1. Derechos de autor

Radio Televisión Nacional de Colombia RTVC SAS es el titular de los derechos de autor del presente documento, en consecuencia, no se permite su reproducción, comunicación al público, traducción, distribución, 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 Decreto 1083 de 2015, Decreto único del Sector Función Pública, modificado por el Decreto 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión - MIPG, el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno.
Dando cumplimiento a lo anterior mediante la Resolución No. 0327 del 2022 “Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, se conforma el Comité Institucional de Desempeño en Radio Televisión Nacional de Colombia – RTVC S.A.S y derogan las resoluciones 421 de 2020, 147 de 2018” , y teniendo en cuenta la incorporación de las políticas que la gestión y el desempeño permite asegurar de manera razonable la ejecución de obligaciones, actividades y tareas de acuerdo con lo planeado, contando con controles necesarios para la realización eficiente y efectiva de los planes, programas, proyectos, políticas operacionales y procesos de la entidad, que permitan evidenciar las posibles desviaciones y tomar las decisiones oportunas para el cumplimiento de objetivos, y así controlar la gestión de la entidad con integridad y calidad en el servicio a través del Modelo Integrado de Planeación y Gestión - MIPG.

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 Entidad:

1. Todos los procesos realizan actividades de autocontrol, de acuerdo con el esquema de líneas de defensa indicado en el Modelo Integrado de Planeación y Gestión MIPG.
2. En RTVC SAS son responsables por la organización, conservación, uso y manejo de los documentos en cualquier soporte, todos los servidores y empleados públicos como los colaboradores, aplicarán las normas adoptadas para tal fin por la Entidad, 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

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

debe ser registrada en el sistema de gestión documental Orfeo para oficializar su trámite, asignándoles un consecutivo único de radicado y cumplir con los términos de vencimiento establecidos por la Ley[3].

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

    - Módulo de actas en el sistema de planeación y gestión en el Aplicativo Vigente, 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 el sistema de planeación y gestión en el Aplicativo Vigente, 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 de la normatividad legal que les aplique para el desarrollo de sus funciones.
6. En todos los procesos de RTVC se da prioridad y estricto cumplimiento a los requerimientos de los órganos de control.
7. Todo trámite, diligencia o proceso adelantado por RTVC, se realiza de conformidad con la normatividad vigente y lo establecido en los diferentes manuales y procedimientos registrados en el sistema integrado de gestión
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.
11. Todas las personas y los procesos deben considerar y aplicar la política gestión ambiental y los diferentes programas dentro de sus actividades y como parte de sus responsabilidades para el buen manejo de los recursos.

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

4. Políticas de Para la Administración de la Infraestructura de TI

El objetivo de las políticas para administración de infraestructura es dar los lineamientos para la Planeación, administración, soporte, y mantenimiento de la infraestructura tecnológica de la Coordinación de Tecnologías de la información, garantizando la disponibilidad, el uso adecuado, responsable, eficiente y correcta operación de los servicios tecnológicos.

Esta Política para la administración de la infraestructura de TI responde, igualmente, a los siguientes ejes estratégicos del PETI:

- APROPIACIÓN A NIVEL DE POLÍTICAS: Este eje estratégico busca que la dirección de TI implemente de forma eficiente, en el marco de la operación, las políticas que gobiernan la prestación de los diferentes servicios tecnológicos.

- APROPIACIÓN DE COMPETENCIAS: Este eje busca generar los mecanismos adecuados para que el conocimiento adquirido y practicado en el ejercicio de las actividades propias de la dirección, permanezca en el tiempo en RTVC y sirva como base para su ejecución. (Tutoriales, documentos, otros).

4.1. Normatividad asociada

- 2002 - Directiva Presidencial No. 10 de 2002 - Programa de renovación de la Administración Pública: hacia un Estado Comunitario
- 2002 - Ley 790 de 2002 - Programa de Reforma de la Administración Pública
- 2003 - Conpes 3248 de 2003 - Renovación de la Administración Pública
- 2003 - Decreto 3816 de 2003 - Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública
- 2010 - Decreto 235 de 2010 - Intercambio de información entre entidades para el cumplimiento de funciones públicas
- 2016 - Decreto 415 de 2016 - Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
- 2016 - Resolución 2405 de 2016 Por el cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité
- 2015 - Acuerdo 003 de 2015 del AGN - Lineamientos generales sobre la gestión de documentos electrónicos
- 2015 - Decreto Reglamentario Único 1081 de 2015 - Decreto 103 de 2015 - Reglamento sobre la gestión de la información pública
- 2014 - 2018 -Plan vive digital 2014-2018 - Busca que el país dé un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional
- 2012 - Ley 1507 de 2012 - Por la cual se establece la distribución de competencias entre

- las entidades del Estado en materia de televisión y se dictan otras disposiciones.
- 2018 - Decreto 1008 de 2018 - "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
- 2021 Directiva Presidencial N° 03 del 15 de marzo de 2021 mediante la cual se rigen los lineamientos para el uso eficiente de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

4.2. Políticas Generales

Teniendo en cuenta el marco y la normatividad descrita anteriormente, RTVC ha establecido las siguientes Políticas Generales para administración de infraestructura:

- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información de RTVC estará protegido contra intercepción o daños, de acuerdo con las normas que apliquen y a las recomendaciones emitidas por el CSIRT-CCIT[4]
- La administración de la red *LAN, WLAN, WAN* y *VOIP* está a cargo de la Coordinación de T.I.
- La Coordinación de T.I. es la responsable de la administración, seguridad y acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operan en los equipos de cómputo de RTVC.
- Es responsabilidad de la Coordinación de T.I. definir y documentar la Infraestructura crítica, definida por el tipo de información que maneja.
- Es responsabilidad de la Coordinación de T.I. tener documentado un plan de contingencia de los servicios Críticos que cumpla con las políticas de RPO (*Recovery Point Objective*) y RTO (*Recovery Time Objective*)

4.2.1. Políticas para mantenimiento preventivo de la infraestructura tecnológica

- Se debe realizar el mantenimiento preventivo siguiendo el proceso de mantenimiento preventivo tecnológico interno documentado.
- Se debe dar cumplimiento al cronograma de mantenimiento preventivo a toda la infraestructura tecnológica a cargo de la Coordinación de T.I. los equipos de RTVC[5].
- Los trabajos de mantenimiento preventivo deben ser realizados por el personal especialista, debidamente autorizado e identificado y cumpliendo con todas las

[4] CSIRT: Centro de coordinación de seguridad informática Colombia

[5] El cronograma de mantenimiento preventivo se elabora anualmente de acuerdo con las necesidades y con la planeación del funcionamiento y operación para el periodo

políticas de seguridad en el trabajo de acuerdo con el procedimiento de control de acceso físico de RTVC

4.2.2. Políticas de copias de respaldo

- El administrador de la infraestructura es responsable de llevar a cabo la copia de respaldo de la información alojada en los repositorios de información administrados por la Coordinación de T.I.
- Se debe realizar una copia de respaldo antes que se realice cualquier cambio de configuración o actividad sobre la infraestructura tecnológica a cargo de la Coordinación de T.I.
- Cualquier restauración de información contenida en las copias de respaldo realizados por la coordinación de tecnologías de información, debe ser solicitada a través de la mesa de servicios por el funcionario interesado en la misma.
- Cada Administrador debe conocer, tener documentado los procedimientos y llevar a cabo de copias de respaldo y recuperación de la configuración, así como tener un esquema RPO y RTO definido para la infraestructura a cargo según las mejores prácticas de los fabricantes.
- El tiempo de conservación de las copias de respaldo es de 5 años para los completos que se realizan mensualmente y de 4 semanas para los incrementales.
- Todas las copias de respaldo locales se deben almacenar en el *datacenter* de la Coordinación de T.I. o en la librería de la gestión de los contenidos
- Todo funcionario y colaborador de RTVC deberá velar por que la información que produce manipula y gestiona para servicio de RTVC, sea almacenada en las unidades compartidas asignadas para el área a la cual presta sus servicios. Esta política no aplica para la información alojada en otras unidades de red o en las unidades físicas de los equipos de cómputo.
- Ningún funcionario y colaborador está autorizado para almacenar en las unidades compartidas información personal y obtener recuperación de esta.
- Cuando una cuenta de *Google Workspace* (Correo electrónico y Drive) es deshabilitada, La Coordinación de T.I. realiza una copia de respaldo y la conserva durante seis meses.
- Las copias de respaldo para los servidores virtuales de producción se realizarán a disco y luego a la nube designada para su fin, de acuerdo a la programación full mensual y se conservaran 3 copias y diario incremental se conservaran por 4 semanas.
- Las copias de respaldo para los servidores virtuales de desarrollo se realizarán a disco y luego a la nube designada para su fin, de acuerdo a la programación full trimestral y se conservaran 3 copias y Semanal incremental y se conservara el trimestre.
- Para los servidores de test (pruebas) no se les realizaran copias de respaldo.

- Las copias de respaldo de las unidades de red compartida se realizarán en cintas de acuerdo con la programación full mensual que se mantendrán por 5 años y diario incremental que se guarda por 4 semanas.
- Para el almacenamiento de información en *Google Drive*, se seguirán las políticas de copias de respaldo del proveedor *Google*.
- En caso de presentarse o evidenciarse algún inconveniente, error y/o problema con la ejecución de las copias de respaldo, el administrador de infraestructura local, renviará la copia de respaldo de manera manual el siguiente día hábil.

4.2.3. Licenciamiento

- La Coordinación de TI debe contar con un único inventario de licenciamiento de software que debe soportarse por los documentos de licenciamiento o contractuales que apliquen. En caso tal que las licencias sean entregadas en medio físico, los documentos asociados a la misma deben almacenarse en la caja fuerte.
- Los proveedores de servicios de tecnología deberán entregar una relación del licenciamiento provisto a RTVC y las condiciones de este.

4.2.4. Base de datos de la configuración

- La Coordinación de T.I., mantendrá una base de datos de configuración (CMDB) de la infraestructura con las características de cada uno de ellos (serial, marca, modelo, número de parte).
- La Coordinación de T.I., deberá revisar la base de datos de configuración por lo menos 1 vez al año. Se debe realizar un informe de los cambios encontrados.

4.2.5. Seguridad de la información

4.2.5.1. Gestión de cuentas y contraseñas

- La Coordinación de T.I. implementa el control de acceso a las diferentes plataformas tecnológicas de la entidad a partir de la identificación de los usuarios mediante cuenta de usuario y contraseña y asignación de roles.
- La Coordinación de T.I. debe mantener un registro actualizado de las cuentas de usuario que administran los recursos de la plataforma tecnológica de la entidad.

4.2.5.1.1. Cuentas de administradores

- Las contraseñas de los usuarios de administración de la infraestructura, como por ejemplo el usuario administrador o *root* no tienen fecha de caducidad y deben cambiarse por lo menos 2 veces al año.

- Las contraseñas de los usuarios de administración de la infraestructura, como por ejemplo el usuario administrador o *root* son responsabilidad del administrador de la infraestructura, por lo cual éste debe cambiar dichas contraseñas, verificarlas con un el Coordinador(a) de Gestión de Tecnologías de la información T.I., almacenarlas en *keepass* (administrador de contraseñas) y almacenar una copia de la base de datos encriptada en la carpeta compartida de la Coordinación de T.I. La documentación debe incluir la dirección IP del dispositivo, el nombre de usuario, la contraseña y el responsable del cambio.
- Las contraseñas de los usuarios de administración de la infraestructura, servidores, servicios y aplicaciones deben ser cambiadas cuando cambie el personal responsable de las mismas.
- Se debe utilizar las cuentas de administración únicamente para realizar labores que requieran permisos de administración.
- Se debe evitar utilizar la misma contraseña para las cuentas de administrador de servidores, bases de datos y otras aplicaciones.
- Se debe deshabilitar la cuenta de usuario "*guest*" o "invitado" de todos los servidores, servicios o dispositivos de comunicaciones.
- Se deben cambiar todas las contraseñas de las cuentas que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware, en cualquier dispositivo conectado a la red.

4.2.5.1.2. Cuentas de usuario

- Para la generación o creación de la cuenta de usuario se tendrán en cuenta los siguientes lineamientos:
  - Se tomará la primera letra del nombre de la persona, seguida del primer apellido, por ejemplo, si el nombre de la persona es Carmen Julieta Ramírez Pérez, la cuenta de usuario será cramirez
  - Si la cuenta ya existe, se debe agregar la segunda letra del nombre, para el ejemplo dado, la cuenta de usuario sería cjramirez
  - Si las dos opciones anteriores ya están definidas, se debe agregar al final la primera letra del segundo apellido, para el ejemplo dado, la cuenta de usuario sería cjramirezp
  - Si el nombre o apellido de la persona contiene "ñ", esta letra se deberá reemplazar con una "n", por ejemplo, si el nombre es Carmen Julieta Peñuela Pérez, la cuenta de usuario será cpenuela
- Las contraseñas deben cumplir con los siguientes requisitos:
  - No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
  - Tener una longitud mínima de diez (10) caracteres
    - Incluir caracteres de tres de las siguientes categorías:
    - Mayúsculas (A-Z)
    - Minúsculas (a-z)

- Dígitos de base 10 (0-9)
- Caracteres no alfanuméricos ($, #, %, *, \)

- No repetir las últimas 6 contraseñas.
- Cambiarse cada 90 días.
- Se debe almacenar cifrada
- El administrador no debe tener acceso a las contraseñas
- El usuario puede cambiarla voluntariamente cuando lo desee

- La asignación de usuarios y contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido. La responsabilidad por el uso indebido del usuario y contraseña es exclusiva del usuario titular.
- La cuenta de usuario será bloqueada si ocurren 5 intentos fallidos de inicio de sesión.
- Si se sospecha que la seguridad de una cuenta de usuario está comprometida, se notificará al usuario para efectuar un cambio de contraseña de manera inmediata
- Cuando un servidor público o contratista finalice relación laboral con RTVC y no se vaya a realizar prórroga o celebración de un nuevo contrato, se procederá desactivar las cuentas que tenga asignadas. Esto se realiza durante la generación del “Paz y salvo” de la Coordinación de Tecnologías de la Información.
- Cuando ingrese un nuevo servidor público o contratista a RTVC, se procederá a crear o activar las cuentas correspondientes, así como a asignar los roles respectivos, previa solicitud por medio de la mesa de servicio del jefe, supervisor o encargado del área a la que pertenece.
- Se recomienda tomar en cuenta los siguientes aspectos, para proteger las contraseñas y minimizar los riesgos de accesos no autorizados:
  - No escribir las contraseñas en papeles de fácil acceso, agenda, ni en archivos sin cifrar.
  - No habilitar la opción “recordar clave en este equipo” ofrecida por algunas aplicaciones y navegadores Web.
  - No enviar la contraseña por correo electrónico, servicios de mensajería electrónica instantánea o vía telefónica.
  - No compartir las contraseñas con otros usuarios.
  - Cambiar su contraseña si sospecha que alguien más la conoce.
  - Seleccionar contraseñas robustas, evitando los siguientes aspectos:
    - Utilizar palabras de diccionario, aún si están en otros idiomas
    - Utilizar datos personales, tales como números de identificación, teléfonos o direcciones, nombres de familiares o mascotas.
    - Utilizar referencias a la cultura popular, tales como nombres de libros, personajes, canciones, bandas musicales.
  - Para generar la contraseña se sugiere utilizar el enfoque de elegir una frase significativa (mínimo de 5 palabras) utilizando mayúsculas y minúsculas, luego sustituir algunas de las letras por caracteres especiales y números.

4.2.5.1.3. Cuentas de usuario de testeo o pruebas

- Las contraseñas para los usuarios de testeo o pruebas deben cumplir con lo especificado a este respecto en la sección de **4.2.5.1.2 Cuentas de usuario**, de la presente política.
- Los usuarios de prueba tendrán un encargado quien será responsable de las actividades ejecutadas con dicha cuenta.
- Los usuarios de prueba se deshabilitarán o eliminarán una vez completadas las actividades para las cuales fue requerido. En caso tal que se requiera mantener la cuenta activa con carácter permanente, la Coordinación de TI deberá autorizarlo siempre y cuando esté debidamente justificado por parte del líder de área ante el Coordinador de TI.
    - En lo posible, los usuarios de prueba deben estar ligados al directorio activo.
    - Es responsabilidad de cada administrador el control de los usuarios de prueba que se definan localmente en servidores, dispositivos, sistemas, aplicaciones o cualquier otro componente tecnológico bajo su gestión.

4.2.5.2. Red privada virtual (VPN)

- La Coordinación de T.I. proveerá el servicio de conexión remota a la plataforma tecnológica institucional a través de red privada virtual (VPN por sus siglas en inglés), con lo cual el tráfico de datos entre usuario remoto y red institucional se encontrará debidamente cifrado.
- El uso de la VPN está permitido solo para el personal que labora en RTVC o contratistas que lo requieran previa autorización y seguimiento de las vigencias de autorización.
- Sólo usuarios previamente autorizados por la Coordinación de T.I. podrán utilizar el servicio VPN, los que, además, serán los responsables del correcto uso del servicio de acceso remoto.
- Cada usuario solo podrá tener activa una única conexión VPN con RTVC y debe desconectarla una vez concluida las operaciones a realizar en la red interna.
- Los usuarios del sistema *VPN* serán automáticamente desconectados de la sesión, una vez que hayan transcurrido máximo 1 hora de inactividad. Si el usuario es desconectado deberá iniciar sesión nuevamente para volver a conectarse a la red.
- El software de VPN debe estar siempre actualizado y con todos los parches de seguridad instalados.
- Se deben verificar periódicamente que las autorizaciones de usuarios para el uso de la VPN se mantengan vigentes.
- Se deben activar y mantener los registros de auditoría (logs) del servicio VPN.

4.2.5.3. Ingreso seguro a los dispositivos

- Los dispositivos para la conectividad de la red local, conexión a internet, seguridad informática, servidores y todos aquellos dispositivos administrados por la Coordinación de T.I. que manejen información, deberán estar ubicados en un lugar físico resguardado de accesos no autorizadas.
- El área deberá estar protegida por un dispositivo de seguridad que tenga un mecanismo de control de acceso y que conserve un registro de los ingresos.
- El área restringida en la que los dispositivos estén ubicados deberá mantenerse a una temperatura de ambiente controlado.
- El área restringida debe contar con un Sistema de Alimentación Ininterrumpida – UPS que soporte la totalidad de los equipos existentes.
- El acceso a la administración directa de los equipos de comunicaciones debe estar debidamente controlado, al realizar algún soporte o mantenimiento a los equipos, sólo personal autorizado por la Coordinación de T.I. puede acceder a estos equipos.
- Si se requiere la visita de personal técnico externo, éste podrá ingresar a la ubicación física de los dispositivos acompañado siempre del personal de la Coordinación de T.I. autorizado para tal fin.
- El ingreso para la gestión remota de dispositivos como equipos de comunicaciones, de seguridad o servidores, debe estar restringida, permitiendo solo usuarios conectados a través de la VPN.
- El ingreso para la gestión remota de equipos críticos debe realizarse desde dispositivos de usuario permitidos.
- Se deben restringir en los dispositivos, los puertos de acceso por defecto salvo en casos particulares y debidamente justificados.
- La gestión de los equipos de red o servidores a través interfaz de línea de comando (CLI) se debe realizar sin excepción a través del protocolo SSH V2 (*Secure Shell*).
- El uso del protocolo Telnet sólo será empleado en los casos en los que el dispositivo no soporte el protocolo SSH, previa verificación, justificación y aprobación.
- La gestión de los servidores con sistema operativo Windows, se debe realizar únicamente a través del Escritorio remoto.
- Se debe limitar el acceso remoto solo a las cuentas que lo requieran.
- No está permitido el uso de programas inseguros o no licenciados, para la administración remota de ningún dispositivo dentro de la red.
- Se debe activar y conservar los registros de auditoría (logs) en todos los dispositivos de comunicaciones, seguridad y servidores.

4.2.5.4. Ingreso seguro a los sistemas de información

- Todo el personal de RTVC o terceros que dispongan de acceso a las distintas plataformas tecnológicas de la entidad, 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 establecidas.

- La Coordinación de T.I. controlará el acceso a los servicios de red tanto internos como externos con el propósito de garantizar la seguridad de los usuarios y mantener la estabilidad de los servicios, para lo cual se restringen los puertos de acceso por defecto, salvo casos particulares debidamente justificados.
- Todos los Sistemas de información o aplicaciones administrados por la Coordinación de T.I. deben tener control de acceso a través de autenticación mediante un usuario y contraseña.
- El control de acceso a la información a través de una aplicación o sistema de información se realizará a través de roles que administren los privilegios de los usuarios y será determinado por el dueño de la información.
- Cuando se termine la relación laboral o contractual de cualquier persona con RTVC, que disponga de acceso a las distintas plataformas tecnológicas de la entidad, se deben retirar los permisos de acceso de forma oportuna.
- Las sesiones iniciadas en los sistemas de información se deben bloquear automáticamente luego de 10 minutos de inactividad.
- El ingreso para la gestión remota de Sistemas de información o aplicaciones debe estar restringida, permitiendo solo usuarios conectados a través de la VPN.
- Se debe restringir el acceso de usuarios finales y personas externas a RTVC, al código fuente de los Sistemas de información y aplicaciones.
- Se deben activar y conservar los registros de auditoría (logs) que reporten las actividades realizadas por los usuarios que accedan a los sistemas de información y aplicaciones de RTVC.

4.2.6. Responsabilidades de los Administradores.

- Analizar, diseñar, asesorar, suministrar y mantener los componentes de la infraestructura necesarios para su correcto funcionamiento.
- Es responsabilidad del administrador de la infraestructura conocer la arquitectura de los dispositivos a cargo, estar informado de los boletines generados por los fabricantes en cuanto a problemas técnicos, como a todos los temas de seguridad.
- Documentar los componentes incluyendo los accesos, las configuraciones en los equipos deben tener un identificador claro que permita relacionarlo fácilmente con su finalidad.
- Documentar las acciones resultantes de las solicitudes de control de cambios, de acuerdo con el procedimiento y los formatos habilitados para tal fin.
- Controlar los accesos, de modo que se disponga de un nivel de seguridad física y lógica de los recursos.
- Administrar de manera integral la infraestructura a cargo, como, por ejemplo: direccionamiento, enrutamiento del tráfico, sistemas operativos, versiones, parches y los mecanismos de identificación, entre otros.

- Es responsabilidad del administrador de la Infraestructura mantener los parches y actualizaciones de los sistemas al día, realizando esta instalación de manera controlada y validando la información de los parches a aplicar.
- Es responsabilidad del administrador de infraestructura realizar un control de parches de seguridad y de corrección de vulnerabilidades, validando que no se afecten las aplicaciones que corren en él.
- Interactuar con el soporte de fábrica para resolver dudas, problemas o generar requerimientos.
- Es responsabilidad de los administradores conocer y administrar el licenciamiento de los componentes o aplicaciones que se encuentren a su cargo.
- Los Administradores de plataforma son responsables de determinar qué otros aspectos se deben monitorear en las aplicaciones según las características de este y documentar las decisiones que se tomen sobre este aspecto
- Garantizar el correcto monitoreo de la infraestructura que tiene a cargo.

4.2.7. Prestación de servicios de Coordinación de Tecnologías de la Información.

- La coordinación de tecnologías de la información calculará los tiempos de atención bajo una matriz de prioridad.
- Para calcular la prioridad se cruza el impacto dado por la Coordinación de Tecnologías de la información y la urgencia dada por el Usuario que requiere el servicio.
- Esta matriz de prioridad se usará para la atención de Incidentes y requerimientos, quedando de la siguiente manera:

PRIORIDAD		Impacto		
		Toda la entidad	Área	Persona
Urgencia	Alta	Alta	Alta	Media
	Media	Alta	Media	Baja
	Baja	Media	Baja	A Planificar

Tabla N°1. Matriz de prioridad
Fuente: Coordinación de TI

- Los tiempos de atención generales para la atención de requerimientos por la Coordinación de Tecnologías de la Información son:

  - Horario de atención: horario hábil (lunes a viernes 8:00 a.m. – 6:00 p.m.)

Prioridad	Tiempo de Atención	Tiempo de solución*
Alta	30 min	24 horas
Media	1 horas	72 horas
Baja	2 horas	135 horas
A planificar	N/A	N/A

Tabla N°2. Tiempos de respuesta – Horario Atención
Fuente: Coordinación de T.I.

- Los tiempos de atención generales para la atención de incidentes por la Coordinación de Tecnologías de la Información son:

  - Horario hábil (lunes a viernes 8:00 a.m. – 6:00 p.m.)

Prioridad	Tiempo de Atención	Tiempo de diagnóstico	Tiempo de solución[6]
Alta	30 min	8 horas	16 horas
Media	1 horas	24 horas	48 horas
Baja	2 horas	48 horas	80 horas
A planificar	N/A	N/A	N/A

Tabla N°3. Tiempos de respuesta – Horario Incidentes
Fuente: Coordinación de TI

  - Horario no hábil (sábados, domingos, festivos y lunes a viernes de 6:00 p.m. – 8:00 a.m.)

Prioridad	Tiempo de Atención	Tiempo de diagnóstico	Tiempo de solución[7]
Alta	1 horas	12 horas	24 horas
Media	N/A	N/A	N/A
Baja	N/A	N/A	N/A

[6] Los tiempos de solución se calcularon en base a tiempos dados a problemas conocidos y en restauración el servicio, estos tiempos pueden variar de acuerdo con la incidencia presentada.

A planificar	N/A	N/A	N/A

Tabla N°4. Tiempos de respuesta – Horario No Hábil
Fuente: Coordinación de TI

- En la Coordinación de Tecnologías de la información existen algunos servicios particulares que no pueden ser atendidos con los tiempos generales. Se podrán tener tiempos adicionales de diagnóstico o solución para servicios que involucran desarrollos o compras, los cuales se especifican en la aplicación mesa de servicios o se especificarán durante la atención del incidente o requerimiento.
- La Coordinación de Tecnología de la Información es responsable de evaluar la satisfacción de los usuarios, para lo cual se realizarán encuestas de cada uno de los servicios prestados y documentados en la mesa de servicio, esta evaluación se realizará tomado como muestra representativa la calificación de por lo menos el 50% de los casos del periodo a evaluar.

4.3. Políticas de administración de Servidores

4.3.1. Estructura y Diseño

- La infraestructura de servidores deberá contener dispositivos o sistemas lógicos que las protejan contra el acceso no autorizado a recursos, información y ataques informáticos internos o externos, de acuerdo con los documentos de arquitectura y de gobierno de TI aplicables.
- Para la creación de nuevos servidores *Linux Open source* RTVC usará por Defecto *Centos*[7] en su última versión para la creación de estos servidores.
- Los servidores de RTVC deben recibir un nombre basado en la siguiente regla DDVSRVWXXFFFFFDSS donde los identificadores significan

DD – Dependencia ejemplo:
TI para coordinación de tecnologías de la información,
TM para tecnología de medios.
SRV/VSRV – Servidor Físico o Virtual
WXX/LXX – Tipo de sistema operativo W para *Windows*, L para *Linux* y M para *MAC* y versión por ejemplo W12 es *Windows* 2012 o LRH es *Linux Red Hat*
FFFF – Servicio principal que presta el servidor
D , P y T – Desarrollo, Producción y Test(pruebas)
SS – Secuencia del servidor para dar secuencia a nombres repetidos

[7] Centos: Sistema operativo linux creado por “The Centos Project”

Por ejemplo
Para el servidor de Dominio quedaría de la siguiente manera: *TIVSRVW12DCP01*

4.3.2. Servidores

- Es responsabilidad del administrador de infraestructura verificar el correcto funcionamiento del antivirus, validar que este se encuentre actualizado.
- Es responsabilidad del Administrador de infraestructura validar y dar permisos de acceso a los sistemas operativos de las máquinas.
- Es responsabilidad del administrador de infraestructura configurar únicamente los servicios esenciales, con base en los requerimientos de las aplicaciones.
- Es responsabilidad del Administrador de la infraestructura cerrar los puertos UDP/TCP abiertos que sean innecesarios
- Es responsabilidad del Administrador de Infraestructura administrar el *firewall* local y sus directivas sobre los servidores, Es importante documentar los cambios realizados en la configuración del *firewall* local.
- Es responsabilidad del Administrador de Infraestructura validar periódicamente los archivos de logs de los servidores
- Es responsabilidad del Administrador de Infraestructura documentar cambios en la configuración de sistema
- Los servidores deben tener un esquema de copias de respaldo y recuperación para casos de desastre.
- La Coordinación de T.I. debe realizar revisiones a los mismos con la finalidad de mejorar la seguridad o detectar fallas. Estas revisiones o mantenimientos preventivos se realizan con los proveedores de los servicios o aplicativos que se tienen en cada servidor o equipo de red y la periodicidad se define en un cronograma de mantenimientos que aprueba La Coordinación de T.I.
- Los servidores deben tener bloqueadores de pantallas con contraseña, Y este se debe habilitar luego de 5 minutos de inactividad

4.3.3. Monitoreo de los Servidores

- El administrador de la infraestructura es el responsable de monitorear el procesamiento, la memoria, la capacidad del disco e interfaz de red de los servidores con la finalidad de resolver problemas de servicio y como parte de las operaciones rutinarias, para diagnóstico, mantenimiento o para resolver problemas de seguridad.
- El Administrador de la infraestructura es el responsable de determinar qué otros aspectos se deben monitorear en los servidores según las características de este.

4.4. Políticas de administración de Aplicaciones

4.4.1. Estructura y Diseño

- Es responsabilidad del administrador de plataforma definir los requerimientos, capacidades y licenciamiento de las aplicaciones que administra.

4.4.2. Aplicaciones

- Es Responsabilidad del Administrador de la plataforma validar y dar permisos de acceso a los aplicativos.
- Es Responsabilidad del Administrador de la plataforma conocer los puertos UDP/TCP abiertos que sean innecesarios para la operación de las aplicaciones y reportarlo al administrador de infraestructura.
- Es Responsabilidad del Administrador de la plataforma validar periódicamente los archivos de logs de las aplicaciones.
- Es responsabilidad del administrador de la plataforma conocer las integraciones que tiene la plataforma y tenerla documentada.

4.5. Políticas de administración de los servicios *Cloud*.

4.5.1. Estructura y Diseño

- Los diferentes servicios en la Nube deben cumplir las mismas políticas de seguridad que se tienen para los servicios alojados en RTVC.
- La Coordinación de T.I. es la responsable de la administración de los diferentes servicios prestados en la Nube
- Para los servicios alojados en la Nube que presten un servicio Misional se debe tener en cuenta que cumpla con todas las políticas de seguridad.
- La coordinación de tecnologías de información es la encargada de validar los acuerdos de nivel de servicio sobre los diferentes servicios adquiridos por RTVC en la Nube.
- La coordinación de tecnologías de Información es la responsable de asesorar y validar los requerimientos de las diferentes áreas de RTVC para la adquisición de servicios en la NUBE.

4.5.2. Infraestructura *Cloud*

- Es responsabilidad del administrador de infraestructura verificar el correcto funcionamiento del antivirus, validar que este se encuentre actualizado.

- Es responsabilidad del Administrador de infraestructura validar y dar permisos de acceso a los sistemas operativos de las máquinas.
- Es responsabilidad del administrador de infraestructura configurar únicamente los servicios esenciales, con base en los requerimientos de las aplicaciones.
- Es responsabilidad del Administrador de la infraestructura cerrar los puertos UDP/TCP abiertos que sean innecesarios.
- Es responsabilidad del administrador de la Infraestructura mantener los parches y actualizaciones de los sistemas al día, realizando esta instalación de manera controlada y validando la información de los parches a aplicar.
- Es responsabilidad de los administradores de plataforma informar al administrador de la infraestructura de los parches de aplicación que se deben instalar y coordinar en conjunta la instalación de estos parches
- Es responsabilidad del Administrador de Infraestructura administrar el firewall local y sus directivas sobre los servidores, Es importante documentar los cambios realizados en la configuración del firewall local.
- Es responsabilidad del Administrador de Infraestructura validar periódicamente los archivos de logs de los servidores
- Es responsabilidad del Administrador de Infraestructura documentar cambios en la configuración del sistema.
- La Coordinación de T.I. debe realizar revisiones a los mismos con la finalidad de mejorar la seguridad o detectar fallas. Estas revisiones o mantenimientos preventivos se realizan con los proveedores de los servicios o aplicativos que se tienen en cada servidor o equipo de red y la periodicidad se define en un cronograma de mantenimientos que aprueba La Coordinación de T.I.
- Los servidores deben tener bloqueadores de pantallas con contraseña, y este se debe habilitar luego de 5 minutos de inactividad
- Es responsabilidad del administrador de infraestructura realizar un control de parches de seguridad y de corrección de vulnerabilidades, validando que no se afecten las aplicaciones que corren en él.

4.6. Políticas de administración de la RED

4.6.1. Estructura y Diseño

- Las redes deberán estar diseñadas y configuradas para cumplir con las necesidades administrativas y misionales de RTVC, las cuales se documentan en el Plan Estratégico de TI (PETI).
- Cada vez que se instale un dispositivo de red nuevo (*Switch, Router, Firewall*, etc.), se debe configurar de acuerdo con las especificaciones de la red existente.
- El Administrador de la red es responsable del diseño, gestión y control de los segmentos de RED manejados por RTVC.

- Los colaborades y/o contratistas que sean designados para administrar las redes de RTVC deberán estar debidamente capacitadas en las tecnologías sobre seguridad informática y administración de redes.
- Deben existir diferentes redes inalámbricas para cada tipo de perfil: usuarios, administradores e invitados.
- Los usuarios administrativos deberán registrarse en la red haciendo uso de sus credenciales de dominio.
- Cuando se requiera realizar modificaciones o ampliación de cobertura sobre la red WLAN se debe realizar un mapa de calor que determine la mejor ubicación de los Access Point, así mismo, cuando se realicen modificaciones estructurales en las áreas de cobertura.
- El colaborador o contratista administrador de la red es responsable del diseño, manejo y control de los segmentos de RED manejados por RTVC.
- La Coordinación de Tecnologías de Información es responsable de dimensionar la capacidad de ancho de banda necesaria para integrar las diferentes sedes de RTVC según las necesidades de cada sede.
- La Coordinación de T.I. es responsable de dimensionar el tráfico necesario para la salida de Internet, este tráfico se debe dimensionar a partir del uso de las herramientas administrativas.
- La Coordinación de T.I. es el encargado de garantizar el tráfico para las aplicaciones misionales que consumen recursos desde RTVC previo diseño y conocimiento de este tráfico.
- La salida de Internet debe priorizar el tráfico de *Streaming* de RTVC y acceso a las herramientas en la Nube, sobre el tráfico a otros sitios.

4.6.2. Gestión de RED

- La configuración de los equipos de red está a cargo del administrador de la red.
- En caso de que se presente una avería del servicio por fallas a nivel de red, el administrador de la red debe realizar el análisis, diagnóstico y solución, la cual debe ser notificada al Coordinador tecnologías de la Información junto con el informe de indisponibilidad por área afectada.
- Los equipos no deben superar el 80% de su capacidad de procesamiento, si lo superan el administrador de la red debe reportar al coordinador de tecnologías de la información para dar una solución.
- Los puertos utilizados deben estar marcados físicamente de acuerdo con el servicio que estén prestando.
- Se deben mantener los puertos configurados en auto negociación en velocidad y transmisión (dúplex – full dúplex) a menos que sea necesario que estén fijos.
- El uso de los puertos físicos de los equipos de la red deberá estar controlado hasta que sean requeridos.
- Para dispositivos móviles existentes, la Coordinación de T.I. garantizará el funcionamiento del servicio *WLAN* a los equipos adquiridos por RTVC.

- El administrador de la red está autorizado para monitorear la red con cualquiera de los métodos existentes con la finalidad de resolver problemas de servicio, como parte de las operaciones rutinarias de la red, para diagnóstico, mantenimiento o para resolver problemas de seguridad.
- El colaborador y/o contratista administrador de la red deberá monitorear el procesamiento de los equipos de acceso, *Core, access point*, controladora *Wireless*, y seguridad para anticipar inconvenientes que puedan afectar la calidad del servicio.
- Los colaboradores y/o contratistas administradores de la red tienen autoridad para cancelar el servicio a cualquier subred o dispositivo de red que afecte el desempeño de la red RTVC y a su vez debe notificar al área responsable para que se aclare el incidente.
- Los colaboradores y/o contratistas administradores de red deberán hacer una evaluación previa de los efectos que tiene en la red la implementación de nuevas soluciones de acuerdo con los manuales técnicos y la estructura propia de la red

4.6.3. Canal de Internet de Respaldo

- El canal de respaldo de internet debe tener una capacidad de transmisión de datos no menor al 70 % de la capacidad del canal principal.
- El canal de respaldo debe ser monitoreado por los administradores de la red de tal manera que se garantice su funcionamiento en caso de que se presente una eventualidad sobre el canal principal.
- Se deben realizar pruebas de la conmutación entre el canal principal y el canal de respaldo, programadas por lo menos una vez al año en horarios que no afecten la funcionalidad de los servicios prestados por RTVC.

4.6.4. Seguridad en los servicios de RED

- La Coordinación de T.I. controlará el acceso interno y externo a los servicios de red de RTVC con el propósito de garantizar la seguridad de los usuarios y mantener la estabilidad de los servicios, cumpliendo con los acuerdos de niveles de servicios establecidos.
- La red deberá contener dispositivos o sistemas lógicos que las protejan contra el acceso no autorizado a recursos, información y ataques informáticos internos o externos.
- Se deben restringir al máximo los accesos a la red, deshabilitando las conexiones por defecto y habilitando únicamente los accesos necesarios.
- Las redes deberán estar separadas en segmentos físicos y/o lógicos aplicando configuraciones de seguridad para cada segmento que permitan el control de tráfico dentro de la red.

- Se debe garantizar, mediante la aplicación de una lista de chequeo estándar, que los dispositivos que se conecten a la red accedan únicamente a los recursos que necesitan.
- La red inalámbrica debe usar protocolos 802.11b/g/n/a/c/x con cifrado WPA2 y autenticación EAP o superior.
- Las configuraciones de los equipos de comunicaciones y de seguridad deben estar debidamente documentadas.
- El administrador de la red debe realizar copias de respaldo de la configuración de los equipos de comunicaciones y seguridad, de manera periódica.
- El colaborador y/o contratista administrador de la red debe asegurarse de mantener actualizados los sistemas operativos y/o firmware de los equipos de comunicaciones y seguridad y estar atento a la publicación de parches de seguridad por parte de los fabricantes para su implementación inmediata.
- Cuando se deban realizar cambios de configuración o actualizaciones de seguridad en las redes, deberá llevarse a cabo de manera planificada y organizada, de forma que se evite cualquier impacto negativo en su funcionamiento.
- Deben desactivarse lógicamente, en los dispositivos de comunicaciones, todos los puertos de red que no estén siendo utilizados para evitar conexiones no autorizadas.
- Ningún dispositivo de comunicaciones debe usar la VLAN por default (Vlan 1) para administración.
- En el firewall se debe denegar el tráfico de forma implícita, es decir, solo se admite el tráfico que esté permitido explícitamente.
- Se deben revisar de manera frecuente las reglas del firewall, para comprobar que se siguen cumpliendo los requisitos de los servicios tecnológicos prestados por la entidad.
- Se debe permitir el tráfico desde la red externa hacia los servicios publicados por medio de puertos seguros tales como https y sftp. Este tráfico debe estar controlado y monitoreado. Cualquier otro tráfico proveniente de la red externa con destino hacia la red interna, deberá estar restringido y monitoreado.
- Se debe crear una línea base del comportamiento usual de la red para poder detectar cuando se presenten anomalías o infracciones.
- Se deben activar y mantener los registros de auditoría (logs) de todas las actividades de la red y deben ser revisados con frecuencia para detectar anomalías y/o mejorar el rendimiento de esta.

4.7. Políticas de Usuarios

4.7.1. Equipos de cómputo

- La asignación de equipos de cómputo (arriendo) a los usuarios y/o colaboradores de RTVC será de acuerdo con la disponibilidad de equipos a disposición de la Coordinación de TI.
- Los usuarios y/o colaboradores de RTVC tendrán un solo equipo de cómputo asignado, a no ser que su cargo o función necesite tener más de uno asignado, previa autorización por parte del supervisor y/o jefe de área, justificando la necesidad ante la Coordinación de T.I.
- Cada equipo está preparado con el *Hardware* y *Software* básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.
- En caso de presentar una falla física del equipo de cómputo, el funcionario deberá notificar a la Coordinación de T.I. a través de la mesa de servicio para su revisión y/o reparación dependiendo de la falla encontrada.
- En ningún caso el usuario intentará reparar el equipo o diagnosticar, únicamente informar de la posible falla a través de la mesa de servicio.
- Solo se utilizará el equipo asignado por RTVC para funciones de interés del área y de ninguna manera para asuntos personales.
- En caso de que el usuario no tenga conocimientos y/o experiencia en el manejo de equipos de cómputo, debe notificar a la Coordinación de T.I. para su correspondiente capacitación.
- El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
- En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre los equipos de cómputo.
- La instalación de cualquier tipo de hardware en los equipos de cómputo administrados por la coordinación de TI , y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por RTVC.
- Es responsabilidad de la Coordinación de T.I., la instalación de cualquier tipo de programa (*software*) en los equipos de cómputo administrados por la Coordinación de TI.
- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por personal autorizado por la Coordinación de T.I.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento o almacenamiento de información de RTVC; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Coordinación de T.I.

- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá solicitar la recuperación de ésta a través de la mesa de servicios.
- Sin importar las circunstancias, los usuarios y las contraseñas nunca se deben compartir o revelar, hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- Los usuarios no deben almacenar las contraseñas en ningún programa, sistema, documento, *Post-It* o cualquier otro elemento de fácil acceso que permita a otra persona tener conocimiento de estas contraseñas.
- Será responsabilidad de cada colaborador o funcionario de RTVC controlar y verificar periódicamente los permisos de acceso de los documentos compartidos en la nube con otros colaboradores, funcionarios y/o terceros. Velando por restringir el acceso solo a personal autorizado y cuyas funciones u obligaciones sean a fin al tratamiento de la información contenida en el documento.

4.7.2. Seguridad del equipo fuera de RTVC.

- El uso de equipos de cómputo, portátiles, discos removibles de RTVC o alquilados por la Coordinación de T.I., entre otros, destinados al procesamiento de información fuera de la instalación de RTVC, será solicitado por el jefe de área al que pertenezca el funcionario y/o contratista y su salida debe ser autorizada por el área de servicios generales, adicionalmente debe ser registrado a la salida e ingreso de RTVC.
- El equipo que se va a retirar debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de RTVC.
- Estas acciones seguirán el procedimiento de retiro de activos definido por la Coordinación de servicios generales

4.7.3. Escritorio y Pantalla Limpia

- Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios y/o contratistas de RTVC que accedan a información de RTVC, deben mantener la información clasificada o reservada bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, *CD´s*, dispositivos de almacenamiento *USB* y medios removibles en general.
- Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- Todas las estaciones de trabajo suministradas a funcionarios y/o contratistas deberán usar el papel tapiz y el protector de pantalla corporativo y se podrá

desbloquear únicamente con la contraseña del usuario; el cambio del papel tapiz en estos terminales de cómputo no está autorizado.

4.7.4. Protección y ubicación de los equipos

- Los equipos que hacen parte de la infraestructura tecnológica de RTVC tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados en áreas cerradas, con acceso restringido y deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.).
- De igual manera, se deben mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua y vandalismo, entre otros.
- Los funcionarios y terceros, que tengan acceso a los equipos que componen la infraestructura tecnológica de RTVC no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos, así como ingresar cualquier tipo de sustancia o material que ante la cercanía de los equipos de cómputo genere alteraciones que puedan afectar a los equipos físicamente como a su buen funcionamiento.

4.7.5. Pérdida de Equipos Informáticos

- Los funcionarios y/o contratistas de RTVC que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien.
- Los funcionarios y/o contratistas de RTVC deberán dar aviso inmediato a la Coordinación de T.I. y servicios generales de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

4.7.6. Acceso a redes sociales y/o plataformas de consumo de contenidos digitales

- Únicamente los colaboradores autorizados por la Coordinación de T.I. pueden acceder a redes sociales previa solicitud por parte del supervisor del contrato o jefe de cada área de RTVC, justificando la necesidad en sus labores del acceso a las mismas por medio de la mesa de ayuda.
- La Coordinación de Tecnología de Información realizará mínimo una y máximo dos veces al año una revalidación con los supervisores de los funcionarios la necesidad de acceso de estos usuarios.

- Se deben seguir las políticas de acceso a Internet y seguridad de la información que se encuentran en la política de operacional para la seguridad de la información.

4.7.7. Acceso WLAN

- Las claves de acceso a las redes inalámbricas son administradas por el administrador de la red, y el grupo de colaboradores de soporte de la Coordinación de T.I., quienes a su vez son los únicos autorizados para configurar el acceso a los dispositivos móviles.
- Está prohibido la divulgación de las claves a personal distinto al mencionado.
- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso a la *WLAN*.

4.7.8. Acceso VPN

- Únicamente los colaboradores y terceros autorizados por la Coordinación de T.I. pueden acceder al servicio de *VPN* previa solicitud por parte del responsable de cada área describiendo las necesidades de acceso y las herramientas a la que debe acceder por medio de la mesa de ayuda.
- Los usuarios con privilegios *VPN* son completamente responsables de todas las actividades realizadas con su cuenta de acceso, y deben asegurarse de que ninguna otra persona utilice la cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les asignan dichos privilegios.
- Mediante el uso de la tecnología *VPN*, los usuarios declaran conocer que sus computadores, ya sea institucionales o personales son una extensión de las redes de RTVC y como tales, están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de la RTVC.
- Todos los computadores conectados a RTVC mediante *VPN* deberán utilizar el software antivirus actualizado.

4.7.9. Cumplimiento de las Políticas para la Administración de la Infraestructura de TI

Toda persona que ingresa como usuario nuevo a RTVC para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en las políticas establecidas por RTVC.

Nota: Esta política fue revisada en el marco del Comité Institucional de Gestión y Desempeño realizado el 21 de noviembre del 2022.

CONTROL DE CAMBIOS

Versión	Descripción del cambio	Area Productora	Fecha de Publicación
1	Se deja como precedente que estas fechas que están dadas son las de aprobación y fecha de publicación		20/12/2022
1	Se realiza nuevamente el cargue del documento en el cual se incluye el logo de RTVC, se ajusta el código de acuerdo con la parametrización de SUITE VISIÓN, se incluye control de cambios, así mismo dando cumplimiento a los lineamientos del manual de marca. V2 y a la Guía de Administración de Información Documentada SIG.	Coordinación de Planeación	05/10/2026