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 que hacer 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].
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

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

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 formato 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.

5. Todas las áreas deben estar en constante actualización del marco normativo 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.
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 DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

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

Establecer la responsabilidad y manejo 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 representan valor para RTVC buscando mantener la confidencialidad, disponibilidad e integridad de la información y, disminuyendo la probabilidad de materialización de riesgos de seguridad de la información y seguridad digital.

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

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

La presente política operacional aplica a todos los activos de información, todos los colaboradores y partes interesadas pertinentes y, a todos los procesos del sistema integrado de gestión de RTVC.

4.3. CONTEXTO

Para el establecimiento de la política de seguridad de la información y seguridad digital se tiene en cuenta la misión, visión y objetivos estratégicos de RTVC; adicionalmente, se toman como criterios rectores los establecidos en la Política de Gobierno Digital[5], la Política Nacional de Seguridad Digital[6], el Modelo de Seguridad y Privacidad de la Información[7] y la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

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

- Todos los colaboradores (servidores y trabajadores públicos, contratistas, practicantes/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 ocurrencia de riesgos sobre los activos de información de RTVC.
- Les corresponde a todos los dueños de los activos y activos de información la verificación, aprobación y actualización de las matrices 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.
- 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.
- 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.
- La Alta Dirección apoya tanto el establecimiento y cumplimiento de la presente política como el mantenimiento, monitoreo y mejora continua del Sistema de Gestión de Seguridad de la Información y Seguridad Digital de RTVC.

[5] Decreto 1008 de 2018 emitido por el MinTIC.
[6] Documento CONPES 3854 de 2016 emitido por el DNP.
[7] Documento maestro y las guías para su implementación, emitido por el MinTIC.

- 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.
- 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.
- Garantizar la continuidad de la seguridad de la información y de la seguridad digital frente a incidentes de seguridad que atenten contra la continuidad de la operación.
- RTVC se compromete con implementar un Sistema de Gestión de Seguridad de la Información y Seguridad Digital, bajo un modelo acorde a las necesidades estratégicas, operativas que requiera RTVC, con el fin de proteger la información y sus componentes en cuanto a la disponibilidad, confidencialidad e integridad de la información.
- RTVC Divulga la Política de Seguridad de la Información y Seguridad Digital que vela por el cumplimiento de esta, aceptada por cada uno de los colaboradores - servidores públicos, contratistas y terceros- desde la premisa que todos son responsables de su cumplimiento.
- 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.
- RTVC protege la Información de las posibles amenazas originadas externa e internamente.
- 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 en relación a la Seguridad Digital y el cumplimiento de la Política de Gobierno Digital en cuanto a su habilitador transversal Seguridad de la Información.

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

4.5. 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”.
- **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"
- Documento maestro del Modelo de Seguridad y Privacidad de la Información del MinTIC y, sus correspondientes guías.
- **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.

4.6. 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.

4.6.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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, y se dictan otras disposiciones." se crea el Comité Institucional de Gestión y Desempeño y, en su *artículo 6 Funciones del Comité* se establece "6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información" y "7. Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información".

4.6.1.1 ROLES Y RESPONSABILIDADES

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN:

- Lidera la implementación del Sistema de Gestión de Seguridad de la Información y Seguridad Digital (SGSI) de RTVC.
- Es responsable de planear, coordinar y administrar los procesos de seguridad de la información y seguridad digital de RTVC.
- Elaborar, promover y mantener la política de seguridad de la información y seguridad digital de RTVC.

- Liderar la gestión de riesgos de la seguridad de la información y seguridad digital de RTVC.
- Liderar el control de los Riesgos y determinar planes de acción cuanto estos sean necesarios.
- Difundir la cultura de seguridad de la información dentro de RTVC.
- Liderar, gestionar y analizar las incidencias de seguridad que se presenten en RTVC.
- Definir y controlar los indicadores definidos por el SGSI.

COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

- Revisar los diagnósticos del estado de la seguridad de la información y seguridad digital de RTVC.
- Aprobar el uso de metodologías, documentos y procesos específicos para la seguridad de la información y seguridad digital de RTVC.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año), estas contemplan los planes de acción presentados para el mejoramiento del sistema.
- Acompañar e impulsar el desarrollo de proyectos de seguridad de la información y seguridad digital.
- Promover el compromiso en el desarrollo y mejoramiento del SGSI.
- Realizar el seguimiento a los indicadores de gestión del Sistema de Gestión de Seguridad de la Información y Seguridad Digital de RTVC.

USUARIOS O COLABORADORES 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 disponga la Coordinación 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 se encuentren bajo su responsabilidad, aún cuando no se utilicen y contenga información de valor para RTVC.

- 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.

4.6.2. GESTIÓN DE ACTIVOS

Se entiende por activo de Información 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.
Los activos de información físicos y lógicos de RTVC, serán identificados y clasificados para establecer los mecanismos de protección necesarios de acuerdo a su valor; el proceso de Gestión Documental, así como las guías del Modelo de Seguridad y Privacidad de la Información del MinTIC y, la normatividad vigente proveen los criterios, instrumentos y mecanismos para la identificación o actualización del inventario de activos de información que permita clasificar y etiquetar la información y definir la propiedad de los activos.

a. USO ADECUADO DE LOS ACTIVOS DE INFORMACIÓN

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 segregado para servidores públicos, contratistas, pasantes y terceros de acuerdo con sus funciones y responsabilidades. Estos permisos deben ser determinados y aprobados por los custodios de la información, dueños de los aplicativos, los supervisores de contrato y/o el comité de seguridad de la información con periodos de inicio y fin claramente establecidos con base en información documentada (contratos, convenios, normatividad, legislación, etc.); 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.

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.

Es responsabilidad institucional de los servidores públicos, contratistas, pasantes y proveedores de RTVC evitar y prevenir la fuga y pérdida de información de RTVC, así como las acciones que van en contra de los principios de preservación y correcta administración de los activos de información.

Los activos de RTVC deben ser identificados, controlados y clasificados para lograr su protección, uso adecuado y recuperación ante situaciones perjudiciales. RTVC cumpliendo con la normatividad vigente y lo establecido en el Modelo de Seguridad y Privacidad de la Información elabora y mantiene el inventario de activos de información. Lo anterior debe permitir la “Identificación de activos”, “Clasificación de activos” y “Etiquetado de la información” para una adecuada gestión de seguridad de la información.

El proceso de Gestión Documental con el apoyo de la Alta Dirección y la asesoría del Oficial de Seguridad de la Información deberán implementar los controles necesarios para que los archivos de

gestión estén debidamente custodiados y protegidos contra amenazas -como acceso no autorizado por personal, humedad, fuego, polvo, etc.- permitiendo lograr los niveles requeridos de confidencialidad, integridad y disponibilidad necesarios.

La clasificación y etiquetado de la información se realiza conforme lo establecido en la normatividad vigente, la guía para la gestión y clasificación de activos de información del MSPI y a procedimiento(s) que correspondan del SGC y que estén aprobados y oficializados.

b. DISPONIBILIDAD DE LOS ACTIVOS DE INFORMACIÓN

RTVC mediante el uso de mecanismos tecnológicos, procedimientos, procesos y directrices permite la disponibilidad necesaria de los activos de información protegiéndola contra eventos negativos que pueden originarse de manera externa o interna, desde fuentes involuntarias o provocadas.
En los contratos de servicios de TI con proveedores se deben establecer los acuerdos de niveles de servicio en donde los niveles de disponibilidad de estos son acordados y aprobados por RTVC.

RTVC cuenta con procedimientos en el proceso de Gestión Tecnológica de la Información, que permiten gestionar y controlar las interrupciones sobre los sistemas de información con el fin de minimizar los tiempos de interrupción.

RTVC con el fin de mantener la disponibilidad de la información, cuenta con sistemas de información cuya arquitectura permite reducir los riesgos y probar los cambios realizados, antes de llevarlos a producción.

4.6.3. 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, selección y contratación de personas con la validación de antecedentes penales y legales, identificación de personal, 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 al personal autorizado.

a. CONTROL DE ACCESO FÍSICO

La identificación del personal que ingresa de manera física es obligatoria y deben portar las identificaciones asignadas, carné, etiquetas, tarjetas de acceso, durante la estancia dentro de las instalaciones de RTVC.
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, es protegida con medidas de control de acceso físico que permitan proteger los activos de información contra amenazas de seguridad de la información y seguridad digital.

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

b. CONTROL DE ACCESO LÓGICO

RTVC implementa los controles necesarios para asegurar el acceso lógico a los activos de información, mediante procedimientos y mecanismos que pueden incluir manejo de usuarios y claves de longitud y complejidad elevada, permisos de autorización, manejo de llaves cifradas, detección biométrica, etc., 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 des habilitación y eliminación previo cumplimiento de requisitos contractuales..

El acceso a plataformas, aplicativos, servicios y en general cualquier recurso de información de RTVC debe ser asignado 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.

c. ACCESO A INTERNET

El acceso a internet se permite como una herramienta de trabajo que facilita a los colaboradores realizar las actividades propias del negocio de RTVC, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear. El uso de este recurso debe atender las siguientes reglas:

- Se prohíbe el uso de este recurso para el acceso a páginas 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.
- Se prohíbe el uso de este recurso 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 a este recurso 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, al igual que los empleados o subcontratistas de estos no deben asumir en nombre de RTVC posiciones personales en encuestas de opinión, foros u otros medios similares que se encuentren en Internet.
- El uso de Internet es considerado permitido, a excepción de las restricciones anteriores, siempre y cuando se realice de acuerdo a las políticas institucionales (ética, razonable, responsable, no abusiva y sin afectar la productividad de RTVC.

4.6.4. 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 TI los cuales sean solicitados por el líder del proceso dueño de la información que se gestiona y la aprobación de la Coordinación de TI -con base en el análisis de viabilidad de la solución-, o por exigencia de un requisito legal.

La política de no repudio es complementaria a los directrices de auditoría y trazabilidad.

4.6.5. 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 puede estar en los respectivos contratos por medio de una cláusula de confidencialidad.

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.

4.6.6. INTEGRIDAD

RTVC establece e implementa mecanismos de control para preservar la exactitud, completitud y orden de la información con el fin de preservar la integridad de esta con los niveles requeridos por la entidad.
RTVC establece mecanismo de control a través de procedimientos, políticas y lineamientos con el fin de preservar la integridad de los activos de información estableciendo conductas y reglas de buen uso de estos.
La pérdida de integridad de los activos de información son responsabilidad de sus dueños 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.

4.6.7. CRIPTOGRAFÍA

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

4.6.8. REGISTRO Y AUDITORÍA

RTVC vela por el mantenimiento y registro de las evidencias y acciones que afectan los activos de información, este mantenimiento permite asegurar, recuperar, o restablecer la información ante un evento de seguridad de la información.

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 físicos, y digitales 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.

RTVC asegura el almacenamiento de registros de logs de operación, monitoreo y auditoria en las bases de datos correspondientes para que estén disponibles y puedan ser consultados con un histórico de 6 meses a partir de la generación de estos.

4.6.9. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

En el procedimiento de gestión de incidentes aseguramiento se establece el proceder y las reglas que aplican la gestión de incidentes de seguridad de la información y seguridad digital; así como también se especifican los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información.

Todo incidente de seguridad de la información o seguridad digital debe ser registrado en el aplicativo destinado para apoyar la mesa de servicios.

La Coordinación de TI de RTVC, apoya el proceso de gestión de Incidentes aseguramiento, definiendo los pasos para el reporte, la atención y el escalamiento 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 para los casos donde 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.

4.6.10. 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 de los usuarios el conocimiento y habilidades en su manejo; por lo tanto, RTVC brinda inducción u 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 afectar a RTVC.
La alta dirección consciente de que el recurso humano es considerado el eslabón más débil pero más importante en la cadena que permite asegurar la preservación de la disponibilidad, la integridad y la confidencialidad de los activos de información de RTVC, promueve el desarrollo de los planes de capacitación de seguridad de la información y seguridad digital a través de campañas de sensibilización, charlas y talleres que faciliten los recursos y el entendimiento a todas las personas que tienen relación directa o indirecta con el uso de activos de información de RTVC.

El área de Gestión de Talento Humano y el área de Comunicaciones apoyan a RTVC en la capacitación y Sensibilización de la Seguridad de la Información incluyendo en los planes de capacitación, las temáticas de la seguridad de la información, con el fin de crear una cultura de seguridad que permita que las personas desarrollen sus actividades sobre los activos de información de manera segura, minimizando los riesgos relacionados o identificados.

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 TI desarrolla 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 de información, de los sistemas de información y las buenas prácticas en el uso aceptable, ética empresarial para ambientes digitales, entre otros y promueve su divulgación.

El área de gestión documental desarrolla políticas y procesos, para el debido comportamiento de las personas como generadoras, modificadoras o custodias 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

- **Certificado digital:** es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. El titular del certificado debe mantener bajo su poder la clave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red.

- **Criptografía:** Es la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar (“encriptar” o “cifrar”) la información. Mediante la Criptografía es posible garantizar

la Confidencialidad, Integridad, disponibilidad y la autenticidad de los mensajes y documentos guardados en un Sistema o Red Informático.

- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

- **Firma Digital:** Mecanismo electrónico seguro que permite identificar a una persona ante un sistema de información y le permite firmar documentos. La firma digital garantiza la identidad y responsabilidad del autor de un documento o transacción electrónica, así como permite comprobar la integridad del mismo, es decir que la información no ha sido alterada.[8].

- **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.

- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

- **Política:** Declaración de alto nivel que describe la posición de RTVC sobre un tema específico.

- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas

[8] https://web.certicamara.com

de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

- **Seguridad de la información:** Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

- **Protocolos https:** (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web.

- **Protocolos IP:** (Protocolo de Internet) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

- **Tipos de información:** Clasificada en el artículo 2 del Decreto 2609 de 2012, como cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por ésta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:
-

  a. Documentos de Archivo (físicos y electrónicos).
  b. Archivos institucionales (físicos y electrónicos).
  c. Sistemas de Información Corporativos.
  d. Sistemas de Trabajo Colaborativo.
  e. Sistemas de Administración de Documentos.
  f. Sistemas de Mensajería Electrónica.
  g. Portales, Intranet y Extranet.
  h. Sistemas de Bases de Datos.
  i. Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
  j. Cintas y medios de soporte (back up o contingencia).
  k. Uso de tecnologías en la nube.

La presente política debe ser divulgada y promovido 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 14 de octubre de 2020.