionarios de la RAP EJE CAFETERO deben mantenerse bloqueados en ausencia de este.
- La asignación de privilegios a las aplicaciones informáticas presentes en la RAP EJE CAFETERO, debe ser solicitada al jefe inmediato o al área de gestión de sistemas de información.
- los entes externos que tienen acceso a información crítica de la RAP EJE CAFETERO, deben suscribir para acuerdos para salvaguardar la información.
- Los subgerentes de las áreas están en la obligación de avisar oportunamente el ingreso, retiro, cambio de funciones del personal al Subproceso de Gestión de TI, para la activación o inactivación de cuentas en los sistemas informáticos.
- Las cuentas de acceso de los Sistemas Informáticos son exclusivamente para cada usuario y no debe compartir.
- El acceso a los aplicativos será bloqueado con 5 intentos fallidos al digitar la contraseña. Su desbloqueo debe ser solicitado la Subproceso de Gestión TI
- El acceso a las instalaciones de procesamiento de datos es restringido a personas no autorizadas, al igual que los cuartos de equipos.
- Todos los funcionarios, deberán portar el carné en un lugar visible para facilitar el control de las personas que ingresan y transitan en la Entidad.
- Los equipos de la entidad deben estar conectados a los tomacorrientes regulados que disponen las instalaciones.

3.8 SERVICIO DE INTERNET

- El acceso a Internet es SOLO de uso laboral. Por tal razón, está restringido según el requerimiento y funciones de cada usuario.
- El uso de salas de chat está prohibido
- Está prohibido la descarga de archivos de música, videos y similares. De ser necesario la descarga este debe ser validado por el personal encargado de la Gestión de TI
- Los usuarios que estén haciendo uso indebido de los recursos informáticos serán notificados a su jefe inmediato y se les suspenderá el servicio por una semana, de reincidir en la falla se le notificará a la subgerencia y el servicio será suspendido hasta nueva orden.
- Se garantiza la disponibilidad de internet en un 90%
- Se autoriza la navegación en ´paginas cuyo contenido este acorde a las necesidades de la entidad

- El uso indebido de internet es responsabilidad del usuario y se considerará una falta al reglamento interno de trabajo y será sancionado como tal.

3.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

- LA RAP EJE CAFETERO debe asegurar que se haga el diseño e implementación de los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.
- La RAP EJE CAFETERO, debe establecer controles para cifrar la información que sea considerada sensible y evitar posibilidad de repudio de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.
- La información tratada por las aplicaciones aceptadas por la empresa debe preservar su confiabilidad desde su ingreso, transformación y entrega.

3.10 GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- LA RAP EJE CAFETERO, debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en la entidad de los incidentes de seguridad de la información.
- Todos los usuarios de la información de la RAP EJE CAFETERO deben reportar los incidentes de seguridad que se presenten, según el procedimiento vigente.
- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables.

3.11 GESTIÓN DE LA CONTINUIDAD DE LOS PROCESOS

Debe evaluarse el impacto de las interrupciones que afectan la operación de los procesos críticos de la Empresa y definir e implementar planes de continuidad y de recuperación ante desastres para propender por la continuidad de esta. Los planes deben considerar medidas tanto técnicas como administrativas para que se puedan recuperar oportunamente las funciones de los procesos y la tecnología que las soporta.

- Los planes de continuidad y de recuperación deben probarse y revisarse periódicamente y mantenerlos actualizados para su mejora continua y garantizar que sean efectivos.
- Para los procesos críticos de la Empresa, se debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad de los procesos, aún en caso de desastre en las instalaciones de los lugares de Operación.

- Cada lugar debe incluir los controles establecidos para este tipo de áreas según su clasificación, para que no se vea disminuida los aspectos de seguridad en caso de desastre.
- Se debe seguir una estrategia de recuperación alineada con los objetivos de la RAP, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos, ante el evento de una contingencia.

3.12 CUMPLIMIENTO

- LA RAP EJE CAFETERO, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros, la privacidad, los, delitos informáticos, el uso inadecuado de recursos de procesamiento, el uso de criptografía y la recolección de evidencia.
- Cumplimiento de la normatividad y los controles relacionados con la seguridad de la información y los que son técnicamente compatibles con los diferentes ambientes o tecnologías de la empresa.
- Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la Empresa deben contar con su respectiva licencia de uso.
- Realización de auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información.
- La Política junto con el Sistema de Gestión de Seguridad de la Información de la RAP EJE CAFETERO, debe ser auditado anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.
- La información de auditoría generada por el. Uso de los controles de seguridad de los Recursos de Tecnología, debe ser evaluada por el responsable para Detectar Violaciones a la Política.
- Reportar incidentes de seguridad. Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.
- Los contratos de trabajo y los contratos de desarrollo realizados por proveedores y contratistas deben contar con cláusulas respecto a la propiedad intelectual que le pertenece a LA RAP EJE CAFETERO.

3.13 NO REPUDIO

- Agregar registros que permite la trazabilidad en la modificación de cualquier dato o información en los sistemas de información.
- Toda información enviada por los medios institucionales debe ser responsabilidad de cada funcionario
- El Subproceso de gestión de TI provee estrategias de seguridad para el tratamiento de mensajes electrónicos 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".

4. POLITICA DE TRATAMIENTO DE DATOS

Política de tratamiento de datos personales en la RAP Región Administrativa y de Planificación del Eje Cafetero garantiza el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar, suprimir los datos o revocar la autorización otorgada que se hayan recogido sobre ellas en bases de datos o en cualquier otro medio aunado al cumplimiento que en la materia desarrolle la Ley.

4.1 IDENTIFICACIÓN DEL RESPONSABLE TRATAMIENTO DE LA INFORMACIÓN

La RAP Región Administrativa y de Planificación del Eje Cafetero, será responsable del tratamiento de los datos personales y los usará específicamente con la finalidad que se mencione a la hora de ser recolectada o con la finalidad que se encuentre facultado por el marco normativo vigente.

A continuación, se mencionan los datos del responsable del tratamiento:

Tabla 1 responsable tratamiento de datos

Tipo de Canal	Mecanismo	Ubicación	Horario de Atención
Presencial	Punto de atención al ciudadano	Cra 12 # 22-37 CDA Rodrigo Gómez Jaramillo Piso 2 Armenia, Quindio.	Lunes a Jueves de 7:30 a.m. a 12 m 1:30 p.m. a 6:00 p.m. Los viernes de 7:30 a.m. a 12 m 1:30 p.m. a 5:00 p.m.
Virtual	Correo institucional	contacto@ejecafeterorap.gov.co	24 horas
Virtual	Página web	https://ejecafeterorap.gov.co/	24 horas
Presencial / Virtual	Radicación de PQRSD	https://ejecafeterorap.gov.co/pqrs/	Lunes a Jueves de 7:30 a.m. a 12 m 1:30 p.m. a 6:00 p.m. Los viernes de 7:30 a.m. a 12 m 1:30 p.m. a 5:00 p.m. 24 horas de manera virtual
Virtual	Redes Sociales	https://www.facebook.com/RapEjeCafetero https://www.instagram.com/rapejecafetero/	24 horas
Presencial / Virtual	Formato de recolección de datos	Formato por definir	

5. FINALIDADES Y TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES

Los datos personales que la Región Administrativa y de Planificación del Eje Cafetero recolecte, almacene, use, circule y suprima, previa autorización del titular en los casos que se requiera serán utilizados para el desarrollo de las funciones propias de la administración pública y cualquier otro tipo de finalidad que se pretenda dar a los datos personales será informado previamente siempre dando cumplimiento al marco normativo vigente y demás normas que desarrollen la protección de los datos personales, así como para alguna de las siguientes finalidades:

- El Tratamiento de los datos se realizará con la finalidad de desarrollar actividades de la administración pública y funcionamiento de la Región Administrativa y de Planificación del Eje Cafetero.
- El Tratamiento de los datos se realizará con fines de desarrollar tareas de promoción de la entidad.

6. DERECHOS DE LOS TITULARES

- Conocer, actualizar y rectificar sus datos personales frente a la Región Administrativa y de Planificación del Eje Cafetero como Responsable y Encargado del Tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada a la Región Administrativa y de Planificación del Eje Cafetero como Responsable y Encargado del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

- Ser informado por la Región Administrativa y de Planificación del Eje Cafetero como Responsable del Tratamiento y Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a los datos personales del Titular.

- Presentar ante la Región Administrativa y de Planificación del Eje Cafetero quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

- Revocar la autorización y/o solicitar la supresión del dato personal cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Región Administrativa y de Planificación del Eje Cafetero haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

7. CASOS EN QUE NO SE REQUIERE LA AUTORIZACIÓN

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por la Región Administrativa y de Planificación del Eje Cafetero en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

8. DEFINICIONES

Tabla 2 Definiciones

Acceso a la información pública	Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados (Ley 1712 de 2014, art4)
Archivo	Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura (Ley 594 de 200, art 3)
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de datos Personales	Datos Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
Ciberseguridad	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas incidentes de naturaleza cibernética (CONPES3701)
Confindencialidad	Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizada
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo
Datos Personales Mixtos	Para efectos de este manual es la información que contiene datos personales públicos junto con datos privados o sensibles.
Datos Personales Privados	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Ley 1581 de 2012, art 3 literal h)
Datos Personales Públicos	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos entre otros, en registros públicos, documentos públicos gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
Datos Personales Sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las

	convicciones religiosas filosóficas, la pertenencia a sindicatos, organización sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
Datos Personales	Cualquier información vinculada o que pueda asociarse a una o varias Personas determinadas o determinables (Ley 1581 de 2012, art 3)
Derecho a la Intimidad	Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional)
Encargado del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).
Gestión de incidente de seguridad de la información	Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
Guía	Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guias son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
Información Pública Clasificada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
Información	Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
Ley de Habeas Data	Se refiere a la Ley Estatuaria 1266 de 2008.
Ley de Transparencia y Acceso a la Información Pública	Se refiere a la Ley Estatuaria 1712 de 2014.

Mecanismos de protección de datos personales	Lo constituye las distintas alternativas con que cuentan las entidades destinarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado.
Plan de continuidad del negocio	Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de evento imprevisto que las ponga en peligro (ISO/IEC 27000)
Política	Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
Privacidad	En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
Registro Nacional de Base de Datos	Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
Responsabilidad Demostrada	Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
Responsable del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que por si de misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000)
Seguridad de la información	Preservación confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad no-repudio y confiabilidad pueden estar involucradas
Sistema de Gestión de Seguridad de la Información SGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, politica, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000)
Titulares de la información	Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
Tratamiento de Datos Personales	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un

	individuo o entidad. (ISO/IEC 27000).
Usuario	Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

9. PROCEDIMIENTO PARA EJERCER LOS DERECHOS

Consultas

Se absolverán en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo.
Cuando no fuere posible responder la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su solicitud, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

Reclamos

Los Titulares que consideren que la información contenida en una base de datos de la Región Administrativa y de Planificación del Eje Cafetero debe ser objeto de corrección, actualización o supresión, o que adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante la misma, a través de cualquiera de los canales de atención descritos anteriormente; y éste deberá contener la siguiente información:

- Nombre e identificación del Titular
- La descripción precisa y completa de los hechos que dan lugar al reclamo
- La dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite
- Los documentos y demás pruebas que se pretendan hacer valer.

En caso de que la Región Administrativa y de Planificación del Eje Cafetero no sea competente para resolver el reclamo presentado ante la misma, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado. Si el reclamo resulta incompleto, la Región Administrativa y de Planificación del Eje Cafetero requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas.

Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el peticionario presente la información solicitada, se entenderá que ha desistido de aquél.

Una vez recibido el reclamo completo, la Región Administrativa y de Planificación del Eje Cafetero incluirá en la respectiva base de datos una leyenda que diga "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda se mantendrá hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles

contados a partir del día siguiente a la fecha de su recibo, y si no fuere posible

responder en dicho término, la Región Administrativa y de Planificación del Eje Cafetero informará al interesado los motivos de la demora y la fecha en que aquél se atenderá, sin llegar a superar, en ningún caso, los ocho (8) días hábiles siguientes al vencimiento del primer término.

10. FECHA DE ENTRADA EN VIGENCIA DE LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN

La presente política rige a partir de su expedición y publicación, las bases de datos sujetas a Tratamiento se mantendrán vigentes mientras ello resulte necesario para las finalidades establecidas en el punto 2 de la misma.

ELABORACIÓN	REVISION	APROBACION
Elaborado por: José Fernando Rodríguez Bernal	Revisado por: Luis Ernesto Salazar Jiménez	Aprobado por: Luis Ernesto Salazar Jiménez
Cargo: Contratista	Cargo: Subgerente Administrativo y Financiero	Cargo: Subgerente Administrativo y Financiero