

 <p>RTVC Sistema de Medios Públicos</p>	<p>GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p>POLITICA OPERACIONAL</p> <p>TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p>Página 1 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

POLÍTICA OPERACIONAL

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.

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 2 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

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 Nación¹.
3. Toda comunicación oficial (Comunicaciones recibidas o producidas en desarrollo de las funciones de una entidad, independiente del medio utilizado²), enviada o recibida debe ser registrada en el sistema de gestión documental Orfeo para oficializar su trámite, asignándoles un consecutivo único de radicado y cumplir con los términos de vencimiento establecidos por la Ley³.
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 electrónicos tales como:
 - Módulo de actas en el sistema de planeación y gestión kawak, apta para todo tipo de reuniones y una vez esta se encuentre aprobada, se debe archivar el documento electrónico en pdf.
 - Empleo del formato de "acta de reunión" publicado en el sistema de planeación y gestión kawak, el cual debe ser diligenciado digitalmente, y enviado y aceptado a través de correo electrónico.
 - Formato de asistencia a reuniones diligenciada y aceptadas a través de correo electrónico (este formato de acuerdo con las recomendaciones de la coordinación de talento humano y en el marco del protocolo de bioseguridad, se evitará en la medida de lo posible, ser diligenciado de manera física, esto hasta que dicha coordinación considere lo contrario).
 - Como soporte de la asistencia a reuniones realizadas de forma virtual, en cualquiera de las aplicaciones tecnológicas disponibles utilizadas, se podrá aportar captura(s) de pantalla en la que se visualicen los asistentes a la misma, como evidencia de su realización y se aportarán las necesarias. En el caso de las reuniones en las que haya quórum, la(s) captura(s) de pantalla se realizará en el momento de su verificación.
5. Todas las áreas deben estar en constante actualización de la normatividad legal que les aplique para el desarrollo de sus funciones.

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

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 3 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

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.

4. Normatividad Asociada

12. **Resolución MinTIC 1519 de 2020:** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
13. **Resolución MinTIC 500 de 2021:** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
14. **Directiva Presidencial No. 03 de 2021,** donde se dictan lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
15. **Directiva presidencial 02 de 2022,** donde se hace reiteración de la política pública en materia de seguridad digital.

5. Políticas transversales de desarrollo e implementación de productos digitales

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 4 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

Los siguientes aspectos descritos, son lineamientos transversales a todos los desarrollos e implementaciones que se realicen en RTVC:

- Todos los desarrollos deben estar aprobados por la Dirección de Tecnologías Convergentes mediante el acta de seguimiento a la Fábrica de Software.
- Todos los desarrollos nuevos deben contar con un documento que describa la(s) necesidad(es) que se soluciona(n) con el desarrollo, así como los perfiles de usuario que interactuaron con el mismo y la descripción de sus interacciones, los ajustes o mejoras pueden ser solicitados por las marcas al dueño de producto correspondiente mediante correo electrónico, describiendo el ajuste o mejora a solicitar.
- Todos los desarrollos deben tener su código en un repositorio en la herramienta de versionamiento de código de la entidad. La cuenta de bitbucket de la entidad debe estar administrada por el administrador del sistema y los dueños de producto.
- Para cada sitio de RTVC se debe crear el prototipado en la herramienta Adobe XD en la cual estará la guía de colores en hexadecimal y los diferentes recursos gráficos disponibles para su descarga para el desarrollo del producto digital.
- Todos los procesos de desarrollo nuevo deben terminar con un manual, guía o protocolo de usuario final (editor web o quien ejecute acciones sobre la plataforma).
- Las tareas de desarrollo y diseño serán gestionadas por medio del software de gestión del desarrollo.

6. Políticas de diseño

El objetivo de la política de desarrollo web y aplicaciones móviles es establecer los lineamientos que se deben tener en cuenta para llevar los procesos de diseño de soluciones de software en RTVC.

- Todos los diseños de sitios web o aplicaciones nuevas deben tener un documento con el mapa del sitio.
- Todos los diseños de sitios web o aplicaciones nuevas deben incluir los wireframes y estos se deben iterar tantas veces como sea necesario para que el área usuaria se sienta satisfecha con los mismos.
- Una vez se hayan terminado los wireframes, se deben socializar con los desarrolladores para evaluar posibles dificultades en la implementación de la propuesta.
- Despues de los wireframes se deben crear 2 o más propuestas de diseño sobre el home y la propuesta elegida debe iterarse hasta que el área usuaria apruebe la propuesta.
- Todos los diseños deben cumplir con el manual de marca de RTVC.
- Todas las propuestas de diseño deben implementarse en una herramienta de comunicación que le permita al área usuaria visualizar la propuesta de diseño con la mayor cercanía al

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 5 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

- producto final posible.
- Es responsabilidad del área usuaria velar por la constante actualización gráfica de su sitio web.

7. Políticas de desarrollo de software

7.1 Políticas de desarrollo web

- Todos los desarrollos web se deben implementar en un CMS (Drupal) a menos que la naturaleza de la necesidad requiera un desarrollo diferente.
- Los desarrollos que no sean implementados en Drupal deben definir y presentar su arquitectura a la Dirección de Tecnologías convergentes para su aprobación.
- La necesidad a solucionar se debe validar con los módulos del Core del CMS (Drupal) para así garantizar el desarrollo más estándar posible.
- Los sitios web desarrollados sobre algún CMS deben mantenerse en la versión más estable identificada por la fábrica de software, para evitar posibles riesgos de seguridad en el código.
- El front end de los sitios web deben basarse en framework, Bootstrap a menos que la naturaleza de la necesidad requiera un desarrollo diferente.
- Todos los desarrollos web que comparten funcionalidades entre sí deben compartirlas a través de un módulo mantenido vía la herramienta de versionamiento de código.
- Cada desarrollo web realizado debe funcionar en Chrome, Mozilla, Safari y Edge en su última versión.
- Todos los desarrollos web deben interactuar con la herramienta de métricas disponible en RTVC.
- Todos los desarrollos que se realicen deben utilizar, en la medida de lo posible, componentes nativos de Drupal (vistas, bloques o módulos contribuidos) con el fin de evitar el desarrollo personalizado de funcionalidades y mecanismos que ya existen y que se encuentran funcionando en otros desarrollos de RTVC.

7.2 Políticas de Desarrollo Móvil

- Las aplicaciones deben ser analizadas en orden de decidir su forma de desarrollo, nativa o framework.
- Todas las aplicaciones móviles públicas en tiendas virtuales deben incluir información acerca de RTVC en la descripción o en una sección de la aplicación.
- Todas las aplicaciones deben funcionar en las versiones más recientes de Android e iOS.

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 6 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

- Todas las aplicaciones deben interactuar con la herramienta de métricas disponible en RTVC.

7.3 Políticas de Implementación y Paso a Producción

- La arquitectura de los desarrollos web debe ser la siguiente:
 - Servicio de Base de datos relacional en la nube
 - Servidor(es) de aplicaciones en la nube
 - Servicio de almacenamiento en la nube
- Cada desarrollo web debe tener las siguientes instancias:

Para la etapa de desarrollo de nuevas características, módulos o sitios web:

 - Instancia de desarrollo -

opcional Para la etapa de mantenimiento y soporte:

 - Instancia de calidad
 - Instancia de producción
- Las pruebas de aceptación se deben ejecutar sobre la rama calidad
- Los merge a calidad deben coincidir con una entrega de funcionalidades al área usuaria.
- Las instancias de producción deben ser elásticas.
- La cuenta de administrador de Jenkins debe ser genérica y los correos deben ser enviados desde la cuenta creada para tal fin: development@rtvc.gov.co
- Todos los dueños de producto deben tener una cuenta de visualización para revisar el estado de sus proyectos en Jenkins.
- Los pasos de producción deben ser los siguientes:
 - Pasar el código de calidad a producción.
 - Realizar los cambios de base de datos necesarios.
 - Asegurarse con los dueños de producto que todas las funcionalidades se conservan.
 - Copiar la base de datos de producción al ambiente de calidad.
- Las ventanas de mantenimiento necesarias para el despliegue de los requerimientos en los ambientes de producción deben concertarse con el dueño de producto y administrador de infraestructura con anticipación y deben programarse después de las nueve de la noche.

8. Políticas de pruebas

8.1 Políticas para Desarrollo Web

 <p>RTVC Sistema de Medios Públicos</p>	<p>GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p>POLITICA OPERACIONAL</p> <p>TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p>Página 7 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

El responsable del área usuaria se encargará de realizar las pruebas de aceptación en la instancia de calidad antes de cualquier paso a producción.

8.2 Políticas de Desarrollo Móvil

El responsable del área usuaria se encargará de realizar las pruebas de aceptación antes de cualquier publicación en las tiendas.

9. Políticas para el aseguramiento del servicio

- Los requerimientos serán recibidos y evaluados por el dueño de producto y el equipo de desarrollo, en cuanto se reciba o aprueben los diseños del proyecto web, el equipo de desarrollo en cabeza del dueño de producto analizará los tiempos de desarrollo y se generará el cronograma inicial de entrega.
- Las áreas usuarias pueden hacer seguimiento de sus requerimientos y reportar errores por medio de correo electrónico.
- Todos los usuarios internos de un desarrollo deben contar con dominio de RTVC (xxxxx@contratista.rtvc.gov.co o xxxx@rtvc.gov.co) y sus nombres de usuario deben coincidir con el nombre de usuario del correo de RTVC.
- Ningún usuario externo al área de TI debe tener cuenta de administrador en los desarrollos de RTVC.

10. Transacciones con el proveedor de nube

- Los requerimientos de nuevas instancias, bases de datos y S3 sólo serán tramitados por el administrador del sistema a través de la mesa de servicio del proveedor.
- Los requerimientos relativos a copias de bases de datos o ambientes pueden ser solicitados directamente por los desarrolladores.
- Las fallas en el servicio deben ser reportadas por el administrador del sistema y compartidas con la Coordinación de T.I.
- El proveedor debe entregar mensualmente el informe de disponibilidad al administrador del sistema y en el caso en el cual la disponibilidad sea menor al 98% debe ser analizado con la Dirección de Tecnologías Convergentes y el desarrollador del proyecto para proponer acciones de mejora.

11. Gestión del desarrollo, Gestión del código, Gestión de Documentación, Gestión de la Integración Continúa y Herramienta de métricas

- Todos los proyectos deben implementar la herramienta de métricas que designe la entidad.
- Todos los proyectos (desarrollos, ajustes y/o modificaciones) deben tener una carpeta en la que repose la documentación asociada al proceso de fábrica de software (diseño) y al proceso técnico del mismo, para este fin se destinará la herramienta que RTVC seleccione para la gestión de correos y documentos virtuales (hojas de cálculos, documentos y almacenamiento nube).
- Los desarrollos nuevos, ajustes y modificaciones deben ser documentados a través de la herramienta de gestión de desarrollo por parte del desarrollador encargado, así mismo, cada tarea que requiera cambios a nivel de código debe tener relacionado el commit correspondiente a la herramienta de gestión de código.
- Los proyectos y funcionalidades nuevas tendrán una rama exclusiva en el repositorio con un nombre que identifique dicho desarrollo. Se debe hacer un merge de la rama mencionada a calidad cuando el desarrollo se encuentre validado por el dueño de producto.
- La cuenta de administración para cualquier servicio web será development@rtvc.gov.co
- Los proyectos y funcionalidades nuevas tendrán una rama exclusiva en el repositorio con un nombre que identifique dicho desarrollo. Se debe hacer un merge de la rama mencionada a calidad cuando el desarrollo se encuentre validado por el dueño de producto.
- Los procesos de soporte y mantenimiento deben tener las siguientes ramas en el repositorio:
 - Máster: versión en producción
 - Calidad: versión en prueba
- Los proyectos en la herramienta de gestión del desarrollo, la herramienta de gestión del código, la herramienta de gestión de correos y documentos virtuales y la herramienta de gestión de la integración continua deben estar organizados en las siguientes categorías:
 - RTVC
 - Televisión
 - Radio
 - Señal Memoria
- El despliegue de infraestructura en la nube le corresponde única y exclusivamente al administrador del sistema.
- Los nombres de las carpetas asociadas a la documentación deben tener la siguiente estructura: año, marca sobre la que se ejecuta el proyecto y nombre del proyecto, ejemplo:
 - 2020 / Señal Colombia / Especial Cóndor de los Andes
 - 2020 / Señal Memoria / INCI
 - 2020 / RTVCPlay / Registro de usuario
- Los nombres de los repositorios deben constar de tres partes: categoría, proyecto e

 <p>RTVC Sistema de Medios Públicos</p>	<p>GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p>POLITICA OPERACIONAL</p> <p>TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p>Página 9 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------

información adicional, ejemplo:

- Parrilla
- SenalColombia
- RadioNacional

Las categorías y proyectos corresponderán a uno de los siguientes:

- RTVC
 - intranet
 - sw_rtvc
 - rtvoplay
 - otros
- TV
 - senal_colombia
 - canal_institucional
 - mi_señal
 - proyecta_informativo
 - proyecta_transaccional
 - así_somos
 - otros
- R
 - Radionica
 - Radio_nacional
 - Otros
- SM
 - SW_señal_memoria

12. Política de desarrollo seguro

Los siguientes aspectos descritos, son lineamientos transversales a todos los desarrollos e implementaciones que se realicen en RTVC.

12.1 Lineamientos de desarrollo seguro

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 10 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------

- Todos los desarrollos de sitios Web y aplicaciones deben contar con un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante su vida útil.
- Todos los frameworks o herramientas para desarrollo deben mantenerse actualizadas a la última versión estable liberada por los fabricantes.
- Todos los desarrollos deben seguir las buenas prácticas de W3C (World Wide Consortium).
- Todos los sitios web y aplicaciones deben garantizar la protección del código fuente a través de la separación del FrontEnd y el BackEnd.
- Garantizar que no se revele información acerca de las versiones y tecnologías de los sitios web y aplicaciones a través de los HTTP headers.
- Implementar mensajes genéricos de error que garanticen que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios.
- Controlar y validar todos los datos de entrada proporcionados por los usuarios en los sitios Web y aplicaciones.
- Controlar adecuadamente los datos de entrada a los sitios web y aplicaciones, considerando los casos de uso con el fin de detectar y corregir posibles errores de configuración o programación.
- Tanto del lado del cliente como del lado del servidor se debe incorporar validación de formularios.
- Utilizar captchas para introducir un mecanismo de validación de las peticiones, en los casos en los que aplique.

12.2 Seguridad de entornos o ambientes

- Implementar y mantener actualizado un sistema de integración, cambio y despliegue continuo.
- Prevenir la revelación de la estructura de directorios en los sistemas implementados.
- Mantener deshabilitados los métodos HTTP peligrosos para dominios fuera de los dominios administrados por RTVC.
- Todo sitio web deberá cifrar todas las comunicaciones entre el cliente y el servidor, a través del protocolo HTTPS, utilizando certificados válidos emitidos por entidades certificadoras

 <p>RTVC Sistema de Medios Públicos</p>	<p align="center">GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p align="center">POLITICA OPERACIONAL</p> <p align="center">TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p align="center">Página 11 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------

debidamente acreditadas.

- Redirigir la navegación a través del protocolo HTTP hacia el protocolo HTTPS para todos los sitios Web.
- Todos los servicios Web expuestos a Internet deben estar protegidos por un WAF (Web application firewall)
- Implementar reglas para:
 - Bloquear o eliminar cualquier tipo de carácter que pueda estar relacionado con la inserción de código (Cross-site scripting).
 - Bloquear o eliminar cualquier tipo de carácter que pueda estar relacionado con inyección SQL (SQL injection).
 - Bloquear o eliminar cualquier tipo de acción que pueda estar relacionada con DoS (Denial-of-service).
- Garantizar el control de versiones que permita planear y controlar la vida de las aplicaciones y sitios Web.
- Realizar copias de seguridad de servidores, configuraciones y bases de datos de los ambientes productivos.

12.3 Control de Acceso

- Definir, implementar y mantener un esquema general de permisos sobre los objetos y recursos de todo el sistema.
- Crear roles de acceso aplicando el principio de mínimo privilegio donde una cuenta de usuario debe tener suficientes permisos para hacer lo que tiene que hacer dada su función y no más que eso.
- Ninguna implementación debe realizarse con credenciales predeterminadas, especialmente para usuarios administradores.
- Las contraseñas utilizadas para la gestión de desarrollos, sitios web o aplicaciones deben seguir los lineamientos establecidos en la Política para la administración de la infraestructura de T.I.
- Los campos de contraseñas no deben ser legibles.
- Se debe establecer un número máximo de reintentos en aquellas operaciones que se consideren críticas para los sitios Web y aplicaciones.
- Restringir la escritura de archivos desde los sitios web a través de la asignación de

 <p>RTVC Sistema de Medios Públicos</p>	<p>GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA</p> <p>POLITICA OPERACIONAL</p> <p>TRANSVERSAL DE DESARROLLO E IMPLEMENTACIÓN DE PRODUCTOS DIGITALES</p>	<p>Código: T-A-3</p> <p>Version: 9</p> <p>Fecha: 28-11-2022</p> <p>Página 12 de 12</p>
-------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

permisos de solo lectura.

- Las conexiones a las bases de datos desde los aplicativos deben ser cerradas tan pronto como estas no sean requeridas.
- No permitir que los sitios web o aplicaciones ejecuten comandos directamente en el sistema operativo con privilegios de administrador.

12.4 Registros de auditoría

- Todos los desarrollos deben incluir la generación de registros de auditoría, que incluyan como mínimo la identidad del usuario, tipo de evento, fecha y hora del evento.
- Todas las fallas de validación de entrada y de control de acceso, deben quedar registradas con suficiente contexto de usuario para identificar comportamientos sospechosos.
- Todos los registros de auditoría deben estar protegidos contra la manipulación no autorizada.
- Los relojes en todos los sistemas de procesamiento de información deben estar sincronizados a una sola fuente horaria de referencia.

12.5 Supervisión y monitoreo

- Ejecutar monitoreo a través del WAF en la Nube para detectar actividades sospechosas y tomar acción oportunamente.
- Monitorear el rendimiento de CPU, I/O y memoria en la infraestructura Nube.
- Se debe realizar por lo menos un (1) ejercicio de Ethical Hacking al año y ejecutar las acciones de mitigación para las vulnerabilidades encontradas.

Nota: Esta política fue revisada en el marco del Comité Institucional de gestión y desempeño realizado el 21 de noviembre de 2022