POLITÍCA OPERACIONAL

1. **Derechos de autor**

RTVC es el titular de los derechos de autor del presente documento, en consecuencia, no se permite su reproducción, comunicación al público, traducción, adaptación, arreglo o cualquier otro tipo de transformación total o parcial, ni almacenamiento en ningún sistema electrónico de datos sin autorización previa y escrita de la Gerencia.

2. **Acerca de este documento**

El Modelo Estándar de Control Interno MECI 2014, define las Políticas de Operación como un elemento fundamental para el direccionamiento de las organizaciones, el cual facilita la ejecución de las operaciones internas a través de guías de acción y define los límites y parámetros necesarios para ejecutar los procesos y actividades, con la intención de mejorar el quehacer de la Administración Pública; las políticas de operación constituyen los marcos de acción necesarios para hacer eficiente la operación, igualmente, facilitan el control administrativo y reducen la cantidad de tiempo en la toma de decisiones sobre asuntos rutinarios. Son guías de acción de carácter operativo y de aplicación cotidiana que dan seguridad y confianza a los responsables de la ejecución de las actividades enmarcadas en el modelo de operación por procesos.

A partir de los principios recogidos y aceptados en estos documentos se propende por tener un marco de referencia que incentive la participación de todos los interesados en el desarrollo y actualización continua de las políticas.

De igual manera, atendiendo la estructura del Modelo Integrado de Planeación y Gestión - MIPG, en cumplimiento del Decreto 1499 de 2017, se adopta la denominación de las políticas establecidas en dicho modelo para cada una de las dimensiones.

3. **Políticas de carácter general o transversal**

Los siguientes aspectos descritos, son lineamientos transversales a todos los procesos y contribuyen al buen funcionamiento de la Empresa:

1. Todos los procesos realizan actividades de autoevaluación, de acuerdo con lo establecido en el Modelo Estándar de Control Interno.

2. En RTVC son responsables por la organización, conservación, uso y manejo de los documentos, todos sus colaboradores tanto los servidores y empleados públicos como los contratistas, aplicando las normas adoptadas para tal fin por la empresa, las cuales están basadas en lo establecido por el Archivo General de la Nación[1].

[1] Artículo 2.8.2.5.3 Decreto 1080 de 2015 Ministerio de Cultura

3. Toda comunicación oficial (Comunicaciones recibidas o producidas en desarrollo de las funciones de una entidad, independiente del medio utilizado[2]), enviada o recibida debe ser registrada en el sistema de gestión documental Orfeo para oficializar su trámite, asignándoles un consecutivo único de radicado y cumplir con los términos de vencimiento establecidos por la Ley[3].

4. En todas las reuniones que se realicen en las áreas, se debe llevar registro de asistencia o acta de reunión, de acuerdo con los formatos establecidos en el Sistema Integrado de Gestión - SIG, así mismo será viable realizar el registro a través de medios electrónico tales como:

    - Módulo de actas en el sistema de planeación y gestión kawak, apta para todo tipo de reuniones y una vez esta se encuentre aprobada, se debe archivar el documento electrónico en pdf[4].
    - Empleo del formato de "acta de reunión" publicado en el sistema de planeación y gestión kawak, el cual debe ser diligenciado digitalmente, y enviado y aceptado a través de correo electrónico.
    - Formato de asistencia a reuniones diligenciada y aceptadas a través de correo electrónico (este formato de acuerdo con las recomendaciones de la coordinación de talento humano y en el marco del protocolo de bioseguridad, se evitará en la medida de lo posible, ser diligenciado de manera física, esto hasta que dicha coordinación considere lo contrario.
    - Como soporte de la asistencia a reuniones realizadas de forma virtual, en cualquiera de las aplicaciones tecnológicas disponibles utilizadas, se podrá aportar captura(s) de pantalla en la que se visualicen los asistentes a la misma, como evidencia de su realización y se aportarán las necesarias. En el caso de las reuniones en las que haya quórum, la(s) captura(s) de pantalla se realizará en el momento de su verificación.

5. Todas las áreas deben estar en constante actualización de la normatividad legal que les aplique para el desarrollo de sus funciones.

6. En todos los procesos de RTVC se da prioridad y estricto cumplimiento a los requerimientos de los órganos de control.

7. Todo trámite, diligencia o proceso adelantado por RTVC, se realiza de conformidad con la normatividad vigente y lo establecido en los diferentes manuales y procedimientos registrados en el sistema integrado de gestión

[2] Acuerdo 027 de 2006 Archivo General de la Nación
[3] Acuerdo 060 de 2001 Archivo General de la Nación

8. El monitoreo y revisión a los mapas de riesgos debe ser realizado por los responsables de los procesos, como parte del ejercicio de autocontrol; lo anterior, para identificar todas las situaciones o factores que pueden influir en la aplicación de las acciones preventivas.

9. Todas las personas y los procesos deben considerar y aplicar la política operacional de seguridad de la información y seguridad digital de RTVC dentro de sus actividades y como parte de sus responsabilidades para el buen manejo de la información de empresa.

10. Todas las personas y los procesos deben considerar y aplicar la política de protección de datos dentro de sus actividades y como parte de sus responsabilidades para el buen manejo de la información de empresa y de los terceros que tenga en su poder.

4. Política operacional administración de riesgos

Establecer los lineamientos clave que contribuirán a la prevención y administración de los riesgos de gestión, riesgos de corrupción y riesgos de seguridad de la información y seguridad digital al interior de RTVC.

Alcance de la política de administración de riesgos

Esta política operacional debe ser aplicada para la administración de los riesgos (gestión, corrupción y de seguridad de la información y seguridad digital) que se hayan identificado para los procesos de RTVC.

Contexto

La Alta Dirección con el fin de lograr los objetivos estratégicos institucionales desarrolla la gestión de riesgos, bajo un enfoque preventivo y detectivo frente a las situaciones de materialización de riesgos, con el fin de dar lineamientos, en este sentido se establece las Políticas de Gestión y Administración del Riesgo alineados con el logro de los objetivos operativos y misionales de la entidad.

La gestión de riesgos en RTVC se alinea con la “Guía para la administración del riesgo y el diseño de controles en entidades públicas -Riesgos de Gestión, Corrupción y Seguridad Digital-” emitida por el Departamento Administrativo de la Función Pública y con el Modelo Integrado de Planeación y Gestión establecido en el marco del Decreto 1499 de 2017. La gestión de riesgos incluye aspectos metodológicos, operativos, de seguimiento y mejoramiento descritos en la “Guía de Administración de Riesgos de RTVC”.

Para una adecuada gestión de riesgos que dé cumplimiento al marco legal y normativo, la presente política atiende principalmente los siguientes compromisos:

- Ley 719 de 2001 Derechos de Autor y conexos
- Ley 1474 de 2011 artículo 73 Plan Anticorrupción y de Atención al Ciudadano
- Ley 1523 de 2012. Política nacional de gestión del riesgo de desastres.
- Ley 1581 de 2012. Protección de datos personales.
- Ley 1712 de 2014. “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
- Decreto 1081 de 2015: Publicación del mapa de riesgos de corrupción
- Decreto 1078 de 2015 Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto 124 del 26 de enero de 2016, Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 deí Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano. Publicación mapa de riesgos de corrupción.
- Decreto 1499 de 2017 Modelo Integral de Planeación y Gestión MIPG – Función Pública
- Decreto 1008 de 2018. Política de Gobierno Digital MinTIC.
- Norma técnica NTC ISO/IEC 27001:2013 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI) Requisitos
- Norma ISO 9001: 2015 Sistema de Gestión de la Calidad
- Norma Técnica Colombiana NTC ISO 31000:2018. Gestión del Riesgo
- Modelo de Seguridad y Privacidad de la información de MinTIC.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas de octubre 4 de 2018

Lineamientos para la administración de riesgos en RTVC

- Los responsables de los procesos deben identificar los riesgos de gestión, los riesgos de corrupción y los riesgos de seguridad de la información y de seguridad digital, que puedan afectar el logro de los objetivos del proceso.

- Les corresponde a todos los líderes de los procesos, identificar e implementar el tratamiento de acuerdo con la importancia del riesgo, lo cual incluye el efecto que puede tener sobre RTVC, la probabilidad e impacto de este y la relación costo beneficio.

- Cuando el riesgo se identifique según las cusas relacionadas, en las zonas de riesgo (Extremo, alto, moderado y bajo) se determina que aquellos controles con zona de riesgo bajo no requerirán de acciones complementarias, sin embargo, se debe continuar con actividades de monitoreo y seguimiento permanente.
- Cuando el cálculo del riesgo residual los ubique en zona de riesgo extremo (probabilidad: probable o casi seguro; impacto: mayor o catastrófico) será necesario que se establezcan acciones correctivas, correcciones, planes de tratamiento o mejoras, de acuerdo con la importancia y características del riesgo.

- Todos los procesos deben realizar el ejercicio de identificación de riesgos y para cada causa del riesgo debe existir su correspondiente acción de control. Los procesos que hayan identificado riesgos que no posean controles, deben diseñar controles (acciones preventivas) o planes de tratamiento (acciones correctivas o mejoras) para evitar la materialización del riesgo.

- Las acciones de control deben fundamentarse en la comprensión y origen de las causas que generan el riesgo, así como en el análisis de las interrelaciones de los procesos, porque de ello depende el grado de control que pueda ejercerse sobre ellas y por consiguiente la efectividad del tratamiento.

- Dado que todos los procesos son susceptibles de ser afectados por la ocurrencia de eventos de riesgos de gestión, riesgos de corrupción y riesgos de seguridad de la información y seguridad digital , los líderes de los procesos deben adelantar la gestión de sus riesgos y cada vez que se presente la materialización de uno de ellos reportar a la Coordinación de Planeación, Oficina de Control Interno y/o la Coordinación de TI, lo anterior con el fin de realizar el análisis efectos de los controles, registros

- y monitoreo correspondiente. Estos a su vez, de acuerdo con la gravedad del riesgo materializado y las consecuencias que el trae para RTVC, deben ser comunicado por el asesor de control interno elevar el caso al asesor de control interno disciplinario para los trámites correspondientes.

- Al implementar nuevos controles, los responsables de los procesos deben comunicarlo a la coordinación de planeación, la coordinación de TI y al oficial de seguridad (o su designado), para efectos de actualización de los mapas de riesgos.

- De acuerdo con la valoración de los riesgos, los responsables de los procesos deben tomar decisiones adecuadas y fijar los lineamientos en la administración de los riesgos, teniendo en cuenta las siguientes opciones:

    - ✓ Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado). Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.
    - ✓ 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. Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.
    - ✓ Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo y se transfiere o comparte una parte de este.

- Los líderes de los procesos, proyectos, supervisores de contratos, entre otros, deben realizar la medición y monitoreo de sus controles en términos de eficacia, eficiencia y efectividad para determinar la pertinencia, la necesidad de ajuste o modificación en caso de presentarse. Segunda línea de defensa de acuerdo con la guía del DAFP. 5

- La coordinación de Planeación de RTVC, realiza acompañamiento a los líderes de los procesos, en el monitoreo de la ejecución de los controles y planes de tratamiento propuestos para la vigencia, si se requieren ajustes en la matriz de riesgos del proceso, estos serán ejecutados conforme sea solicitado o de acuerdo con el plan de trabajo para la actualización de las matrices diseñados con los líderes de los procesos anualmente.

- Los ajustes sobre el mapa de riesgos de corrupción, de acuerdo con la pertinencia, se presentan al asesor de control interno, coordinador de planeación o a quien ellos deleguen, para su autorización, el cambio será reflejado en el mapa de riesgos de corrupción publicada en la página Web de RTVC y se realizarán las acciones de divulgación interna dispuestas por la coordinación de comunicaciones o las definidas por la coordinación de planeación.

- La evaluación al cumplimiento de las matrices de riesgos de gestión, corrupción y seguridad de la información y seguridad digital obedecerá a los planes definidos por la Oficina de Control Interno y las acciones definidas en el plan anticorrupción de la vigencia, esto incluye la publicación de los resultados de esta verificación.

- Los propietarios de los activos de información realizan la verificación de la matriz de riesgos de seguridad de la información y seguridad digital.

- Anualmente los líderes de los procesos o a quien estos deleguen, realizarán la revisión del contexto organizacional pertinente a la seguridad y privacidad de la información y cuando surjan cambios se y notificará al Oficial de Seguridad de la Información (o su designado) para realizar la actualización del contexto general de la organización frente a la administración de riesgos de seguridad de la información y seguridad digital.

- La administración de riesgos de seguridad de la información y seguridad digital debe contar con el análisis del líder del proceso y el asesoramiento del Oficial de Seguridad de la Información.

- La metodología de administración de riesgos de seguridad de la información y seguridad digital se alinea al contexto del “Modelo Integrado de Planeación y Gestión – MIPG-” y a la “Guía para la administración del riesgo y el diseño de controles en entidades públicas[6]”. La metodología se actualiza con base en los cambios realizados al modelo y la guía referenciados en el presente numeral.

[5] DAFP. Guía para la administración de riesgo y el diseño de controles de entidades públicas. 2018 página 79
[6] http://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

- El Oficial de Seguridad de la Información (o su designado) realiza el acompañamiento a los responsables del tratamiento de los riesgos de seguridad de la información y seguridad digital, orientando en las actividades de los correspondientes planes de tratamiento.

- El monitoreo y la revisión de las matrices de riesgos deben realizarse por lo menos una vez al año para su actualización y mantenimiento, salvo solicitud hecha por las partes interesadas pertinentes y/o por la Alta Dirección.

  RTVC adopta los niveles de impacto establecidos en la Guía de Administración de Riesgos del Departamento Administrativo de la Función pública -DAFP-, los cuales son: insignificante, menor, moderado, mayor y catastrófico. La definición de los niveles de impacto mencionados, se desarrollan en la metodología de gestión de riesgos de seguridad y privacidad de la información y seguridad digital.

  Para la definición de los niveles de impacto se debe considerar[7]:
  - Nivel de clasificación del activo de información impactado, de los procesos.
  - Violaciones de la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad)
  - Operaciones deterioradas (internas o de terceros)
  - Pérdida de negocio y valor financiero.
  - Interrupción de planes y plazos.
  - Daño de reputación

- Incumplimiento de requisitos legales, reglamentarios o contractuales.

  Nota: Esta política fue revisada en el marco del Comité Institucional de Gestión y desempeño realizado el 29 de abril de 2020.

[7] Tomado de la ISO 27005:2011, sección 7.2.3 Criterios de impacto.