Contenido

1. DERECHOS DE AUTOR

2. ACERCA DE ESTE DOCUMENTO

Este documento presenta la POLÍTICA OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

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.

Así mismo este documento tiene por objeto estandarizar un esquema de administración y uso de los recursos de software de RTVC, de manera centralizada y simplificada, basándose en las mejores prácticas que garanticen un óptimo funcionamiento y cumplimiento de las necesidades.

Este documento hace parte de una serie de documentos cuyo objetivo es establecer una serie de políticas para orientar el desarrollo de las tecnologías de la información de tal manera que se facilite su implementación, integración y crecimiento.

Este documento se alinea con los tres (3) principios fundamentales de la seguridad de la información, de preservar la Confidencialidad, la Integridad y la Disponibilidad sobre la información; los procesos y las personas involucradas; dichos principios se contemplan como referencia de buenas prácticas de Seguridad Digital para el desarrollo del documento.

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:

- Todos los procesos realizan actividades de autoevaluación, de acuerdo con lo establecido en el Modelo Estándar de Control Interno. Control interno
- 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].
- 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 Orfeo para oficializar su trámite, asignándoles un consecutivo único de radicado y cumplir con los términos de vencimiento establecidos por la ley[3].
- En todas las reuniones que se realicen en las dependencias se debe llevar registro de asistencia, participación y/o acta, de acuerdo con los formatos establecidos en el Sistema Integrado de Gestión.
- Todas las áreas deben estar en constante actualización de la normatividad legal que les aplique para el desarrollo de sus funciones.
- En todos los procesos de RTVC se da prioridad y estricto cumplimiento a los requerimientos de los órganos de control. Control interno
- Todo trámite, diligencia o proceso adelantado por RTVC, se realiza de conformidad con la normatividad vigente y las reglas establecidas en los diferentes manuales y procedimientos establecidos al interior de la Empresa.
- 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. Control interno

---

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

[2] Acuerdo 027 de 2006 Archivo General de la Nación

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

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

4. POLÍTICA DEL PROCESO DE SOPORTE CLIENTE INTERNO – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Entiéndase como Seguridad de la Información el conjunto de medidas preventivas y reactivas de una organización y de los sistemas tecnológicos que permiten resguardar, preservar y proteger la información y los datos que representan algún valor para la misma organización, buscando mantener la confidencialidad, la disponibilidad e integridad.

Por lo tanto, La Política General de Seguridad de la Información de RTVC, se establece con el objetivo de proteger los activos de información de RTVC, "Personas, Procesos, Información y la Tecnología utilizada para su procesamiento", frente a riesgos y amenazas, internas o externas, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información, todo esto soportado, en el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI).

RTVC Sistemas de medios públicos alineado con el cumplimiento de su misión, visión y objetivos estratégicos, establece el desarrollo de un sistema para la Gestión de la Seguridad de la Información en la RTVC, basado en un modelo que opera sobre un ciclo PHVA (Planear, Hacer, Verificar, Actuar) de acuerdo a las recomendaciones del estándar internacional ISO27000 con el objetivo de:

- Minimizar el riesgo sobre los activos de información de RTVC y sus procesos misionales.
- Cumplir con los principios de seguridad de la información para asegurar la disponibilidad, la integridad y la confidencialidad.
- Apoyar la innovación tecnológica y que cumpla con las condiciones de la Seguridad Digital.
- Planear, Implementar, mantener, monitorear y mejorar un sistema de gestión de seguridad de la información SGSI.
- Velar por la protección de los activos de Información de RTVC y una adecuada gestión de los eventos en materia de seguridad de la información.
- Establecer y mantener políticas, procedimientos y guías en materia de seguridad de la información.
- Promover la cultura de seguridad de la información en los funcionarios, contratistas, proveedores de RTVC.
- Garantizar la continuidad del negocio frente a incidentes de seguridad que atenten contra la disponibilidad e integridad de los activos de información.

- Fortalecer las debilidades en materia de seguridad digital de los sistemas de información.

De acuerdo con lo anterior, esta política aplica a funcionarios, contratistas, practicantes, proveedores, clientes y la ciudadanía en general que tenga vínculo o relación con RTVC, quienes aceptan y apoyan la política de Seguridad de la Información, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones, controles o toma de decisiones alrededor del SGSI estarán determinadas por las anteriores directrices.

4.1 Políticas generales de seguridad de la información

Para el logro del cumplimiento de la Política de Seguridad de la información, RTVC se apoya en unas políticas generales que permiten guiar y consolidar los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) que incluyen las siguientes consideraciones:

- RTVC se compromete con planear e implementar un Sistema de Gestión de la Seguridad de la Información, bajo un modelo acorde a las necesidades estratégicas, operativas y legales que requiera RTVC, con el fin de proteger la información y sus componentes en cuanto a la disponibilidad, confidencialidad e integridad.
- RTVC Divulga la Política de Seguridad y vela por el cumplimiento de la misma, aceptada por cada uno de los funcionarios, 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 amenazas originadas por parte del personal, funcionarios, contratistas o terceros.
- 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 del Componente GEL en cuanto a la Seguridad y Privacidad de la Información.

4.2 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 14 Julio 2011.** "Lineamientos de Política para ciberseguridad y ciberdefensa".

- **Documento CONPES-3854 11 Abril 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 20 Enero 2015.** "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".
- **Decreto 1078 del 26 de Mayo de 2015.** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **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.

4.3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

RTVC ha establecido las siguientes Políticas Específicas de Seguridad de la Información, las cuales representan la visión de RTVC en cuanto a la protección de sus activos de Información y que están soportadas en procesos y procedimientos que apoyan su cumplimiento.

4.3.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- La alta dirección de RTVC es la responsable de facilitar los recursos humanos, técnicos, financieros necesarios para llevar a cabo la implementación de esta política y promoverá el compromiso con su aplicación y cumplimiento.
- El comité institucional de gestión y desempeño de RTVC asume el rol de Comité de Seguridad de la Información, quien revisa, los temas primordiales sobre el desarrollo del SGSI como son los riesgos, los controles, políticas y procedimientos que se desprendan del sistema, los planes de remediación y la aprobación o actualización de los mismos.
- Los funcionarios, contratistas y proveedores de RTVC son responsables de proteger la información a la cual acceden y procesan, para evitar su pérdida, alteración, manipulación no autorizada, o destrucción.
- Los Funcionarios, contratistas y proveedores de RTVC deben reportar los incidentes de seguridad de la Información, eventos sospechosos y el mal uso de los recursos que identifiquen, a la Coordinación de Tecnologías de la Información por los medios que disponga la Coordinación, para garantizar la atención oportuna y la contención de los mismos.
- Los Funcionarios, contratistas, proveedores de RTVC y terceros tienen la obligación de proteger las unidades de almacenamiento físicas y lógicas que se encuentren bajo su

responsabilidad, aun cuando no se utilicen y contengan información crítica para los procesos de RTVC.

- Los Funcionarios, contratistas, proveedores de RTVC y terceros, 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 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 funcionarios, los contratos para proveedores y demás contratos o acuerdos y se vigila su cumplimiento en la gestión de contratación de RTVC.

4.3.1.1 Comité de Seguridad de la Información

El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

El Comité de Seguridad de la Información de RTVC tendrá dentro de sus funciones las siguientes:

- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en RTVC.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de RTVC.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
- Las demás funciones inherentes a la naturaleza del Comité.

4.3.2 GESTIÓN DE ACTIVOS

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 de Documental, así como la guía de Mintic sobre la gestión de activos de información y la normatividad vigente (Ley 1581de 2012, Ley 1712 de 2014 Decreto 103 de 2015, etc), son los instrumentos guía para la identificación o actualización del inventario de activos de información con sus atributos, que permita clasificar la información, etiquetar y definir la propiedad de los activos.

4.3.2.1 Uso adecuado de los activos de información

En general toda la información generada, modificada y almacenada en la infraestructura física y tecnológica de RTVC que no sea oficialmente considerada como pública, es propiedad de RTVC y para uso exclusivo en sus procesos de negocio, cualquier uso distinto debe ser autorizado explícitamente por RTVC como dueño de la misma.

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 de los funcionarios, contratistas y terceros, de acuerdo a sus funciones y responsabilidades. Estos permisos deben ser determinados y aprobados por los custodios de la información, los supervisores de contrato y/o al comité de seguridad de la información, con vigencias definidas de inicio y fin, tales controles deben ser gestionados por los administradores de los sistemas de información y los responsables de archivo y gestión documental, asegurando la trazabilidad de los mismos.

Es responsabilidad legal, jurídica y económica de los Funcionarios y Contratistas de RTVC evitar 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.

4.3.3 POLÍTICAS CONTROL DE ACCESO

La política de RTVC respecto al control de acceso implica que se implementan y mantienen 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.

4.3.3.1 Controles 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 soporte a los sistemas de información y comunicaciones, es protegida con medidas de control de acceso físico en el perímetro, que permiten proteger la información, el software y el hardware de daños intencionales.

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

4.3.3.2 Control de acceso lógico

RTVC diseñará e implementará 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., estas credenciales, llaves y accesos protegidos tienen vigencias definidas y son creadas con la previa autorización de los supervisores de contrato o lideres funcionales, así mismo, tales vigencias una vez expiradas deben surtir las fases de deshabilitación y eliminación previa solicitud de los lideres funcionales o supervisores de contrato.

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de RTVC debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de RTVC, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

4.3.3.3 Acceso a internet

El acceso 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, considerando, para todos los casos, los siguientes lineamientos que indican de manera general lo que no está permitido sobre este recurso:

- El acceso a páginas relacionadas con pornografía, sustancias alucinógenas, armas, terrorismo, racismo, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El intercambio no autorizado de información de propiedad de RTVC, de sus funcionarios, con terceros.
- 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 funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden 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 manera ética, razonable, responsable, no abusiva y sin afectar la productividad de RTVC, ni la protección de la información de RTVC.

4.3.4 NO REPUDIO

Los servicios de No repudio son procedimientos que protegen a cualquiera de las partes involucradas en una comunicación, de que alguna de las demás tenga éxito al negar ilegítimamente que un determinado evento o acción haya tenido lugar; para ello, el sistema de información de RTVC que se clasifique como sistema de administración de mensajes (sistemas de correo) o de aplicaciones de comercio electrónico o transaccional y/o de negocios, ha de producir, validar, mantener y poner a disposición de las partes, pruebas ó evidencias irrefutables, respecto a la transferencia de información desde el emisor al receptor y del contenido de ésta, donde se ha de garantizar la entrega eficiente, confiable y segura tanto de pagos como de productos digitales.

El enfoque de esta directiva sobre los servicios de no-repudio, es que las partes (funcionarios, contratistas, proveedores, clientes, entes de control y ciudadano) han de obtener suficientes pruebas para resolver sus diferencias, entre ellas mismas, o empleando algún tipo de arbitraje (Entidad certificadora, notario, agente de entrega o juez). Para la construcción de este servicio y de sus pruebas, RTVC hará uso de mecanismos criptográficos tales como la firma digital, el cifrado de mensajes, los códigos de autenticación de mensajes (MACs) y la notarización de documentos, además de otros servicios clásicos de seguridad aplicados a los dos tipos de No repudio reconocidos como No-repudio de origen o No-repudio de recepción.

La utilización de protocolos de no-repudio garantizará que las tradicionales transacciones comerciales basadas en soporte papel como contratos, órdenes de compra, facturas, cheques entre otros, pueden ser trasladadas al entorno digital de RTVC con una mayor seguridad.

4.3.5 PRIVACIDAD Y CONFIDENCIALIDAD

En cumplimiento de la de Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 del 27 de junio de 2013, ley 1712 del 6 de marzo de 2014 y el Decreto 103 del 20 de Enero de 2015, por la cual se dictan disposiciones para la protección de datos personales, RTVC a través de la Oficina Asesora Jurídica, propenderá por la protección de los datos personales de sus funcionarios, contratistas, proveedores, clientes, ciudadanos y demás terceros de los cuales reciba y administre información, mediante los mecanismos legales, jurídicos y tecnológicos que considere RTVC a través de una política para la protección de datos.

La Oficina Asesora Jurídica de RTVC identifica, documenta y mantiene actualizados los requisitos legales, reglamentarios o contractuales aplicables a RTVC relacionados con seguridad de la información.

De la misma manera, RTVC buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que RTVC conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de RTVC y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización y contará con el apoyo del Comité de Seguridad de la Información (CSI) y la Coordinación de TI para tal fin.

4.3.5.1 Acuerdos de confidencialidad

Todos los funcionarios, contratistas de RTVC y terceros que tengan algún tipo de vínculo con RTVC deben aceptar los acuerdos de confidencialidad definidos por la misma, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de RTVC a personas o empresas externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos que aplica durante y posterior a la firma de los mismos y por el tiempo que considere RTVC.

4.3.6 INTERCAMBIO DE INFORMACIÓN

- Todo Funcionario 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.

4.3.7 INTEGRIDAD

RTVC entendiendo la Integridad como pilar fundamental a proteger sobre los activos de información, establece las directrices que permiten conservar la integridad y el valor de la información de RTVC durante los procesos de generación, custodia, respaldo y divulgación.

La integridad de la información de RTVC, será preservada por mecanismos de cifrado, de respaldo, de comprobación, no repudio y la prevención de incidentes de seguridad que atenten contra esta característica, mediante una gestión de incidentes y mitigación de riesgos.

4.3.8 DISPONIBILIDAD DE LOS ACTIVOS Y SERVICIOS DE INFORMACIÓN

RTVC mantiene la disponibilidad de los activos de información, haciendo uso de mecanismos tecnológicos, procedimientos, procesos y directrices que permiten asegurar 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.

RTVC cuenta con un plan de Continuidad BCP para asegurar, recuperar y restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la información y los procesos misionales de RTVC.

El plan define los niveles de disponibilidad de servicios acordados con los proveedores, terceros y desarrolla los acuerdos internos de servicio.

De la misma manera, brinda un plan de recuperación, con las necesidades primordiales para la operación del negocio.

RTVC cuenta con unos procesos de soporte cliente interno, 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.

4.3.9 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 los mismos.

Se cuenta con un proceso de monitoreo tecnológico interno que permite identificar la eficiencia en los sistemas de información y asegurar el continuo seguimiento al comportamiento de los sistemas que alojan los activos de información digital, esta actividad contribuye en la identificación de riesgos y amenazas sobre los activos de información.

4.3.10 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Como parte de la identificación, evaluación y tratamiento de riesgos sobre la seguridad de los activos de información y tomado en cuenta dentro del Sistema de Gestión de la Seguridad de la Información, una vez materializadas las amenazas, RTVC cuenta con una directriz general de gestión de eventos e incidentes de seguridad, apoyada por la alta dirección que permite hacer una gestión integral y oportuna de los eventos que se presenten sobre la información de RTVC.

Este procedimiento de gestión de incidentes de seguridad define cómo actuar en caso de ocurrir alguno de los incidentes o eventos de seguridad de la información que se ocasionen o detecten sobre los sistemas de información y repositorios físicos o digitales que hacen la función o soportan los activos de información de RTVC.

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.

Abarca desde la identificación, resolución y cierre que incluye la mejora continua en la mitigación de los incidentes de seguridad de la información.

La Coordinación de TI de RTVC, apoya el proceso de gestión de Incidentes de Seguridad de la Información, definiendo los pasos para el reporte, la atención, 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 ante el riesgo inminente de afectación de la seguridad de la información de RTVC.

4.3.11 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 o entrenamiento o capacitación, en el uso y seguridad sobre los mismos, con el objetivo de minimizar los riesgos de seguridad de la información, que puedan afectar a RTVC.

La alta dirección consciente de que el recurso humano es considerado el eslabón más débil 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, las campañas de sensibilización y facilita los recursos, supervisa su ejecución y entendimiento, para todas las personas que tienen relación directa o indirecta con 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 las amenazas relacionadas con el recurso humano.

Todos los funcionarios, contratistas y proveedores, están obligados a participar en las sensibilizaciones, como parte de sus responsabilidades contractuales; así mismo, deben demostrar el entendimiento y compromiso aplicando las buenas practicas instruidas en sus actividades desarrolladas para RTVC.

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 de los servicios de información, el uso 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.

4.4 GLOSARIO

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

- Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
- 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.
- 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 ó 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 Desarrollo Administrativo realizado el 24 de noviembre de 2017.