Comisión de Regulación de Agua Potable y Saneamiento Básico

Manual de Políticas del Sistema Integrado de Gestión y Control (SIGC)

04 de noviembre de

2021

Este documento recoge todas las políticas del Sistema Integrado de Gestión y Control que han sido aprobadas en la entidad, las cuales, deberán ser cumplidas en todos los cargos y para servidores y contratistas que presten sus servicios al interior de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA.

La vivienda y el agua son de todos | Minvivienda

INTRODUCCIÓN

Las políticas de operación de la Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA, parten del reconocimiento del marco legal en el que se desarrolla la misión de la entidad. Los lineamientos de la función institucional están documentados a través de la definición de sus procesos, procedimientos, manuales, planes, guías e instructivos internos, por cuanto se describen allí las líneas de acción, objetivos, actividades y controles en cada uno de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.

Este documento resume las políticas como directrices generales para todos los niveles y cargos, las cuales, deben ser cumplidas por todos aquellos que realizan labores y actividades en la entidad.

CAPÍTULO I

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN Y CONTROL

La Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA está comprometida con la integración de todas las partes interesadas en el proceso de toma de decisiones regulatorias, a través de la prestación de un servicio calificado y oportuno orientado a satisfacer las necesidades de la ciudadanía y del sector. Para lograrlo, la CRA protege la seguridad, la salud y el bienestar de sus servidores y contratistas, identifica los peligros, evalúa y valora los riesgos aplicando los respectivos controles, gestionando la ciber-resiliencia, la seguridad y la privacidad de la información implementando acciones orientadas a la mejora continua de su Sistema Integrado de Gestión y Control en el marco de la normatividad aplicable. Lo anterior, de la mano de un equipo de trabajo comprometido y calificado.

CAPÍTULO II

POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información de la Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA, son una serie de lineamientos, reglas, instrucciones y prácticas que regulan y parten del reconocimiento del marco legal en el que se desarrolla la misión de la entidad.

Este documento presenta las políticas de seguridad de la información, donde se indica la forma en que se llevan a cabo determinados procesos, así como la manera de dirigir y proteger la información generada, modificada y administrada por la CRA. Estas políticas de seguridad han sido aprobadas por el Comité Institucional de Gestión y Desempeño. Los lineamientos de la función institucional están documentados a través de la definición de sus procesos, procedimientos, manuales, planes, guías e instructivos internos, por cuanto se describen allí las líneas de acción, objetivos, actividades y controles en cada uno de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.

1. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

Esta política se aplica a todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones y actividades requieren acceso a la información de la Entidad., igualmente describe las consideraciones generales sobre la protección y el control de acceso a la información de la CRA para evitar el acceso no autorizado a sistemas y/o servicios y hacer que los usuarios rindan cuentas por la administración y protección de su información y sus claves.

1.1. OBLIGACIONES

- El acceso a la información de la Entidad se otorga bajo los siguientes principios:
  - Solamente se concede acceso a la información que la persona o sistema necesitan para la realización de sus tareas (diferente tarea/rol significa diferentes cosas que necesita saber y en consecuencia diferente perfil de acceso).
  - Al cesar una función o rol se deben retirar los derechos de acceso a la información.
- La información debe ser usada para los fines de la Entidad y del ciudadano, su uso en beneficio propio o de un tercero no está autorizado.
- Los responsables de la información deben establecer, comunicar y revisar periódicamente las reglas de control de acceso y restricciones sobre la información que sean necesarias para prevenir la pérdida de confidencialidad, de integridad y/o la disponibilidad de la información a su cargo.
- El acceso a los sistemas de información de la CRA debe estar sujeto a controles que posibiliten -hasta donde sea factible- la trazabilidad de las acciones realizadas sobre los mismos, considerando la identificación de la persona, que realiza el acceso, las acciones realizadas, el instante de tiempo en el que se realizan las acciones y la ubicación desde la cual se realiza el acceso a la información.
- Al otorgar acceso a la información se debe dar una indicación clara al usuario sobre los requisitos de seguridad que debe cumplir para proteger apropiadamente la información.

- Al otorgar acceso a la información se debe indicar claramente al usuario el nivel de clasificación que tiene la información suministrada de acuerdo con el esquema de clasificación adoptado por la Entidad.

- Cuando se tiene acceso a la información de la CRA se está obligando a la aceptación formal de la reglamentación de acceso y tratamiento de la información que definan las leyes de Colombia, acuerdos internacionales suscritos por Colombia, normas del sector, políticas, estándares o cualquier tipo de control establecido para la protección o tratamiento de la información

- Todos los funcionarios, contratistas y terceros que presten sus servicios a la CRA deben aplicar todos los controles de seguridad definidos por la Entidad para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades o que por otras situaciones esté bajo su custodia.

- Periódicamente la CRA debe realizar evaluaciones de seguridad y pruebas para determinar la efectividad y pertinencia de los controles de acceso a la información definidos y adoptados.

- En los contratos suscritos con contratistas, proveedores o terceros que presten sus servicios a la CRA, se deben establecer y acordar los requisitos de seguridad que deben cumplir para poder tener acceso, procesar, almacenar, comunicar y transmitir información de la entidad. En estos acuerdos se deben incluir las medidas necesarias para el tratamiento de los riesgos de seguridad de la información derivados de las actividades realizadas por el contratista, el proveedor o tercero. Los acuerdos deben ser formalizados antes del inicio de las actividades contractuales.

- En cuanto al uso y acceso a la información y sistemas de información de la entidad se consideran usos no autorizados:

  - Modificación de la información sin contar con la autorización formal para dichas modificaciones.
  - Divulgación no autorizada de información.
  - Impedir el acceso a la información sin justificación real.
  - Modificación y/o eliminación de los controles de seguridad que protejan la información.
  - Cualquier acción sobre la información considerada como ilegal o no autorizada por las leyes, regulaciones, normas o procedimientos a los que está sometida la CRA.

- Se debe seguir el proceso formal de registro y cancelación de usuarios, para poder asignar los derechos de acceso a la información y servicios de la entidad.

- Se deben establecer los roles de acceso de usuarios con base en los requisitos de la entidad identificando claramente derechos de acceso.

- Los derechos de acceso a la información y a los activos asociados se deben retirar antes de que el empleo termine o cambie, dependiendo de la evaluación de factores de riesgo.

- El oficial de seguridad, el administrador o administradores de acceso y/o el responsable del área o proceso deben verificar periódicamente los accesos, con el fin de validar la autenticidad de los usuarios con acceso activo a la información.

- La asignación de contraseñas se realiza de forma controlada mediante el procedimiento para el registro y cancelación de usuarios definido por el sistema de gestión de seguridad de la información.

- Los jefes de área y el proceso de Gestión de talento humano son los únicos autorizados para tramitar ante la mesa de ayuda la asignación de cuenta de usuario y contraseña para los empleados, contratistas y terceros que presten sus servicios a la CRA.

- Cualquier servicio, sistema de información o equipo informático que tenga contraseñas por defecto configuradas por el proveedor o fabricante, deben ser cambiadas por nuevas contraseñas cuando se realice el proceso de configuración del servicio, sistema o equipo. Al momento de poner en producción el servicio, sistema o equipo se debe volver a cambiar la contraseña por una nueva.

- La contraseña asignada a un usuario es personal e intransferible. Los usuarios no deben divulgar, prestar, exhibir, comunicar en forma escrita o verbal su contraseña. Cuando por labores de soporte o mantenimiento se requiere la contraseña de usuario, el usuario es quién debe digitarla y al final de las actividades de soporte se debe cambiar por una contraseña nueva.

- Los usuarios deben cambiar mínimo una vez cada mes (1) mes sus contraseñas de acceso a servicios, sistemas de información o equipos informáticos.

- Los administradores de servicios, sistemas de información, equipos informáticos deben cambiar sus contraseñas una (1) vez al mes.

- Los administradores de servicios, sistemas de información y equipos informáticos deben utilizar contraseñas diferentes para sus cuentas de usuario y para sus cuentas como administradores.

- Los usuarios son responsables de todas las acciones que se realicen con sus contraseñas. En caso de que la contraseña haya sido conocida por terceros, el usuario debe informar inmediatamente al responsable del proceso o del área para bloquear cualquier acceso a servicio, sistema de información o equipo informático que utilice la contraseña comprometida.

- El oficial de seguridad podrá verificar el cumplimiento de estas directrices a través de diversos métodos incluyendo recorridos esporádicos, videos de vigilancia, auditorías internas y externas, y la retroalimentación de los funcionarios, contratistas o terceros.

2. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Esta política describe las consideraciones generales para asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información de la CRA. Igualmente describe las consideraciones sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida y aplica para todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones requieren uso de alguna técnica de protección de información mediante controles criptográficos o llaves criptográficas en la Entidad.

2.1. OBLIGACIONES

El uso de controles criptográficos en la CRA se basa en las siguientes directrices:

- [1] 1 Los controles criptográficos están enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, se impone establecer un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad ‘ https://normaiso27001.es/a10-criptografia/

- La información de la Entidad que por su naturaleza de pública clasificada o pública reservada pueda generar daño a los intereses públicos o a los derechos de personas naturales o jurídicas debe permanecer protegida mediante controles de criptografía.

- La información reservada y la información clasificada de la Entidad que deba ser transportada por líneas de comunicación, dispositivos móviles o sistemas de almacenamiento removible debe ser cifrada antes de su transporte o almacenamiento.

- En el intercambio de información con terceros que exijan uso de controles criptográficos se dará prioridad al mecanismo más fuerte entre el propuesto por el tercero y el adoptado por la Entidad.

- En los casos en los que la ley lo exija la Entidad hará uso de certificados de firma digital emitidos por entidades de certificación autorizadas.

- El acceso y uso de controles de criptografía se autoriza bajo las directrices de la política de control de acceso a la información.

- Las llaves criptográficas son generadas por la Oficina Asesora de Planeación y TIC's.

- Al realizar el cifrado de información, se debe mantener copia de las llaves de cifrado en la oficina asesora de planeación y TIC's de forma que la recuperación de la información cifrada sea factible en caso de ausencia temporal o permanente del responsable de la información cifrada.

- Para la recuperación de una llave criptográfica se debe seguir el GTI-INS01 Instructivo solicitud soporte aplicativo HelpDesk de la Oficina Asesora de Planeación y TIC's.

- Las llaves criptográficas únicamente son suministradas presencialmente al solicitante y no se trasmiten por canales de comunicación inseguros como correo electrónico, mensajes de texto, sistemas mensajería instantánea o líneas telefónicas. Toda llave que haya sido comprometida mediante divulgación no autorizada o se sospeche comprometida debe ser reemplazada sin demora injustificada.

- Las copias de respaldo de los sistemas de información que requieran almacenamiento fuera de las instalaciones de la Entidad deben permanecer cifrados.

- Toda llave de cifrado utilizada en entornos de pruebas y desarrollo no debe ser instalada en entornos de producción.

- Por su nivel de seguridad y ser un algoritmo abierto se dará preferencia al uso del algoritmo SHA-3, siendo válido igualmente el uso del algoritmo SHA-2.

- En el caso de requerirse funciones HASH para generar resúmenes de archivos se adoptará el algoritmo SHA-2 en sus versiones de 224, 256, 384 o 512 bits.

2.2. RESTRICCIONES

Respecto al uso de controles de criptografía no está autorizado:

- Cifrar información sin la autorización del responsable de la información.
- Cifrar información de datos abiertos.
- Divulgar claves, contraseñas o llaves de cifrado de datos a personal no autorizado.
- El uso del token de autenticación en sistemas bancarios o sistemas de información del estado es personal e intransferible.

- Utilizar software de cifrado de datos que no esté autorizado por el sistema de gestión de seguridad de la información de la CRA.

3. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Esta política describe las consideraciones generales para mantener la seguridad de la información transferida dentro de las instalaciones de la CRA, entre sus diferentes dependencias o entre funcionarios y entre la Entidad y cualquier otra entidad externa. Se aplica a funcionarios, contratistas y terceras partes interesadas en tener acceso a la información de la CRA.

3.1. OBLIGACIONES

- Al transferir información a partes externas de la CRA se debe contar con la autorización del jefe responsable de la información a transferir.

- Al transferir información clasificada como reservada o pública a partes externas , se deben aplicar controles criptográficos para su protección durante la transmisión.

- Al recibir información transferida por terceros o dentro de la misma entidad se deben aplicar controles de software que permitan detectar la presencia de códigos maliciosos en la información transferida.

- La transferencia de información debe cumplir con la política de acceso a la información de la CRA.

- Las transferencias de información que usen los recursos tecnológicos de la Entidad deben tener como fin el cumplimiento de las obligaciones misionales de la CRA.

- El uso de los recursos de tecnología de información y comunicaciones de la Entidad para fines contrarios a la legislación colombiana, los tratados internacionales suscritos por Colombia y las funciones asignadas al funcionario, contratista o tercero que preste sus servicios al CRA se tratarán como incidentes de seguridad de la información y se debe reportar a las instancias competentes y al oficial de la seguridad de la información de la Entidad.

- Para propósitos de seguimiento y control a potenciales eventos e incidentes de seguridad de la información, la CRA puede inspeccionar las transferencias de información que se realicen desde o hacia su infraestructura de tecnología de información y comunicaciones.

- Las transferencias de información asociadas con actuaciones legales de la Entidad deben solicitar acuse de recibo del destinatario. La respuesta del acuse de recibo de la transferencia de información se debe preservar en condiciones que garanticen su disponibilidad e integridad cuando sea requerida su consulta.

- Los responsables de procesos y actos oficiales de la CRA pueden establecer mecanismos de control para garantizar la trazabilidad y no repudio de las transferencias de información realizadas desde o hacia la Entidad.

- Las transferencias de información enmarcadas por contratos o acuerdos de intercambio de información deben contar con acuerdos de confidencialidad y uso de información.

- La transferencia de información de carácter personal deberá observar los procedimientos descritos en el Art. 25 de la Ley 1581 de 2012 y el Decreto 1377 de 2013.

- Para el intercambio de información entre entidades para el cumplimiento de funciones públicas, la Entidad debe establecer mecanismos tecnológicos para integrar, compartir o suministrar la información que por mandato legal se requiere, o permitir el acceso total dentro del marco de la Constitución y el derecho fundamental a la intimidad, a las bases de datos completas que requieran otras Entidades para el ejercicio de sus funciones según lo dispuesto en el Decreto 235 de 2010 del Ministerio del Interior y de justicia.

- La información clasificada como reservada o pública clasificada que deba ser transferida a un tercero, debe ser protegida mediante controles de criptografía. El uso de controles de criptografía debe seguir la política de controles criptográficos de la CRA.

- Al transferir información reservada o pública clasificada empleando servicios de correo electrónico se deben cifrar los adjuntos que contienen la información y las claves para el descifrado de la información deben ser comunicadas por un medio diferente al correo electrónico.

- Cualquier información recibida a manera de transferencia de datos debe ser verificada por software de detección de código malicioso para prevenir incidentes de seguridad de la información dentro de la CRA. Todo adjunto recibido por correo electrónico debe ser verificado para detectar la presencia de software malicioso.

- Los mensajes de correo electrónico que implican comunicaciones oficiales de la Entidad se deben almacenar por el tiempo que determine la Ley, la Oficina Asesora de Planeación y TIC´s determina los mecanismos técnicos para que los usuarios puedan almacenar dichas comunicaciones en forma segura.

- El uso de firmas digitales y certificados electrónicos son mecanismos que protegen la autenticidad e integridad de las transferencias de información, la Oficina Asesora de Planeación y TIC´s determina los mecanismos técnicos que permitirán el uso de esos controles tecnológicos, para cuando este aplique.

- La información de copias de respaldo de los sistemas de información y copias de respaldo de la información de los funcionarios y contratistas de la Entidad que deba ser transferida fuera de la Entidad por medio físico o electrónico, debe ser protegida contra interceptación, modificación o divulgación usando los controles criptográficos definidos por la Entidad.

- Cuando se apruebe el intercambio de información con un tercero, se debe suscribir previamente acuerdo de confidencialidad en el cual se deben señalar los términos y condiciones para la entrega de la información requerida y las medidas de seguridad que exigirá la Entidad para su protección una vez sea entregada.

- La información, datos o documentos entregados por la CRA a entidades con las que se encuentre en un convenio establecido, o terceras partes no se podrá comercializar, ni prestar, ni copiar, ni compartir, ni reproducir, ni arrendar, ni enajenar, ni prestar servicios a terceros no autorizados, sin que se cuente previamente con una autorización formal escrita emitida por un funcionario debidamente autorizado por la CRA y sólo podrá ser copiada, compartida, reproducida o utilizada exclusivamente para realizar las actividades que sean expresamente autorizadas por la CRA al momento de la entrega de la información.

- Los documentos o Información transferida por la CRA se utilizarán exclusivamente para las actividades propias del acuerdo que se establezca en el convenio con otra entidad o tercero. En el caso que este objeto genere algún tipo de documento o publicación estos deberán contener la atribución de derechos de propiedad de CRA indicando que la nueva información generada

"incluye información de propiedad de la Comisión de Regulación de Agua Potable y Saneamiento Básico y se utiliza bajo su autorización".

- La información de la Entidad debe ser empleada para servir a una finalidad operativa y administrativa. Cualquier Transferencia de Información de la CRA es susceptible de ser auditada para propósitos de control interno, control de calidad o investigación de incidentes de seguridad de la información, en consecuencia, el usuario reconoce y acepta que la información institucional que sea objeto de intercambio puede ser analizada siguiendo los procedimientos administrativos a los que está sujeta la CRA, en todo momento se preservará el Derecho a la Intimidad de las personas.

- Los funcionarios, contratistas o terceros que reciban información de la CRA se deben comprometer a proteger dicha información, sin importar su nivel de clasificación para evitar su divulgación no autorizada, aplicando los procedimientos administrativos, técnicos o definidos por la CRA.

- Los contratistas, o terceros que reciban información de la CRA deben informar a cada uno de sus empleados o colaboradores sobre el nivel de clasificación de la información recibida y de la existencia de acuerdos de confidencialidad con la Entidad. Igualmente, el contratista o tercero debe instruir a quién reciba la información o documentos, acerca de las medidas de protección y mecanismos para manejar la información y la obligatoriedad de no utilizarla sino para los temas necesarios para el desarrollo del acuerdo suscrito entre la CRA y el contratista o tercero quién será enteramente responsable por cualquier uso inadecuado de la información suministrada por la Entidad.

- Cualquier excepción a la política de transferencia de información debe ser aprobada previamente por el oficial de Seguridad o por el Comité Institucional de Gestión y Desempeño de la Entidad, tanto su justificación como aprobación debe ser motivada; ninguna de estas excepciones podrá vulnerar la reserva, salvo las excepciones consagradas en la ley.

3.2. RESTRICCIONES

Respecto a la transferencia de información con terceros no está autorizado:

- Transferir información de carácter personal sin el cumplimiento de los requisitos de la ley de protección de datos personales (contrato/acuerdo de transferencia de información, autorización del titular).
- Transferir información pública reservada o secreta de privados, sin la autorización del responsable del proceso en la CRA.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN CON PROVEEDORES Y CONTRATISTAS

Está política aplica a proveedores de servicios de la CRA y a los contratistas, y busca preservar los niveles de seguridad y privacidad de los activos de información de la CRA cuando se autorice el acceso o administración por parte de proveedores de servicios o contratos de prestación de servicios.

4.1. OBLIGACIONES

- Los proveedores que deban tener acceso a la información y sistemas de información de la CRA deben aceptar y cumplir las políticas, directrices y controles de seguridad de la información de la Entidad.

- Los proveedores y/o contratistas que presten sus servicios a la CRA para la ejecución de sus actividades se comprometen a mantener en su equipo un antivirus y a mantener las actualizaciones de su sistema operativo con el fin de mitigar alguna amenaza informática, y así garantizar la integridad, confidencialidad e integrada de la información

- La autorización de acceso a la información de la Entidad para un proveedor debe realizarse cumpliendo la política de acceso a la información.

- Todos los proveedores deben suscribir acuerdo de confidencialidad y no divulgación de la información de la Entidad al momento de iniciar las labores contratadas.

- De acuerdo con el tipo de servicio que el proveedor prestará a la Entidad se debe determinar el tipo de información, sistemas de información y áreas físicas de la Entidad a la que se le otorgará acceso.

- Los proveedores deben aceptar y cumplir las leyes y acuerdos suscritos por Colombia en materia de protección de información personal, derechos de autor y propiedad intelectual. El responsable del contrato debe definir mecanismos administrativos para verificar el cumplimiento de estas obligaciones legales.

- Al finalizar sus contratos los proveedores que presten sus servicios a la CRA deben efectuar la devolución de la información o activos de información propiedad de la Entidad que estuvieron bajo su responsabilidad y procurar la destrucción o borrado seguro de las copias de la información reservada o publica clasificada que aún este bajo su control.

- Cuando se requiera realizar transferencias de información de la CRA con proveedores se debe cumplir con la política de transferencia de información.

- Los responsables de los contratos deben identificar y tratar los riesgos de seguridad de la información asociados a la autorización de acceso de la información e infraestructura de la CRA.

- Los responsables de los contratos con proveedores, de acuerdo con el tipo de actividad que desarrollará el proveedor y los resultados de los análisis de riesgos, deben determinar los controles de seguridad sobre el acceso a la información y recursos de la entidad.

- Los requisitos de seguridad de la información para la ejecución de actividades por parte de los proveedores deben ser documentados por el responsable del contrato en la CRA antes del inicio de las actividades del proveedor.

- Los proveedores deben cumplir con el procedimiento de gestión de incidentes de seguridad de la información de la Entidad.

- Los proveedores deben cumplir con el procedimiento de gestión de cambios definido por la Entidad.

- Los proveedores que presten sus servicios a la CRA deben aceptar y cumplir las directrices de asociadas a la política de seguridad para relaciones con proveedores.

- Para el desarrollo de las actividades a cargo del proveedor se debe contemplar un ciclo de vida de prestación de servicio que considere como mínimo: inicio de actividades, planificación de la prestación del servicio, definición de controles específicos de seguridad, seguimiento al cumplimiento de controles de seguridad, cierre de las actividades y entrega de información suministrada.

- Los supervisores de los contratos deben mantener un inventario de la información que se suministra a los proveedores.

- Se debe comunicar al proveedor el esquema de clasificación de información definido por la CRA, en caso de diferencias entre los esquemas de clasificación de información de la entidad y del proveedor primará el nivel de clasificación de la CRA.

- El proveedor debe aceptar la implementación de controles de seguridad razonables que protejan la información de la CRA que quede bajo su responsabilidad. El proveedor debe aceptar el derecho de la CRA de realizar seguimiento, revisión y evaluación de la efectividad de las medidas de seguridad acordadas para proteger la información de la Entidad.

- Se debe solicitar al proveedor que periódicamente, de acuerdo con la duración del contrato, remita un informe del estado de los controles de seguridad implementados para preservar la seguridad de la información de la Entidad.

- Los supervisores de contrato deben comunicar a los proveedores las reglas de uso aceptable y las prohibiciones sobre el uso de información de la Entidad para fines diferente al cumplimiento del contrato.

- Los proveedores deben informar a los supervisores de contrato una lista explicita de las personas que tendrán acceso a la información de la Entidad.

- El proveedor debe designar una persona de contacto responsable de atender los aspectos relacionados con la seguridad de la información del servicio que se prestará.

- El proveedor debe informar a la Entidad sobre los mecanismos de seguridad que aplicará para la selección del personal involucrado en el servicio, así como los aspectos relacionados con la comunicación de sus obligaciones sobre seguridad de la información, toma de conciencia y mecanismos de retiro de derechos de acceso a la información de la Entidad.

- Los equipos y software que utilice el proveedor para el desarrollo de sus actividades, deben cumplir con los requisitos del sistema de gestión de seguridad de la información de la Entidad, incluidos, derechos de autor, controles contra código malicioso, control de acceso y los demás controles acordados con la Entidad.

- Los proveedores a cargo de actividades que involucran cambios en la configuración de los equipos de tecnología de información y comunicaciones de la Entidad, deben asegurar mediante los procedimientos de control de cambios, la correcta instalación y pruebas que aseguren el buen funcionamiento y la protección de la seguridad de la información de los activos de información de la Entidad.

- El proveedor no está autorizado a usar los recursos de información y tecnología y la información de la Entidad para fines diferentes a los especificados en los contratos suscritos con la Entidad.

- El uso de las redes de telecomunicaciones de la Entidad, solo está autorizado para el cumplimiento del objeto contractual suscrito, no está autorizado el uso de las redes de la Entidad para descargas de material protegido por derechos de autor (música, video, software, libros).

- El proveedor no está autorizado a conectar, desconectar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización del supervisor del contrato

- El proveedor no está autorizado a instalar o ejecutar programas que perjudiquen la estabilidad de los equipos, su sistema operativo o sus programas internos o aplicaciones de la Entidad. Esto incluye los programas conocidos como virus informáticos, cualquier tipo de ensayo o experimento, hardware, software o cualquier software considerado como malicioso.

4.2. RESTRICCIONES

Respecto al control de acceso a la información por parte de proveedores, se consideran usos no autorizados:

- Otorgar permiso de acceso a información que no es necesaria para el cumplimiento de las obligaciones del proveedor.
- Otorgar acceso la información a proveedores que no tengan vigente relación contractual y compromiso de confidencialidad.

5. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Esta política establece los lineamientos generales para reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo durante o fuera de las horas laborales de la Entidad. Aplica a funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones deban tener acceso a estaciones de trabajo o puestos de trabajo dentro de las instalaciones de la CRA.

5.1. OBLIGACIONES

- Todos los funcionarios, contratistas y terceros que presten sus servicios a la CRA deben aplicar los controles recomendados por el sistema de gestión de seguridad de la información para impedir el acceso no autorizado de terceros a la información de la Entidad.

- Los lugares de trabajo de funcionarios, contratistas y terceros que prestan sus servicios a la Entidad y cuyas funciones no obliguen a la atención directa de ciudadanos deben localizarse preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados a acceso no autorizado a la información o a los equipos informáticos.

- Durante las ausencias temporales o definitivas el personal de la CRA debe bloquear la pantalla de los computadores a su cargo, para impedir el acceso de terceros no autorizados a la información almacenada en el computador o visible en pantalla.

- Durante ausencias temporales o definitivas el personal de CRA debe guardar en un lugar seguro los documentos físicos o medios de almacenamiento para impedir su pérdida, daño o acceso por parte de personal no autorizado.

- Los documentos impresos y los archivos electrónicos clasificados con carácter reservado o público clasificado siempre deben permanecer custodiados o protegidos en áreas seguras para evitar su divulgación no autorizada.

- Cuando esté autorizada la impresión o reproducción de documentos clasificados con carácter reservado o público clasificado, se deben retirar inmediatamente de los dispositivos empleados para su impresión o reproducción.

- En todos los computadores y cuando sea factible en equipos de impresión o reproducción se debe tener configurada una cuenta con privilegios de administrador que permita realizar labores de instalación, configuración, soporte y mantenimiento; el uso de dicha cuenta es de responsabilidad exclusiva del personal que presta los servicios de soporte tecnológico.

- Para el acceso a cualquier computador de la Entidad, se debe hacer uso de una cuenta y una contraseña que serán únicos, exclusivos, personales e intransferibles para cada usuario de la Entidad.

- Todos los computadores de la CRA deben tener configurado y operativo un protector de pantalla que se active cuando el equipo no esté en uso y bloquee el acceso con contraseña al equipo cuando no esté en uso por parte del funcionario, contratista o tercero que presten sus servicios a la Entidad.

- Los funcionarios o contratistas deben asegurar que toda la información en formato impreso o electrónico esté segura en su área de trabajo al finalizar el día y cuando se encuentre fuera de su puesto de trabajo durante un período prolongado.

- Las estaciones de trabajo deben apagarse completamente al final de la jornada de trabajo, con la excepción para los casos en los que se haga uso de la VPN, para lo cual la estación de trabajo deberá permanecer encendida, bloqueada y con la pantalla apagada.

- Cualquier información reservada o pública confidencial debe ser retirada del escritorio o mesa de trabajo y guardada bajo llave quedando desocupada al final de la jornada de trabajo.

- Los gabinetes de archivo que contienen información reservada o pública clasificada deben mantenerse cerrados y bloqueados cuando no se encuentren en uso o en horarios no laborales.

- Las llaves o tarjetas que permitan el acceso a la información reservada o pública clasificada deben llevarse consigo o guardadas con las debidas medidas de seguridad y nunca deben ser prestadas a personal no autorizado.

- Las computadoras portátiles deben estar guardadas bajo llave o aseguradas con un cable de seguridad o guaya fuera del horario de trabajo o cuando deban quedar desatendidas.

- Las impresiones desechadas con información reservada o pública confidencial deben ser destruidas con el uso de destructoras de papel.

- Las impresiones que contienen información reservada o pública clasificada no se deben dejar como papel reciclable disponible en lugares de libre acceso.

- La información reservada o pública clasificada que haya sido consignada en los tableros de las salas de juntas o de las oficinas durante el desarrollo de reuniones, deberá ser borrada al término de las mismas.

- Los dispositivos de almacenamiento masivo, como CD-ROM, DVD o unidades USB con información reservada o pública clasificada deben quedar desconectadas y se deben guardar en lugar seguro.

5.2. RESTRICCIONES

Respecto al control de acceso a las estaciones de trabajo y documentos en escritorios, no se debe:

- Dejar sin bloqueo la sesión de trabajo cuando esté ausente el responsable del equipo.
- Mantener en el puesto de trabajo documentos con información pública clasificada o pública reservada que no estén en uso.
- Dejar al alcance de los visitantes información pública reservada o pública clasificada en áreas de atención al público.

6. POLÍTICA DE RESPALDO DE INFORMACIÓN

Esta política cubre a funcionarios, contratistas y terceros que por la naturaleza de sus funciones deban realizar copias de respaldo de la información institucional y define los lineamientos para la generación, administración, retención y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información de la CRA.

6.1. OBLIGACIONES

- La información de los diferentes procesos, procedimientos y actividades que forman parte de las funciones de la Entidad se respaldará de acuerdo con requisitos legales, nivel de clasificación, períodos de retención documental y requerimientos de uso que permitan la recuperación de las funciones de la Entidad en caso de pérdida de los originales.

- Las copias de respaldo de la información deben ser preservadas por el tiempo previamente establecido en las tablas de retención documental, resguardando su acceso de acuerdo con su nivel de clasificación y la disposición final definida en las tablas de retención documental.

- Toda información que soporte procesos, procedimientos o actividades definidas en el Sistema de Integrado de Gestión y Control (SIGC) de la CRA debe tener una definición documentada formalmente, que debe ser aprobada por el responsable del proceso que incluya mínimo: información a respaldar, periodicidad del respaldo, nivel de clasificación de la información, período de retención de las copias de respaldo, ubicación del original de la información a respaldar.

- El respaldo de la información almacenada en computadores personales, dispositivos móviles u otros medios de procesamiento de información diferentes a la infraestructura tecnológica que soporta los sistemas de información de la CRA debe ser solicitado formal y expresamente utilizando los procedimientos de soporte a usuario adoptados por la CRA. Los responsables de la realización de las copias de respaldo evaluarán con el solicitante, la estrategia que mejor se ajuste a la solicitud considerando mínimo: requisitos de negocio, clasificación de la información, necesidades de recuperación y medios tecnológicos disponibles.

- Todos los sistemas de información que soportan procesos, procedimientos o actividades definidas en el Sistema de Integrado de Gestión y Control de la CRA deben contar con las herramientas tecnológicas apropiadas que garanticen la realización de las copias de respaldo de acuerdo con los requerimientos de uso de la información, niveles acceso autorizados y períodos de retención definidos por el responsable de la información.

- Los períodos de retención de la información respaldada se deben definir de acuerdo con los requisitos legales, objetivos de los procesos dueños de la información y niveles de riesgo identificados por los procesos de gestión de riesgo de la CRA.

- Los procedimientos específicos para la realización de las copias de respaldo deben establecer los mecanismos que permitan mantener y realizar trazabilidad de la ejecución de la copia de respaldo, su resultado, responsables, medios usados, información respaldada y trazabilidad de las acciones realizadas durante la ejecución de la copia de respaldo o su restauración.

- Las copias de respaldo se almacenarán en sitios seguros con controles físicos y tecnológicos que permitan el cumplimiento de los estándares mínimos necesarios para preservar las copias durante los períodos definidos, limitar su acceso a los debidamente autorizados y garantizar su disponibilidad cuando el responsable de la información los requiera.

- Cuando se realicen copias de respaldo de información clasificada como reservada o publica clasificada, se deben cifrar siguiendo la política de cifrado de información adoptada por la CRA.

- Cuando se requiera la ejecución de respaldos que no estén considerados en la estrategia definida, los responsables de los procesos tramitarán su ejecución mediante los procedimientos de gestión de cambios definidos por la CRA. La ejecución de copias de respaldo de computadores personales se debe solicitar explícitamente y su aprobación dependerá de la disponibilidad de recursos tecnológicos.

- Las copias de respaldo se deben someter a pruebas periódicamente para certificar que cumplen con los propósitos para las cuales fueron realizadas. Los resultados se deben usar para actualizar los procedimientos de respaldo, recursos tecnológicos necesarios, evidenciar oportunidades de mejora o riesgos en la realización de copias de respaldo y restauración de información. El responsable de la información debe participar en las pruebas para certificar formalmente, que las estrategias de respaldo y restauración se ajustan a las necesidades de sus procesos.

- Cuando los requisitos legales, requisitos de retención o condiciones de los medios de respaldo de información así lo dictaminen, se debe proceder a la destrucción o disposición final del medio, garantizando que la información contenida en los mismos ya no será accesible. Cuando se requiera destrucción de medios se deben seguir los procedimientos aprobados por el sistema de integrado de gestión de la CRA para la preservación del medio ambiente.

6.2. RESTRICCIONES

No está autorizado y no es responsabilidad de la Entidad, crear copias de seguridad a información que esté tipificada como personal, como lo es música, videos, imágenes, software y, en general, toda información que no esté clasificada como institucional y que no impida el ejercicio las funciones y responsabilidades.

7. POLÍTICA DE DESARROLLO SEGURO

Cuando la Comisión de Regulación de Agua Potable y Saneamiento Básico desarrolle software o contrate el desarrollo de software con proveedores, deberá considerar los siguientes lineamientos generales para el desarrollo, mantenimiento y adquisición de software, con el fin de adoptar los controles de seguridad en el desarrollo del software:

7.1. OBLIGACIONES

- Es obligatorio adoptar prácticas y controles de seguridad de la información en todos los proyectos de desarrollo de software y sistemas de información que adelante la Entidad, así como en las actividades de creación de servicios o arquitecturas de tecnologías de información y comunicaciones de la Entidad.

- El desarrollo de software debe realizarse en un ambiente seguro, diferente y aislado de los ambientes de producción de la Entidad.

- El desarrollo de software debe cumplir con la metodología de desarrollo seguro definida por la Oficina Asesora de Planeación y TIC´s de la Entidad.

- El desarrollo de software debe cumplir con directrices de codificación segura de acuerdo con el lenguaje de programación seleccionado para el desarrollo del software.
- Durante la fase de diseño del software o el sistema de información se deben considerar los requisitos de seguridad de la información.
- El software en desarrollo debe permanecer protegido de acceso o modificación no autorizada.
- El desarrollo de software contratado externamente debe cumplir con las políticas de desarrollo seguro de la Entidad.
- El software destinado a transmitir información por redes de la Entidad o por redes externas a la infraestructura de tecnología de la Entidad debe cumplir con la política de transferencia de información.
- El software que contemple transacciones electrónicas comerciales debe contemplar controles que eviten pérdida de confidencialidad e integridad.
- Los cambios en el software deben cumplir el procedimiento de control de cambios definido por la Oficina Asesora de Planeación y TIC´s de la Entidad.
- El desarrollo del software debe contemplar las actividades de análisis y gestión de riesgos de seguridad de la metodología de riesgos adoptada por la Entidad.
- Los requisitos de seguridad de la información para el software deben ser formalmente documentados y aprobados por parte de los interesados en el software.
- Los requisitos de seguridad deben considerar las situaciones de potencial abuso del sistema de forma que se implementen controles para evitar el abuso del mismo.
- Durante la fase de análisis de requerimientos, se deberá identificar los riesgos correspondientes a seguridad de la información.
- El diseño del sistema debe considerar revisión independiente del mismo.
- El software debe considerar controles que eviten pérdida de confidencialidad durante la transferencia de información.
- Dentro de los controles de seguridad a implementar en el software se debe considerar:

  - Control de acceso a la información
  - Validación de datos de entrada
  - Definición y autenticación de usuarios
  - Mecanismos de detección de intrusos
  - Definición de mecanismos de cifrado de datos
  - Auditoría de las acciones realizadas por el usuario con el software
  - Autenticación centralizada
  - Mecanismos de autorización de acuerdo al rol y privilegio de usuario
  - Separación de las instrucciones de control y datos

- El código fuente del sistema debe ser sometido a pruebas de análisis de vulnerabilidades con herramientas de análisis de código.

- El código ejecutable de los sistemas se debe someter a pruebas de análisis de vulnerabilidades y penetración, como marcos de referencia reconocidos como OWASP o OSSTM.

- Los sistemas de información deben ser probados cuando se realicen cambios en el sistema operacional en los que se ejecutan.

8. POLÍTICA DE USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN

Esta política cubre a funcionarios, contratistas, terceras partes y todos los activos de información de la Entidad y define las pautas para realizar un uso seguro y aceptable de los activos de información de la CRA, incluyendo sus sistemas de información, estaciones de trabajo, áreas de almacenamiento de información (física o electrónica), medios de almacenamiento de información (física o electrónica), entre otros.

8.1. OBLIGACIONES

8.1.1. SOBRE EL MANEJO DE LA INFORMACIÓN Y SUS ACTIVOS ASOCIADOS

- Toda persona, proceso o sistema de información que realice actividades para CRA debe tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas, de conformidad con el principio de “necesidad de conocer para para realizar la actividad”.

- Todo acceso a la información debe cumplir con los requisitos legales, normativos, reglamentarios, procedimentales o de cualquier otra índole que haya definido el responsable de la información.

- Todo acceso a la información debe ser autorizado formalmente por el área responsable de la información. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.

- Todo acceso a la información debe considerar el nivel de clasificación definido por el responsable de la información, según el procedimiento de clasificación de la información de la CRA.

- La información es uno de los activos más valiosos de la CRA, es por esa razón que todos los funcionarios y contratistas que prestan sus servicios a la Entidad se deben comprometer a realizar sus mejores esfuerzos para aplicar todos los controles de seguridad de la información definidos por el sistema de gestión de seguridad de la información de CRA, para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades.

- Todas las actividades de administración, operación y uso de la información y de sus activos asociados deben estar orientadas a garantizar la prestación de los servicios necesarios para el cumplimiento de la misión de la Entidad, los usos diferentes deben ser formalmente autorizados, tal y como lo establece la Ley 734 de 2002, por la cual se expide el Código Disciplinario Único. “Artículo 34, Deberes. Numeral 4: Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.”

- Todos los funcionarios y contratistas de la CRA deben reportar sin demoras injustificadas a los responsables de sus áreas, a los responsables de los procesos o al oficial de seguridad de la información cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información de la Entidad.

- Los responsables de proceso y áreas de la Entidad deben generar y conservar un registro detallado de todos los eventos que sucedan sobre los diferentes activos de información su cargo, los eventos se registran en la herramienta de mesa de ayuda GLPI.

- Todos los funcionarios y contratistas de la CRA deben aplicar el procedimiento institucional de gestión de riesgos para identificar y tratar los riesgos que puedan afectar a sus activos de información. Cada responsable de proceso o área debe coordinar la aplicación del procedimiento institucional de gestión de riesgos sobre los activos a su cargo.

- Las modificaciones a los activos de la Entidad, deben cumplir con los procedimientos para la gestión del cambio definidos por el sistema de gestión de seguridad de la información.

- Todos los funcionarios de la CRA deben aplicar los controles de seguridad de la Información definidos el sistema de gestión de seguridad de la información para reducir los riesgos que afectan a la seguridad de la información.

- Todos los funcionarios de la CRA se comprometen a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está sometida la Entidad para la protección de la información a su cargo.

8.2. RESTRICCIONES

- Modificaciones a la información sin contar con la autorización formal para realizarlas..
- Divulgación no autorizada de información.
- Impedir el acceso a la información sin justificación real.
- Modificación o eliminación de los controles de seguridad que protejan la información.
- Cualquier acción sobre la información considerada como ilegal o no autorizada por las leyes, regulaciones, normas o procedimientos a los que está sometida la Entidad.
- Utilizar la información de la Entidad para fines personales o diferentes a los requeridos para el cumplimiento de las funciones asignadas o el cumplimiento de las funciones de la Entidad.

8.3. SOBRE EL USO DEL CORREO ELECTRÓNICO

- El servicio de correo electrónico institucional debe ser utilizado primordialmente para las tareas propias de la función desarrollada por la Entidad los usos diferentes a los necesarios para el cumplimiento de las funciones encargadas al funcionario, contratista o tercero y son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio. Por lo anterior el uso con fines personales del correo institucional es responsabilidad del usuario.

- El acceso al servicio de correo electrónico debe ser autorizado por el responsable del proceso al que pertenece el funcionario, contratista o tercero que presta sus servicios a la Entidad

- El servicio de correo electrónico oficial de la CRA es el que es suministrado y gestionado por el Grupo de Tecnología e Informática, el cual cumple los requerimientos técnicos y de seguridad necesarios para garantizar la confidencialidad, integridad y disponibilidad de las comunicaciones oficiales por correo electrónico. Los usuarios reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.

- La clave de acceso al servicio de correo electrónico no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información de la CRA.

- En cumplimiento del artículo 15 de la Constitución Política de Colombia *"La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley"*. El usuario del servicio de correo institucional debe recordar que tal y como lo establece el Numeral 4, Artículo 34, la Ley 734 de 2002, por la cual se expide el Código Disciplinario Único. Son deberes del funcionario público *"Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos."*, por lo anterior no se recomienda el uso del correo institucional para comunicación personal privada.

- La CRA puede supervisar, siguiendo los procedimientos legales y respetando el derecho a la intimidad del titular, el uso del servicio de correo electrónico institucional para verificar que se está usando para el cumplimiento de las funciones misionales de la Entidad.

- En los casos en los que se requiera envío o recepción de información clasificada con carácter reservado o pública clasificada, el usuario del servicio de correo electrónico puede solicitar el servicio de cifrado de datos al Grupo de Tecnología e Informática quien seguirá el procedimiento de controles criptográficos del SGSI.

- Todos los mensajes de correo enviados deben contener como mínimo los siguientes datos del remitente (Texto en Fuente Calibri 12):

  Nombre completo del funcionario: Robertino Smith
  Cargo: Asesor Tecnologías de la Información
  Oficina: Oficina Asesora de Planeación y TIC´S
  Correo electrónico: rsmith @cra.gov.co
  Dirección: Carrera 12 N° 97-80 Piso 2. Código Postal: 110221 Bogotá, Colombia
  Teléfono: PBX: +57 (1) 487 3820 Ext: 305 Línea gratuita nacional: 01 8000 517565
  Ciudad: Bogotá, Colombia

- Los correos electrónicos deben contener una nota de confidencialidad ubicada al final del texto, después de la firma del mismo, este mecanismo es una medida preventiva de divulgación no autorizada de contenidos de correo electrónico. La nota de confidencialidad debe seguir el estándar definido por el Sistema de Gestión de Seguridad de la Información de la CRA así:

  NOTA DE CONFIDENCIALIDAD: La información contenida en esta transmisión puede contener información confidencial, protegida legalmente o de propiedad de la CRA. La información debe ser recibida por un destinatario o entidad específica o para otras personas autorizadas para recibirla. Si usted no es el destinatario de esta información, pero por error la recibe, por favor borre inmediatamente el correo electrónico junto con la información contenida en éste y todas las copias de su sistema, destruya cualquier copia en papel que se tenga de la información y notifique de tal hecho al remitente. Si Usted no es el destinatario, no está autorizado para que directa o indirectamente use, destruya, imprima o copie la totalidad o parte de este mensaje. El hecho de que reciba la información sin ser su destinatario, no es una renuncia a los privilegios de confidencialidad que pueda tener la información. La CRA no asumirá responsabilidad ni obligación legal alguna por cualquier información incorrecta o alterada contenida en este mensaje.

- La "confirmación de lectura" sólo debe ser utilizada en situaciones estrictamente necesarias con el fin de evitar la congestión de mensajes

- La responsabilidad del contenido de los mensajes de correo será del usuario remitente. El receptor no deberá alterar los mensajes sin la autorización del emisor.

- Cuando un funcionario requiere ausentarse de la Entidad por un período superior a 8 días debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.

- El envío de mensajes a grupos de usuarios múltiples como “Todos los Usuarios” cuyo tamaño pueda ocasionar saturación en el tráfico de la red pone en riesgo la disponibilidad de los servicios informáticos de la CRA al exceder su capacidad, por lo que este servicio se restringe a mensajes exclusivamente de carácter oficial. Como alternativa, cuando se desee publicar documentos o manuales se deben publicar mediante el servicio de carpeta compartida

- Antes de enviar un correo el usuario deberá verificar que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades o desmejoramiento en el servicio y operación de la red.

- El mantenimiento del buzón de correo será responsabilidad del usuario y se deberán conservar únicamente los mensajes necesarios con el fin de no exceder el máximo límite de almacenamiento.

- Al finalizar su relación laboral todo funcionario, contratista o tercero que preste sus servicios a la CRA, debe realizar la devolución de la cuenta de usuario de correo electrónico al responsable del proceso para el cual labora. Para la supresión o suspensión de la cuenta se debe seguir el procedimiento Administración de Usuarios Nuevos y Usuarios Inactivos en el Sistema.

8.4. USOS NO AUTORIZADOS DEL SERVICIO DE CORREO ELECTRÓNICO

Como lo establece el artículo 13 de la Constitución Política de Colombia *“Todas las personas nacen libres e iguales ante la ley, recibirán la misma protección y trato de las autoridades y gozarán de los mismos derechos, libertades y oportunidades sin ninguna discriminación por razones de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica.”*, por lo anterior el uso del correo electrónico para comunicaciones personales o institucionales no debe:

- Difundir mensajes que promuevan, induzcan o inciten a la discriminación de las personas en razón a sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica.

- Usar el correo institucional con fines diferentes al cumplimiento de las funciones asignadas, por ejemplo: difusión avisos clasificados o publicidad comercial no deseada o beneficio personal.

- Como lo establece la Ley 1273 de 2009, está prohibida la Interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, por lo que está prohibida la interceptación de los mensajes de correo electrónico sin autorización legal.

- Como lo establecer la Ley 1273 de 2009, está prohibido el acceso abusivo a un sistema informático, por lo tanto, está prohibido acceder al buzón de correo electrónico de otros funcionarios sin la debida autorización.

- Crear, almacenar o intercambiar de mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.

- Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.

8.5. SOBRE EL USO DEL SERVICIO DE NAVEGACIÓN POR INTERNET

8.5.1. OBLIGACIONES

- El servicio de acceso a Internet debe utilizarse primordialmente para las tareas propias de la función desarrollada en la CRA, los usos diferentes a los necesarios para el cumplimiento de las funciones de la Entidad son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio.

- El acceso al servicio de Internet podrá ser asignado a las personas que tengan algún tipo de vinculación con la CRA, ya sea como funcionario, contratista o tercero. El acceso al servicio es solicitado por el responsable del área o proceso en el que se desempeña el usuario.

- En cumplimiento del artículo 15 de la Constitución Política de Colombia *"La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley"*. El usuario del servicio de acceso a internet debe recordar que tal y como lo establece el Numeral 4, Artículo 34, la Ley 734 de 2002, por la cual se expide el Código Disciplinario Único. Son deberes del funcionario público *"Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos."*, por lo anterior no se recomienda el uso del servicio a Internet de manera racional y ajustada a la ley.

- Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en la Entidad y para los cuales esté formal y expresamente autorizado, por lo que el uso de servicios como acceso a redes sociales depende de la función asignada para esto. La Dirección Ejecutiva aprueba para los siguientes perfiles una navegación:

    - Expertos comisionados, Jefes de Oficina, profesionales de comunicaciones: Navegación en redes sociales, portales de noticias (periódicos, emisoras y canales de televisión).

    - Asesores, profesionales especializados, profesionales universitarios, técnicos, administrativos, conductores, secretarias y contratistas: Navegación estándar con restricciones para redes sociales (Facebook, Twitter, Youtube, entre otras), streaming, emisoras y canales de televisión.

    - Profesionales de Tecnologías de la Información: Navegación en YouTube para consulta de tutoriales de tecnología, descargas de programas aprobados y verificados por el Jefe de la Oficina Asesora de Planeación y TIC'S que sean congruentes con el quehacer misional de la CRA, navegación y consulta de páginas de TI, restricción para navegación en redes sociales (Facebook, Twitter, entre otras).

- Los usuarios son responsables tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de la Entidad o se descargue desde Internet empleando la cuenta de acceso a Internet que se le ha suministrado.

- Cuando un funcionario o contratista al que le haya sido autorizado el uso de una cuenta de servicio de Internet o de acceso a la red local de la Entidad finalice su vinculación, deberá seguir los procedimientos definidos por la Entidad para entregar su cuenta de usuario y accesos a servicios informáticos provistos por la Entidad.

8.5.2. RESTRICCIONES

- Todas las conductas definidas como delito informático en la Ley 1273 de 2009 están prohibidas y no se debe hacer uso del servicio de acceso a Internet de la Entidad para fines no lícitos.
- No se debe realizar envío o descarga de información sometida a derechos de autor cuando no se tiene autorización.
- No se debe realizar envío o descarga de información cuyo volumen ponga potencialmente en riesgo la disponibilidad del servicio, los usuarios del servicio deben informarse de los procedimientos para descarga de información con los responsables del grupo TIC.
- No es aceptable el uso del servicio de acceso a Internet para actividades comerciales.
- Está prohibido el uso del servicio de acceso a Internet de la CRA para realizar o propiciar propaganda de productos o propaganda política.
- Está estrictamente prohibido el uso no autorizado de una cuenta de acceso a Internet diferente a la formalmente asignada al usuario.
- No está autorizado el acceso a sitios WEB relacionados con actividades de juego, apuestas, o actividades ilegales en general.
- No está autorizado el acceso a material pornográfico o a sitios WEB de contenido para adultos relacionados con desnudismo, erotismo o pornografía, salvo en los casos que estén expresa y formalmente autorizados con apego a funciones explícitamente definidas para el funcionario, caso particular de investigaciones en procesos disciplinarios o administrativos; en dichos casos se deben gestionar los mecanismos de acceso seguro en canales protegidos configurados por los responsables de administración de tecnología durante el tiempo requerido para el cumplimiento de la asignación.
- No está autorizado el acceso a sitios de música, juegos, vídeos u otros sitios de entretenimientos on-line.
- No está autorizado el acceso a sitios WEB de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.
- No está autorizado el acceso a sitios de “hacking” o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de la Entidad.

8.6. USO DE SERVICIO DE ANTIVIRUS

8.6.1. OBLIGACIONES

- Es obligatorio usar el software de protección contra código malicioso (antivirus) en todos los computadores, dispositivos móviles, teléfonos inteligentes y cualquier tipo de equipo de cómputo empleado para acceder a los servicios y sistemas de información de la Entidad.
- Es obligatorio que el software contra código malicioso (antivirus) siempre se encuentre actualizado con la versión más reciente de base de datos de virus.

- El software de antivirus siempre debe estar activo en los computadores y equipos de cómputo de la CRA.

- Es obligatorio aplicar los controles de seguridad que defina el Sistema de Gestión de Seguridad de la Información de la CRA para evitar incidentes de seguridad de la información generados por la presencia de código malicioso en los equipos de cómputo, redes de comunicaciones, dispositivos de almacenamiento fijos o removibles de los computadores o dispositivos informáticos.

- Los usuarios finales de los computadores no deben detener, desinstalar o alterar el funcionamiento del software de antivirus. Las modificaciones sobre el software de antivirus solo deben ser realizadas por personal formalmente autorizado por el grupo TIC de la CRA.

- Todo dispositivo de almacenamiento externo que se conecte a las estaciones de trabajo de la CRA debe ser verificado por el software de antivirus (código malicioso).

8.6.2. RESTRICCIONES

Está formalmente prohibida la utilización de software de código malicioso dentro de la infraestructura tecnológica de la CRA. El personal que cuenta con autorización para atención de incidentes de seguridad de la información debe tramitar autorización específica para la utilización de software de código malicioso con propósitos de tratamiento de incidentes de seguridad en equipos de la CRA y siempre en ambientes aislados no productivos.

8.7. RESPECTO A LA ADMINISTRACIÓN Y GESTIÓN DE ACTIVOS

8.7.1. OBLIGACIONES

- Mantener y aplicar los procedimientos de operación de los equipos o servicios informáticos definidos por el sistema de gestión de seguridad de la Información.

- Aplicar y mantener los acuerdos de confidencialidad sobre la información a su cargo.

- Mantener actualizado el registro de riesgos que afecte a los activos bajo su responsabilidad.

- Reportar los cambios que sucedan sobre los activos a su cargo ante los responsables de áreas o procesos.

- Aplicar los procedimientos que defina el Sistema de Gestión de Seguridad de la Información de la CRA para el acceso de terceros a los componentes a su cargo en situaciones como mantenimiento o garantía.

- Mantenimiento de registros del desempeño de los equipos o servicios a su cargo.

- Mantenimiento de registros que muestren las actividades realizadas por los administradores o los operadores de los equipos o servicios a su cargo.

- Mantenimiento de los registros de las fallas sobre los equipos o servicios a su cargo.

- Mantener registros de los usuarios a los cuales se les ha otorgado acceso a cada activo, servicio o componente.

- Realizar una revisión periódica de los privilegios de acceso otorgados a los usuarios de los servicios o componentes a su cargo.

- Coordinar la aplicación de los procedimientos definidos en el Sistema de Gestión de Seguridad de la Información para la asignación de cuentas de usuario y contraseñas de acceso a servicios y componentes.

- En coordinación con los responsables de los procesos y áreas de la CRA, aplicar las medidas de mitigación que se definan en el Sistema de Gestión de Seguridad de la Información, para contrarrestar las vulnerabilidades que se identifiquen sobre los componentes o servicios de tecnología.

- Mantener y aplicar de los procedimientos de respaldo de la información.

- Mantener, mejorar y probar periódicamente los procedimientos de contingencia, recuperación ante desastres y continuidad en la prestación de servicios de tecnología.

- Implementar, mantener y mejorar de los controles de protección física lógica o procedimental que defina el Sistema de Gestión de Seguridad de la Información para la protección de los activos de información, componentes o servicios a su cargo.

- Implementar, preservar y garantizar la seguridad de la información referente a la configuración de los diversos componentes o servicios de información y tecnología de la Entidad que estén a su cargo.

- Las actividades de administración y operación de equipos y servicios de tecnología de la Entidad deben estar orientadas a garantizar los servicios necesarios para el cumplimiento de la misión de la entidad.

9. POLÍTICA DE TELETRABAJO

Esta política define las pautas generales para asegurar la información de la entidad frente a riesgos asociados al teletrabajo. Aplica a todos los funcionarios de la entidad que se encuentren autorizados para realizar actividades de teletrabajo con el pleno cumplimiento de los requisitos del Decreto 1072 de 2015, Capítulo 5 Teletrabajo.

9.1. OBLIGACIONES

- Todo acceso a servicios de teletrabajo debe ser autorizado por el responsable del proceso al que pertenece el funcionario que lo solicita, considerando las evaluaciones de riesgos de seguridad de la información y riesgos administrativos.

- Antes de su aprobación, todo acceso a servicios de teletrabajo debe ser sometido a una evaluación de riesgos de seguridad de la información y de seguridad y salud en el trabajo.

- Los responsables de áreas y procesos que autoricen servicios de teletrabajo deben realizar las evaluaciones de riesgos tecnológicos sobre los accesos solicitados y formular las recomendaciones de controles de seguridad necesarios para la implementación del acceso. En caso de identificar riesgos que no son aceptables, notificará al peticionario del servicio la imposibilidad de activar los servicios de teletrabajo en las condiciones presentadas en la solicitud.

- El acceso a teletrabajo no debe impedir el acceso a la información de la CRA cuando la requieran los debidamente autorizados.

- Para el acceso al teletrabajo se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que el funcionario cuente con las herramientas necesarias para poder realizar su trabajo, así como las configuraciones de acceso seguro, los medios y horarios que solicite el responsable del proceso, manteniendo en todo momento los Principios de Eficiencia, Eficacia y Uso racional de los recursos del Estado.

- Los servicios de teletrabajo deben ser implementados con controles del sistema de gestión de seguridad de la información que garanticen en todo momento que la seguridad de la información de la Entidad esté salvaguardada.

- Cualquier dispositivo que se emplee para las actividades de teletrabajo deberá cumplir con los requisitos y controles de seguridad que defina el Sistema de Gestión de Seguridad de la Información de la Entidad.

- Las conexiones a servicios de teletrabajo deben permanecer cifradas con los controles de seguridad del sistema de gestión de seguridad y utilizando conexiones seguras o redes privadas entre el lugar dónde se realiza el teletrabajo y los sistemas de información de la CRA.

- El acceso a los servicios de teletrabajo se debe usar para el cumplimiento de las funciones asignadas y el cumplimiento de la misión y objetivos de la CRA. Cualquier uso diferente está expresamente prohibido.

- Antes de iniciar la utilización de los servicios de teletrabajo el funcionario autorizado debe aceptar formalmente que acatará, aplicará y cumplirá las políticas de seguridad de la información de la CRA.

- Los funcionarios que realicen teletrabajo son responsables de reportar a la mayor brevedad posible la pérdida o hurto de los equipos y dispositivos móviles usados para teletrabajo y que se encuentren bajo su responsabilidad

- Todo responsable del proceso que tenga funcionarios usando los servicios de teletrabajo debe realizar seguimientos periódicos sobre el cumplimiento de la política de teletrabajo para certificar su cumplimiento.

- Los lugares desde los que se desarrollen actividades de teletrabajo deben contar con medidas de seguridad física que impidan el acceso a personal no autorizado a los equipos, desde los que se realizan las actividades de teletrabajo.

- Las conexiones de teletrabajo deben implementar mecanismos de cifrado siguiendo la política de cifrado de datos de la CRA. Se debe dar preferencia a soluciones tecnológicas que faciliten el uso de escritorio remoto, de forma que se impida el almacenamiento de información de la Entidad en equipos que no son propiedad de la CRA.

- El teletrabajador debe aceptar que en el lugar del teletrabajo también se deben cumplir las políticas de seguridad de la Información de la CRA.

- La estación de trabajo del teletrabajador debe cumplir con la reglamentación en cuanto a uso de software legal.

- La estación de trabajo del teletrabajador debe contar con software de protección contra código malicioso.

- El acceso a actividades de teletrabajo debe cumplir con la política de control de acceso a la información de la Entidad.

10. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

Esta política aplica a todos los dispositivos y equipos móviles de los funcionarios, contratistas o terceros de la entidad que estén autorizados para conectarse a las redes de datos de la CRA y busca garantizar la seguridad de la información cuando se administre, transmita o almacene información de la entidad en dichos dispositivos. La autorización de conexión a servicios institucionales debe ser tramitada siguiendo los procedimientos institucionales.

10.1. OBLIGACIONES

- La conexión y uso de dispositivos móviles a las redes de telecomunicaciones e infraestructura de tecnología de información y comunicaciones de la CRA debe ser autorizado por la oficina asesora de planeación y TIC´s.

- Se debe mantener un registro de los dispositivos móviles autorizados a conectarse a las redes de telecomunicaciones e infraestructura de tecnología de información y comunicaciones de la CRA.

- La autorización de la conexión de dispositivos móviles debe considerar las restricciones de acceso a la información y los privilegios de uso de información del usuario.

- Los responsables de los procesos y áreas de la CRA determinarán bajo qué circunstancias se autorizará el uso de dispositivos móviles para almacenar o procesar información institucional, así como la aplicación de las políticas de seguridad requeridas para la información que se almacene y gestione en el dispositivo móvil.

- El usuario al que se le autorice el uso de dispositivo móvil para conexión a las redes o sistemas de información de la Entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.

- Se debe capacitar a los propietarios o responsables de los dispositivos móviles acerca de los cuidados y responsabilidades que tienen sobre cada uno de los componentes de procesamiento electrónico de información. (Portátiles, teléfonos celulares, Smartphone, Tablet, IPad, teléfonos inteligentes, entre otros).

- Todos los dispositivos móviles que almacenen información de la Entidad deben estar protegidos contra software malicioso y ser actualizado regularmente.

- En caso de pérdida del dispositivo móvil el funcionario, contratista o tercero responsable del dispositivo móvil debe comunicarlo inmediatamente a su jefe y reportar este hecho como un incidente de seguridad al oficial de seguridad de la información de la CRA, para atender el incidente de acuerdo con el procedimiento de gestión de incidentes.

- Los dispositivos móviles autorizados se deben revisar periódicamente para certificar que están cumpliendo con las políticas de seguridad de la información de la Entidad, las revisiones preservarán el derecho fundamental a la intimidad del usuario y las normas sobre protección de datos de carácter personal.

- Los responsables de los dispositivos móviles deben garantizar el cuidado requerido cuando se usen dispositivos móviles en lugares públicos, salas de reuniones y áreas no protegidas.

11. POLÍTICA DE PROTECCIÓN DE DISPOSITIVO PROPIO (BYOD)

Esta política define las medidas necesarias para evitar que la información pública reservada o pública clasificada se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos de propiedad de funcionarios o contratistas de la CRA. Esta política aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes y tabletas, los computadores portátiles que no pertenecen la Entidad pero que son utilizados por funcionarios y contratistas para acceder o almacenar información. A estos dispositivos se les conoce comúnmente dentro del área de seguridad informática como BYOD (*Bring Your Own Device*). Como política general la Entidad no autoriza el uso de dispositivos BYOD para el tratamiento de información institucional. La Entidad determinará mediante sus procedimientos en qué momento se considera viable autorizar uso de dispositivos personales que no sean propiedad de la Entidad para el tratamiento de la información institucional.

11.1. OBLIGACIONES

- Los responsables de los procesos y áreas deben determinar en qué procesos y bajo qué circunstancias se autorizará el uso de dispositivos que no pertenecen la entidad (BYOD) para almacenar o procesar información institucional pública reservada o información pública clasificada, así como la aplicación de las políticas de seguridad requeridas para la información que se almacene y gestione en el dispositivo personal del funcionario o contratista.

- Los responsables de los procesos deben evaluar los riesgos asociados a la divulgación de información pública reservada o información pública clasificada antes de autorizar el uso de los BYOD.

- El funcionario o contratista tercero al que se autorice un BYOD debe garantizar bajo compromiso de confidencialidad que la información pública reservada o información pública clasificada correspondiente a sus labores asignadas será almacenada de forma aislada a la información personal que guarde en su dispositivo.

- Todo dispositivo BYOD autorizado para almacenar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.

- La Oficina Asesora de Planeación y TIC´s, puede realizar periódicamente revisiones a los equipos BYOD para certificar que están cumpliendo con las políticas de seguridad de la información, las revisiones preservarán el Derecho Fundamental a la Intimidad del usuario del BYOD y las normas sobre Protección de Datos de carácter personal.

- El propietario del dispositivo BYOD debe aplicar todas las medidas de seguridad razonables que estén a su alcance para preservar la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.

- El propietario del dispositivo debe informar sin demoras injustificadas a la Oficina Asesora de Planeación y TIC´S y a la autoridad competente, el robo o pérdida de su dispositivo. La CRA gestionará la pérdida o divulgación de información almacenada en los dispositivos BYOD mediante el procedimiento de gestión de incidentes de seguridad de la información.

12. POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

El objetivo de la política de servicios de computación en la nube es mantener la seguridad de la información y de los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la entidad garantizando su continuidad, cumpliendo los niveles de servicio requeridos, reduciendo los riesgos legales y técnicos a niveles aceptables. Aplica para todos los servicios de computación en nube que sean utilizados o contratados por la entidad, así como a los procesos que hagan uso de dichos servicios. La autorización de uso de servicios de procesamiento de información en la nube se debe realizar a través del proceso de Gestión de tecnologías de información.

12.1. OBLIGACIONES

- En los procesos de contratación y uso de servicios de computación en la nube se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información institucional, acceso a información personal, protección de secretos comerciales, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información institucional o personal. La gestión de riesgos de seguridad de servicios de computación en la nube se debe realizar aplicando el Manual de Administración del Riesgo y de oportunidades.

- No se deben utilizar servicios de computación en la nube cuyo análisis de riesgos indique niveles no tolerables para la protección de información institucional o personal. Los resultados del análisis y gestión de riesgos deben ser determinantes para aceptar o rechazar la utilización de servicios de computación en la nube de pago.

- Los servicios de computación en la nube que utilice la Entidad deben ser aprobados por el proceso de gestión de tecnologías de información.

- A fin de reducir los riesgos de pérdida de confidencialidad de información se dará prioridad al uso de servicios de nube privada.

- Para almacenar información de datos personales, en los términos definidos por la Ley 1266 de 2008 o 1581 de 2012, en servicios de almacenamiento en la nube fuera del territorio nacional, se debe contar con la autorización del titular del dato personal.

- En los contratos celebrados en Colombia con proveedores de servicios de computación en la nube, se debe incluir el cumplimiento de las políticas de seguridad de la información de la Entidad, la conformidad de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.

- Al contratar servicios de computación en la nube, se debe analizar, identificar, clasificar y cuantificar los riesgos con los respectivos tratamientos, asociados a fallas en las plataformas computacionales que originen pérdida en la disponibilidad y continuidad de los servicios, conforme al tratamiento dado por los proveedores del servicio.

- En los casos que se requiera el almacenamiento de información en la nube clasificada como reservada, pública clasificada e información de carácter personal, está debe permanecer cifrada para evitar su divulgación o acceso no autorizados. El cifrado se debe realizar de acuerdo con las políticas de seguridad de la información de la Entidad.

- Los usuarios deben mantener en estricta confidencialidad las contraseñas para acceso a los servicios de computación en la nube.

- El uso de los servicios de computación en la nube institucional debe ser exclusivo para el cumplimiento de las funciones propias de la Entidad; no está autorizado el uso de estos servicios de computación para fines personales.

- En los servicios de almacenamiento en la nube institucional, no está autorizado el almacenamiento de información personal, incluidos, pero sin limitarse a: fotografías, videos, documentos sujetos a derechos de autor, software o utilitarios que no sean propiedad de la CRA.

- Los siguientes lineamientos específicos se aplican de acuerdo con el tipo de servicio de computación en la nube:

  - En los servicios de correo electrónico se debe cumplir la política institucional de correo electrónico.
  - En los servicios de correo electrónico y almacenamiento en la nube, se deben cumplir los límites de espacio de almacenamiento que determine el proceso de gestión de tecnologías de información.
  - El periodo de permanencia de los archivos alojados, guardados en almacenamiento bajo modalidad nube, estarán sujetos a los mismos lineamientos que se encuentran establecidos en las tablas de retención documental de cada proceso para sus respectivos registros electrónicos y conservación de los mismos.

13. POLÍTICA DE USO DE REDES SOCIALES

Establecer el uso adecuado de las redes sociales, las cuales son empleadas para comunicar masivamente y de forma responsable, la estrategia digital de la Entidad sin que sea comprometida de forma penal, administrativa y disciplinaria. Así mismo, brindar lineamientos de las responsabilidades correspondientes al control de contenido de estas; la custodia controlada de las cuentas de acceso que permite interactuar con usuarios; destino de bases de datos; violación de datos personales y el uso inadecuado de la información.

La Comisión de Regulación de Agua Potable y Saneamiento Básico - CRA, ha creado diferentes sitios en internet que permiten a la ciudadanía contactarse con la Entidad, en los cuales se le brindará información actualizada del que hacer de la Comisión.

La creciente necesidad por parte del gobierno de modernizarse y hacer mayor presencia a lo largo del territorio nacional ha convertido a las redes sociales digitales en un instrumento efectivo, oportuno y fundamental que permite construir nuevas y mejores relaciones de proximidad y participación con la ciudadanía. Ya que esta interacción posibilita la transparencia, cercanía y genera lazos de confianza entre los ciudadanos y las instituciones públicas.

En consecuencia, la CRA ha elaborado la presente política, con el objetivo de dar orientaciones relacionadas a la gestión de las cuentas institucionales en redes sociales. Estos lineamientos están apoyados en normativas nacionales e internaciones de buenas prácticas de seguridad informática y de la información.

Es importante resaltar que la CRA tiene a disposición de la ciudadanía las siguientes redes sociales:

Facebook: Comisión de Regulación CRA

Twitter: @cracolombia

You Tube: cracolombia

LinkedIn: linkedin.com/company/cracolombia

Teniendo en cuenta que se debe velar por la veracidad, la transparencia, la identidad e imagen institucional, además del uso adecuado de la información a través de la web, se establece que:

OBLIGACIONES:

- La CRA facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un canal de comunicación con la ciudadanía en el cual se difunden diversas actividades que realiza la entidad. Por lo tanto, es necesario hacer uso de ellas de forma correcta y moderada.
- Todas las herramientas virtuales que representen el nombre de la CRA, deben ser creadas por la Oficina Asesora de Planeación y TIC´S.
- Toda dependencia que desee publicar información a través de las redes sociales debe contar con la autorización de la Oficina Asesora de Planeación y TIC´S- Comunicaciones.
- La información publicada a través de estas herramientas será monitoreada por la Oficina Asesora de Planeación y TIC´S.
- El acceso y manejo de la cuenta de una red social, bien sea de Facebook, Twitter, YouTube, LinkedIn u otra, estará a cargo de una sola persona o funcionario. De esta manera, las acciones y publicaciones que se realicen allí corresponderán a la gestión de esa única persona.
- El responsable de la red social deberá realizar el cambio periódico de las contraseñas y asociar todas las cuentas a correos institucionales y no personales.
- Todos los usuarios autorizados para hacer uso de los servicios de redes sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la CRA.
- El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas de la CRA.
- El líder de la red social dará respuesta oportuna a los comentarios de usuarios de la red, teniendo presente los tiempos de respuesta establecidos en el programa de gestión documental.
- La respuesta a un comentario negativo nunca podrá ser de forma grosera, conflictiva o de cualquier forma que genere una agresión al usuario. No se dará respuesta a un comentario negativo sin la debida autorización.
- Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.
- No se deben realizar publicaciones mentirosas o engañosas.

- No publicar contenido difamatorio o ilegal, así como contenido en Internet sin cumplir con las normas de derechos de autor, propiedad intelectual, y especialmente, contrario a las normas constitucionales sobre privacidad y habeas data.
- No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.
- No se permiten descargas, distribución de material obsceno, degradante, terrorista, abusivo o calumniante a través del servicio de redes sociales.
- No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad al servicio de internet de la CRA, o aprovechar el acceso a redes sociales para fines ilegales.

La Oficina Asesora de Planeación y TIC's, será el encargado de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en la CRA.

14. POLÍTICA DE GESTIÓN DE ALMACENAMIENTO

El objetivo de la política es preservar la información velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento internas, externas y nube.

14.1. OBLIGACIONES

Se restringe el uso de carpetas compartidas desde equipos de escritorio físicos y virtuales. Si el colaborador no adopta esta política, la Oficina Asesora de Planeación y TIC's no se hace responsable de la pérdida o infiltración de la información.

Las carpetas compartidas en red dispuestas por la Oficina Asesora de Planeación y TIC'S como File server, SharePoint, OneDrive, serán administradas por las áreas, mediante la figura de persona autorizada por el líder del proceso, emplearán el correo institucional para informar a la Oficina Asesora de Planeación y TIC'S y a la cuenta helpdesk@cra.gov.co, nombres y apellidos completos del funcionario a quien se le asigne esta responsabilidad, quienes estarán en la obligación de velar por el buen uso de la información y de las carpetas.

Se deben documentar los permisos y accesos sobre la carpeta compartida, usando los siguientes criterios:

- ✓ Permisos de Lectura
- ✓ Permisos de Escritura y modificación
- ✓ Permisos de Control Total

Dichos permisos serán documentados por la Oficina Asesora de Planeación y TIC'S a través de la Mesa de Ayuda.

La información que está catalogada como CLASIFICADA o RESERVADA, se deberá ubicar o alojar en las carpetas destinadas, para que sean incluidos en las tareas programadas de copia de respaldo conforme al procedimiento GTI-PRC01 Procedimiento realización de copia de respaldo y recuperación de la información V03.docx.

Para la información clasificada como pública perteneciente a cada proceso o área institucionales, se deberá ubicar o alojar en las carpetas destinadas en el OneDrive, en consecuencia, cada funcionario o contratista, es responsable de la administración y custodia de esta información que la persona misma ubicó.

La información pública para uso interno de la institución debe utilizarse en las carpetas destinadas en el Sharepoint, para que sean incluidos en GTI-PRC01 Procedimiento realización de copia de respaldo y recuperación de la información V03.docx**.**

El administrador de cada carpeta es directo responsable de establecer el límite de tiempo durante el cual mantendrá publicada la información y compartido el recurso, así mismo, será quien asigne permisos de lectura y escritura a los diferentes usuarios. Los permisos de administrador asignado a la cuenta de red, serán gestionados por la OAP Y TIC, a través de la mesa de ayuda.

Las carpetas compartidas tendrán una capacidad de 300 Gigas en Onedrive, si el área requiere mayor capacidad de almacenamiento debe justificarlo a la OAP Y TIC para ajustar la capacidad como se defina según acuerdo por los dos procesos.

Se prohíbe el acceso a las carpetas compartidas a colaboradores desde equipos de cómputo que no cuenten con antivirus corporativo actualizado.

Se prohíbe el acceso a carpetas compartidas a usuarios que no tengan una vinculación con la CRA.

Se prohíbe la publicación de archivo ejecutables (.exe, bat y dll entre otros) en las carpetas compartidas de Onedrive, SharePoint, File server, si el área requiere usar alguna de las extensiones mencionadas, debe justificarlo a la OAP Y TIC.

La OAP Y TIC realizará monitoreo y revisiones periódicas, con el fin de velar por una correcta administración de las carpetas compartidas cada semestre.

Está prohibido a funcionarios y contratistas usar los recursos computacionaleses entregados, para almacenar o guardar archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionado con los objetivos misionales de la Entidad.

Los permisos a las carpetas compartidas administrados por la OAP Y TIC sobre los diferentes ambientes (Pruebas, calidad y producción) serán autorizadas a través de la mesa de ayuda.

Los nombres de los archivos y carpetas deben ser lo suficientemente descriptivos, para lo cual no se deberá utilizar caracteres especiales como */$% y que no superen los 120 caracteres (un carácter puede ser una letra, número o un símbolo).

El único medio de respaldo de la información para los colaboradores es OneDrive, el cual será configurado por la OAP Y TIC.

CAPÍTULO III

POLÍTICAS DE BUEN GOBIERNO PARA LA GESTIÓN DE LA ENTIDAD

1. POLÍTICAS PARA LA GESTIÓN ÍNTEGRA

1.1. COMPROMISO PARA LA ERRADICACIÓN DE PRÁCTICAS CORRUPTAS

La CRA se compromete a luchar contra la corrupción, para lo cual todos sus servidores públicos y colaboradores participarán activamente en la identificación y mitigación de riesgos de corrupción en los procesos de la entidad, así como en los procesos de publicidad y rendición de cuentas de la entidad de acuerdo con la Ley de Transparencia y del derecho de acceso a la información pública nacional.

En el desarrollo de esta política de lucha anticorrupción, la UAE-CRA vinculará a la ciudadanía, por medio de los mecanismos de participación ciudadana para el control social de la gestión.

1.2. ACCIONES PARA LA INTEGRIDAD Y LA TRANSPARENCIA

La UAE-CRA está en contra de toda práctica de corrupción; para impedir, prevenir y combatir estos fenómenos, adopta como mínimo las siguientes medidas:

- Guiar sus actuaciones por los principios éticos establecidos en el Código de Integridad y Buen Gobierno.
- Dar publicidad a las normas éticas y advertir sobre la determinación inquebrantable de cumplirlas en el quehacer ordinario de sus actividades.
- Promover la identificación y mitigación de los riesgos de corrupción en la entidad.
- Realizar el seguimiento y publicidad de la matriz de riesgos de corrupción a través del Plan Anticorrupción y de Atención al Ciudadano, publicado en la página web de la entidad.
- Garantizar que todos los procedimientos sean claros, equitativos, viables y transparentes.
- Denunciar las conductas irregulares, tanto para que las entidades competentes conozcan de los hechos, como para que la sociedad esté al tanto del comportamiento de sus servidores.
- Capacitar a los servidores en materia de ética ciudadana y responsabilidad social.
- Articular las acciones de control social con los programas de la institución y con los gubernamentales.
- Realizar la rendición de cuentas a los grupos de interés, garantizando la disposición al público de la información no confidencial de la entidad de manera permanente y usando los medios necesarios, como redes sociales, página web, ferias de atención al ciudadano, atención personal, telefónica, escrita, correo electrónico, medios escritos y carteleras, entre otros.
- En materia de contratación, implementar y adoptar las normas vigentes; publicar la contratación de servicios y la adquisición de bienes de acuerdo con lo expresado en la legislación vigente en el manual de contratación actual; y establecer mecanismos de seguimiento a los contratos.

1.3. COLABORACIÓN INTERINSTITUCIONAL EN LA ERRADICACIÓN DE PRÁCTICAS CORRUPTAS

La UAE-CRA, a fin de combatir la corrupción, se compromete a mejorar los sistemas de comunicación e información, sosteniendo una comunicación fluida con otras instituciones públicas, privadas y gremiales, y estableciendo pactos éticos frente al desempeño de la función administrativa y la contratación estatal, con el objetivo de construir cadenas éticas que vayan configurando buenas prácticas de integridad, transparencia y eficiencia en el ejercicio de la función pública.

1.4. COMPROMISO CON LA FINALIDAD DE LA CONTRATACIÓN PÚBLICA

La UAE-CRA podrá contratar personas naturales y/o jurídicas a través de la modalidad de prestación de servicios sólo cuando ello sea estrictamente necesario para el desempeño de sus funciones, para lo cual dará cumplimiento riguroso al Estatuto de la Contratación Pública y otras disposiciones legales complementarias.

Las decisiones para otorgar los contratos serán tomadas sin ningún tipo de sesgos o preferencias, sino de manera exclusiva con base en el análisis objetivo de las propuestas presentadas por los participantes o de las competencias requeridas por un profesional o persona para desempeñar un rol.

La selección y contratación se hará con base en el establecimiento previo de los objetos contractuales y competencias necesarias para apoyar su ejecución, mediante procesos sustentados en la igualdad y el mérito.

1.5. CONTROL SOCIAL

La UAE-CRA promoverá la participación de la ciudadanía, organizaciones sociales y comunitarias, usuarios y beneficiarios, veedurías, entre otros, para prevenir, racionalizar, proponer, acompañar, vigilar y controlar la gestión pública, sus resultados y la prestación de los servicios públicos suministrados por el Estado y los particulares, garantizando la gestión al servicio de la comunidad. Así mismo, se compromete a facilitar de manera oportuna la información requerida por la ciudadanía para el ejercicio del control social.

2. POLÍTICAS DE GESTIÓN DEL RECURSO HUMANO

2.1. EL DESARROLLO DEL TALENTO HUMANO

La Unidad Administrativa Especial Comisión de Regulación de Agua Potable y Saneamiento Básico UAE – CRA, buscará atraer, mantener y retener a los servidores comprometidos y competentes para desarrollar la gestión, lograr la Visión y paralelamente propenderá por el desarrollo integral de los mismos.

Para garantizar lo anterior llevará a cabo procesos de selección de personal que garanticen la prestación adecuada de los servicios a la ciudadanía. Los procesos de selección y vinculación de los servidores que conforman la planta estarán ajustados a lo establecido por la Comisión Nacional del Servicio Civil.

Se realizará el entrenamiento correspondiente a cada servidor público propiciando la ejecución de programas de inducción, capacitación y entrenamiento, tanto en las generalidades de la entidad como en las especificidades que requiera el desempeño del cargo o rol que se le asigne.

Se velará por el bienestar de los servidores trazando estrategias y desarrollando actividades que permitan mejorar permanentemente el clima laboral y desarrollar una cultura basada en los principios y valores éticos compartidos.

Para determinar el desempeño del personal, se efectuará evaluación sistemática y periódica de los aportes individuales al logro de los objetivos institucionales, conforme a los parámetros establecidos por el Departamento Administrativo de la Función Pública DAFP. Adicionalmente, se efectuará seguimiento permanente a las responsabilidades individuales establecidas en los planes estratégicos, agendas regulatorias y planes de acción de cada proceso.

Cuando sea necesario, contratar personal que vaya a desarrollar labores que no sea posible ejecutar con los servidores de la planta, deberá darse la inducción o entrenamiento necesario para el logro adecuado de los objetivos del contrato pactado.

2.2 POLÍTICA DE SEGURIDAD Y SALUD EN EL TRABAJO

La Comisión de Regulación de Agua Potable y Saneamiento Básico CRA, como una Unidad Administrativa Especial encargada de la regulación de los Servicios Públicos de Acueducto, Alcantarillado y Aseo, consciente de su responsabilidad en materia de seguridad y salud en el trabajo tiene como uno de sus compromisos velar por el bienestar de funcionarios y contratistas, partiendo de métodos seguros, los cuales están basados en la implementación del sistema de gestión de seguridad y salud en el trabajo SG-SST, en la identificación de los peligros, evaluación y valoración de los riesgos con sus respectivos controles y en la protección de la seguridad y salud de todos los trabajadores, mediante la mejora continua del sistema de gestión de seguridad y salud en el trabajo, dando cumplimiento al Decreto 1072 de 2015 y a la normatividad que le complemente y/o modifique, en materia de riesgos laborales.

La Comisión de Regulación de Agua Potable y Saneamiento Básico CRA, asumiendo su compromiso, orienta los siguientes objetivos a la política del sistema de gestión de seguridad y salud en el trabajo:

- La prevención de lesiones, incidentes, accidentes laborales y enfermedades laborales, la protección de la integridad física y mental de los servidores, mediante la identificación de peligros, evaluación y valoración de riesgos, estableciendo los controles respectivos.
- La implementación, funcionamiento, mejora continua del Sistema de Gestión de Seguridad y Salud en el Trabajo, con el cumplimiento de las normas legales vigentes aplicables en materia de riesgos laborales.
- El fomento en la cultura del autocuidado, desarrollando actividades de prevención y promoción, proporcionando un ambiente de trabajo seguro y saludable.
- La generación de espacios que permiten el desempeño del Comité Paritario en Seguridad y Salud en el Trabajo-COPASST, el Comité de Convivencia Laboral y de los Brigadistas de emergencia, garantizando la presencia y cubrimiento en materia de seguridad y salud para todas las áreas e instancias de la entidad.
- La designación de los recursos humanos, económicos y logísticos necesarios para la ejecución del Sistema de Gestión de seguridad y salud en el trabajo SGSST.
- La revisión periódica del Sistema de gestión de Seguridad y Salud en el Trabajo, con el fin de asegurar el cumplimiento de la presente política, objetivos y obtener información sobre el estado de implementación de la misma.

Adicional al cumplimiento de lo establecido en el Decreto único reglamentario del sector trabajo por todos los grupos que hacen parte del sistema de gestión de seguridad y salud en el trabajo, cada grupo de ellos se rige y acata lo establecido en:

- El Comité paritario de seguridad y salud en el trabajo COPASST, se rige por lo establecido en la Resolución 2013 de 1986 expedida por el Ministerio de Trabajo y Seguridad Social, Resolución 1016 de 1989 expedida por el Ministerio de Trabajo y Seguridad Social, Decreto 1295 de 1994 expedido por el Ministerio de Trabajo y Seguridad Social, Decreto 1562 de 2012 expedido por el Ministerio de Salud y Protección Social, Decreto 1443 de 2014 expedido por el Ministerio de Trabajo.
- Brigadas de emergencia, se rige por lo establecido en el Decreto 2157 de 2017 expedido por el Departamento Administrativo de la Presidencia de la República, Ley 1523 de 2012, Resolución

1016 de 1989 del Ministerio de Trabajo y Seguridad Social, Ley 46 de 1988, la Resolución 2400 de 1979 del Ministerio de Trabajo y Seguridad Social y las normas técnicas colombianas referentes a la gestión del riesgo NTC-5254 entre otras.

- El Comité de convivencia laboral se rige por lo establecido en la Ley 1010 de 2006 y las Resoluciones 652 de 2012 expedida por el Ministerio de Trabajo y 1356 de 2012 expedida por el Ministerio de Trabajo.

La Dirección Ejecutiva de la Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA, de la mano del Comité Paritario en Seguridad y Salud en el Trabajo se compromete a cumplir lo estipulado en la presente política.

2.3. POLÍTICA DE PREVENCIÓN DEL CONSUMO DE ALCOHOL, TABACO Y DROGAS

La Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA consciente de la importancia de establecer una política para reducir el consumo de alcohol, tabaco y otras sustancias psicoactivas (SPA), asume una posición de prevención de la enfermedad y promoción de la salud a través de la generación de hábitos de vida saludables, cuyo principal objetivo es promover el bienestar laboral de los colaboradores; dicha política será dada a conocer a todo el personal que tenga que ver con la Comisión para que sea cumplida. Las medidas establecidas para cumplir con este objetivo son:

- Se prohíbe el consumo de tabaco, alcohol o cualquier tipo de sustancia psicoactiva dentro de las instalaciones de la CRA o en sitios en donde el funcionario cumpla órdenes, así como su posesión y/o venta.
- Se prohíbe que los funcionarios se presenten al sitio de trabajo, laboren en estado de embriaguez o bajo efectos del consumo de cualquier sustancia psicoactiva.
- Los funcionarios que estén tomando cualquier medicamento que pueda interferir en sus habilidades para realizar sus normales labores de trabajo en forma segura y eficiente deberán reportarlo en forma anticipada a su jefe inmediato.
- La posesión, uso, distribución o venta de bebidas alcohólicas, en instalaciones de la entidad no está permitida.
- Los funcionarios no podrán operar vehículos o cualquier medio de transporte durante su jornada laboral bajo los efectos del alcohol, drogas y/o alguna sustancia psicoactiva o medicamento que pudiera afectar su capacidad para trabajar de manera segura.
- Para los funcionarios con problemas de alcoholismo y/o fármaco dependencia la CRA implementará un proceso de orientación. Para este caso, el funcionario con problemas voluntariamente debe solicitar la ayuda en la Subdirección Administrativa y Financiera quién direccionará el caso al profesional especializado encargado de Seguridad y Salud en el Trabajo y este lo remitirá a su EPS o al Centro de Rehabilitación para que inicie su tratamiento de rehabilitación. El costo de este será asumido directamente por el funcionario. La CRA autorizará los permisos necesarios para el cumplimiento del tratamiento.
- Todo funcionario vinculado a la CRA deberá participar en las diferentes actividades de promoción y prevención que se programen sobre el NO consumo de cualquier tipo de sustancia psicoactiva.

- El incumplimiento de cualquiera de los numerales de la presente política constituye falta grave, por consiguiente, dará lugar a la apertura de una investigación disciplinaria de oficio.
- La prevención del alcoholismo, tabaquismo y drogadicción forma parte del sistema de gestión de seguridad y salud en el trabajo, por lo que su divulgación se realizará en la inducción de los funcionarios de la entidad.

La Dirección Ejecutiva de la Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA, de la mano del Comité Paritario en Seguridad y Salud en el Trabajo se compromete a cumplir lo estipulado en la presente política.

2. POLÍTICAS DE COMUNICACIÓN E INFORMACIÓN

3.1. COMPROMISO CON LA COMUNICACIÓN PÚBLICA

La UAE-CRA se compromete a asumir la información que produce como un bien público, a conferirle un carácter estratégico y orientarla hacia el fortalecimiento de la identidad institucional y a la expansión de la capacidad productiva de los miembros de la entidad, para lo cual las acciones comunicativas se efectuarán de acuerdo con los parámetros que establezca la ley y el Plan de Comunicaciones de la entidad.

Los actos regulatorios aprobados y expedidos por la Comisión serán emitidos de acuerdo con lo establecido en las normas constitucionales y legales y publicadas mediante diario oficial, y difundidas en la página Web y los demás canales disponibles en la entidad.

La institución reconoce que la realización de eventos abiertos a las comunidades permite conocer de primera mano las verdaderas necesidades, problemáticas y temáticas que debe abordar el sector en las diferentes regiones del país.

Se establecerán y mantendrán canales directos de comunicación con la Contraloría General de la República, Procuraduría General de la Nación, Defensoría del Pueblo, Congreso de la República, Concejos municipales, autoridades sectoriales, academia, asociaciones de usuarios, gremiales y las demás entidades que tengan relación de causalidad con su misión y que hacer institucional.

3.2. COMPROMISO CON LA COMUNICACIÓN ORGANIZACIONAL

La UAE- CRA se compromete a brindar conocimiento y fortalecer las competencias en los líderes, para que analicen y estimulen las actitudes positivas de sus colaboradores, en los eventos que se requieran destacar; motivando a su vez, a los servidores, y cuando fuere procedente dar a conocer las actitudes o acciones que son susceptibles de mejora en las que incurran los integrantes de los equipos.

La comunicación que circule en la Institución será transparente; es decir, todo lo que ocurra se hará visible a través de los diferentes mecanismos de comunicación adoptados.

Las relaciones internas serán abiertas, habrá igualdad entre los integrantes de la institución y cordialidad en la comunicación verbal. Se procurará la adecuada coherencia interna en la actuación de las áreas y en las actitudes de los servidores. Todos los integrantes de la institución, podrán posicionarse por sus propias capacidades y competencias y tendrán las mismas oportunidades.

Las capacitaciones y/o entrenamientos se planificarán para procurar un mejor desempeño de las funciones, y en los contratistas la ejecución óptima del objeto contractual, redundando en el éxito de la gestión y elevando, a su vez, el nivel de cada uno de los miembros de la Institución.

El talento humano de la entidad se desarrollará a través de procesos de capacitación y entrenamiento, bajo análisis de estructuración de procesos de Gestión de Talento Humano, que permitan definir las competencias y el desarrollo de potencialidades, sin importar el cargo. La entidad se preocupará por rescatar los valores agregados que aporten los integrantes, con el fin de promover para el alto rendimiento y desarrollo de la CRA.

Se hará circular dentro de las instalaciones de la Comisión información suficiente y necesaria para asegurar la adecuada coordinación y cumplimiento de tareas y responsabilidades por parte de los servidores y colaboradores.

3.3. COMPROMISO DE CONFIDENCIALIDAD

La UAE-CRA se compromete a vigilar que los servidores públicos que manejan información privilegiada que es de reserva de la entidad, no la hagan pública a terceros que se puedan ver afectados o beneficiados por ésta.

Quienes incumplan los acuerdos o compromisos de confidencialidad serán sancionados de acuerdo con el régimen disciplinario. Para ello, la UAE-CRA se compromete a desarrollar mecanismos que establezcan niveles de confidencialidad, tomando todas las precauciones para garantizar que la información confidencial no sea divulgada ni facilitada a ninguna persona no autorizada.

La información confidencial será usada única y exclusivamente con el propósito de adelantar actividades propias de la entidad. En consecuencia, los servidores y colaboradores de la UAE-CRA no deberán divulgar la información que pueden recibir sobre algún proyecto, así como, estudios de costos, balances comerciales, cifras y en general toda aquella información a la que puedan tener acceso por participación en proyectos regulatorios ya sean de carácter general o particular; sin previa autorización expresa del Director Ejecutivo.

La UAE-CRA debe tener dentro de sus recursos humanos, personas no sólo con habilidades, experiencia y gran talento profesional, sino, además que, estén comprometidas con el decálogo de valores y de ética de la entidad, trasparentes y dignos de formar parte de un equipo de trabajo para el desarrollo de las actividades regulatorias.

Ninguno de los grupos de interés podrá directa o indirectamente utilizar información privilegiada y confidencial de la entidad para sus propios intereses.

3.4. COMPROMISO CON LA CIRCULACIÓN Y DIVULGACIÓN DE LA INFORMACIÓN

La UAE - CRA se compromete a mantener en su Plan de Comunicaciones, herramientas de contacto permanente y correlativo con sus grupos de interés, adoptando mecanismos que garanticen que la regulación expedida y la información necesaria lleguen a sus grupos de interés de manera integral, oportuna, actualizada, clara, veraz y confiable. Para ello, buscará que se publiquen las novedades misionales, administrativas y aquellas que tengan relación con el talento humano de la institución, implementando mecanismos adecuados de información a los cuales tenga acceso la comunidad a la que va dirigida.

Se propenderá por una mayor integración interinstitucional. Igualmente se presentarán novedades, actualidad, información misional y administrativa de la institución y del sector, procurando la mayor participación de los servidores y/o colaboradores del mismo, cuyas contribuciones y aportes enriquecerán los mecanismos informativos adoptados.

En cuanto al derecho de petición, la entidad se compromete a definir y mantener actualizadas políticas encaminadas a mejorar la oportunidad y calidad de las respuestas a las peticiones planteadas por la comunidad, con el fin de que el acceso a la información sea eficaz.

3.5. COMPROMISO CON LA RENDICIÓN DE CUENTAS

La UAE-CRA se compromete a rendir cuentas de manera periódica, con el objeto de informar a la ciudadanía sobre el proceso de avance y cumplimiento de las metas contenidas en la agenda regulatoria indicativa y los planes de desarrollo administrativo y la forma como se está ejecutando el presupuesto de la entidad. El mecanismo preferente será la audiencia pública de Rendición de Cuentas, evento público entre ciudadanos, organizaciones y servidores públicos, la cual podrá ser transmitida por radio y/o televisión cuando existan los recursos financieros suficientes, con el fin de que la actividad pueda llegar a todos los ciudadanos interesados. Para el efecto se compromete a hacer pública la información necesaria como mínimo con treinta (30) días de anticipación a la realización de la audiencia, a través del Gobierno en Línea.

3.6. ATENCIÓN DE QUEJAS Y RECLAMOS

La entidad, a través de sus diferentes dependencias, prestará atención a la comunidad, con el fin de que puedan presentar solicitudes, consultas o informes referentes a la administración, reclamaciones, quejas, etc., sean éstas verbales o escritas, a las cuales se les dará respuesta en los términos previstos por la ley y con base en un procedimiento claro y público sobre el trámite que se da a los requerimientos que se hagan. Adicionalmente, la UAE-CRA contará permanentemente con un buzón de sugerencias, disponible para todos los usuarios que visitan sus instalaciones y en la página Web el Código de Ética para su consulta por parte de todos los interesados.

3.7. COMPROMISO CON EL GOBIERNO EN LÍNEA

El Comité de Expertos y todo el equipo de colaboradores de la entidad, se comprometen a poner especial interés en la aplicación efectiva del Gobierno en Línea, a través de la implantación de las acciones necesarias para mantener actualizados los procesos y canales de comunicación de la entidad con la más completa información sobre la marcha de la administración, en cuanto a procesos y resultados de la contratación, estados financieros, concursos para proveer cargos, Plan Estratégico Institucional, avances en el cumplimiento de metas y objetivos definidos en los planes, indicadores de gestión, informes de gestión, servicios que la entidad presta a la ciudadanía y forma de acceder a ellos, trámites que desarrolla la entidad, y funcionamiento general de la entidad, entre otros.

3.8 COMPROMISO FRENTE AL SISTEMA DE CONTROL INTERNO

La UAE-CRA se compromete a implementar el Modelo Estándar de Control Interno- MECI (adoptado mediante Decreto 943 de 2014), así como todas las nuevas políticas que se dicten al respecto.

3.9 COMPROMISO SOBRE RIESGOS

La UAE-CRA adopta mecanismos y acciones necesarias para la gestión integral del riesgo, que minimice el impacto de las decisiones que toma, así como a posibles eventos que afecten el cumplimiento de sus objetivos institucionales.

4. POLÍTICAS FRENTE A LOS GRUPOS DE INTERÉS

5.1. COMPROMISO FRENTE A LOS CONFLICTOS DE INTERÉS

La UAE-CRA evitará el favorecimiento de intereses individuales, que no sean los relativos al bien común o que la imparcialidad de las decisiones se comprometa distorsionándola por motivos personales o particulares, para lo cual velará por el cumplimiento de los deberes, derechos y prohibiciones de los servidores de la administración pública, propendiendo por la transparencia en las decisiones.

Deberá declararse conflicto de interés, cuando el interés general propio de la función pública se encuentre en conflicto con el interés particular y directo de un servidor público de la UAE-CRA, circunstancia que aplica cuando respecto de un asunto, tenga interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho, debiendo declararse impedido. Será necesario el análisis en cada caso particular pues la conducta humana admite de manera necesaria matices y, por tanto, el instituto del conflicto de intereses, al ser del resorte del fuero interno, debe ser valorado con especial cuidado para no vulnerar los derechos y garantías de los asociados.

De acuerdo con el mandato constitucional contenido en el artículo 209 de la Carta Política, la función administrativa está al servicio de los intereses generales y deberá desarrollarse con fundamento, entre otros, en los principios de igualdad, moralidad, eficacia, imparcialidad, etc.

5.1.1. Procedimiento para la declaración de conflicto de interés

El procedimiento que debe seguirse ante un posible impedimento para conocer y pronunciarse al respecto de un asunto que se encuentre en trámite en la entidad, por parte de los Expertos Comisionados, será el siguiente:

Inmediatamente un Experto Comisionado advierte un posible impedimento respecto de una solicitud que se presente ante la CRA, debe proceder, dentro de los tres (3) días hábiles siguientes, a presentar la solicitud de declaratoria de impedimento ante la entidad encargada de resolverlo, es decir, la Superintendencia de Servicios Públicos Domiciliarios –SSPD, de acuerdo con el artículo 110 de la Ley 142 de 1994.

Una vez presentada la anterior solicitud, el Experto Comisionado mediante memorando interno, el siguiente día hábil se lo informará al jefe de la Oficina Asesora Jurídica, en su calidad de Secretario Técnico del Comité de Expertos, y éste a su vez, en el siguiente Comité de Expertos Ordinario, lo informará.

Luego de presentada la solicitud de declaratoria de impedimento, de acuerdo con el artículo 12 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, la UAE-CRA procederá a suspender la actuación administrativa correspondiente. A partir también de dicha presentación, la Superintendencia de Servicios Públicos Domiciliarios, de acuerdo con la misma norma precitada, debe decidir de plano la solicitud, en los siguientes diez (10) días hábiles.

Posterior a que la SSPD tome la decisión, deberá notificar al Experto Comisionado que la presentó de manera personal y, de no ser posible este tipo de notificación, se hará mediante aviso. Dicha decisión es susceptible de recurso de reposición, el cual podrá ser interpuesto dentro de los diez (10) días hábiles siguientes, a partir de la notificación del acto administrativo. En caso de que el Experto Comisionado interponga recurso de reposición, la SSPD cuenta con un término de dos (2) meses para resolverlo, a partir de su presentación.

Una vez en firme la resolución mediante la cual se resuelve el impedimento (porque no fue interpuesto el recurso de reposición; porque este fue decidido; o porque el Comisionado renunció a su interposición) y de ser el mismo aceptado, en la cual también se nombra el correspondiente Experto Comisionado Ad – Hoc por parte de esta Comisión, inmediatamente se reanuda la correspondiente actuación administrativa y se sigue su curso ordinario.

Para el caso de los demás servidores públicos de la Comisión de Regulación de Agua Potable y Saneamiento Básico, se seguirá el siguiente procedimiento:

Frente a impedimento, el servidor deberá enviar dentro de los tres (3) días siguientes a su conocimiento, la actuación con su correspondiente motivación por escrito, a su superior, quien dentro de los diez (10) días siguientes a la fecha de su recibo, decidirá de plano; si lo acepta, determinará el responsable para conocer del asunto, que puede ser un funcionario ad-hoc, ordenando de todas maneras la entrega del expediente.

Cualquier persona se encuentra facultada para recusar a los funcionarios de la UAE-CRA; el recusado deberá manifestar si acepta o no la causal invocada, dentro de los cinco (5) días posteriores a la fecha de su formulación. Vencido éste término, tendrá curso el trámite explicado en el párrafo anterior.

La actuación administrativa quedará suspendida desde la manifestación de impedimento o desde la presentación de la recusación, hasta cuando se decida.

5.1.2. Sanciones por la no declaración del conflicto de intereses

Los servidores que hubieren actuado incumpliendo sus deberes éticos, serán sancionados disciplinaria y penalmente cuando a ello hubiere lugar.

La UAE-CRA proporcionará los mecanismos e instancias necesarias para tramitar los conflictos de intereses, tomando como punto de partida lo dispuesto por la Ley, a través de la adopción de buenas prácticas y de sus procesos y procedimientos. El Comité de Ética llevará el registro de las declaraciones de intereses privados, que estará disponible para el conocimiento público, encargándose de actualizarlo periódicamente.

5.1.3. Prácticas que deben evitarse para la prevención de conflictos de intereses

La UAE-CRA rechaza, condena y prohíbe que el Director Ejecutivo, los Expertos Comisionados, miembros de comités especiales, servidores públicos y todos aquellos que deban participar en procesos de decisión, incurran en cualquiera de las siguientes prácticas al estar involucrados en un conflicto de interés en el cual puedan verse favorecidos sus intereses personales sobre los colectivos:

- Recibir remuneración, dádivas o cualquier otro tipo de compensación en dinero o especie por parte de cualquier persona jurídica o natural, en razón del trabajo o servicio prestado a la entidad o a sus grupos de interés.
- Otorgar compensaciones no autorizadas por las normas pertinentes.
- Utilizar indebidamente información privilegiada o confidencial para obtener provecho o salvaguardar intereses individuales propios o de terceros.
- Realizar proselitismo político o religioso aprovechando su cargo, posición o relaciones con la Entidad, no pudiendo comprometer recursos económicos para financiar campañas políticas; tampoco generará burocracia a favor de cualquier otra persona natural o jurídica.
- Todas aquellas prácticas que atenten contra la integridad y la transparencia de la gestión de la Entidad y en contra del buen uso de los recursos públicos.

- Todo tráfico de influencias para privilegiar trámites.

5.1.4. Deberes del equipo humano y demás colaboradores con respecto a los conflictos de interés

Sin perjuicio del establecimiento de otros, los deberes de los servidores públicos de la UAE-CRA son:

- Revelar a tiempo y por escrito a los entes competentes cualquier posible conflicto de interés que crea tener.
- Contribuir a que se permita la adecuada realización de las funciones encomendadas a los órganos de control interno y externo de la Entidad.
- Guardar y proteger la información que la normatividad legal haya definido como de carácter reservado.
- Contribuir a que se le otorgue a todos los ciudadanos y habitantes del territorio nacional un trato equitativo, y a que se le garanticen sus derechos.
- Revelar a tiempo cuando incurran en alguna de las situaciones enunciadas en el artículo sobre prevención de conflictos.

5.1.5. Prohibiciones para los servidores con respecto a los conflictos de interés

Sin perjuicio de la ampliación de estas prohibiciones, el personal de la UAE-CRA se abstendrá de utilizar las siguientes prácticas en su accionar diario:

- Utilizar indebidamente información privilegiada y confidencial en contra de los intereses de la administración.
- Participar, directa o indirectamente, en interés personal o de terceros, en actividades que impliquen competencia de la administración o en actos respecto de los cuales exista conflicto de intereses.
- Realizar actividades que atenten contra los intereses de la administración.
- Gestionar, por sí o por interpuesta persona, negocios que le originen ventajas que, conforme a las normas constitucionales, legales, reglamentarias y el Código de Ética, lesionen los intereses de la administración.
- Utilizar su posición en la entidad o el nombre de la misma para obtener para sí o para un tercero, tratamientos especiales en negocios particulares con cualquier persona natural o jurídica.
- Entregar dádivas a otros servidores públicos a cambio de cualquier tipo de beneficios.
- Utilizar los recursos de la entidad para labores distintas de las relacionadas con su actividad, ni encausarlos en provecho personal o de terceros.
- Gestionar o celebrar negocios con la entidad para sí o para personas relacionadas, que sean de interés para los mencionados.
- Aceptar, para sí o para terceros, donaciones en dinero o especie por parte de proveedores, contratistas o cualquier persona relacionada o no con la administración, o de personas o entidades con las que la Entidad sostenga relaciones en razón de su actividad, que conlleve a generar cualquier clase de compromiso no autorizado;
- Participar en procesos de selección o contratación cuando estén incursos en alguna de las situaciones enunciadas en el acápite sobre prevención de conflictos.

6. POLÍTICA ANTISOBORNO, ANTIFRAUDE, ANTIPIRATERÍA Y DE INTEGRIDAD COMPROMISO ANTISOBORNO Y ANTIFRAUDE

La CRA, buscando una gestión transparente y eficaz, se compromete a adoptar prácticas de buen gobierno que permitan prevenir y detectar potenciales situaciones de soborno, fraude y conductas

irregulares en el accionar de la Entidad. Del mismo modo, cada una de las actividades, planes y programas emprendidos se realizarán en el marco de los valores y la integridad aplicadas en el código de integridad de la **CRA**, cumpliendo además los lineamientos y leyes antisoborno, anticorrupción y antifraude.

DESARROLLO DE LA POLÍTICA

La política antisoborno y antifraude es parte integral del Plan Anticorrupción y de Atención al Ciudadano de la CRA, la cual se encuentra articulada con el Código de Integridad y Buen Gobierno, documentos que generan estrategias y actividades encaminadas a la lucha contra la corrupción y la transparencia en las actuaciones de los colaboradores de la entidad.

Frente a la lucha contra la corrupción y cero tolerancias a actos de soborno y fraude la entidad se compromete a:

- Gestionar los riesgos de corrupción y sobornos asociados a actividades relacionadas con la misionalidad y que tenga vinculación con terceros.
- Contar con controles internos que permitan la mitigación o la detección de actividades que ponen en riesgo las buenas conductas y el buen accionar de la entidad.
- Promover una cultura de integridad basada en la prevención, mitigación y tratamiento de posibles riesgos de corrupción y soborno.
- Evitar cualquier conduta que pueda afectar el desarrollo transparente de su misionalidad.
- Proteger a los servidores públicos, contratistas y/o grupos de interés, ante cualquier represalia, como consecuencia de denuncias por prácticas que constituyan soborno.
- Garantizar la confidencialidad de los datos de quien reporte hechos de corrupción.
- Proteger la identidad de los informantes y de las personas que participan en la denuncia.
-

CONDUCTAS INDEBIDAS

De igual manera, los servidores públicos de la CRA evitarán y reportarán la realización de cualquiera de las siguientes prácticas, y de cualquier otra conducta que atente contra los deberes constitucionales y legales propios de los servidores públicos, así como contra los principios y propósitos del Código de Integridad y Buen Gobierno:

- Alterar o manipular la información financiera y contable, dando lugar a que refleje hechos que no correspondan con la realidad y a la normativa aplicable.
- Utilizar indebidamente bienes y/o recursos de la Entidad.
- Obtener mediante engaño, beneficios para sí o para terceros.
- Infringir las normas de protección a la protección intelectual y los derechos de autor, para lo cual la Entidad se compromete a excluir el uso de cualquier tipo de herramienta tecnológica que no esté debidamente licenciada, o a utilizar desarrollos intelectuales de expertos en temas regulatorios sin el debido reconocimiento de su autoría.
- Obtener de manera indebida y/o darle un uso inadecuado a secreto comercial y/o industrial del que sea titular cualquier persona natural o jurídica.
- Modificación de una base de datos.
- Entrega de información confidencial.
- Modificar actos administrativos en beneficio de un particular.
- Facilitar la adjudicación de un contrato a un particular.
- Direccionar las condiciones de contratación.
- Pérdida injustificada de expedientes o pérdida de documentos dentro de un expediente.

- Recibir documentos a la mano y cambiarlos dentro un expediente.

Para el cumplimiento de sus competencias institucionales, la CRA contará con una gestión transparente e íntegra en lo público, a través de la prevención de los comportamientos contrarios a éste, buscando que sus empleados y contratistas dirijan todos sus conocimientos y esfuerzos individuales a la gestión responsable de lo público y a la generación y arraigo de sentido de pertenencia.

A continuación, se expone la metodología a aplicar en esta política, en armonía con el Mapa de Riesgos de Corrupción de la **CRA.**

1. **Identificar puntos críticos:**

   - La omisión de poner en conocimiento a la Dirección de la entidad y a los entes competentes los presuntos actos de corrupción evidenciados en la evaluación del Sistema de Control Interno y/o denuncia por actos de corrupción.
   - Presiones de terceros o la falta de integridad, pueden dar lugar a una aplicación incorrecta de la normatividad que rige los procedimientos y las actuaciones administrativas de carácter particular.
   - La apropiación indebida de bienes y/ o recursos de la entidad por parte de un servidor público y/o un tercero.
   - Que el servidor público se apropie o use indebidamente en provecho suyo o de una tercera información de la Entidad.
   - El servidor público que en ejercicio de sus funciones intervenga en provecho suyo o de un tercero en las etapas precontractual, contractual y post contractual, con violación al régimen legal de la contratación pública.
   - Presiones de terceros o la falta de integridad, pueden dar lugar a una aplicación incorrecta de la normatividad que rige los procedimientos y las actuaciones administrativas de carácter general.

2. **Adopción de medidas de control:**

   Para dar respuesta a las señales de alerta anteriormente mencionadas, se contemplan las siguientes medidas a adoptar, las cuales apuntan a la prevención y mitigación del riesgo de la comisión del soborno:

   - Presentación de informes y seguimientos elaborados por Control Interno al Comité de Coordinación del Sistema, actividad incluida en el procedimiento de auditoría de gestión de la entidad.
   - Verificación del trabajo de campo adelantado por los funcionarios adscritos a Control Interno, por parte del asesor, de acuerdo con el procedimiento de auditoría de gestión de la entidad.
   - Revisión y validación de las actuaciones, y de la aplicación en ellas de los criterios técnicos y jurídicos que corresponden.

- Conciliación de saldos mensuales de la propiedad planta y equipo con la contabilidad (SIIF) y gestión de bienes (TRIDENT), pólizas vigentes que protejan los bienes de la entidad, conciliaciones bancarias y arqueos de fondo
- Establecer controles de acceso a la información de la entidad. Fortalecer los valores éticos en los funcionarios y contratistas.
- Aplicar los lineamientos internos para los procesos de contratación en la adquisición de bienes, obras y servicios. - Publicar los procesos de selección a través del SECOP. Cumplimiento del código de ética.
- Revisión y validación de las actuaciones, y de la aplicación en ellas de los criterios técnicos y jurídicos que corresponden

Para esto se ha creado el correo: **Red Interinstitucional de Transparencia y Anticorrupción**: soytransparente@cra.gov.co. Estos canales están comprometidos en la protección y anonimidad de los denunciantes.

CAPÍTULO IV

POLÍTICAS DE OPERACIÓN INSTITUCIONAL

1. POLÍTICA DE DERECHOS DE AUTOR

La presente política define los lineamientos que debe seguir la Comisión de Regulación de Agua Potable y Saneamiento Básico - CRA para la aplicación de derechos de autor. Lo anterior, con el fin de mantener un equilibrio apropiado entre los intereses de los titulares del derecho y los usuarios de contenidos protegidos, así como con las leyes sobre derecho de autor que permiten ciertas limitaciones respecto de los derechos patrimoniales, y en los casos en los que las obras protegidas pueden ser utilizadas sin autorización del titular de los derechos y contra el pago o no de una remuneración.

1.1. DEBERES

1.1.1. Tecnologías de Información:

Todo ordenador o dispositivo móvil debe tener software (programa de ordenador) con licencia de uso, que la entidad ha adquirido con el fin de lograr un resultado específico. En virtud de licencia de uso, a la CRA le es permitido:

- Hacer una fijación del programa en la memoria del computador (artículo 26 de la Decisión Andina 351 de 1993).
- Hacer una copia de seguridad o de backup (artículo 24 literal b) de la Decisión Andina de 1993)
- Hacer una adaptación del programa para su exclusiva utilización (artículo 24 de la Decisión Andina 351 de 1993).
- El representante legal de la CRA en sus informes de gestión dará noticia sobre el estado de cumplimiento de las normas sobre propiedad intelectual y derechos de autor por parte de la entidad.
- Respecto al uso de software gratis descargado de internet debe ser de uso libre y sin costo, siempre y cuando cuente con la previa autorización del líder de Tecnología de la Información (TI), para tal caso se debe realizar la solicitud mediante el HELPDESK en el apartado Software – Instalación.
- Se prohíbe a los contratistas y empleados la copia de archivos, programas informáticos u otro contenido que se encuentre en los diferentes ordenadores o dispositivos de la CRA sin previa autorización de los jefes de área, o facilitar su copia, su distribución o permitir descargas de contenido a terceros.

1.1.2. Seguridad de la información:

Toda información de la CRA que sea de su propiedad constituye un activo que debe protegerse de los riesgos que atentan contra su confidencialidad, integridad y disponibilidad. El incumplimiento a este deber de confidencialidad, le acarreará al contratista o empleado infractor la correspondiente responsabilidad por todos los perjuicios tanto patrimoniales como extrapatrimoniales que sufra la CRA. En la Página Web y la Intranet: Todos los derechos de los contenidos y las fotografías publicadas en el sitio Web CRA.GOV.CO e INTRANET.CRA.GOV.CO son propiedad de esta institución, o están autorizados por sus autores o referenciadas las fuentes de las cuales se extrajeron. Su uso y/o publicación está autorizado, con la consecuente incorporación de la fuente y enlace a la página principal.

2. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La CRA cuenta con dos sistemas de información, por un lado, el Sistema de Gestión Documental ORFEO, donde aparecen registrados los datos de las personas naturales como de los prestadores que se han obtenido por alguna solicitud o respuestas a los mismos y, de otra parte, el sistema SINFONIA que se sincroniza con el Sistema Único de Información (SUI) que contiene los datos de todos los prestadores de los servicios públicos de acueducto, alcantarillado y aseo.

2.1. DEBERES

En virtud de la presente política de tratamiento y protección de datos personales son deberes de la CRA los siguientes, sin perjuicio de las disposiciones previstas en la ley:

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Solicitar y conservar, copia de la respectiva autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente.
- Respetar las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados en los términos señalados por la ley.
- Identificar cuando determinada información se encuentra en discusión por parte del titular.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.
- Usar únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley 1581 de 2012.
- La CRA hará uso de los datos personales del titular solo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de datos personales.

2.2. AUTORIZACIONES Y CONSENTIMIENTO DEL TITULAR

Sin perjuicio de las excepciones previstas en la Ley, en el tratamiento de datos personales del titular se requiere la autorización previa e informada de éste, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

2.2.1. Medio y manifestación para otorgar la autorización del titular:

La CRA en los términos dispuestos en la Ley generó un aviso en el cual se comunica a los titulares que pueden ejercer su derecho al tratamiento de los datos personales a través de la página www.cra.gov.co, correo electrónico habeasdata@cra.gov.co las solicitudes registradas en el Sistema de Gestión Documental – ORFEO.

2.2.2. Eventos en los cuales no es necesaria la autorización del titular de los datos personales:

La autorización del titular de la información no será necesaria en los siguientes casos:

- Información requerida por una entidad pública o administrativa 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.

2.2.3. Personas a quienes se les puede suministrar la información:

La información que reúna las condiciones establecidas en la ley podrá suministrarse a las siguientes personas:

- A los titulares, sus causahabientes (cuando aquellos falten) o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el titular o por la ley.

2.3. PERSONA O ÁREA RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS RELACIONADOS CON LA PROTECCIÓN DE DATOS PERSONALES

La CRA ha designado como área responsable de velar por el cumplimiento de esta política al interior de la institución a la Dirección Ejecutiva, con el apoyo de la Oficina Asesora Jurídica, áreas funcionales que manejan los datos personales de los titulares y profesionales en seguridad de la información. Esta dependencia estará atenta para resolver peticiones, consultas y reclamos por parte de los titulares y para realizar cualquier actualización, rectificación y supresión de datos personales, a través del correo electrónico habeasdata@cra.gov.co

2.3.1. Procedimiento para la atención de consultas, reclamos y peticiones

2.3.1.1. Consultas:

- Los titulares o sus causahabientes podrán consultar la información personal del titular que repose en la CRA quien suministrará toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.
- La consulta se formulará a través del correo habeasdata@cra.gov.co.
- La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

2.3.1.2. Reclamos:

El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante la CRA el cual serán tramitados bajo las siguientes reglas:

- El reclamo del titular se formulará mediante solicitud dirigida a la CRA por el correo electrónico habeasdata@cra.gov.co con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
- Una vez recibido el correo habeasdata@cra.gov.co con el reclamo completo, éste se catalogará con la etiqueta "reclamo en trámite" y el motivo del mismo en un término no mayor a dos (2) días hábiles. Dicha etiqueta 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. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

2.3.1.3. Petición de actualización, rectificación y supresión de datos

La CRA rectificará y actualizará, a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados, para lo cual el titular allegará la solicitud al correo electrónico habeasdata@cra.gov.co indicando la actualización, rectificación y supresión del dato y aportará la documentación que soporte su petición.

2.3.1.4. Revocatoria de la autorización y/o supresión del dato

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual, para ello la CRA pondrá a disposición del titular el correo electrónico habeasdata@cra.gov.co. Si vencido el término legal respectivo, la CRA según fuera el caso, no hubiera eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

3. POLÍTICA DE SERVICIO AL CIUDADANO

1. INTRODUCCIÓN

La Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA), es una entidad del orden nacional, adscrita al Ministerio Vivienda, Ciudad y Territorio-MVCT, con autonomía administrativa, técnica y patrimonial, creada por la Ley 142 de 1994 con el fin de regular los monopolios en la prestación de los servicios públicos domiciliarios de acueducto, alcantarillado y aseo en Colombia, cuando la competencia no sea, de hecho, posible; y, en los demás casos, la de promover la competencia entre quienes presten servicios públicos, para que las operaciones de los monopolistas o de los competidores sean económicamente eficientes, no impliquen abuso de la posición dominante, y produzcan servicios de calidad.

Como parte del cumplimiento de este propósito, la entidad busca ofrecer y entregar a los usuarios de la CRA por medio de diferentes mecanismos, una experiencia de servicio orientada a resolver y facilitar la atención de peticiones, quejas, recursos, solicitudes y denuncias con calidad, oportunidad y efectividad, para lo cual se incorpora la presente política institucional la cual facilitará al ciudadano el acceso a sus derechos mediante el despliegue de diversos y distintos canales de atención.

La presente política se encuentra soportada en la Constitución Política de Colombia, alineada con el Plan Nacional de desarrollo 2018-2022 “Pacto por Colombia, pacto por la equidad” y el Modelo Integrado de Planeación y Gestión - MIPG, con sus componentes de mejora de procesos y procedimientos, cultura de servicio al ciudadano, medición de la calidad del servicio e información confiable; así como con los lineamientos de la política pública de servicio al ciudadano del Departamento Administrativo de la Función Pública -DAFP.

2. MARCO NORMATIVO

Cualificación Servicio al Ciudadano	Constitución Política de 1991	Guía de Perfiles y Vinculación / Guía de Unidades por competencias / Pensum cultura al servicio
	Ley 909 de 2004	
	Ley 1437 de 2011	
	Decreto 1083 de 2015	
	Decreto 815 de 2018	
Atención Peticiones, quejas, reclamos y denuncias	Constitución Política de 1991	Caracterización de ciudadanos, usuarios y grupos de interés / Modelo Carta de Trato Digno / Mecanismos de atención diferencial / Planes de contingencia
	Ley 190 de 1995	
	Ley 594 de 2000	
	Ley 1437 de 2011	
	Ley 1474 de 2011	
	Ley 1755 de 2015	
	Ley 1952 de 2019	
	Decreto 2641 de 2012	
Racionalización de Trámites	Ley 962 de 2005	Ley Anti-trámites / Racionalización de trámites / Directrices de accesibilidad web
	Ley 1955 de 2019	
	Ley 2052 de 2020	
	Decreto Ley 019 de 2012	
	Decreto Ley 2106 de 2019	
	Decreto 1450 de 2012	
	Resolución 1519 de 2020	
	CONPES 3292 de 2004	
Transparencia	Ley 1712 de 2014	Acceso a la información / Gestión documental
	Ley 1757 de 2015	
	Decreto 103 de 2015	
Sistema de Gestión de Calidad	Ley 87 de 1993	Lineamientos mediciones de percepción ciudadana
	Ley 489 de 1998	
	Ley 1955 de 2019	
	Decreto Ley 2106 de 2019	
	Decreto 4110 de 2004	
	Decreto 943 de 2014	
	Decreto 1083 de 2015	
	Decreto 1499 de 2017	
Accesibilidad	Ley 361 de 1997	NTC 6047 / Diagnóstico espacios físicos de atención al ciudadano /
	Ley 1145 de 2007	

	Ley 1287 de 2009	Protocolos de servicio al ciudadano/ Manual de atención incluyente / Guía de lenguaje claro / Accesibilidad de infraestructura / Repositorio Jurídico
	Ley 1306 de 2009	
	Ley 1346 de 2009	
	Ley 1618 de 2013	
	Ley 1996 de 2019	
	Decreto 19 de 2012	
	Decreto 103 de 2015	
	NTC 6047 de 2013	
Habeas Data	Ley 1581 de 2012	Hoja de ruta diseño Política de Tratamiento de Datos Personales / Autodiagnóstico bases de datos
	Decreto 1377 de 2013	
Planeación y gestión	Decreto 1499 de 2017	Modelo Integrado de Planeación y Gestión – MIPG
Legalidad, emprendimiento y equidad	Ley 1955 de 2019	Plan Nacional de Desarrollo 2018-2022.

3. DIRECCIONAMIENTO ESTRATÉGICO INSTITUCIONAL

MISIÓN: La Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA) es la entidad del orden nacional, encargada de promover la competencia y regular las condiciones del mercado, para mejorar la calidad y eficiencia en la prestación de los servicios de Acueducto, Alcantarillado y Aseo en Colombia, impulsar el bienestar social y el desarrollo sostenible, apoyado en un equipo

VISIÓN: En el año 2024, la Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA), apoyada en un equipo humano altamente calificado y articulada con sus grupos de interés, será reconocida a nivel nacional e internacional, como referente técnico regulatorio y agente transformador del mercado de los servicios públicos de Acueducto, Alcantarillado y Aseo, con énfasis en la sostenibilidad económica, social y ambiental.

POLÍTICA DE CALIDAD:

La Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA, está comprometida con la integración de todas las partes interesadas en el proceso de toma de decisiones regulatorias, a través de la prestación de un servicio calificado y oportuno orientado a satisfacer las necesidades de la ciudanía y del sector. Para lograrlo, la CRA protege la seguridad, salud y el bienestar de sus servidores y contratistas, identifica los peligros, evalúa y valora los riesgos, aplicando los respectivos controles, gestionando la ciber-resiliencia, la seguridad y privacidad de la información e implementando acciones orientadas a la mejora continua de su Sistema Integrado de Gestión y Control en el marco de la normatividad aplicable. Lo anterior, de la mano de un equipo de trabajo comprometido y calificado.

Dentro de los objetivos estratégicos institucionales se encuentra el fortalecimiento institucional, orientado al componente de servicio al ciudadano el cual cita: *Fortalecer la gestión institucional con base en su independencia y capacidad técnica y así los agentes del sector reconozcan a la entidad, como eficiente, moderna y con un capital humano valioso*.1

4. POLÍTICA INSTITUCIONAL DE SERVICIO AL CIUDADANO

De conformidad con lo anterior se definió una política institucional de servicio al ciudadano de la Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA) así:

[1] Plan Estratégico Quinquenal, Comisión de Regulación de Agua Potable y Saneamiento Básico CRA.

4.1 DECLARACIÓN DE LA POLÍTICA INSTITUCIONAL DE SERVICIO AL CIUDADANO

La Comisión de Regulación de Agua Potable y Saneamiento Básico – CRA, promueve una cultura de servicio al ciudadano facilitando el acceso a la información y orientación de manera completa, clara, con igualdad, moralidad, economía, celeridad, imparcialidad, eficiencia, transparencia, consistencia, calidad y oportunidad, que garantice los derechos fundamentales teniendo presente las necesidades, realidades y expectativas de los ciudadanos, mejorando así los niveles de satisfacción de los servicios prestados.

4.2 OBJETIVO

Garantizar al ciudadano el acceso a trámites y servicios que sean "*incluyentes, dignos, efectivos, oportunos, claros, transparentes, imparciales y de calidad*"[2], así como atender las necesidades de información y requerimientos de manera oportuna, optimizando la percepción y en nivel de satisfacción de los ciudadanos.

4.3 ALCANCE

La política institucional de Servicio al Ciudadano de la Comisión de Regulación de Agua Potable y Saneamiento Básico (CRA), será transversal a todos los procesos de la entidad, y contara con la participación de todos los servidores y contratistas que tengan relación directa o indirecta con el ciudadano por cualquiera de los canales de comunicación, así mismo, el grupo de atención al ciudadano lidera la implementación, seguimiento y evaluación de la presente política, con el fin de verificar la confianza de los ciudadanos por la entidad y sus servidores públicos.

4.4 PRINCIPIOS

La política institucional de servicio al ciudadano de la Comisión de Regulación de Agua Potable y Saneamiento Básico **(CRA),** se basa en los siguientes principios que proporcionan lineamientos enfocados a la satisfacción del ciudadano:

[2] ABC del servicio al Ciudadano, DNP, p. 2

4.5 RESPONSABLES

Todo el personal de la entidad estará involucrado en la Política, con el fin de buscar el desarrollo de una cultura de servicio al ciudadano, sin embargo, se tendrán 3 actores directamente responsables así:

Director y asesores a través de sus dependencias	Comité Institucional	Grupo de Atención al Ciudadano
•Garantizan el desarrollo e implementación de la política de servicio al ciudadano, promueven cultura organizacional orientada al servicio al ciudadano y aseguran recursos para el cumplimiento de la política. •Facilitan el acceso de los ciudadanos a la información y orientación, oportuna, clara, transparente, imparcial, efectiva y de calidad de los planes, programas, proyectos, trámites y servicios ofrecidos por la **CRA**.	•Garantizan la armonización de recursos y esfuerzos institucionales enfocados a la mejora continua en el marco del MIPG, particularmente en las siguientes políticas de la relacion Estado - Ciudadano. •Transparencia y acceso a la información pública. •Racionalización de trámites. •Rendición de cuentas. •Participación ciudadana en la gestión.	•Lidera la formulación, seguimiento y evaluación de los componentes de servicio al ciudadano en el **Plan de acción institucinal y el Plan Anticorrupción de Atención al Ciudadano.**
Responsable de la implementación	**Coordinar la implementación**	**Liderazgo de la implementación**

*Fuente: Elaboración propia a partir del documento de actualización de lineamientos de la política pública de servicio al Ciudadano del DNP vigencia 2020.

5. LINEAMIENTOS ESTRATÉGICOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA

La presente política establece lineamientos estratégicos, con el fin de alinear el compromiso de todos los colaboradores de la CRA para garantizar la participación ciudadana y establecer un comportamiento y una visión compartida, para ello se dictan los siguientes lineamientos:

5.1 CARACTERIZACIÓN DE USUARIOS

Con el fin de atender los requerimientos de los ciudadanos de manera oportuna y bajo parámetros de calidad, se hace necesario identificar los usuarios y partes interesadas de forma periódica, para así entender las necesidades, expectativas y preferencias de éstos, de tal manera que los servicios de la entidad sean brindados de manera focalizada para responder satisfactoriamente a sus inquietudes, sugerencias, observaciones y lograr su participación activa e incluyente.

5.2 FORMACIÓN Y RETROALIMENTACIÓN DEL TALENTO HUMANO

Los servidores públicos de la CRA sin importar el área a la que pertenezcan recibirán formación y retroalimentación en relación con la atención al ciudadano, para fortalecer sus competencias y vocación hacia el servicio, haciendo énfasis en la normatividad vigente y el deber de ser proactivo en la atención y suministro de información a los ciudadanos y partes interesadas.

5.3 ¿COMUNICACIÓN ASERTIVA

La CRA promueve el lenguaje claro y comprensible entre los ciudadanos y los servidores públicos como una estrategia para garantizar que la información que se ofrezca a través de todos los canales institucionales sea homogénea, oportuna, objetiva, veraz, completa, actualizada, accesible, motivada y en lenguaje claro, donde el ciudadano sepa con certeza cuáles serán las condiciones de tiempo, lugar y modo en las que serán solucionados sus trámites e inquietudes.

5.4 ATENCIÓN INCLUYENTE Y ACCESIBILIDAD

Con el fin de proporcionar una información con las características del numeral anterior la entidad garantiza su acceso a todos ciudadanos, así como proporcionar atención especial y preferente para infantes, personas en situación de discapacidad, embarazadas, niños, niñas, adolescentes, adulto mayor y en general de personas en estado de indefensión y o de debilidad manifiesta, teniendo en cuenta los espacios físicos de la entidad.

5.5 PUBLICACIÓN DE INFORMACIÓN

La CRA, deberá publicar la información de interés de la entidad a través de su página web en la sección de transparencia, en lenguaje claro y de fácil acceso, consulta y descarga para el ciudadano.

5.6 MEDICIÓN DE SATISFACCIÓN Y PERCEPCIÓN DEL CIUDADANO

Anualmente se realizarán mínimo tres mediciones trimestrales de satisfacción y percepción sobre de la atención que se presta a los ciudadanos-clientes de la entidad. Igualmente se deben estructurar ejercicios de rendición de cuentas y espacios de participación ciudadana. Los resultados obtenidos servirán de insumo para tomar acciones de mejora en la atención al ciudadano.

5.7 SISTEMAS DE INFORMACIÓN

A través del sistema de información **ORFEO** se deberá realizar el registro ordenado y la gestión de todas las peticiones, quejas, reclamos, sugerencias y denuncias de los ciudadanos.

5.8 CANALES DE COMUNICACIÓN

Para una adecuada atención y servicio al ciudadano, la **CRA** debe establecer canales de comunicación que garanticen el contacto entre los ciudadanos y la entidad, estos **canales deben ser informados en el documento de Protocolo de servicio al ciudadano y en la página web de la entidad**, con el fin de facilitar la participación ciudadana, estos canales son:

Canal	Medio	Ubicación	Horario de Atención	Descripción
Correspondencia	Correo postal y certificado	Carrera 12 N° 97-80, Piso 2, Bogotá D.C., Colombia.	Días hábiles de lunes a viernes de 8:00 am a 4:00 pm	Recibe, radica y direcciona las comunicaciones que ingresan a la CRA
Atención Presencial	Atención personal	Carrera 12 N° 97-80, Piso 2, Bogotá D.C., Colombia.	Días hábiles de lunes a viernes de 8:00 am a 4:00 pm	Se brinda información de manera personalizada y se contacta con los asesores y/o profesionales de acuerdo a su consulta, solicitud, queja y/o reclamo.
Atención Telefónica	Línea Gratuita Nacional	01 8000 517565	Días hábiles de lunes a viernes de 8:00 am a 4:00 pm	Brinda información y orientación sobre trámites y servicios que son competencia de la CRA
	Línea fija desde Bogotá	Desde Colombia: (1) 4873820 / 4897640 y Desde el exterior: con +57(1) – Fax: (1) 4897650		
	Línea anticorrupción	4897640 Extensión 235		
Atención Virtual	Aplicativo página Web	www.cra.gov.co	24 horas, los requerimientos registrados por	

Canal	Medio	Ubicación	Horario de Atención	Descripción
			éste medio se gestionan dentro de días hábiles.	Para radicar PQRSD en línea, se accede con el link: http://www.cra.gov.co/es/atencion-a-la-ciudadania/pqr Así mismo, puedes estar pendiente del trámite de su solicitud en el siguiente link: http://www.cra.gov.co/es/atencion-a-la-ciudadania/pqr/seguimiento-pqr
	Chat	www.cra.gov.co/es/participacion/chat	Todos los martes de 8:00 am a 10:00 am	Orienta al ciudadano sobre información general de la entidad.
	Redes Sociales	twitter.com/cracolombiafacebook.com/Comisión de Regulación CRAyoutube.com/crapsbcol	Disponibilidad 24 horas, los requerimientos solicitados se direccionan a la Página Web para su radicación y posterior trámite	Esta dispuesto para fortalecer la imagen institucional de la entidad, relacionarse de una manera más ágil con el ciudadano y posicionar a la entidad.
	Correo electrónico	correo@cra.gov.co notificacionesjudiciales@cra.gov.co	24 horas Los requerimientos registrados por este medio se gestionan dentro de días y horarios hábiles y horarios.	Recibe, radica y direcciona las comunicaciones que ingresan a la CRA

6. ALINEACIÓN DE LA POLÍTICA INSTITUCIONAL DE SERVICIO AL CIUDADANO CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN MIPG

La planeación y ejecución de Modelo Integrado de Planeación y Gestión en cuanto a servicio al ciudadano en la CRA debe ser parte del reflejo del compromiso de los servidores con el ciudadano, que puedan satisfacer las necesidades, realidades y expectativas de los usuarios.

Es importante considerar que el cumplimiento de estos objetivos requiere de la formulación, implementación y gestión de actividades que involucran a todas las áreas a través de la interacción de los distintos procesos

Por tal motivo se definieron los siguientes lineamientos generales para la implementación:

1. Talento humano – como principal factor dinamizador de la gestión pública y conforme con lo dispuesto por el Modelo Integrado de Planeación y Gestión MIPG, este es el factor que facilita el éxito, la gestión y el logro de los objetivos y resultados de la entidad, razón por la cual para garantizar una adecuada calidad del servicio a la ciudadanía, los servidores de la CRA de todas las áreas, niveles y procesos, atendiendo las disposiciones del Decreto 815 de 2018 y la Resolución 667 de 2018 y las normas que los modifiquen o sustituyan, deben cumplir con las competencias comportamentales comunes, y siguiendo el enfoque de transversalidad de la política de servicio al ciudadano y la necesidad de garantizar la excelencia en la prestación del servicio en todos los momentos de interacción del ciudadano con el Estado. A través de las siguientes acciones:

Los servidores públicos que se encuentran en el primer nivel de servicio (contacto directo con los ciudadanos) deben:

- **a.** Conocer claramente los protocolos de atención para orientar a los ciudadanos, teniendo en cuenta criterios diferenciales cuando se trata de población vulnerable o de especial protección constitucional.
- **b.** Contar con el perfil adecuado y el conocimiento necesario sobre la entidad, en especial sobre sus funciones, estructura organizacional, portafolio de servicios y sus requisitos, normas que rigen el funcionamiento de la entidad, los canales de atención, procesos y flujos de información internos para resolver directamente el mayor número de inquietudes en este 12 primer nivel de servicio.
- **c.** Eliminar las barreras actitudinales que por diferentes criterios puedan generar discriminación respecto de cualquier grupo poblacional.

Frente a los servidores públicos que se encuentran fuera del primer nivel de atención (no tienen contacto directo con los ciudadanos):

- **a.** Responder las peticiones de conformidad con los lineamientos técnicos y jurídicos que rige el quehacer institucional.
- **b.** Participar en las jornadas de capacitación y sensibilización sobre la importancia del Servicio al Ciudadano como eje fundamental en la relación Estado – Ciudadano, la planeación institucional sobre esta política y los criterios de tiempo, modo y lugar establecidos por la entidad para dar respuesta a las PQRSD.
- **c.** Los servidores públicos que elaboran respuestas a los ciudadanos deberán implementar estrategias de Lenguaje Claro, respetando el rigor técnico y jurídico que exige determinada materia.[3]

2. Esquemas de reconocimiento e incentivos a los servidores públicos y equipos de trabajo que tienen relación directa con el ciudadano. A través del desarrollo de estrategias que permitan fortalecer las competencias comportamentales, académicas, funcionales y capacidades técnicas específicas requeridas por los funcionarios. Lo anterior a través de una estrategia de

[3] Documento Lineamientos de la Política Pública de servicio al ciudadano DNP, noviembre 2020.

capacitación, orientación, sensibilización e incentivos contemplada en el Plan Institucional de Capacitación y Plan de Incentivos.

3. Caracterización de usuarios. Para atender de manera oportuna y bajo parámetros de calidad los requerimientos de los ciudadanos, se hace necesario identificar las necesidades, expectativas y preferencias de los grupos de valor de la entidad con el fin de adecuar la oferta institucional y la estrategia de servicio al ciudadano y de esta manera garantizar el efectivo ejercicio de sus derechos.

4. Adecuación de la prestación del servicio. Las preferencias y necesidades de los grupos de valor, identificadas a través de la caracterización de usuarios y ejercicios de evaluación participativa de la oferta institucional serán el insumo principal para adecuar los trámites y los servicios ofertados por la entidad.

5. Acceso a la información. La divulgación proactiva de la información pública y la respuesta de manera ágil, oportuna, eficaz, clara y accesible a las solicitudes de información realizadas por los usuarios es una función permanente por parte de los funcionarios de la entidad.

6. Uso del lenguaje claro estado - ciudadano. La comunicación entre los ciudadanos y las entidades del Estado es el medio que permite que el ejercicio de derechos de los ciudadanos sea efectivo. La información que se transmita a través de todos los canales institucionales debe ser en lenguaje claro, oportuna, objetiva, veraz, completa, actualizada y accesible.

7. Accesibilidad a espacios físicos de la entidad. Todos los ciudadanos, con independencia de sus características (menor de edad, adulto mayor, mujer embarazada, persona de talla baja o en condición de discapacidad, entre otros) tienen el derecho a acceder en igualdad de condiciones a los servicios que presta la entidad.

8. Gestión de valores para resultados:

De la ventanilla hacia adentro:

- **a.** Estructura organizacional adecuada que permite el cumplimiento misional.
- **b.** Procesos y procedimientos claramente definidos y generan valor en el cumplimiento de los objetivos misionales.
- **c.** Talento humano suficiente y calificado para garantizar la atención requerida.
- **d.** Sistemas de información que facilitan la interacción con los ciudadanos y simplifican los trámites.

e. Herramientas tecnológicas que integran, automatizan facilitando la gestión interna.
f. Canales de atención que garantizan la accesibilidad.

De la ventanilla hacia afuera:

a. Información disponible para los ciudadanos actualizada de manera permanente, es homogénea y clara.
b. La entidad se comunica con sus grupos de valor de manera precisa, certera y clara.
c. El acceso físico y virtual al portafolio de servicios de la entidad atiende a las necesidades de los grupos de valor.
d. La entidad garantiza la accesibilidad de los canales de atención y de los medios dispuestos para que los ciudadanos accedan a la información teniendo en consideración sus características especiales.
e. La entidad fortalece los procesos de peticiones optimizando el proceso interno de respuesta, los controles a los mismos y el seguimiento por parte de los usuarios para garantizar los términos y la calidad requerida.

7. PLANES DE ATENCIÓN AL CIUDADANO PARA IMPLEMENTACIÓN DE LA POLÍTICA

7.1 DEFINICIÓN

La definición de las actividades del componente de servicio al ciudadano se realizará anualmente por el Grupo de Atención al Ciudadano, en el Plan Anticorrupción y de Atención al Ciudadano PAAC y el Plan de Acción Institucional (PAI), conforme lo dispuesto en el Decreto 612 de 2018, para que de esta manera se garantice su ejecución y la disponibilidad de recursos, así como el seguimiento a la implementación de las mismas.

Su finalidad es plantear actividades trasversales dentro de la entidad con un compromiso por parte de la alta dirección para realizar un efectivo seguimiento y control a las actividades y la gestión de recursos necesarios para su ejecución, adicionalmente se requiere la participación activa de todas las dependencias para el cabal cumplimiento.

7.2 MEDICIÓN DEL SERVICIO

Teniendo en cuenta que la percepción de los ciudadanos es la base que permite identificar las principales oportunidades de mejora y tener retroalimentación sobre la atención al ciudadano en la entidad, la medición de percepción debe ser un ejercicio constante.

En cumplimiento de esta premisa, el Grupo de Atención al Ciudadano definirá los lineamientos detallados para la aplicación de estas mediciones, a través de la utilización de herramientas como:

a. Buzones de quejas, reclamos, sugerencias y felicitaciones
b. Encuestas de satisfacción frente al desarrollo de trámites y servicios
c. Desarrollo de ejercicios de cliente incógnito
d. Otros instrumentos que se consideren pertinentes

7.3 SEGUIMIENTO

El seguimiento se desarrollará a través de las acciones definidas anualmente en el Plan Anticorrupción y de Atención al Ciudadano (PAAC) y el Plan Anual Institucional (PAI).

Se realizará a través de análisis sistemáticos y periódicos de la gestión y los resultados obtenidos en el ejercicio de participación ciudadana con el propósito de establecer acciones para una mejora continua en la calidad de la información suministrada y una adecuada ejecución de las estrategias institucionales implementadas para garantizar la participación ciudadana en la Entidad.

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

1. INTENCIÓN DE LA ALTA DIRECCIÓN

La CRA se compromete a realizar gestión de los riesgos relacionados con las actividades ejecutadas por la entidad para garantizar el cumplimiento de los objetivos institucionales, adoptando diversos mecanismos de transparencia en la gestión. Los equipos operativos de los procesos son los responsables de identificar los riesgos de los procesos, así como de formular los controles para mitigarlos y documentar los avances, no obstante, estos deberán ser verificados y aprobados por el jefe de cada oficina. El líder de cada sistema de gestión se asesorará sobre la implementación de la metodología de administración de riesgos y hará seguimiento al reporte de avance documentado desde cada dependencia. Para el caso de los riesgos de corrupción, la Unidad de Control Interno realizará sensibilizaciones y capacitaciones en la administración de riesgos con énfasis en controles, la prevención del fraude, el buen gobierno, la rendición de cuentas, las prácticas éticas y las políticas anticorrupción.

2. OBJETIVO

Establecer el marco general para la administración de los riesgos en la Comisión de Regulación de Agua Potable y Saneamiento Básico, orientando las acciones necesarias que conduzcan a disminuir la vulnerabilidad de la entidad frente a situaciones que puedan interferir en el logro de su misionalidad y objetivos institucionales.

3. ALCANCE

La política de riesgos es aplicable a todos los procesos, proyectos y a las demás actividades realizadas por los funcionarios y contratistas durante el ejercicio de sus funciones. Inicia con el contexto de la situación del proceso y finaliza con los seguimientos periódicos establecidos.

4. MARCO NORMATIVO

Ver normograma del proceso de evaluación y control.

5. DOCUMENTOS RELACIONADOS

Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

Guía Técnica Colombiana GTC 45".

6. FACTORES DE RIESGO

La identificación de los riesgos de gestión, corrupción y seguridad digital en la operación de los procesos se obtiene a partir del análisis del contexto de la entidad, utilizando el documento GSM-FOR16 Formato identificación de contexto por proceso.

Para la identificación de los riesgos que pueden afectar los diferentes procesos de la entidad, se contemplaron los siguientes factores:

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	• Falta de procedimientos • Errores de grabación en reuniones presenciales y virtuales • Errores en cálculos para pagos internos y externos • Errores en la aplicación de procedimientos • Desactualización de documentos • Fallas en los canales de comunicación
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	• Falta de capacitación, temas relacionados con el personal • Posibles comportamientos no éticos de los empleados o contratistas • Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	• Daño de equipos • Caída de aplicaciones • Caída de redes • Errores en programas • Virus • Fallas de interoperabilidad
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	• Derrumbes • Incendios • Inundaciones • Daños a activos fijos

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Evento externo	Situaciones externas que afectan la entidad.	• Suplantación de identidad • Asalto a la oficina • Atentados, vandalismo, orden público • Disminución del presupuesto • Cambio de planes y programas del Gobierno Nacional • Sucesos que afecten la imagen institucional

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Página 36.

7. RESPONSABILIDADES

De acuerdo con la Guía de administración de riesgos, las responsabilidades para la gestión, evaluación y seguimientos de riesgos son:

LÍNEA DE DEFENSA	RESPONSABLES	ACTIVIDADES
Línea estratégica	Alta dirección, Comité de Coordinación del Sistema de Control Interno y Comité	• Establecer la Política de Administración del Riesgo. • Hacer seguimiento de los riesgos en el Comité Institucional de Gestión y Desempeño.

LÍNEA DE DEFENSA	RESPONSABLES	ACTIVIDADES
	Institucional de Gestión y Desempeño	• Hacer seguimiento al mapa de riesgos en el Comité de Coordinación de Control Interno. • Monitorear la efectividad de la gestión de riesgos y controles de la entidad. • Aprobar el plan de continuidad del negocio de la entidad.
Primera Línea de defensa	Líderes de proceso	• Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora, que pueden afectar el logro de los objetivos institucionales • Definir y diseñar los controles a los riesgos incluidos los de corrupción. • Informar a la OAP cuando se materialice un riesgo • Socializar y delegar en su equipo de trabajo las actividades concretas para la debida administración de riesgo. • Presentar justificación ante el Comité Institucional de Gestión y Desempeño cuando se presente una actividad de control vencida o plazo de ejecución vencido. • Presentar ante el Comité Institucional de Gestión y Desempeño justificación y plan de mejoramiento cuando se presente materialización de un riesgo.
Segunda Línea de defensa	Jefe de la Oficina Asesora de Planeación y TIC´S, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comité de contratación	• Soporta y guía la línea estratégica y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y llevar a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. • Hacer seguimiento y presentar la gestión de los riesgos al Comité

LÍNEA DE DEFENSA	RESPONSABLES	ACTIVIDADES
		Institucional de Gestión y Desempeño. • Supervisar la adecuada ejecución de los controles y si se detectan oportunidades de mejora, documentarlas.
Tercer Línea de defensa	Unidad de control interno	• Provee aseguramiento (evaluación) independiente y objetiva sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales, de proceso y de prevención de la corrupción. • Comunicar al Comité de Coordinación del Sistema de Control Interno posibles cambios e impactos en la evaluación de los riesgos detectados en las auditorías. • Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas

8. ANÁLISIS Y CALIFICACIÓN DE RIESGOS

Riesgo de gestión

Ahora bien, teniendo claridad sobre los factores de riesgo que se deben considerar en su gestión, se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto con el fin de estimar la zona de riesgo inicial (Riesgo inherente):

Probabilidad

ACTIVIDADES RELACIONADAS CON LA GESTIÓN

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Como referente, a continuación, se muestra una tabla de actividades relacionadas con la gestión de procesos, bajo las cuales se definen las escalas de probabilidad:

ACTIVIDAD	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD FRENTE AL RIESGO
Seguimiento Plan Acción Institucional	Mensual	Media
Seguimiento Plan de mejoramiento Institucional	Semestral	Muy Baja
Vinculación de personal	Semestral	Muy Baja
Liquidación de Nómina	Mensual	Media
Seguimiento Plan Institucional de capacitación y Bienestar social	Semestral	Muy Baja
Seguimiento a las decisiones de Gestión regulatoria	Mensual	Media
Representación en actuaciones administrativas o judiciales	Mensual	Media
Conciliaciones de Tesorería	Mensual	Media
Recaudo de Contribución	Mensual	Media
Transacciones, hechos y operaciones contables	Mensual	Media
Evaluación del Sistema de Control Interno	Semestral	Muy Baja
Custodia y preservación documental	Mensual	Media
Perdida de información	Semestral	Muy Baja

ACTIVIDAD	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD FRENTE AL RIESGO
Clasificación documental	Semestral	Muy Baja
Seguimiento Proyectos regulatorios de Agenda regulatoria Indicativa	Mensual	Media
Requerimientos GLPI de Tecnología	Trimestral	Baja
PQRSD	Anual	Muy Baja

CRITERIO PARA DEFINIR PROBABILIDAD

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 10 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 11 a 30 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 31 a 200 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 201 veces por año	100%

Impacto

Después de conocer los criterios y aplicación de la probabilidad se establecen los criterios de impacto que facilitarán al líder del proceso su aplicación, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Se debe tener en cuenta en el evento que se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

CRITERIO PARA DEFINIR IMPACTO

	AFECTACIÓN PRESUPUESTAL DE GASTOS ANUAL	REPUTACIONAL
Leve 20%	Afecte la ejecución presupuestal en un valor menor al 1%	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Afecte la ejecución presupuestal en un valor igual o mayor al 1% y menor al 10%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, Comités.
Moderado 60%	Afecte la ejecución presupuestal en un valor igual o mayor al 10% y menor al 20%	El riesgo afecta la imagen de la entidad con algunos grupos de valor frente al logro de los objetivos.
Mayor 80%	Afecte la ejecución presupuestal en un valor igual o mayor al 20% e inferior al 50%	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel sectorial.
Catastrófico 100%	Afecte la ejecución presupuestal en un valor igual o superior al 50%	El riesgo afecta la imagen de la entidad a nivel nacional e internacional.

Riesgos de seguridad digital

Antes de iniciar la identificación de riesgos de seguridad digital, se debe considerar como insumo la matriz activos de información identificados por cada proceso, como resultado de la valoración del activo.

La identificación de riesgos consiste en identificar las amenazas y vulnerabilidades de cada uno de los diferentes activos, para lo cual se tomarán como base los siguientes listados de amenazas y vulnerabilidades:

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.

Tipo de activo	Ejemplos de amenazas	Ejemplos de vulnerabilidades
Hardware	Robo o pérdida de medios o documentos	Almacenamiento de medios sin protección
Software	Ataque cibernético	Ausencia de parches de seguridad
Red	Escucha encubierta (chuzada)	Líneas de comunicación sin protección

Información	Robo o pérdida de información	Falta de controles de acceso físico
Personal	Error en el uso	Falta de capacitación en el manejo de las herramientas
Organización	Abuso de los derechos	Ausencia de políticas de seguridad

Amenazas Comunes:

Tipo	Amenazas	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la Información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no Autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
	Error en el uso o abuso de derechos	D, F

Tipo	Amenazas	Origen
Compromiso de las funciones	Falsificación de derechos	D

Origen: Deliberadas (D), fortuito (F) o ambientales (A).

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros:

Fuente de Amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso Ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información	Crimen por computador
	Divulgación ilegal de la información	Acto fraudulento
Terrorismo	Chantaje	Ataques contra el sistema DDoS
	Destrucción	Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ganancia monetaria	Chantaje

Vulnerabilidades:

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética

Tipo	Vulnerabilidades
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio

Tipo	Vulnerabilidades
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso
	aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

Lluvia de ideas: Mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la entidad pública o en el sector. Deben existir un orden de la sesión, un líder y personas que ayuden con la captura de las memorias.

Juicio de expertos: A través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración.

Análisis de escenarios: En este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: explosión de un pozo, sobrecarga de un nodo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué puede llegar a suceder, desde la perspectiva digital, a los activos de información y las consecuencias de la afectación.

Otras técnicas que pueden ser empleadas son: entrevistas estructuradas, encuestas o listas de chequeo.

REGISTRO Y REPORTE DE INCIDENTES DE SEGURIDAD DIGITAL

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Impacto

Para realizar el análisis de riesgos de seguridad digital se deben tener presente la confidencialidad, integridad, disponibilidad y así como otras variables que se deben tener presentes como la norma ISO 27001:2013, la Ley 1712 de 2014 y la Ley 1581 de 2012.

Requerimientos de seguridad – Confidencialidad

La información debe estar debidamente protegida para que sea accedida por el usuario autorizado.

Pública	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
Clasificada	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
Reservada	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica
No Clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Conforme al Artículo 5° de la Ley 1581 de 2012, se consideran datos sensibles (o datos personales) “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 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”.

Requerimientos de seguridad – Integridad

Para calificar los requerimientos de integridad se debe tener presente que la información debe estar completa.

Requerimientos de seguridad- Disponibilidad

Para calificar los requerimientos de disponibilidad (consiste en garantizar que la información puede ser consultada por quien la solicite y cuando lo requiere.)

CRITERIO PARA DEFINIR PROBABILIDAD

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 10 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 11 a 30 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 31 a 200 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 201 veces por año	100%

TABLA 1. RIESGOS DE SEGURIDAD DIGITAL

TIPO DE RIESGO	VALOR DEL IMPACTO	VARIABLES	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO	MEDIO AMBIENTE	AFECTACIÓN ECONÓMICA
RIESGOS DE SEGURIDAD DIGITAL	Leve 20%	INTEGRIDAD		Información técnica regulatoria AAA inexacta que genera pérdida de imagen de la entidad a nivel de proceso.	No hay afectación medioambiental.	Afectación del presupuesto anual en un valor menor al 20%
		DISPONIBILIDAD / POBLACION	Interrupción de servicios tecnológicos ≤ 5% de los usuarios y/o beneficiarios basados en el catalogo de servicios tecnológicos ofertados.			
		CONFIDENCIALIDAD / REPUTACIONAL		El riesgo afecta la imagen de algún área de la organización.		
	Menor 40%	INTEGRIDAD		Información técnica regulatoria AAA inexacta que genera pérdida de imagen de la entidad a nivel organizacional. Información inexacta que genera problemas en la toma de decisiones en procesos de apoyo.	Afectación en caso de ocurrencia de hechos catastroficos, los cuales requieren ≥15 días para dar continuidad y garantizar la disponibilidad de los servicios tecnológicos que permitan la atención de los usuarios internos y externos.	Afectación del presupuesto anual en un valor igual o mayor al 21% y menor al 40%
		DISPONIBILIDAD / POBLACION	Interrupción de servicios tecnológicos 5.1% y 20% los usuarios y/o beneficiarios,basados en el catalogo de servicios tecnológicos.			
		CONFIDENCIALIDAD / REPUTACIONAL		El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, Comités.		
	Moderado 60%	INTEGRIDAD / AFECTACIÓN ECONÓMICA		Información técnica regulatoria AAA inexacta que genera pérdida de imagen de la entidad a nivel Bogotá. Información inexacta que genera problemas en la toma de decisiones en procesos misionales	Afectación en caso de ocurrencia de hechos catastroficos, los cuales requieren ≥ 4 semanas para dar continuidad y garantizar la disponibilidad de los servicios tecnológicos que permitan la atención de los usuarios internos y externos. o.	Afectación del presupuesto anual en un valor igual o mayor al 41 % y menor al 60%
		DISPONIBILIDAD / POBLACION	Interrupción de servicios tecnológicos 21% y 50% de los usuarios y/o beneficiarios, basados en el catalogo de servicios tecnológicos ofertados.			
		CONFIDENCIALIDAD / REPUTACIONAL		El riesgo afecta la imagen de la entidad con algunos grupos de valor frente al logro de los objetivos.		
	Mayor 80%	INTEGRIDAD / AFECTACIÓN ECONÓMICA		Información técnica regulatoria AAA inexacta que genera pérdida de imagen de la entidad a nivel nacional. Información inexacta que genera problemas en la toma de decisiones en procesos estratégicos.	Afectación en caso de ocurrencia de hechos catastroficos, los cuales requieren ≥ 6 meses para dar continuidad y garantizar la disponibilidad de los servicios tecnológicos que permitan la atención de los usuarios internos y externos.	Afectación del presupuesto anual en un valor igual o mayor al 61% e inferior al 80%
		DISPONIBILIDAD / POBLACION	Interrupción de servicios 51% y 80% de los usuarios y/o beneficiarios, basados en el catalogo de servicios tecnológicos ofertados.			
		CONFIDENCIALIDAD / REPUTACIONAL		El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel sectorial.		
	Catastrófico 100%	INTEGRIDAD / AFECTACIÓN ECONÓMICA		Información técnica regulatoria AAA inexacta que genera problemas en la toma de decisiones a nivel estado. Información inexacta que genera pérdida de imagen de la entidad a nivel internacional.	Afectación en caso de ocurrencia de hechos catastroficos, los cuales requieren ≥1 año para dar continuidad y garantizar la disponibilidad de los servicios tecnológicos que permitan la atención de los usuarios internos y externos.	Afectación del presupuesto anual en un valor igual o superior en 81%
		DISPONIBILIDAD / POBLACION	Interrupción de servicios tecnológicos mayores al 81% de los usuarios y/o beneficiarios, basados en el catalogo de servicios tecnológicos ofertados.			
		CONFIDENCIALIDAD / REPUTACIONAL		El riesgo afecta la imagen de la entidad a nivel nacional e internacional.		

Variables analizadas frente a tabla 1. riesgos digitales

1.Tipo de riesgos evaluados en este apartado están relacionados con los activos de información de la CRA que se ven involucrados dentro la seguridad digital.

2. Valor del impacto brindan una clasificación del riesgo definiéndolos en leve 20%, menor 40%, moderado 60%, mayor 80%y catastrófico 100%.

3. Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

4. La variable cuantitativa hace referencia a interrupción de los servicios tecnológicos que se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, en la población máxima estimada en el marco del catálogo del árbol de servicios TI [4] de la CRA, en el cual se prestan servicios tecnológicos o trámites en el entorno digital, ya sean internos o externos, para lo cual se analiza en la franja de tiempo de un (1) día.

5.La variable cualitativa hace referencia a la información técnica regulatoria AAA inexacta, la cual produce que haya una pérdida de imagen nacional, internacional y que a su vez dificultara la toma de decisión para el cumplimiento de sus objetivos, que pueden ser consultadas en plataformas tecnológicas en fuentes internas y externas. Una vez detectadas serán analizadas por el Comité Institucional de Gestión y Desempeño, el cual deberá indicar el nivel de afectación de la imagen institucional.

6. La variable ambiental estará alineada con la afectación de los servicios tecnológicos ante la materialización de los riesgos previamente identificados y cuantificados en el cuadro de variables de los riesgos digitales. Para efecto de probabilidad de ocurrencia, se debe considerar que esta variable podría no aplicar en la mayoría de los casos, pero se debe tener en cuenta dado el evento que se presente alguna catástrofe ambiental (terremotos, sismos, explosión e incendios entre otros).

La determinación del grado de afectación ambiental, está asociada a garantizar la continuidad de los servicios tecnológicos, sobre los cuales le permite a la CRA atender a los usuarios externos e internos, en donde el rol de la oficina asesora de planeación y TIC será definir técnicamente las soluciones tecnológicas y estratégicas para continuar operando y así garantizar los servicios, a pesar de la ocurrencia de dichos eventos; estas soluciones están sustentadas en la identificación de la necesidad, estudios previos del mercado. Teniendo en cuenta lo anterior la Subdirección administrativa y financiera conforme a la necesidad manifestada por parte de la OAP/TIC, validara la disponibilidad de los recursos presupuestales que permitan a la entidad la ejecución e implementación de todas las actividades propuestas.

---

4 Catalogo del árbol de servicios de TI contiene un conjunto de información de los servicios tecnológicos, los cuales buscan satisfacer la necesidad del cliente interno y externo, para lo cual se define la población máxima a satisfacer.

7. La variable de afectación económica es la consideración del presupuesto anual de la entidad debido a la materialización del riesgo, la cual contempla sanciones económicas e impactos directos en la ejecución presupuestal.

Riesgo de corrupción

Probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Impacto

RIESGOS DE CORRUPCIÓN	5	CATASTRÓFICO	Para calificar el impacto de los riesgos de corrupción deberá remitirse a los 19 criterios que se incluyeron en la matriz de los cuales: Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico. MODERADO: Genera medianas consecuencias sobre la entidad. MAYOR: Genera altas consecuencias sobre la entidad. CATASTRÓFICO: Genera consecuencias desastrosas para la entidad. NOTA: Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre
	4	MAYOR	
	3	MODERADO	

			serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos. Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera de impacto catastrófico.

CRITERIOS PARA CALIFICAR EL IMPACTO EN RIESGOS DE CORRUPCIÓN

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Es importante tener en cuenta que entre más respuestas afirmativas se den, así mismo el nivel de riesgos va aumentando. Por ejemplo: si la respuesta a las 19 preguntas son afirmativas será un impacto catastrófico.

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

NIVEL	IMPACTO	DESCRIPTOR
5	Moderado	• Afectación parcial al proceso y a la dependencia • Genera a medianas consecuencias para la entidad.
10	Mayor	• Impacto negativo de la Entidad • Genera altas consecuencias para la entidad.
20	Catastrófico	• Consecuencias desastrosas sobre el sector • Genera consecuencias desastrosas para la entidad.

9. NIVELES DE TRATAMIENTO DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL.

La guía presenta las siguientes estrategias para combatir el riesgo:

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Página 57.

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).
Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

*Ningún riesgo de corrupción podrá ser aceptado.
*Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad

Para la Comisión de Regulación de Agua Potable y Saneamiento Básico para el tratamiento de los riesgos se establece de la siguiente manera:

Nivel BAJO: se ACEPTARÁ el riesgo.
*Ningún riesgo de corrupción podrá ser aceptado.
*Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad

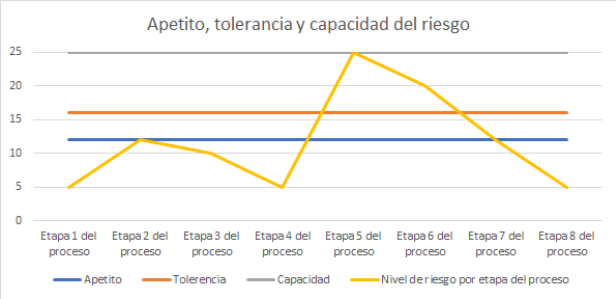
Nivel MEDIO O MODERADO: se REDUCIRÁ, EVITARÁ o COMPARTIRÁ el riego.

Nivel ALTO: se REDUCIRÁ, EVITARÁ o COMPARTIRÁ el riego.

Nivel EXTREMO o CATASTRÓFICO: se REDUCIRÁ, EVITARÁ o COMPARTIRÁ el riego.

APETITO, TOLERANCIA Y CAPACIDAD DEL RIESGO

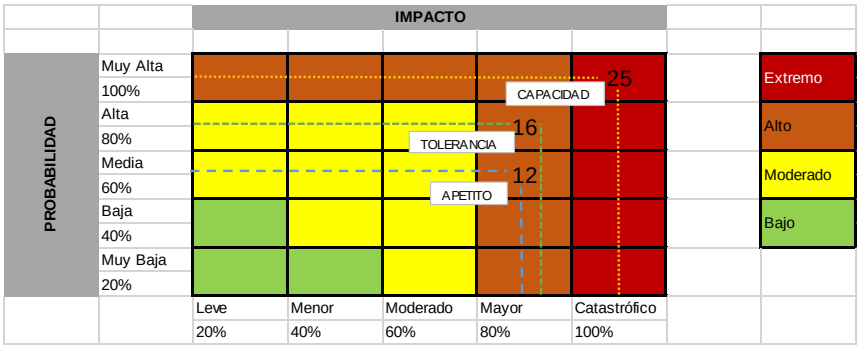
De acuerdo con lo revisado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, el apetito, tolerancia y capacidad del riesgo para la CRA será la misma para los riesgos de gestión, corrupción y seguridad digital y se calculó de la siguiente forma:



Elaborada por la Oficina Asesora de Planeación y Tic´s

- El apetito del riesgo corresponde a 12, valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.
- La tolerancia es 16, valor que es superior al apetito de riesgo y menor a la capacidad de riesgo.
- La capacidad del riesgo es 25, teniendo en cuenta qué es el valor máximo al combinar la escala de probabilidad e impacto.

Mapa de calor



Elaborada por la Oficina Asesora de Planeación y Tic´s

10. CLASIFICACIÓN DEL RIESGO

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

11. CLASIFICACIÓN ACTIVIDADES DE CONTROL

Tipologías de controles

Controles preventivos: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Controles Detectivos: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Controles Correctivos: Atacan el impacto frente a la materialización del riesgo.

Atributos para el diseño de controles

Características		
Atributos de eficiencia	Tipo	Preventivo
		Detectivo
		Correctivo
	Implementación	Automático
		Manual
***Atributos Informativos**	Documentación	Documentado
		Sin documentar
	Frecuencia	Continua
		Aleatoria
	Evidencia	Con registro
		Sin registro

*Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

La CRA para mitigar/tratar los riesgos de seguridad de la información empleará los controles del Anexo A de la norma ISO/IEC 27001:2013, considerando las características de diseño y ejecución definidas para su valoración.

12. INFORMACIÓN Y COMUNICACIÓN

Se realizarán divulgaciones de los lineamientos de los riesgos de gestión, corrupción y seguridad digital y así mismo de la matriz de identificación de peligros y valoración de riesgos de seguridad y salud en el trabajo establecidos en la entidad, los cuales se encuentran públicos en SharePoint para consulta y seguimiento.

13. MONITOREO Y ACTUALIZACIÓN DEL MAPA DE RIESGOS

El monitoreo del mapa de riesgos de gestión, corrupción y seguridad digital y la matriz de identificación de peligros y valoración de riesgos de seguridad y salud en el trabajo está a cargo de cada líder de proceso acorde con la periodicidad definida y de la Oficina Asesora de Planeación y TIC'S en su calidad de segunda línea de defensa.

1. El informe de seguimiento de riesgos de gestión y seguridad digital y de corrupción será presentado por la Oficina Asesora de Planeación y TIC'S y el seguimiento de los riesgos de seguridad y salud en el trabajo será presentado por la Subdirección Administrativa y Financiera en el Comité Institucional de Gestión y Desempeño una vez sea consolidado de manera semestral.

2. Por su parte, la Unidad de Control Interno realizará el seguimiento a los riesgos de corrupción de manera cuatrimestral y presentará los informes respectivos en el Comité de Coordinación del Sistema de Control Interno y serán publicados en la página web de la CRA.

3. Los líderes de los procesos actualizarán y aprobarán el mapa de riesgos (de gestión, seguridad digital y de seguridad y salud en el trabajo) por lo menos una vez cada año, dando cumplimiento a los lineamientos metodológicos establecidos en la presente política. Si por algún motivo, un líder de proceso identifica la necesidad de modificar los riesgos antes de este tiempo, podrá ajustar la información requerida y lo informará en el Comité Institucional de Gestión y Desempeño cuando los cambios correspondan a:
   a) Eliminación de alguno de los riesgos identificados
   b) Inclusión de un nuevo riesgo que ha evidenciado que podría impactar algún proceso crítico de la entidad

4. Si la necesidad de eliminar, incluir y/o modificar actividades de control es para los riesgos de corrupción, esta solicitud deberá escalarse al Comité Institucional de Gestión y Desempeño para su aprobación.

5. Los líderes de los procesos que requieran realizar algún ajuste al mapa de riesgos de gestión y seguridad digital y al mapa de riesgos de seguridad y salud en el trabajo, que no esté contemplado en los ítems 3 y 4, deberán informar a la Oficina Asesora de Planeación y TIC'S con la respectiva justificación, quien a su vez revisará y enviará al Equipo Facilitador para su revisión y sugerencias a la solicitud presentada. Finalmente, la OAP remitirá al líder del proceso para su aprobación y realizará la actualización en la carpeta de calidad el "Mapa de

riesgos" o "Mapa de riesgos SST" que se requiera. Es importante resaltar que estos ajustes podrán realizarse sin requerir para ello, la aprobación de alguna instancia de Comité.

Es importante recordar que los responsables de los riesgos deben realizar modificaciones a las actividades de control, plazo y soporte de actividad de control antes del vencimiento de estas.

Si se presenta alguna actividad de control vencida o plazo de ejecución vencido, el líder de proceso presentará su respectiva justificación ante el Comité Institucional de Gestión y Desempeño.

6. Una vez materializado un riesgo el líder del proceso deberá presentar ante el Comité Institucional de Gestión y Desempeño con la respectiva justificación y el plan de mejoramiento que se va a desarrollar de acuerdo con la materialización, para que los miembros tomen acciones pertinentes y estén al tanto del avance de cumplimiento y así mismo, determinar si las acciones propuestas eliminan el riesgo o se debe volver a realizar el análisis de riesgo con sus respectivos controles que eviten nuevamente la materialización.

   La OAP se encargará de hacer seguimiento al plan propuesto hasta la ejecución total del mismo.

   Nota: Es importante tener en cuenta que aquellos riesgos que no cuenten con soporte de las actividades de control no necesariamente serán un riesgo materializado, pero sí se debe revisar y valorar con el responsable del riesgo si esa actividad de control aporta al riesgo.

La CRA para su gestión de riesgos aplica las directrices de la Guía de Administración de Riesgos del DAFP y cada una de sus etapas se describe de manera detallada en el EVC-MAN Manual de administración de riesgos y de oportunidades, la cual se encuentra en la ruta: Sharepoint/calidad/Dirección Estratégica/ / EVC-MAN Manual de administración de riesgos y de oportunidades.

CAPÍTULO V

POLÍTICAS DE GESTIÓN DOCUMENTAL Y CERO PAPEL

1. POLÍTICA DE GESTIÓN DOCUMENTAL

A continuación, se documenta la Política de Gestión Documental para la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA, formulada en el marco de lo establecido en el artículo 2.8.2.5.6 del Decreto 1080 de 2015 y el numeral 6.1 y 6.2 de la Norma Técnica Colombiana NTC:2010.

La Comisión de Regulación de Agua Potable y Saneamiento Básico -CRA- con el propósito de salvaguardar el acervo documental que gestiona en el marco del cumplimiento de su propósito fundamental y de las funciones que le han sido asignadas por la Ley 142 de 1994, se propone adoptar los lineamientos establecidos en marco normativo y técnico que garantice la adecuada planeación, gestión, conservación, preservación y disposición para la consulta de los documentos de archivo físicos y electrónicos, así como a proporcionar las condiciones que permitan la modernización de su sistema de información para el apropiado desarrollo de la función archivística en la entidad, para lo cual:

Esto mediante la utilización de Tecnologías de Información en el marco del Sistema de Gestión de Calidad y el programa de gestión documental, brindando el debido manejo de seguridad de la información garantizando su autenticidad, fiabilidad y usabilidad en concordancia con la normatividad archivística emitida por el Archivo General de la Nación.

1.1. DESCRIPCIÓN GENERAL

La política de gestión documental en el Estado Colombiano, *acorde con el Artículo 2.8.2.5.6. Componentes de la política de gestión documental del Decreto 1080 de 2015,* debe ser entendida como el conjunto de directrices establecidas por una entidad para tener un marco conceptual claro para la gestión de la información física y electrónica, un conjunto de estándares para la gestión de la información en cualquier soporte, una metodología general para la creación, uso, mantenimiento, retención, acceso y preservación de la información, independiente de su soporte y medio de creación, un programa de gestión de información y documentos, una adecuada articulación y coordinación entre las áreas de tecnología, la oficina de archivo, las oficinas de planeación y los productores de la información. Esta política debe estar ajustada a la normativa que regula la entidad, alineada con el plan estratégico, el plan de acción y el plan institucional de archivos – PINAR y deberá estar documentada e informada a todo nivel de la entidad.

1.2. Marco conceptual claro para la gestión de la información física y electrónica de entidad.

En el Programa de Gestión Documental -PGD- de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA se registra el marco estratégico institucional, la estructura orgánico-funcional, las funciones de cada una de sus unidades administrativas, el mapa de procesos del

sistema de gestión de la calidad y los respectivos procedimientos mediante los cuales se desarrollan las funciones asignadas a la entidad.

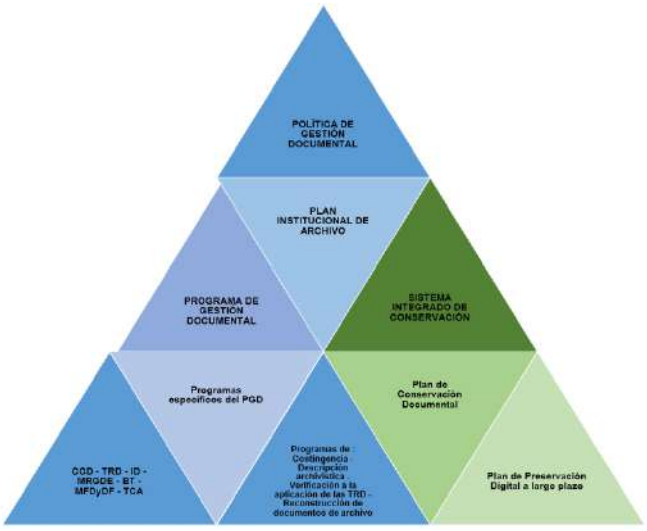


FIGURA 1. MARCO CONCEPTUAL PARA LA GESTIÓN DE INFORMACIÓN

El Plan Institucional de Archivos –PINAR: Es un instrumento para la planeación de la función archivística, el cual se articula con los demás planes y proyectos estratégicos previstos por la entidad. (http://www.archivogeneral.gov.co/pinar)[5]

El Programa de Gestión Documental – PGD: es estratégico para la gestión documental, pues con él se establecen las estrategias que permitan a corto mediano y largo plazo, la implementación y el mejoramiento de la prestación de servicios, desarrollo de los procedimientos, la implementación de programas específicos del proceso de gestión documental. El PGD hace parte del Plan Estratégico Institucional y del Plan de Acción Anual, es aprobado por el Comité de Desarrollo Administrativo y está armonizado con los otros sistemas administrativos y de gestión, establecidos por el gobierno nacional, dando alcance al cumplimiento a la aplicación de la normatividad vigente en la materia. (http://www.archivogeneral.gov.co/pgd)[6]

Las Tablas de Retención Documental –TRD: constituyen un instrumento archivístico que permite la clasificación documental de la entidad, acorde con su estructura orgánico - funcional, e indica los criterios de retención y disposición final resultante de la valoración documental por cada una de las agrupaciones documentales. (http://www.archivogeneral.gov.co/trd)[7]

[5] Colombia, Archivo General de la Nación, Plan Institucional de Archivo-PINAR.
[6] Colombia, Archivo General de la Nación, Programa de Gestión Documental-PGD.
[7] Colombia, Archivo General de la Nación, Tablas de Retención Documental-TRD.

1.3. CONJUNTO DE ESTÁNDARES PARA LA GESTIÓN DE LA INFORMACIÓN EN CUALQUIER SOPORTE.

Estándares internacionales.
Desde el punto de vista funcional: (Ver Normograma)
Desde el punto de vista de la normalización archivística: (Ver Normograma).
Desde el punto de vista de la preservación: (Ver Normograma)
Desde el punto de vista de la seguridad INTERNACIONAL: (Ver Normograma)

Estándares Nacionales.
(Ver Normograma)

Normatividad Nacional relacionada con la gestión documental.
(Ver Normograma)

Normatividad Nacional relacionada con las Funciones de la Comisión de Regulación Nacional de Agua Potable y Saneamiento Básico CRA.
(Ver Normograma)

1.4. METODOLOGÍA GENERAL PARA LA CREACIÓN, USO, MANTENIMIENTO, RETENCIÓN, ACCESO Y PRESERVACIÓN DE LA INFORMACIÓN, INDEPENDIENTE DE SU SOPORTE Y MEDIO DE CREACIÓN.

Armonización entre: ISO 15489, Decreto 1080 de 2015 (Instrumentos archivísticos y programas específicos).

NORMA ISO 15489 Parte 2	Decreto 1080 de 2015 (antes Decreto 2609 de 2012)	Instrumentos Archivísticos	Programas específicos
4.3.2. Incorporación	a. Planeación	Plan Institucional de Archivos- PINAR	Programa de contingencia en archivos
	b. Producción	Programa de Gestión Documental – PGD Tabla de Retención Documental – TRD Bancos terminológicos de tipos, series y subseries documentales	Programa de normalización de formas y formulario electrónico Programa de documentos vitales o esenciales
4.3.3. Registro	c. Gestión y trámite	Tabla de Retención Documental – TRD Bancos terminológicos de tipos, series y subseries documentales Mapas de procesos, flujos documentales y la descripción de las funciones de las unidades administrativas Tablas de control de acceso	Programa de verificación a la aplicación de las TRD Programa de gestión de documentos electrónicos
4.3.4. Clasificación	d. Organización	Cuadro de clasificación documental-CCD Tabla de Retención Documental – TRD Inventario Documental	Programa de verificación a la aplicación de las TRD Programa de descripción archivística
4.3.5. Asignación de categorías de acceso y seguridad	c. Gestión y trámite	Mapas de procesos, flujos documentales y la descripción de las funciones de las unidades administrativas Tablas de control de acceso	Programa de verificación a la aplicación de las TRD
4.3.6. Identificación del tipo de disposición	f. Disposición de documentos	Tabla de Retención Documental – TRD	Programa de verificación a la aplicación de las TRD

NORMA ISO 15489 Parte 2	Decreto 1080 de 2015 (antes Decreto 2609 de 2012)	Instrumentos Archivísticos	Programas específicos
4.3.7. Almacenamiento	d. Organización	Tabla de Retención Documental – TRD Bancos terminológicos de tipos, series y subseries documentales	Programa de verificación a la aplicación de las TRD
	e. Transferencia	Tabla de Retención Documental – TRD	Programa de descripción archivística Programa de archivos descentralizados
	g. Preservación a largo plazo	Tabla de Retención Documental – TRD	Plan de preservación digital a largo plazo Programa de reprografía Programa de documentos especiales
4.3.8. Uso y trazabilidad	c. Gestión y trámite	Mapas de procesos, flujos documentales y la descripción de las funciones de las unidades administrativas Tablas de control de acceso	Programa de verificación a la aplicación de las TRD Programa de gestión de documentos electrónicos
4.3.9. Disposición	f. Disposición de documentos	Tabla de Retención Documental – TRD	Programa de verificación a la aplicación de las TRD
	g. Preservación a largo plazo	Modelo de requisitos para la gestión de documentos electrónicos	Plan de conservación documental Plan de preservación digital a largo plazo Programa de reprografía
	h. Valoración	Tabla de Retención Documental – TRD	Programa de auditoría y control

Tabla 21. Armonización entre ISO 15489 e Instrumentos

1.5. PROGRAMA DE GESTIÓN DE INFORMACIÓN Y DOCUMENTOS QUE PUEDA SER APLICADO EN CADA ENTIDAD.

La Comisión de Regulación de Agua Potable y Saneamiento Básico - CRA debe llevar a cabo la formalización del Sistema de Gestión Documental para lo cual requiere:

- Formular, aprobar, publicar, comunicar (a todo nivel en la organización) e implementar la política de gestión documental.
- Conformar un equipo interdisciplinario que apoye el desarrollo, implementación, control y seguimiento del Sistema de Gestión Documental.
- Formular, aprobar, publicar, comunicar (a todo nivel en la organización) e implementar los instrumentos archivísticos, y, si es necesario, actualizar los existentes.
- Formular, aprobar, publicar e implementar un Sistema Integrado de Conservación -SIC- que incluya el Plan de Conservación Documental y el Plan de Preservación Digital a largo plazo en armonía con lo prescrito en el Acuerdo 006 de 2014 del Archivo General de la Nación
- Elaborar el mapa de riesgos del Sistema de Gestión Documental formulando un plan de acción y el plan de trabajo respectivo encaminado a mitigar los riesgos identificados.
- Notificar sobre los beneficios frente a la gestión e integración del Sistema de Gestión Documental a los sistemas de gestión que componen el Sistema Integrado de Gestión de la Comisión de Regulación de Agua Potable y Saneamiento Básico CRA
- Comunicar a todos los funcionarios las razones por las que se requiere implementar el Sistema de Gestión Documental y los beneficios que este traerá para la entidad y los colaboradores.

1.6. LA COOPERACIÓN, ARTICULACIÓN Y COORDINACIÓN PERMANENTE ENTRE LAS ÁREAS DE TECNOLOGÍA, LA OFICINA DE ARCHIVO, LAS OFICINAS DE PLANEACIÓN Y LOS PRODUCTORES DE LA INFORMACIÓN.

Mediante la inclusión del sistema de gestión documental dentro de los componentes del sistema integrado de gestión, se podrá garantizar la coordinación y articulación de los sistemas que lo componen y aquellos que se vayan incorporando hasta lograr la completitud del Sistema Integrado de Gestión. Es importante tener en cuenta que la gestión documental se relaciona con el Sistema de Gestión de Calidad (SGC), el Sistema de Gestión de Seguridad de la Información (SGSI), el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG SST), el Sistema de Control Interno (SCI), el Modelo Estándar de Control Interno (MECI) y el Modelo Integrado de Planeación y Gestión (MIPG).

2. POLITICA DE GESTIÓN DE DOCUMENTO ELECTRÓNICO DE ARCHIVO

La Comisión de Regulación de Agua Potable-CRA, con el propósito de salvaguardar el acervo documental que la entidad produce y recibe en soporte electrónico, se propone adoptar buenas prácticas que garanticen el acceso, conservación e integridad de los documentos electrónicos de archivo; mediante lineamientos y directrices que aseguren el adecuado manejo de las herramientas tecnológicas, la seguridad de la información y fomentando la cultura de cero papel, permitiendo un mejor aprovechamiento de los recursos, para facilitar y garantizar el acceso a la información.

3. POLÍTICA DE CERO PAPEL

Esta política busca promover la responsabilidad con el ambiente y el compromiso con el desarrollo sostenible. El interés de la entidad es apoyar el proceso de sustitución de trámites basados en papel, por trámites y/o procedimientos que puedan desarrollarse por medios electrónicos aunando esfuerzos para mejorar la eficiencia de la administración pública con las buenas prácticas ambientales.

Esta política pretende establecer buenas prácticas sobre el consumo de papel, para avanzar hacia una gestión que sea más eficiente y amigable con el medio ambiente porque promueve:

- El ahorro de papel.
- La reducción de emisión de residuos.
- La disminución del consumo de recursos naturales empleados en la fabricación del papel: árboles, agua y energía.
- La disminución de la contaminación producida por los productos blanqueadores de papel.
- La disminución en el consumo de energía empleada en imprimir, fotocopiar, etc.
- La reducción en los residuos contaminantes como tóner, cartuchos de tinta, etc.
- La contribución al desarrollo sostenible, el consumo responsable de recursos que no comprometa el desarrollo social y ambiental de las generaciones futuras.
- Generar una cultura ecológica en los servidores de la CRA.

Para dar cumplimiento a lo anterior, todos los funcionarios y/o contratistas se comprometen con las siguientes actividades como buenas prácticas administrativas para la reducción del consumo del papel:

- Fotocopiar e imprimir a doble cara.
- Reducir el tamaño de los documentos al imprimir o fotocopiar (Arial 10).
- Configurar de manera correcta las páginas y verificar los documentos antes de enviarlos a imprimir.
- Leer cuidadosamente y corregir en pantalla aquellos documentos que deben ser obligatoriamente impresos.
- No imprimir documentos que sean utilizados para revisiones personales. Toda verificación se debe hacer en el computador, esto le permitirá conservar todas las versiones de los documentos sin incurrir en gastos innecesarios.
- Las impresoras y fotocopiadoras deberán utilizarse para el cumplimiento de las labores propias de la gestión de la entidad, en ningún caso para impresiones que sean de tipo personal.
- Reutilización de papel que sólo sea impreso por una cara, estas hojas podrán reemplazar el uso de aquellas que no se han utilizado y que se utilizan como hojas de borrador.
- Identificación de documentos que pueden ser entregados mediante correo electrónico.
- Intercambiar información de forma rápida y efectiva, evitando la utilización del papel y utilizando herramientas de colaboración como espacios virtuales de trabajo, aplicaciones de teleconferencia, calendarios compartidos, aplicaciones para uso y edición de documentos compartidos, entre otros.
- Uso de aplicaciones/sistemas de información de gestión de documentos electrónicos de archivo y gestión de contenido.
- No imprimir los correos electrónicos, salvo que sea estrictamente necesario.
- Si un documento debe ser enviado a varias dependencias, es compromiso del iniciador digitalizarlo por medio de scanner o grabarlo en formato PDF para que a través del correo institucional sea comunicado. En todo caso siempre se guardará el archivo físico original en la dependencia gestora para posteriores consultas.
- La CRA dispondrá en sus instalaciones dos (2) puntos ecológicos, donde los recipientes deben ser de un material resistente que no se deteriore con facilidad y cuyo diseño y capacidad optimicen el proceso de almacenamiento.
- Diseño de un programa de capacitación y sensibilización de los servidores de la CRA que permita una interiorización del esquema del manejo responsable de los residuos, lo cual permitirá entregar dichos residuos seleccionados al operador del servicio, de conformidad con lo establecido en el Decreto 596 de 2016.

La disposición de los materiales relacionados con esta política será administrada por la Subdirección Administrativa y Financiera.

CAPÍTULO VI

POLÍTICAS GENERALES DEFENSA JUDICIAL UAE-CRA

El Decreto 1069 de mayo 26 de 2015, "*Por medio del cual se expide el decreto único reglamentario del sector justicia y del derecho.",* dispone que las normas sobre Comités de Conciliación y Defensa Judicial son de obligatorio cumplimiento para las entidades de derecho público, los organismos públicos del orden nacional, departamental, distrital, los municipios que sean capital de departamento y los entes descentralizados de estos mismos niveles (art. 2.2.4.3.1.2.1.).

Dentro del referido decreto se encuentra como función precisamente la que señala al Comité como instancia administrativa que actúa como sede de estudio, análisis y formulación de políticas sobre prevención del daño antijurídico y defensa de los intereses de la entidad (art. 2.2.4.3.1.2.2. Decreto 1069 de 2015).

Igualmente, de conformidad con el artículo 2.2.4.3.1.2.5, numeral 2 del Decreto 1069 de 2015, le corresponde al Comité de Conciliación y Defensa judicial de la CRA el cumplimiento de la función de diseñar las políticas generales que orientaran la defensa de los intereses de la entidad.

Para el caso específico de la Comisión de Regulación de Agua Potable y Saneamiento Básico –CRA-, la Resolución UAE-CRA 950 de 27 de noviembre de 2007, prescribe en el artículo 4º, que es función del Comité de Conciliación de la CRA, diseñar las políticas generales que orientaran la defensa de los intereses de la entidad (núm. 2o).

El Comité de Conciliación y Defensa judicial de la CRA, ha venido formulando políticas generales para la mejora y eficiencia de la defensa de los intereses de la entidad, se hace conveniente y necesario actualizar, las políticas que orientaran la defensa, con el propósito de asegurar su efectividad y conocimiento por parte de los destinatarios.

La política busca que la CRA oriente sus actividades en el marco de un modelo de Gerencia Juridica Pública eficiente y eficaz que permita lograr de manera sostenible una disminución del número de demandas en su contra y del valor de las condenas a su cargo. Lo anterior aunado a un mejoramiento de su desempeño en la etapa judicial y en la recuperación por vía de la acción de repetición o del llamamiento en garantía con fines de repetición de las sumas pagadas por sentencias, conciliaciones o laudos arbitrales cuando a ello haya lugar.

El 8 de marzo de 2021, la CRA fue seleccionada para la implementación del Modelo Óptimo de Gestión – MOG al interior de la entidad, fruto del trabajo desarrollado y los análisis efectuados conforme el informe presentado en la sesión ordinaria No. 13 de 2021 del Comité de Conciliación y Defensa Judicial, se consideró indispensable actualizar las políticas generales formuladas con anterioridad.

Se encontró que las políticas deben estar orientadas al conjunto de actuaciones, trámites y gestiones que estén orientados a garantizar la defensa adecuada de los derechos litigiosos de la CRA, se indican a continuación las directrices generales y políticas de Defensa Judicial, para su observancia y cumplimiento así:

1. Cualquier documento relacionado con procesos judiciales debe ser enviado en forma prioritaria e inmediata al jefe de la Oficina Asesora Jurídica para su asignación al abogado con el perfil que mejor se adecue para la defensa de la entidad, procurando mantenerlo de inicio a fin del mismo.

El área de correspondencia y en general todas las áreas que intervienen en la proyección de respuestas a despachos judiciales, tendrán que otorgar prioridad a los temas judiciales en su asignación, gestión y trámite correspondiente.

2. Siempre que se demande un acto administrativo, contrato y /u operación expedida, suscrito y/ o ejecutado por la CRA, y se tenga conocimiento por la Oficina Asesora Jurídica se deberá proceder a otorgar el respectivo poder, en el menor tiempo posible.

3. El apoderado de la entidad, deberá proceder a analizar, estudiar el caso, y solicitar en coordinación con el jefe de la Oficina Asesora Jurídica, apoyo a las áreas respectivas competentes, con la finalidad de asegurar que se respondan en forma adecuada y oportuna las pretensiones, hechos y argumentos que esboza el demandante. Igualmente, debe estar atento al seguimiento de términos, envío de pruebas y soportes.

4. De igual manera, el apoderado debe aportar dentro de las oportunidades procesales del caso, las pruebas documentales que reposen en las dependencias de la entidad y que se le hayan entregado. Las áreas deben procurar mantener al día los expedientes administrativos y entregar en oportunidad debidamente organizados para la custodia todos los documentos que puedan servir de prueba en los procesos judiciales.

5. El apoderado de la CRA deberá entregar al jefe de la Oficina Asesora Jurídica, el proyecto de contestación de demanda, integrando las recomendaciones del área técnica respectiva para observaciones, comentarios o aval de las mismas.

6. El apoderado de la CRA debe vigilar aquellos procesos que se encuentren en rama judicial con una periodicidad de dos veces a la semana e incluirlo en la hoja de ruta de seguimiento a procesos judiciales.

7. Se implementará un cuadro de control Excel que permita establecer cuáles son los procesos activos y terminados en que haya hecho parte la CRA, el cual estará a cargo de la Oficina Asesora Jurídica, sin perjuicio de que cada apoderado debe mantener actualizado el eKOGUI de conformidad con las obligaciones establecidas en el Decreto 1069 de 2015, o la norma que lo adicione, modifique o derogue.

8. Se preferirá la utilización de los mecanismos de llamamiento en Garantía y Conciliación como política para evitar mayores desgastes de la Administración, del aparato judicial y de mayores condenas futuras contra la entidad, siempre que se cumplan los presupuestos normativos para aplicación de los mismos.

9. El apoderado de la CRA, deberá estudiar la procedencia del llamamiento en garantía para fines de repetición en los procesos judiciales de responsabilidad patrimonial.

10. Cuando la CRA, demande a sus contratistas, deberá accionar contra la aseguradora que ampare el riesgo que origina la acción y cuando actúe como accionado por ciudadanos o personas jurídicas de derecho privado o de derecho público por actos, hechos, omisiones u operaciones atribuibles a contratistas suyos, deberá llamar en garantía y/o denunciar el pleito al contratista y a su aseguradora, dependiendo del riesgo de que se trate.

11. Cuando comparezca la CRA ante los estrados judiciales, el apoderado, en razón del mandato a él conferido, debe proceder a defender los intereses públicos de la entidad de manera diligente, técnica y respetuosa, conforme a las reglas y ritos procesales y los principios y obligaciones que regulan el ejercicio de la abogacía, especialmente los deberes del abogado.

12. En los procesos que la CRA actúe como parte, los antecedentes, las pruebas y en general cualquier información que se brinde deberá ser coordinada directamente por el apoderado que atiende el proceso con el jefe de la Oficina Asesora Jurídica. En el caso de procesos relacionados con la liquidación de las contribuciones especiales a cargo de la CRA, el apoderado debe consultar junto con los antecedentes, la herramienta judicial actualizada para contribuciones elaborada con ocasión del Plan de Acción de prevención del daño antijurídico de las vigencias 2020-2021, que contiene los módulos de Marco Legal, Marco Legal 2020, Jurisprudencia, Fallos de Primera Instancia de procesos en curso, y Conceptos y Demandas en contra de la CRA.

13. El abogado encargado de la defensa judicial para la contestación de la demanda tendrá en cuenta los siguientes criterios:

13.1. Debe señalarse el marco normativo que regula las competencias orgánicas de la CRA y del sector respecto del problema planteado, al igual que las normas que reglamentan los aspectos particulares del caso concreto.

13.2. Deben presentarse o exponerse claramente los actos, procedimientos, operaciones, actuaciones que la CRA hubiere desarrollado, así como los antecedentes en cada caso, especialmente se deberán tener en cuenta los expedientes administrativos creados, las

resoluciones, antecedentes y los documentos de trabajo desarrollados con respecto a los actos administrativos regulatorios.

13.3. Debe hacerse el señalamiento al juez de la falta de personería jurídica de la CRA, no obstante, lo anterior, debe exponerse razones de defensa de los actos, contratos u operaciones que sean demandadas.

13.4. El apoderado en la contestación de la demanda deberá responder cada uno de los conceptos e imputaciones presentados por el actor y contener adicionalmente la explicación y justificación de los actos administrativos y de la conducta de la CRA, en cada caso concreto.

13.5. El apoderado de la CRA debe verificar los lineamientos actualizados de la tendencia jurisprudencial del Consejo de Estado, Corte Constitucional y aquellos aplicables al caso particular de que se trate, así como lineamientos y líneas jurisprudenciales compiladas por la Agencia Nacional de Defensa jurídica del Estado -ANDJE-.

14. En los procesos para seleccionar y contratar abogados externos bien como asesores o para que asuman la defensa judicial o extrajudicial de la CRA, además de las exigencias establecidas en el Manual de Contratación, se incluirá como requisito, no estar asesorando o adelantando procesos judiciales contra la CRA y mantener dicha prohibición mientras el contrato de prestación de servicios profesionales permanezca vigente; como las cláusulas de confidencialidad, exclusividad y la prohibición de litigar contra la Nación.

15. Al analizar la procedencia de las acciones de repetición, el abogado deberá efectuar un estudio conforme los formatos de la Agencia Nacional de Defensa Jurídica del Estado –ANDJE, especialmente se debe verificar la oportunidad o configuración del fenómeno jurídico de la caducidad de la acción, la fecha de ejecutoria de la sentencia, la fecha del pago total de la sentencia (último pago), la procedencia de las medidas cautelares dentro de la acción de repetición, el pronunciamiento del Comité de Conciliación en el caso particular.

16. La CRA como perjudicado de un delito contra la administración pública preferirá promover el incidente de reparación integral, y deberá verificar la etapa procesal para que la CRA como víctima participe en la práctica de pruebas y reconocimiento de perjuicios derivados de la conducta punible.

17. La CRA establecerá los mecanismos, procedimientos y controles necesarios a efecto de responder con eficiencia y eficacia al deber legal de acatar oportunamente las decisiones de las autoridades judiciales, estrictamente en los términos en que éstas son proferidas, evitando las sanciones disciplinarias, generación de intereses moratorios y su correspondiente pago.

18. En la segunda sesión de cada mes del comité de conciliación y defensa judicial de la CRA, la oficina Asesora Jurídica presentará un informe mensual de vigilancia de procesos judiciales con el fin de estudiar y evaluar los procesos que cursen o hayan cursado en contra, con el objeto de conocer el objeto de la controversia, su estado y realizar seguimiento sobre los procesos encomendados a los apoderados.

19. Semestralmente la secretaria técnica del comité de conciliación y defensa judicial de la CRA presentara un informe en sesión del Comité de Conciliación para determinar las causas comunes generadoras de los conflictos; el índice de condenas; los tipos de daño por los cuales resulta demandado o condenado; y las deficiencias en las actuaciones administrativas de las entidades, así

como las deficiencias de las actuaciones procesales por parte de los apoderados, con el objeto de proponer correctivos.

20. Las decisiones adoptadas por el Comité de Conciliación, serán de obligatorio cumplimiento para los apoderados de la CRA.

21. Los lineamientos de la ANDJE que se exponen en las sesiones del comité de conciliación y defensa judicial serán de obligatorio cumplimiento por parte de las áreas de la CRA y de los apoderados, la adopción de medidas será de responsabilidad del jefe de cada área.

22. La Oficina Asesora jurídica remitirá un informe semestralmente como mínimo a la Subdirección Administrativa y Financiera para que esta última de conformidad con la normativa correspondiente efectué las provisiones de las contingencias judiciales respectivas.

23. Se efectuarán las gestiones correspondientes para coordinar la defensa judicial con el Ministerio de Vivienda, Ciudad y Territorio, entregando los conceptos jurídico-técnicos y las pruebas que reposen en la UAE-CRA.

24. Sera obligatorio para los abogados la utilización de los formatos establecidos por la ANDJE en el EKOGUI.

25. Se utilizarán los instrumentos diseñados por la ANDJE en la comunidad jurídica del conocimiento. Especialmente, se deben aplicar las líneas jurisprudenciales que ha construido la ANDJE con respecto a las causas más relevantes de litigiosidad en la UAE-CRA (acciones populares, y acciones de tutela).

26. El Comité de Conciliación revisará estrategias de defensa formuladas, las cuales siempre deben estar focalizadas en la reiteración, la complejidad de los casos y el impacto del caso en términos de pretensiones, posibilidad de éxito, visibilidad ante los medios de comunicación, entre otros. Para ello la Oficina jurídica de la CRA debe tener en cuenta, al momento de responder demandas:

26.1.- Respuesta otorgadas en procesos similares, y pronunciamientos efectuados por los despachos que los hayan conocido.

26.2.- Complicaciones de orden jurídico y técnico que cuando lo ameriten, impliquen la convocatoria de mesas transversales para fijar líneas de respuesta.

26.3.- Revisar los planteamientos del Comité de Expertos, los documentos de trabajo, respuestas a derechos de petición y /o solicitudes de revocatoria directa, cuando a ello haya lugar, y que sean favorables para la defensa.

26.4.- Debe proceder a incluir el proceso en eKOGUI, calificar el riesgo de conformidad con la metodología de la ANDJE y determinar su posibilidad de éxito.

26.5.- De existir pronunciamientos y comunicados de prensa debe evaluarlos y recoger los planteamientos favorables a la defensa de la entidad.

27. Estas etapas deberán ser realizadas con respecto a cada uno de los procesos nuevos, desde la presentación de la demanda o del traslado de la misma, hasta el resultado final plasmado en sentencia ejecutoriada, con el fin darle continuidad en el tiempo.

27.1.- RECAUDACIÓN DE INFORMACIÓN

Previa la contestación de las demandas, se deberá recaudar la información relacionada con la misma, y se pedirá apoyo a las diferentes áreas de la entidad, incluyendo todas las pruebas que permitan la defensa adecuada de los intereses de la CRA.

27.2.- IDENTIFICACIÓN DE CADA PROCESO

Para cada proceso, se llenará el formato de hoja de ruta del proceso que se encuentra en calidad. Esta información será consignada en un cuadro que alimentará el informe mensual que presenta la Oficina Asesora Jurídica al Comité de Expertos. Al finalizar a cada proceso la hoja de ruta será la última parte del expediente que reposa en la entidad.

27.3.- ESTABLECIMIENTO DE UNA TIPOLOGÍA DE DAÑO ANTIJURÍDICO

Con base en la información recaudada y analizada es pertinente determinar la relación de tipos de daño antijurídico constituirá uno de los productos finales del estudio de causas de daño que se han imputado judicialmente a la administración durante un periodo determinado, facilitando analizar el tema como insumo de las políticas de prevención del daño antijurídico.

27.4.- DISEÑO DE PROPUESTA DIRIGIDA A LA ADOPCIÓN DE MEDIDAS DE ÍNDOLE PREVENTIVO Y CORRECTIVO.

En el interés de optimizar la actividad administrativa de la CRA, la prevención del daño antijurídico, así como la de la actividad de Defensa Judicial de la entidad, deberá realizarse anualmente el estudio para identificar las demandas, condenas y reclamaciones de mayor ocurrencia, como sus causas, y en último lugar analizar las falencias y debilidades en la actividad administrativa y de defensa, se realizará un informe en el que se anotarán los resultados de cada una de las etapas al igual que las recomendaciones y sugerencias que podrán ser enriquecidas con los aportes del comité de conciliación en el momento del informe y se tendrán en cuenta para priorizar los planes de acción de la política de prevención del año siguiente.

Los correctivos que se planteen, se convertirán en medidas o líneas de acción que procuren evitar la ocurrencia de las acciones u omisiones irregulares de la administración. Estos correctivos estarán a cargo del Comité de Conciliación.

27.5.- INFORME AL COMITÉ DE CONCILIACIÓN

Semestralmente se presentará un informe, con las demandas, la relación de conciliaciones y acciones de repetición analizadas y decididas, si a ello hubiera lugar, se presentará la relación de las demás actividades que contempla la normatividad, especialmente el Decreto 1069 de 2015, entre ellas, la identificación de causas de demandas, sentencias y conciliaciones en contra de la entidad.

28. Los apoderados cuando intervengan en defensa de la CRA, dentro de medios de control de protección de derechos e intereses colectivos en los que se cuestione la legalidad de un acto

administrativo, deberán alegar la presunción de legalidad de los actos administrativos que no hayan sido objeto de suspensión provisional o fallo condenatorio en firme; igualmente deberán recalcar sobre la existencia de medios de control autónomos para anularlos.

Así mismo, cuando los medios de control de protección de derechos e interés colectivos estén relacionados con reclamaciones de facturación de servicios públicos, debe argumentarse que existen medios administrativos ideados al efecto (art. 154 de la Ley 142 de 1994) y que esta no es la vía para recuperación de dineros.

29. Los apoderados deben verificar que se haya agotado oportunamente el requisito de procedibilidad de la conciliación extrajudicial y que la solicitud de conciliación cumpla con las exigencias mínimas para su admisión.

I.-IMPLEMENTACION DE OTROS MECANISMOS JURIDICOS:

1. LLAMAMIENTO EN GARANTÍA

El llamamiento en garantía debe ser una prioridad para la CRA. El ejercicio de esta figura deberá hacerse en el momento de la contestación de la demanda. A través de esta figura se decide si los funcionarios que intervinieron en la actuación en su momento los llamamos en garantía para que ayuden a la defensa judicial de la Entidad. Siendo una función del apoderado Judicial de la entidad realizar el Llamamiento en Garantía, se adopta como política de la entidad, que el apoderado cite extraordinariamente si es necesario, y escuche la recomendación del Comité cuando tenga duda sobre el llamamiento en garantía.

2.- ACCION DE REPETICIÓN

La acción de repetición es una acción civil de carácter patrimonial que deberá ejercerse en contra del servidor o exservidor público que como consecuencia de su conducta dolosa o gravemente culposa haya dado reconocimiento indemnizatorio por parte del Estado, proveniente de una condena, conciliación u otra forma de terminación de un conflicto. La misma acción se ejercitará contra el particular que investido de una función pública, haya ocasionado, en forma dolosa o gravemente culposa, la reparación patrimonial.

El Comité de Conciliación de la Comisión de Regulación de Agua Potable y Saneamiento Básico deberá realizar los estudios pertinentes para determinar la procedencia de la acción de repetición.

Es deber de la CRA ejercitar la acción de repetición o el llamamiento en garantía, cuando el daño causado por el Estado haya sido consecuencia de la conducta dolosa o gravemente culposa de sus agentes. El incumplimiento de este deber constituye falta disciplinaria de acuerdo con el numeral 36 del artículo 40 de la Ley 734 de 2002 que señala lo siguiente*: "No instaurarse en forma oportuna por parte del Representante Legal de la entidad, en el evento de proceder, la acción de repetición contra el funcionario, ex funcionario o particular en ejercicio de funciones públicas cuya conducta haya generado conciliación o condena de responsabilidad contra el Estado*".

II. MECANISMOS ALTERNATIVOS DE SOLUCIÓN DE CONFLICTOS

Los mecanismos alternativos de solución de conflictos son herramientas jurídicas por medio de las cuales se permite a las personas solucionar las controversias que se vean envueltos, sin tener que

acudir a los mecanismos ordinarios establecidos en la ley, dentro de los mecanismos alternativos tenemos los siguientes:

1. ARREGLO DIRECTO.

Es un mecanismo de resolución pacífica de conflictos por medio del cual dos o más personas gestionan por sí mismas, y sin la intervención de un tercero, la solución de sus controversias o previenen un conflicto futuro.

El acuerdo al que llegan las partes puede ser escrito o verbal y se puede materializar de distintas formas: puede verse reflejado en un acta de compromiso, en cuyo caso el documento tendrá valor probatorio, pero no prestará mérito ejecutivo; puede igualmente materializarse en un contrato de transacción, caso en el cual será un título ejecutivo válido para iniciar el proceso correspondiente.

2. CONCILIACIÓN

El Comité de Conciliación es un espacio privilegiado y necesario para la prevención del daño antijurídico de la CRA. El Comité de Conciliación por sus competencias legales termina siendo el paso obligado para el conocimiento de los asuntos judiciales de la entidad, hoy en día la conciliación es un requisito de procedibilidad para acceder a la administración de justicia, por consiguiente, el Comité de Conciliación analizará todas las propuestas de conciliación de quienes demandan a la Comisión de Regulación por falsas motivaciones, desviaciones de poder, etc, ya sea a través de acciones de nulidad y restablecimiento o de cualquier otra acción contenciosa en la que haga parte la entidad.

2.1.- Situaciones que son evidentes.

Si el Comité de Conciliación detecta que la entidad se equivocó y resulta procedente conciliar, ya sea por solicitud de la contraparte, de la Comisión de Regulación, o conjunta, así debe hacerse para evitar que esa condena le cueste a la Comisión mucho más dinero.

2.2.-. Hay otras situaciones que NO son evidentes.

Conciliar con una duda razonable no es lo recomendable, porque la conciliación puede ser fuente de detrimento patrimonial del Estado.

Sin embargo, la duda nos puede estar señalando unas medidas que deben ser tomadas en la entidad para solucionar errores futuros. El Comité de Conciliación deberá analizar cada uno de estos casos para trazar las medidas pertinentes.

Es importante que en el Comité de Conciliación de la Comisión de Regulación estén representadas las diferentes oficinas, teniendo en cuenta que la situación motivo de controversia puede ser de cualquiera de las dependencias de la entidad y el conocimiento que se tenga de la situación concreta por parte de los Directivos aportará información necesaria en el momento de la toma de decisiones.

Siempre que el Procurador Judicial proponga reconsiderar la decisión tomada por el Comité de Conciliación, éste deberá someter de nuevo el tema a Comité con el fin de estudiar nuevamente la solicitud y decidir sobre ella, ya sea confirmando su decisión o modificándola.**2. LA**

3. TRANSACCIÓN.

De acuerdo con el artículo 2469 del Código Civil la transacción es un contrato por medio del cual las partes terminan extrajudicialmente un litigio pendiente, o precaven un litigio eventual.

Se puede entender como un acuerdo de voluntades por medio del cual las partes, en ejercicio de la autonomía de la voluntad, solucionan directamente y de forma definitiva sus conflictos. Se trata entonces de un mecanismo alternativo de solución de conflicto de carácter netamente auto compositivo y que tiene aplicación en la etapa pre procesal –como mecanismo de prevención de un litigio futuro- y en la etapa procesal propiamente dicha, como medio anticipado de terminación del proceso.

4. LA AMIGABLE COMPOSICIÓN.

La amigable composición es un mecanismo de solución de conflictos, por medio del cual dos o más particulares delegan en un tercero, denominado amigable componedor, la facultad de precisar, con fuerza vinculante para ellas, el estado, las partes y la forma de cumplimiento de un negocio jurídico particular. El amigable componedor podrá ser singular o plural.

5. EL ARBITRAJE.

El arbitraje es un mecanismo por medio del cual las partes involucradas en un conflicto de carácter transigible, defieren su solución a un tribunal arbitral, el cual queda transitoriamente investido de la facultad de administrar justicia, profiriendo una decisión denominada laudo arbitral.

El arbitraje puede ser en derecho, en equidad o técnico. El arbitraje en derecho es aquel en el cual los árbitros fundamentan su decisión en el derecho positivo vigente. En este evento el Árbitro deberá ser abogado inscrito. El arbitraje en equidad es aquel en que los árbitros deciden según el sentido común y la equidad. Cuando los árbitros pronuncian su fallo en razón de sus específicos conocimientos en una determinada ciencia, arte u oficio, el arbitraje es técnico.

III. CONFLICTO ENTRE ENTIDADES PÚBLICAS

Teniendo en cuenta los principios de economía y eficacia administrativa, la CRA autoriza que los conflictos suscitados entre entidades y organismos del orden nacional sean sometidos al trámite de la mediación ante la Agencia Nacional de Defensa Jurídica del Estado, conforme los artículos 6º y 17 del Decreto Ley 4085 de 2011, reglamentado en el Decreto 2137 de 2015 e incorporado en el Decreto Único Reglamentario del Sector Justicia y del Derecho 1069 de 2015 o las normas que las modifiquen, adicionen o sustituyan.

El plan de acción que deberá seguir la CRA para atender los litigios con otras entidades del orden nacional será el siguiente:

1.- Asignación de apoderado.

2.- Elaboración de análisis técnico-jurídico al interior de la entidad para determinar la procedencia y pertinencia de la solicitud de mediación o cualquier medio alternativo de solución de conflictos.

3.- Exposición del caso al Comité de Conciliación para recomendación de la acción a tomar.

4.- La CRA puede acceder al servicio de mediación elevando una petición al Director de Defensa Jurídica Nacional a través del medio definido por la ANDJE, donde se describa la problemática que se pretende solucionar, los datos del proceso si a ello hubiere lugar, las entidades involucradas y los anexos que se consideren pertinentes para caracterizar el caso.

5.- La ANDJE procederá a convocar a las entidades a una primera reunión en la que se definirá su voluntariedad de iniciar el proceso de negociación previa autorización de los comités de conciliación o quien haga sus veces, así como la designación del funcionario o equipo negociador

El inicio de la mediación ante la ANDJE, al no tratarse de un mecanismo alternativo de solución de conflictos, no suspende ningún término de prescripción de derechos, de caducidad de las acciones a las que hubiere lugar, ni interrumpe los trámites extrajudiciales o procesos judiciales en curso, así como tampoco los mecanismos alternativos de solución de conflictos previstos en la ley que se encuentren en trámite.

La mediación es un proceso voluntario que se lleva a cabo con carácter confidencial. El mediador designado por la Agencia presta ayuda a las entidades oficiales enfrentadas entre sí, para llegar a un acuerdo negociado y evitar eventuales controversias o para poner fin a los conflictos que surtan en etapa judicial o extrajudicial. La mediación NO suspende términos de caducidad y su resultado o acuerdo puede consistir en cualquier acto o negocio jurídico que posibilite la solución de la controversia, por ejemplo: una transacción, un desistimiento, un convenio, una revocatoria de un acto administrativo, una conciliación ante la Procuraduría General de la Nación, entre otros.

La CRA, podrá hacer uso del artículo 112 de la Ley 2080 de 2021 o la norma que lo adicione, modifique o sustituya, para precaver un eventual litigio o poner fin a un existente con otras entidades, para ello debe evaluar la procedencia y pertinencia de solicitar a la ANDJE o al Ministerio de Vivienda, Ciudad Territorio que pidan concepto a la Sala de Consulta y Servicio Civil del Consejo de Estado, en relación con las controversias jurídicas que se presenten entre la CRA y otra entidad pública del orden nacional o territorial. El concepto emitido por la Sala no está sujeto a recurso alguno.

IV.-INDICADORES

Con la finalidad de efectuar el seguimiento correspondiente, el Comité de Conciliación y Defensa Judicial de la CRA, medirá y evaluará los resultados de los indicadores de eficiencia, eficacia y efectividad en materia de defensa judicial, con la periodicidad indicada en el plan de acción del Comité de Conciliación de cada vigencia, la cual, en todo caso será por lo menos una vez en el semestre, así:

Política de defensa	Indicador	Tipo de indicador
El apoderado de la entidad, deberá proceder a analizar, estudiar el caso, y solicitar en coordinación con el jefe de la Oficina Asesora Jurídica, apoyo a las áreas respectivas competentes, con la finalidad de asegurar que se respondan en forma adecuada y oportuna las pretensiones, hechos y	Demandas o tutelas nuevas notificadas cuyo término ya haya vencido/ Demandas o tutelas nuevas respondidas en término	Eficacia

Tabla con formato

argumentos que esboza el demandante.		
En la segunda sesión de cada mes del Comité de Conciliación y defensa judicial de la CRA, la oficina Asesora Jurídica presentará un informe mensual del estado de procesos judiciales con el fin de verificar correctivos si a ello hubiese lugar	Informe de procesos judiciales con correctivos formulados / informe de procesos judiciales mensual programado en que haya lugar a formular correctivos	Eficiencia
La Oficina Asesora jurídica remitirá un informe semestralmente como mínimo a la Subdirección Administrativa y Financiera, para que esta última de conformidad con la normativa correspondiente, efectué las provisiones de las contingencias judiciales respectivas.	Informe de contingencias judiciales presentados / Informe de contingencias judiciales programado	Eficacia
Se utilizarán los instrumentos diseñados por la ANDJE en la comunidad jurídica del conocimiento.	Abogados inscritos y capacitados en materia judicial a la fecha de corte / abogados apoderados por la UAE CRA a la fecha de corte	Efectividad

CAPÍTULO VII

POLÍTICA DE PREVENCIÓN DEL DAÑO ANTIJURÍDICO DE LA CRA

El Decreto 1069 de mayo 26 de 2015, "*Por medio del cual se expide el decreto único reglamentario del sector justicia y del derecho."*, dispone que las normas sobre Comités de Conciliación y Defensa Judicial son de obligatorio cumplimiento para las entidades de derecho público, los organismos públicos del orden nacional, departamental, distrital, los municipios que sean capital de departamento y los entes descentralizados de estos mismos niveles (art. 2.2.4.3.1.2.1.).

Dentro del referido decreto se encuentra como función precisamente la que señala a ese comité como instancia administrativa que actúa como sede de estudio, análisis y formulación de políticas sobre prevención del daño antijurídico y defensa de los intereses de la entidad (art. 2.2.4.3.1.2.2.).

Por tanto, le corresponde al Comité de Conciliación y Defensa Judicial de la CRA el cumplimiento de la función de formular y ejecutar políticas de prevención del daño antijurídico (art. Artículo 2.2.4.3.1.2.5., núm. 1).

Así mismo, la Agencia Nacional de Defensa Jurídica del Estado –ANDJE-, expidió la Circular Externa 06 de 6 de julio de 2016 en la cual se imparten lineamientos para el seguimiento a la formulación e implementación de las políticas de prevención del daño antijurídico. Según los mismos, las entidades públicas del orden nacional deben formular cada año su política de prevención del daño antijurídico teniendo en cuenta la litigiosidad del año inmediatamente anterior; entre los meses de noviembre y diciembre de cada año, deberán enviar a esa entidad la política que se va a implementar el año siguiente.

Para el caso específico de la Comisión de Regulación de Agua Potable y Saneamiento Básico –CRA-, la Resolución UAE-CRA 950 de 27 de noviembre de 2007, prescribe en el artículo 4º, que es función del Comité de Conciliación formular y ejecutar políticas de prevención del daño antijurídico (núm. 1o), al igual que evaluar los procesos que cursen o hayan cursado en contra de la Comisión, las deficiencias en las actuaciones administrativas con el objeto de proponer correctivos (núm. 3o).

La Política de Prevención del Daño Antijurídico se puede consultar en el aplicativo que ha designado la Agencia Nacional de Defensa Jurídica del Estado.

PLAN DE ACCIÓN

Ubique el cursor encima del nombre de cada columna, para ver unas breves instrucciones

Insumo	Causa eKogui	Justificación	Subcausa	Nº Medida	Medida ¿qué?	Otra Medida	Período de implementación de		Nº Mecanis	Mecanismo	Otro Mecanismo	Ejecución del mecanismo	Área responsable	Divulgación
							Fecha inicio	Fecha fin						
Ayuda	Ayuda	Ayuda	Ayuda	Ayuda	Ayuda	Ayuda	Ayuda			Ayuda	Ayuda	Ayuda	Ayuda	Ayuda
Litigiosidad	ILEGALIDAD DEL ACTO ADMINISTRATIVO QUE LIQUIDA UNA CONTRIBUCION ESPECIAL	Frecuencia y valor. El valor de las pretensiones es alto e impacta el presupuesto de la entidad puesto que con ese valor se financia la CRA	falta de unificación de criterios sobre la correcta interpretación del Artículo 85 de la Ley 142 de 1994 por el Consejo de Estado.	1	Unificar criterios		01/06/2020	30/11/2021	1	Otro (escriba a en la siguiente columna)	Crear una herramienta que compendie las respuestas a conceptos, demandas, lineas jurisprudenciales, jurisprudencia relevante y normatividad sobre la contribución especial	Explorar la herramienta que mejor compendie los temas relevantes de la contribución especial; crearla, socializarla y actualizarla	Subdirección Administrativa y Financiera	Correo electrónico
			Ausencia de socialización del procedimiento de fijación , liquidación y pago de la contribución especial.	1	Otra (escriba a en la siguiente columna)	Lograr socializar el procedimiento de fijación, liquidación y pago de la contribución especial	01/06/2020	30/11/2021	1	Otro (escriba a en la siguiente columna)	Capacitaciones a los actores involucrados en el tema.	Propiciar un espacio (virtual o presencial) semestral, cercanos al vencimiento del pago de la contribución para socializar	Subdirección Administrativa y Financiera	Correo electrónico

INDICADORES DE GESTIÓN

Ubique el cursor encima del nombre de cada columna, para ver unas breves instrucciones

			FORMULACIÓN DEL INDICADOR		
			Ayuda		
Subcausa	Nº Del Mecanismo	Mecanismo	Descripción del numerador	Descripción del denominador	Fórmula del indicador
falta de unificación de criterios sobre la correcta interpretación del Artículo 85 de la Ley 142 de 1994 por el Consejo de Estado.	1	Crear una herramienta que compendie las respuestas a conceptos, demandas, lineas jurisprudenciales, jurisprudencia relevante y normatividad sobre la contribución especial	herramienta creada	herramienta planeada	(herramienta creada / herramienta planeada) * 100
Ausencia de socialización del procedimiento de fijación , liquidación y pago de la contribución especial.	1	Capacitaciones a los actores involucrados en el tema.	capacitaciones realizadas	capacitaciones planeadas	(capacitaciones realizadas / capacitaciones planeadas) * 100

INDICADORES DE RESULTADO

Ubique el cursor encima del nombre de cada columna, para ver unas breves instrucciones

			FORMULACIÓN DEL INDICADOR		
			Ayuda		
Subcausa	N° Medida	Medida	Descripción del numerador	Descripción del denominador	Fórmula del indicador
falta de unificación de criterios sobre la correcta interpretación del Artículo 85 de la Ley 142 de 1994 por el Consejo de Estado.	1	Unificar criterios	criterios unificados	criterios planeados unificar	(criterios unificados / criterios planeados unificar) * 100
Ausencia de socialización del procedimiento de fijación , liquidación y pago de la contribución especial.	1	Lograr socializar el procedimiento de fijación, liquidación y pago de la contribución especial	capacitaciones realizadas	capacitaciones planeadas realizar	(capacitaciones realizadas / capacitaciones planeadas realizar) * 100

INDICADORES DE IMPACTO

Ubique el cursor encima del nombre de cada

		IMPLEMENTACIÓN DEL PLAN DE ACCIÓN									
	Ayuda	INFORME ANUAL DE IMPLEMENTACIÓN AÑO 1				INFORME ANUAL DE IMPLEMENTACIÓN AÑO 2					
Causa e-kogui	Fórmula del indicador	# ddas año de implementación 1	# ddas año de formulación	Resultado	Explicación del resultado	# ddas año de implementación 2	# ddas año de implementación 1	Resultado	Explicación del resultado	**Tasa de crecimiento prom. anual**	**Explicación del resultado total**
ILEGALIDAD DEL ACTO ADMINISTRATIVO QUE LIQUIDA UNA CONTRIBUCION ESPECIAL	[(#ddas año X - #ddas año Y) / #ddas año Y]*100										

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de los cambios.
06	04/11/2021	Se actualiza el documento incluyendo la política de servicio al ciudadano, política d administración de riesgos y la última versión de la política de defensa jurídica.
05	10/06/2021	Se actualiza el documento de acuerdo con la última versión aprobada de las políticas que manejan los procesos.

NOMBRE DEL PROCESO	ELABORA	REVISA	APRUEBA
Dirección Estratégica (DES)	Sirley Corredor Monsalve Profesional Responsable del Sistema Integrado de Gestión y Control Karen Fonseca Contratistas Oficina Asesora de Planeación y Tic´s	Equipo Facilitador de MIPG	Yamile Angélica Medina Walteros Jefe Oficina Asesora de Planeación y Tic´s