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 en cualquier soporte, 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].
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

[1] Artículo 2.8.2.5.3 Decreto 1080 de 2015 Ministerio de Cultura
[2] Acuerdo 027 de 2006 Archivo General de la Nación

Ley[3]. Si es recibida a través del correo electrónico del colaborador, éste debe enviarla al correo correspondencia@rtvc.gov.co para su radicación en la Plataforma Orfeo.

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.
    - Empleo del formato de "acta de reunión" publicado en kawak, el cual debe ser diligenciado digitalmente, y enviado y aceptado a través de correo electrónico y firmado digital o electrónicamente conforme a los manuales de firma electrónica y digital.
    - 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).

5. Todas las áreas deben verificar de forma constante con fines de actualización, la normatividad legal vigente, manuales y procedimientos internos que aplique para el desarrollo en oportunidad y calidad de las funciones, trámites y/o procesos que se encuentren a su cargo.
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 que deban ser adelantados por RTVC, se deberán realizar de conformidad con la normatividad vigente que aplique para cada caso en concreto y lo definido por la Entidad en los diferentes manuales y procedimientos internos que se encuentren registrados en el sistema integrado de gestión.
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 la empresa.
10. Todas las personas deben aplicar la política operacional de tratamiento y protección de datos personales dentro de sus procesos y actividades como parte de sus responsabilidades, garantizando el buen manejo de la información que tenga en su poder o custodia, de la empresa y de los terceros con los que tenga relación directa y, asegurando la autorización del tratamiento de los datos

[3] Acuerdo 060 de 2001 Archivo General de la Nación

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

4.1. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La presente política operacional gobierna la Seguridad de la información de todos los procesos formalizados en el Sistema Integrado de gestión de RTVC, cubriendo a toda la organización. Debe ser cumplida por los directivos, servidores públicos, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con RTVC.

4.2. OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Establecer los lineamientos y responsabilidades frente a la gestión de la seguridad de la información bajo el ámbito institucional y marco normativo, que deben ser cumplidos por todos los colaboradores y partes interesadas pertinentes de RTVC, permitiendo resguardar, preservar y proteger los activos de información que tienen valor para RTVC, buscando mantener los niveles de confidencialidad, disponibilidad e integridad de la información requeridos por la entidad y, disminuyendo la probabilidad de materialización de riesgos de seguridad de la información y seguridad digital.

4.3. OBJETIVOS ESPECÍFICOS

- Definir las directrices para la protección de la información de RTVC junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar los niveles de confidencialidad, integridad y disponibilidad requeridos por la organización.
- Presentar en forma clara los elementos que conforman la política de seguridad de la información y seguridad digital que deben conocer, acatar y cumplir los directivos, servidores públicos, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con RTVC.
- Establecer las responsabilidades frente a la gestión de la seguridad de la información y seguridad digital en RTVC.

4.4. NORMATIVIDAD ASOCIADA

- **Ley 1341 de 2009.** "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC".
- **Documento CONPES 3701 de 2011.** "Lineamientos de Política para ciberseguridad y ciberdefensa".
- **Documento CONPES 3854 de 2016.** "Política Nacional de Seguridad Digital".
- **Ley Estatutaria 1581 de 2012.** "Protección de datos personales".
- **Ley 1266 de 2008.** "Disposiciones generales de habeas data y se regula el manejo de la información".
- **Ley 1712 de 2014.** "Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional".

- **Decreto 103 de 2015.** "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- **Decreto 1078 de 2015.** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1499 de 2017.** "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"
- **Decreto 1008 de 2018.** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información la Comunicaciones"
- **Ley 1928 de 2018.** "Por medio de la cual se aprueba el "Convenio sobre la ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest"
- **Resolución número 500 de 2021.** "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
- **NTC-ISO 27001:2013.** Es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información.
- **Directiva Presidencial No. 03 de 2021,** donde se dictan lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

4.5. LINEAMIENTOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y DE LA SEGURIDAD DIGITAL

- El propósito de la gestión de la seguridad de la información en RTVC es velar por el cumplimiento de los niveles de disponibilidad, integridad y confidencialidad de la información requeridos por la Organización.
- La Alta Dirección apoya tanto el establecimiento y cumplimiento de la presente política como la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información y Seguridad Digital, bajo un modelo acorde a las necesidades estratégicas y operativas de RTVC y en cumplimiento con el Modelo de Seguridad y privacidad de la información emitido por el MinTIC, con el fin de proteger la información y sus componentes en cuanto a la disponibilidad, confidencialidad e integridad de la información.
- Todos los elementos, políticas, procedimientos, lineamientos, controles, reglas, instructivos, etc., que constituyen el Sistema de Gestión de Seguridad de la Información y Seguridad Digital de RTVC deben ser revisados y actualizados con base en nuevas necesidades de las partes interesadas pertinentes y nueva normatividad y legislación aplicable. La revisión debe realizarse mínimo cada dos (2) años.
- RTVC divulga la Política de Seguridad de la Información y Seguridad Digital y vela por el cumplimiento de esta por parte de los servidores públicos, contratistas y terceros, desde la premisa que todos son responsables de su cumplimiento.

- RTVC promueve la cultura de seguridad de la información en los servidores públicos, contratistas, proveedores y partes interesadas pertinentes al Sistema de Gestión de Seguridad de la Información y Seguridad Digital, a través de campañas de sensibilización.
- RTVC promueve la protección de la información generada, procesada o almacenada, producto de sus procesos de negocio con el fin de minimizar impactos operativos, financieros, legales y aplicará los controles necesarios para tal fin.
- Se debe garantizar la seguridad de la información y la seguridad digital frente a incidentes de seguridad que atenten contra la continuidad de la operación.
- RTVC vela por mantener los controles y procedimientos que permitan proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos internos críticos.
- RTVC cumplirá la normatividad y la regulación definida por el Estado Colombiano con relación a la Seguridad Digital y el cumplimiento de la Política de Gobierno Digital en cuanto a su habilitador transversal "Seguridad de la Información".
- Los responsables de la gestión de la seguridad de la información y de la seguridad digital, respaldan la innovación tecnológica, por medio de una adecuada gestión de riesgos e identificación de requisitos de seguridad bajo un entorno de trabajo colaborativo en los proyectos y ámbitos de trabajo que lo requieran.
- Todos los servidores públicos, contratistas, pasantes, proveedores y partes interesadas pertinentes, deben atender las políticas institucionales y legales en materia de seguridad de la información y seguridad digital, con el fin de minimizar la materialización de riesgos sobre los activos de información de RTVC.
- Es responsabilidad institucional de los servidores públicos, contratistas, pasantes y proveedores de RTVC prevenir la fuga y pérdida de información de la entidad, así como, las acciones que van en contra de los principios de preservación y correcta administración de los activos de información.
- Les corresponde a todos los propietarios de los activos y activos de información la verificación, aprobación y actualización de la matriz de inventario y clasificación de activos y la matriz de riesgos de seguridad de la información y seguridad digital.
- Anualmente, los dueños de los procesos o sus delegados realizarán la revisión del contexto organizacional pertinente a la seguridad y privacidad de la información y, cuando surjan cambios les corresponde notificar y enviar los ajustes o cambios al Oficial de Seguridad de la Información, para realizar la actualización del contexto general de la organización frente a la administración de riesgos de seguridad de la información y seguridad digital.

De acuerdo con lo anterior, esta política aplica a los servidores públicos, contratistas, pasantes o practicantes, proveedores, clientes y la ciudadanía en general que tenga vínculo o relación con RTVC.

4.6. Organización De La Seguridad De la Información

4.6.1 Liderazgo y Compromiso

La Alta Dirección de RTVC es la responsable de facilitar los recursos humanos, técnicos y financieros necesarios para llevar a cabo la implementación y mantenimiento de esta política y promoverá el compromiso con su aplicación y cumplimiento.

En la resolución 147 de 2018 “Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, se crea el Comité Institucional de Gestión y Desempeño en Radio Televisión Nacional de Colombia – RTVC - y se dictan otras disposiciones”, se definen las funciones del Comité Institucional de Gestión y Desempeño, con respecto a la seguridad de la información, de la siguiente manera:
“Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información”.
“Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información”.
“Orientar la implementación de la política de Gobierno Digital”.

4.6.2. ROLES Y RESPONSABILIDADES

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:

- Liderar la implementación del Sistema de Gestión de Seguridad de la Información y Seguridad Digital (SGSI) de RTVC según el Modelo de Seguridad y privacidad de la Información para la entidad y de conformidad con la normatividad vigente.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del SGSI.
- Liderar y brindar acompañamiento a los procesos de la Entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Elaborar, promover y mantener la política de seguridad de la información y seguridad digital de RTVC.
- Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad de la información para servidores públicos y contratistas.
- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad
- Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

- Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.
- Realizar, por lo menos una vez al año, revisiones del Sistema de Gestión de Seguridad de la Información - SGSI y promover el compromiso en el desarrollo y mejoramiento de este.
- Acompañar e impulsar el desarrollo de proyectos de seguridad de la información y seguridad digital.

- Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información con los procesos de la entidad.

OFICINA ASESORA JURÍDICA

- Brindar asesoría a los procesos de la Entidad en temas jurídicos y legales relacionados con seguridad y privacidad de la información, que involucren acciones ante las autoridades competentes.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes relacionados con seguridad y privacidad de la información, que involucren acciones ante las autoridades competentes
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Representar a la Entidad ante las autoridades competentes, en procesos judiciales relacionados con seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

USUARIOS INTERNOS, EXTERNOS DE RTVC

- Los servidores públicos, contratistas, pasantes y proveedores de RTVC son responsables de proteger la información que generan, procesan, presentan, transmiten o almacenan, evitando su pérdida, alteración, manipulación no autorizada o destrucción.
- Los servidores públicos, contratistas, pasantes y proveedores de RTVC deben reportar los incidentes de seguridad de la Información, eventos sospechosos y el mal uso de los recursos tecnológicos que identifiquen, a la Coordinación de Tecnologías de la Información por los medios que se dispongan para garantizar la adecuada gestión de estos.
- Los servidores públicos, contratistas, pasantes y proveedores de RTVC tienen la obligación de proteger las unidades de almacenamiento físicas y lógicas que contengan información de RTVC y se encuentren bajo su responsabilidad.
- Los servidores públicos, contratistas, pasantes y proveedores de RTVC deben aceptar los acuerdos de confidencialidad, las políticas y controles de seguridad definidos por RTVC, los cuales reflejan los compromisos de protección y buen uso de la información y sus activos de acuerdo con los criterios establecidos en la normatividad vigente y la política de seguridad de la información. Estos acuerdos se encuentran estipulados y establecidos en los contratos de trabajo de los servidores públicos, los contratos para proveedores y demás contratos o acuerdos y se vigila su cumplimiento en la gestión de contratación de RTVC.
- Los servidores públicos, líderes de procesos o sus delegados, deben realizar la identificación, clasificación y valoración de los activos de información de su área, así como la identificación y gestión de riesgos de seguridad de la información y seguridad digital con el acompañamiento del equipo de seguridad de la información.

- Los servidores públicos, líderes de procesos o sus delegados, que tengan activos de información bajo su responsabilidad, deben ejecutar los controles definidos durante el proceso de identificación y valoración de riesgos de seguridad de la información y seguridad digital, así como, presentar las evidencias durante los seguimientos que se realicen.

4.7 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

RTVC ha establecido las siguientes políticas específicas de Seguridad de la Información y Seguridad Digital, las cuales atienden las necesidades en cuanto a la protección de sus activos de información y se soportan en los procesos y procedimientos que apoyan su cumplimiento.

4.7.1 GESTIÓN DE ACTIVOS

Los activos de información de RTVC, serán identificados y clasificados para establecer los mecanismos de protección necesarios de acuerdo con su valoración, al menos una vez al año y según la **Guía para la Gestión y Clasificación de activos de Información de RTVC,** la cual provee, de acuerdo a la normatividad vigente, los criterios, instrumentos y mecanismos para la identificación y clasificación de los activos de información con el fin de determinar su nivel de criticidad con respecto a las propiedades de la información que se deben preservar (confidencialidad, disponibilidad e integridad).

La identificación y valoración de activos debe ser realizada por líderes de los procesos y/o sus designados para tal fin, con acompañamiento del equipo de Seguridad de la información y conforme a los procesos documentados en el Sistema de Gestión de calidad de RTVC. Cada activo identificado deberá tener un propietario designado, quien será el responsable por la adecuada protección de los activos y de la ejecución de los controles.

Los servidores públicos, contratistas y terceros que tengan relación con RTVC, deben devolver los activos de información que tengan asignados, según los mecanismos previstos, una vez finalizada su relación laboral, acuerdo o contrato con la Entidad.

4.7.2 USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

- Toda la información generada, modificada y almacenada en la infraestructura física y tecnológica de RTVC que no sea pública, es para uso exclusivo en sus procesos de negocio y cualquier uso distinto debe ser autorizado explícitamente por RTVC como dueño de esta.
- El acceso a los documentos físicos y digitales, así como a los sistemas de gestión de documentos e información será controlado. Este control incluye restricción o permisos y niveles de acceso detallado para servidores públicos, contratistas, pasantes y terceros de acuerdo con sus funciones y responsabilidades. Estos permisos deben ser definidos y aprobados por los custodios de la información, dueños de los aplicativos y/o supervisores de contrato, estableciendo claramente periodos de inicio y fin con base en la información documentada (contratos, convenios, normatividad, legislación, etc.) y cumpliendo con el principio de mínimo privilegio; tales controles deben ser gestionados por los administradores de los sistemas de

información y los responsables de archivo y gestión documental -según corresponda-, asegurando la trazabilidad de estos.

- Los servidores públicos, contratistas y colaboradores de RTVC deben ejecutar sus actividades laborales desde equipos corporativos o equipos que cumplan con los controles de seguridad mínimos. Estos equipos deben surtir un proceso de alistamiento y aseguramiento por parte de la Coordinación de T.I.
- Cada equipo de cómputo de escritorio o móvil asignado a servidores públicos, contratistas y colaboradores de RTVC estará preparado con los componentes de hardware y software requerido para el cumplimiento de sus funciones. No se podrá alterar el contenido físico, lógico o de configuración del equipo de cómputo asignado, sin la autorización de la Coordinación de T.I.
- El equipo de cómputo de escritorio o móvil asignado a servidores públicos, contratistas y colaboradores de RTVC solo podrá ser utilizado para la ejecución de sus funciones y no para asuntos personales.
- Los servidores públicos, contratistas y colaboradores de RTVC deberán utilizar únicamente los programas y equipos autorizados por la Coordinación de T.I. No está permitida la instalación de programas o extensiones de navegadores de fuentes desconocidas ya que estas pueden traer *malware* (software malintencionado) que puede afectar la integridad de los dispositivos y exponer la información sensible.
- Las cuentas de usuario son de uso personal y por ninguna razón debe compartirse. Cada usuario es responsable de las transacciones y acciones que se ejecuten con su cuenta de usuario.
- Ningún usuario deberá acceder a la red o a los servicios de RTVC, utilizando la cuenta de usuario de otra persona.
- Cuando se utilicen aplicaciones de mensajería instantánea desde los equipos de cómputo o desde la red interna de RTVC, estas deben garantizar el uso de encriptación extremo a extremo *(end-to-end)* y contar con una política de privacidad y tratamiento de datos aceptable que incluya entre otras cosas, información y contacto del responsable del uso y mantenimiento de los datos, propósito del uso de los datos y límites de conservación.
- La información de RTVC debe ser almacenada en las unidades compartidas asignadas a cada área para garantizar que cuenta con copias de respaldo y pueda ser recuperada en caso de incidentes, según lo indicado en la **Política operacional para la administración de infraestructura de T.I.**
- Las conexiones remotas que se establezcan por parte de los administradores de tecnología, grupos de soporte y usuarios en general, a equipos ubicados en la red interna de RTVC deben realizarse siempre a través de la VPN (Red privada virtual).
- El uso del correo electrónico institucional deberá regirse por los siguientes lineamientos:
    - Los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
    - El servicio de correo electrónico institucional debe utilizarse exclusivamente para las tareas propias de la función desarrollada en RTVC y no debe utilizarse para ningún otro fin.

- Los mensajes y la información contenida en los buzones de correo electrónico institucional son propiedad de RTVC y cada responsable debe mantener únicamente los mensajes relacionados con el desarrollo de sus obligaciones.
- No está permitido el envío de cadenas de mensajes de ningún tipo.
- No está permitido el envío de correos con contenido que atenten contra la integridad y dignidad de las personas o instituciones.
- Es responsabilidad del usuario titular, informar a la Coordinación de T.I. cuando un correo electrónico sea de dudosa procedencia, con el fin de que se tomen las medidas necesarias para evitar su propagación dentro de la entidad.
- Es responsabilidad de cada usuario verificar los destinarios a los cuales va dirigida una comunicación, si son listas de distribución, deben revisarse con detalle con el fin de evitar compartir información con personas no autorizadas.

- El servicio de acceso a Internet se presenta como una herramienta de trabajo que facilita a los colaboradores realizar las actividades propias de sus responsabilidades en RTVC, por lo cual el uso adecuado de este recurso se debe monitorear y controlar, así mismo, debe estar sujeto a los siguientes lineamientos:
  - No está permitido el uso del servicio de acceso a internet de RTVC para ingresar a páginas web relacionadas con pornografía, sustancias alucinógenas, armas, terrorismo, racismo, alcohol, web proxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
  - No está permitido el uso del servicio de acceso a internet de RTVC para el intercambio no autorizado de información de propiedad de RTVC o de sus servidores públicos.
  - Cada uno de los usuarios es responsable de dar un uso adecuado al servicio de acceso a internet de RTVC y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra los activos de información de RTVC, contra terceros, contra la legislación vigente o los lineamientos de seguridad de la información.
  - Los servidores públicos, contratistas, pasantes y terceros que tengan relación con RTVC, no deben asumir en nombre de RTVC posiciones personales en encuestas de opinión, foros u otros medios similares que se encuentren en Internet.
  - La descarga de archivos desde Internet debe ser con propósitos institucionales, de forma razonable para no afectar el servicio y manteniendo las buenas prácticas de seguridad para evitar ser víctima de ataques por virus u otros programas maliciosos.
  - El uso de Internet es considerado permitido, a excepción de las restricciones anteriores, siempre y cuando se realice de acuerdo con las políticas institucionales (ética, razonable, responsable, no abusiva y sin afectar la productividad de RTVC).
- Uso de dispositivos móviles:
  - Todos los dispositivos móviles que almacenen o procesan información de RTVC deben tener instalado un software antivirus y mantener el sistema operativo actualizado.
  - Los usuarios de dispositivos móviles institucionales deben tener instaladas únicamente las aplicaciones autorizadas y configuradas por la Coordinación de T.I.
  - No está permitido cambiar la configuración, instalar o desinstalar software, formatear o restaurar de fábrica los dispositivos móviles entregados por el RTVC a servidores públicos, contratistas y colaboradores.

    - Los usuarios de dispositivos móviles asignados por RTVC, deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo, así mismo deben evitar conectarse a redes inalámbricas (WIFI) públicas donde pueda ponerse en riesgo la seguridad de la información de la entidad.
    - Ante la pérdida de un dispositivo móvil asignado por RTVC, ya sea por extravío o hurto, el responsable deberá informar de manera inmediata a la Coordinación de T.I.
- El uso de las redes sociales dentro de las redes internas y/o haciendo uso de los recursos y servicios tecnológicos de RTVC, estará autorizado solo para aquellos usuarios que lo requieran para el cumplimiento de sus funciones y para facilitar canales de comunicación con la ciudadanía, en estos casos deberá regirse por los siguientes lineamientos:
    - Los responsables de las cuentas corporativas no deben divulgar el usuario y/o contraseña de acceso a las cuentas corporativas de RTVC en redes sociales.
    - Los responsables de las cuentas corporativas deben cambiar las contraseñas de manera periódica y usar doble factor de autenticación en los casos que aplique.
    - No se debe iniciar sesión en redes sociales desde dispositivos públicos o cuando se está conectado a redes públicas.
    - Se deben mantener actualizados los ajustes en cuanto a seguridad y privacidad en las cuentas corporativas de RTVC en redes sociales.
    - No se debe abrir, desde los perfiles corporativos, enlaces o adjuntos que presenten comportamientos sospechosos.
- Los servidores públicos, contratistas y colaboradores de RTVC que realicen impresiones de documentos con clasificación “pública reservada” o “pública clasificada”, deben supervisar la impresión y no dejarla desatendida, así mismo, deben retirar de la impresora todos los documentos impresos, incluso si han sido generados con errores de impresión.
- Los servidores públicos, contratistas, pasantes y proveedores de RTVC deben informar sobre cualquier violación de las políticas de seguridad, uso indebido de recursos tecnológicos e información y debilidades de seguridad de la información de RTVC de las cuales tenga conocimiento, así como, reportar los incidentes de seguridad de la Información y eventos sospechosos, a la Coordinación de T.I. por los medios que se dispongan para garantizar la adecuada gestión de estos.

4.7.3 POLÍTICAS DE CONTROL DE ACCESO

RTVC implementa y mantiene controles de acceso físico y lógico sobre las instalaciones, infraestructura, sistemas y servicios de información, que incluyen, la selección y contratación de personal con la validación de antecedentes penales y legales, procedimientos de identificación, manejo de usuarios y contraseñas, manejo de control de accesos biométricos y sistemas de vigilancia física, circuitos cerrados de video vigilancia y monitoreo, todo con el fin de asegurar que los activos de información sean preservados, protegidos y estén disponibles cuando sean requeridos por personal autorizado.

4.7.3.1 CONTROL DE ACCESO FÍSICO

La identificación del personal que ingresa a la entidad es obligatoria, éste debe portar, durante su estancia dentro de las instalaciones de RTVC, las identificaciones asignadas: carné, etiquetas y/o tarjetas de acceso, entre otras.

RTVC implementa mecanismos y procedimientos necesarios para realizar un control de acceso físico adecuado sobre sus instalaciones y sobre su infraestructura física.

Todas las áreas de RTVC destinadas al procesamiento o almacenamiento de información física o electrónica, confidencial y reservada, así como aquellas en las que se encuentren los equipos y demás infraestructura que soporta los sistemas de información y comunicaciones, están protegida con medidas de control de acceso físico que permiten proteger los activos de información contra amenazas de seguridad de la información y seguridad digital.

4.7.3.2 CONTROL DE ACCESO LÓGICO

RTVC implementa los controles necesarios para asegurar el acceso lógico a los activos de información, mediante procedimientos y mecanismos que incluyen la gestión de identidades a través del uso de nombre de usuario y contraseña y la asignación de permisos de autorización bajo el principio de mínimo privilegio, manejo de llaves cifradas, detección biométrica, entre otros, estos deben contar con el debido licenciamiento y funcionalidad plena y son implementados previa autorización de los supervisores de contrato o líderes de proceso, así mismo, tales vigencias una vez expiradas deben surtir las fases de desactivación y eliminación previo cumplimiento de requisitos contractuales.

Los privilegios de acceso a plataformas, aplicativos, servicios y en general cualquier recurso de información de RTVC deben ser asignados de acuerdo con la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de RTVC, así como con el cumplimiento a la normatividad vigente a la protección de acceso a la información presente en los sistemas de información.

Los servidores públicos, contratistas y terceros que dispongan de acceso a las plataformas tecnológicas de RTVC son responsables del cuidado de su información de autenticación y de la información institucional a la que acceda, cumpliendo con todas las normas de seguridad de la entidad.

Así mismo, se deben seguir todos los lineamientos para el control de acceso estipulados en la **Política operacional para la Administración de infraestructura de T.I.**

4.7.4 AMBIENTES DE TESTEO

La Coordinación de T.I. dispondrá de ambientes controlados para realizar tareas de testeo, calidad o pruebas funcionales, de rendimiento y/o seguridad de la infraestructura tecnológica y sistemas de información.

En la infraestructura en producción se podrán utilizar usuarios de prueba, siempre y cuando cumplan con lo especificado en la **Política para la administración de la infraestructura de T.I.**, numeral 4.2.5.1.3 Cuentas de Usuario de testeo o pruebas.

4.7.5 POLÍTICA DE NO REPUDIO

RTVC establece los mecanismos y controles pertinentes en los sistemas de información, los servicios de información y en los servicios en línea por medio de los cuales se realicen solicitudes, procesamiento y entrega de información para determinar el directo responsable de dicha acción. Los mecanismos y controles de no repudio se aplicarán a aquellos servicios de T.I. que sean solicitados por el líder del proceso dueño de la información que se gestiona y la aprobación de la Coordinación de T.I., con base en el análisis de viabilidad de la solución, o por exigencia de un requisito legal.

4.7.6 PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La protección de datos personales es atendida por la **Política de Protección de Datos de RTVC**.

Todos los servidores públicos, contratistas, pasantes y proveedores de RTVC deben aceptar los acuerdos de confidencialidad definidos por la entidad, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella. Este compromiso de confidencialidad debe estar en los respectivos contratos por medio de una cláusula de confidencialidad.

No se debe exponer información personal o sujeta a reserva en enlaces de internet públicos cuyo acceso se genere sin autenticación.

4.7.7 INTEGRIDAD

Toda información verbal, física o electrónica, debe ser procesada y entregada o transmitida exacta y completa, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

La pérdida de integridad de los activos de información son responsabilidad de sus propietarios y/o responsables. Cualquier evento en el cual haya pérdida de integridad de un activo de información debe ser reportado a la autoridad pertinente (supervisor del contrato, jefe inmediato, oficina de control interno disciplinario, autoridades de orden público), con el fin de realizar el debido proceso ante la situación presentada.

4.7.8 DISPONIBILIDAD DE LOS ACTIVOS DE INFORMACIÓN

RTVC mediante el uso de mecanismos tecnológicos, procedimientos y directrices garantiza la disponibilidad requerida de los activos de información protegiéndola contra eventos negativos que puedan originarse de manera externa o interna, desde fuentes involuntarias o provocadas.

RTVC cuenta con procedimientos en el proceso de Gestión de Tecnología de la Información, formalizado en el Sistema de Integrado de Gestión, que permiten monitorear, gestionar y controlar las interrupciones de los sistemas y servicios de información.

RTVC con el fin de garantizar la disponibilidad de la información, cuenta con procedimientos para la gestión de cambios en la infraestructura tecnológica.

En los contratos de servicios de tecnología con proveedores o externos, se deben establecer los acuerdos de niveles de servicio en donde los niveles de disponibilidad sean los acordados y aprobados por RTVC.

4.7.9 INTERCAMBIO DE INFORMACIÓN

Todo servidor público y contratista de RTVC es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

RTVC no se hace responsable por la pérdida o daño de la información de los usuarios que sea de uso personal.

4.7.10 CRIPTOGRAFÍA

Todos los servicios expuestos al ciudadano deben proteger la información haciéndola ilegible, a través de mecanismos que permitan codificar los datos para impedir el acceso a usuarios no autorizados y garantizar la confidencialidad, disponibilidad, integridad y autenticidad de esta (certificados, firmas digitales, protocolos de conexión seguros, hash, entre otros)

4.7.11 GESTIÓN DE LOGS Y REGISTRO DE AUDITORÍA

Todos los sistemas de información, aplicativos, sistemas operativos, bases de datos, dispositivos de comunicaciones, dispositivos de seguridad y servidores, deben contar con los logs de auditoría que registren las actividades de los usuarios, las fallas y eventos de seguridad.

Es responsabilidad de los administradores de sistemas, aplicativos, servidores y dispositivos de T.I., activar y conservar los registros de auditoria existentes en cada componente, así mismo se debe mantener un inventario de los registros de auditoria existentes y su ubicación.

4.7.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Coordinación de T.I. mantendrá un servicio de monitoreo continuo para detectar, revisar, analizar e informar sobre eventos e incidentes de seguridad, a través de herramientas tecnológicas, servicios de terceros, y/o recursos humanos internos. Cada herramienta de monitoreo debe dejar registro de los servicios monitoreados y de los eventos detectados.

Los servidores públicos, contratistas y colaboradores de RTVC deberán informar, a través de la mesa de servicios, tan pronto como sea posible, debilidades, eventos o incidentes que pueda tener un impacto en la seguridad de los activos de la organización.

La Coordinación de T.I. de RTVC, apoya el procedimiento de Gestión de Incidentes de Seguridad de la información, definiendo la matriz de escalamiento y el mecanismo para realizar el reporte y la atención de los casos que se identifiquen como incidentes de seguridad de la información.

Las áreas de Servicios Generales y la Oficina asesora jurídica apoyan el proceso de gestión de incidentes de seguridad de la información para los casos en los que se requiera la denuncia policial o penal por impactos a nivel económico, legal, de imagen y demás que se consideren y que requieran surtir dicho proceso.

5 AUDITORÍA

La Oficina de control interno de RTVC mantiene la Política operacional de Control Interno y dentro de su plan de auditorías, lleva a cabo las auditorias periódicas a los sistemas de información al igual que las actividades relacionadas a la gestión de activos de la información, de la misma manera divulga los resultados, para que de allí se establezcan las acciones de mejora, planes de remediación y se genere la sensibilización a las personas para que optimicen sus procesos y actividades en función de la seguridad de la información.

6 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El uso eficiente de los recursos y servicios informáticos, así como el adecuado manejo de los activos de información, exige por parte de los usuarios el conocimiento y habilidades en su manejo; por lo tanto, RTVC brinda orientación en el uso y seguridad sobre los mismos, con el objetivo de minimizar los riesgos de seguridad de la información o seguridad digital que puedan presentarse.

La alta dirección consciente de que el recurso humano es considerado el eslabón más importante en la cadena de la Seguridad de la Información, promueve el desarrollo de los planes de capacitación de seguridad de la información y seguridad digital.

El área de Gestión de Talento Humano, la Coordinación de T.I. y el área de Comunicaciones apoyan en la capacitación y sensibilización sobre seguridad de la información, incluyendo esta temática en los planes de capacitación, con el fin de fortalecer la cultura en seguridad de todos los colaboradores de la entidad.

Todos los servidores públicos, contratistas, pasantes y proveedores de RTVC están obligados a participar en las sensibilizaciones como parte de sus responsabilidades contractuales; así mismo, deben demostrar el entendimiento y compromiso aplicando las buenas prácticas transmitidas en las actividades desarrolladas.

La Coordinación de T.I. establece y promueve políticas y/o procedimientos para guiar el debido comportamiento de las personas en su rol de usuarios de los sistemas de información de RTVC, en estas se imparten las directrices principales sobre el uso adecuado de los servicios y sistemas de información, así como, las buenas prácticas para el uso aceptable, ética para ambientes digitales, entre otros.

El área de gestión documental desarrolla guías, políticas y procedimientos, para el debido comportamiento de las personas como generadoras, modificadoras o custodios de los documentos físicos o electrónicos de RTVC, y sobre estas promueve la capacitación y la sensibilización, para que se realice la adecuada identificación, clasificación y preservación de la información.

GLOSARIO

- **Activo de información**: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.[4]

- **Criptografía:** Es un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por aquellos usuarios que no estén autorizados a hacerlo.

- **Certificado digital:** Es un documento digital que prueba la identidad de una persona o entidad en Internet.

- **Control**: Medidas que se implementan para modificar el riesgo.

- **Firma Electrónica:** Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permiten identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.[5] La firma electrónica es un género que incluye la firma digital.

- **Firma digital**: Mecanismo criptográfico que, aplicado a un documento electrónico, permite al receptor identificar al firmante de manera inequívoca y garantizar que el documento es original y no ha sufrido ningún tipo de manipulación o alteración desde su firma.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.[6]

- **Hash:** Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

- **Incidente de Seguridad de la Información**: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.[7]

[4] CONPES 3854 de 2016
[5] Decreto 2364 de 2012
[6] Modelo de seguridad y privacidad de la información – MinTIC
[7]Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información – MinTIC

- **Logs:** Registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.[8]

- **Principio de mínimo privilegio**: Se refiere a la práctica de otorgar los permisos necesarios y suficientes a un usuario para desempeñar sus actividades, por un tiempo limitado, y con el mínimo de privilegios necesarios para la realización de sus tareas.

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

- **Seguridad de la información:** Hace referencia a la preservación de la confidencialidad (que la información no se revelada a personas no autorizados), integridad (que se conserve su exactitud y completitud) y disponibilidad (que sea accesible y utilizable cuando se requiera por personas autorizadas) de la información en cualquier medio: impreso o digital.

- **Seguridad digital**: es la preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.[9]

- **T.I.**: Tecnologías de la información

La presente política debe ser divulgada y se debe promover su cumplimiento, por las partes interesadas, entendiéndose que el incumplimiento de alguno de sus propósitos puede conllevar a sanciones legales, judiciales, o económicas, dependiendo de cada caso en particular, definidas por RTVC y el Estado Colombiano en la normatividad vigente, asociada a la seguridad de la información en las Entidades del Estado de Orden Nacional.

Nota: Esta política fue revisada en el marco del Comité Institucional de Gestión y desempeño realizado el 22 de junio de 2022.

[8] CONPES 3701 de 2011
[9] Modelo de seguridad y privacidad de la información – MinTIC