2025

Plan de Seguridad y Privacidad de la Información

ENERO 2025

RTVC Sistema de Medios Públicos | Señal Colombia | Canal Institucional TV | Radio Nacional de Colombia | radiónica | Señal Memoria | RTVCPlay

TABLA DE CONTENIDO

INTRODUCCIÓN

Para RTVC la información es un activo estratégico que requiere protección especial. Elaborar e implementar un Plan de Seguridad y Privacidad de la Información no solo es una buena práctica, sino una obligación contemplada en el marco normativo colombiano, incluyendo la Ley 1581 de 2012 (protección de datos personales), la Ley 527 de 1999 (comercio electrónico) y las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Este plan es fundamental para:

- **Garantizar la continuidad de las operaciones y la prestación de servicios a la ciudadanía:** Protegiendo la información de ciberataques, desastres naturales y errores humanos.
- **Preservar la confianza pública:** Asegurando la confidencialidad, integridad y disponibilidad de la información, especialmente aquella relacionada con datos personales de los ciudadanos.
- **Cumplir con el marco legal vigente:** Evitando sanciones y responsabilidades legales derivadas del incumplimiento de la normativa.
- **Promover la transparencia y la rendición de cuentas:** Facilitando el acceso a la información pública y protegiendo la información sensible.

En resumen, el Plan de Seguridad y Privacidad de la Información es esencial para el cumplimiento de la misión institucional, la protección de los datos ciudadanos y la gestión responsable de la información pública.

OBJETIVO

El PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE RTVC tiene como objetivos:

- Identificar las acciones concretas que permitan un avance significativo del porcentaje de cumplimiento de la autoevaluación del MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) del 2025.

- Crear una hoja de ruta con las acciones mencionadas incluyéndolas en un cronograma de actividades y entregables

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

MARCO NORMATIVO

El PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN de RTVC se basa, principalmente, en las siguientes leyes, normas o decretos:

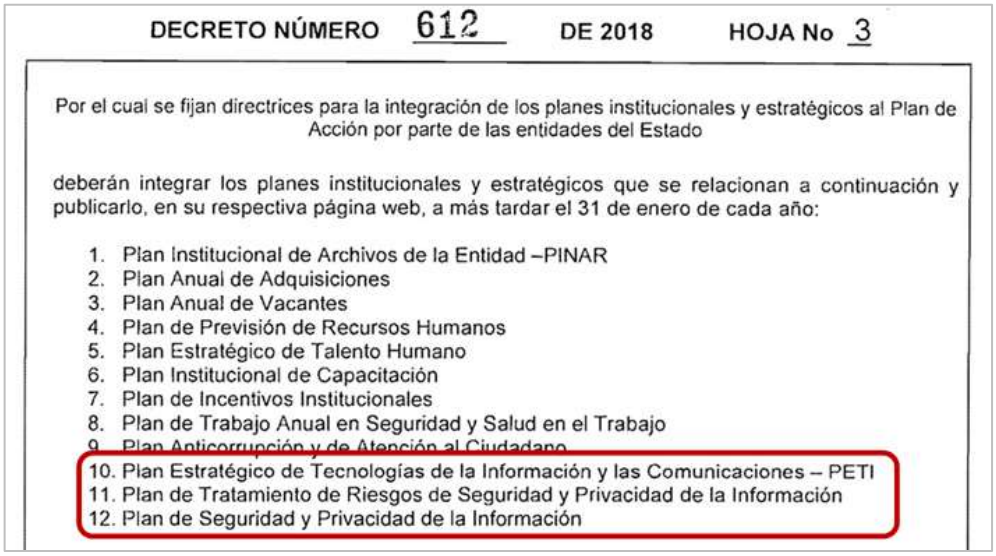
Ley, norma o decreto	Ámbito de aplicación
Ley No 2294 19 de mayo de 2023	Plan Nacional de Desarrollo
Constitución Política de Colombia.	Artículos 15, 209 y 269.
Ley 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012.	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 1377 de 2013.	Por el cual se reglamenta parcialmente la Ley 1581 de 2012. • Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Ley 1712 de 2014.	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015.	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
Decreto 1081 de 2015.	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Decreto 1083 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
CONPES 3854 de 2016.	Política Nacional de Seguridad digital.

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

Ley, norma o decreto	Ámbito de aplicación
Ley 1915 de 2018.	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018.	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 2106 de 2019.	establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 1952 de 2019.	Por medio de la cual se expide el código general disciplinario

CONTEXTO ESTRATEGICO

El Plan de Seguridad y Privacidad de la Información de RTVC hace parte del Modelo de Seguridad y privacidad (MSPI) y hace parte de los planes institucionales y estratégicos definidos en el marco del decreto 612 de 2018.



DECRETO NÚMERO 612 DE 2018 HOJA No 3

Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado

deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:

1. Plan Institucional de Archivos de la Entidad –PINAR
2. Plan Anual de Adquisiciones
3. Plan Anual de Vacantes
4. Plan de Previsión de Recursos Humanos
5. Plan Estratégico de Talento Humano
6. Plan Institucional de Capacitación
7. Plan de Incentivos Institucionales
8. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
9. Plan Anticorrupción y de Atención al Ciudadano
10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI
11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
12. Plan de Seguridad y Privacidad de la Información

Ilustración 1. Vista del decreto 612 de 2018 e identificación del plan de seguridad y privacidad

Tanto el modelo como el plan de seguridad y privacidad de RTVC se articulan y resultan de la aplicación de la Política de Gobierno Digital, de sus componentes, propósitos y habilitadores. A continuación, se muestra esta articulación:

Ilustración 2. Política de gobierno digital

La ilustración a continuación se muestra el Modelo de Seguridad y Privacidad de la Información de RTVC y cada uno de sus componentes, entradas y salidas. El modelo se basa en el habilitador de la política Gobierno Digital del Ministerio de Tecnología de la Información:

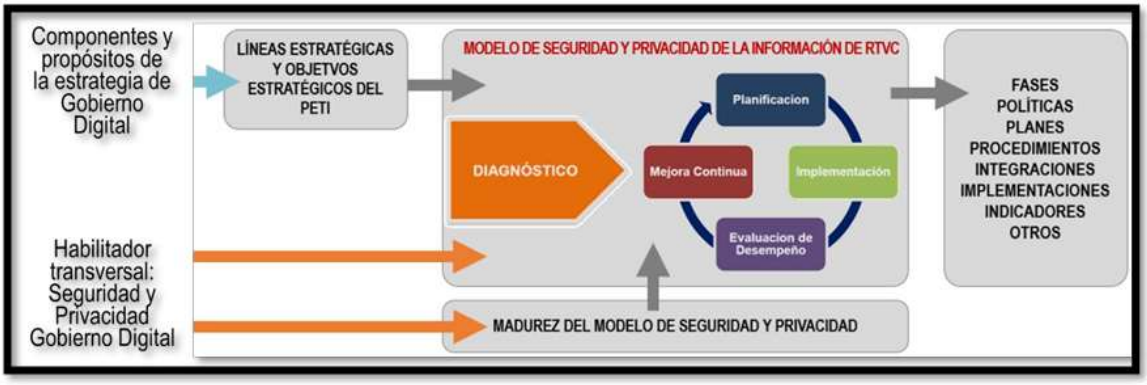


Ilustración 2. Modelo de privacidad y seguridad de la información RTVC

PROCESO DE FORMULACIÓN

Situación actual

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2022 es de:

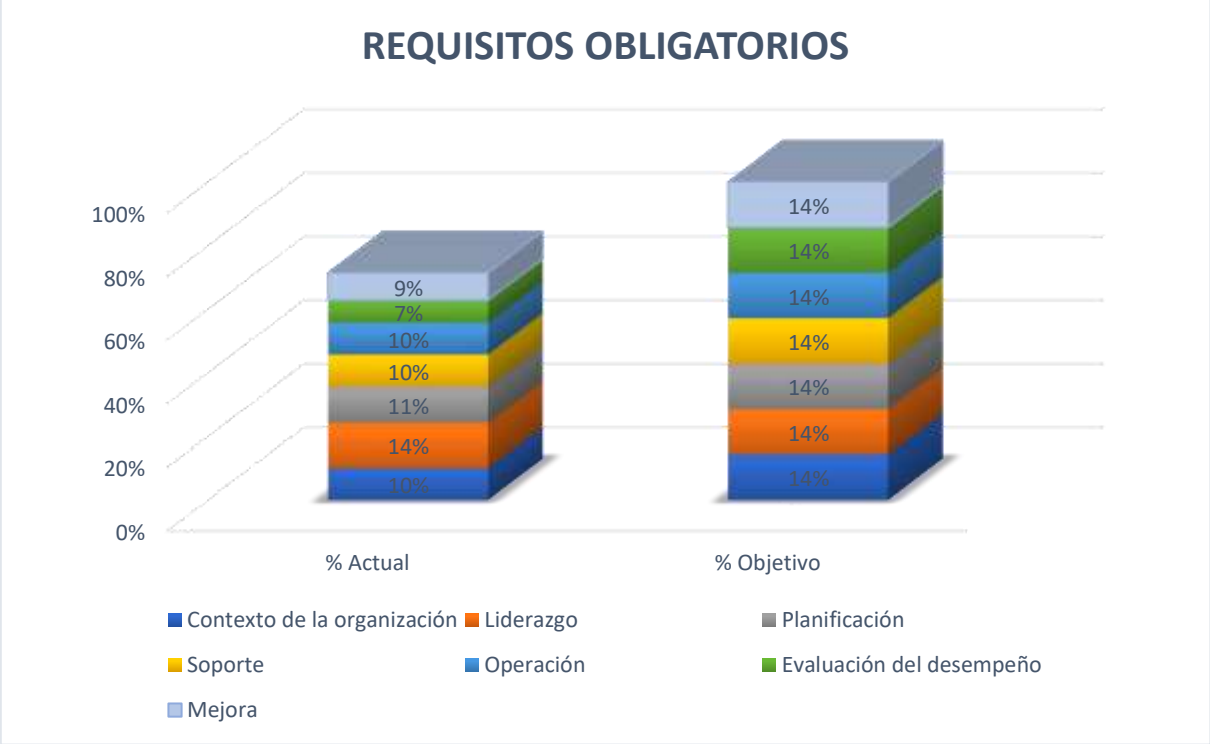


Grafico 1. Resultado de la evaluación cuantitativa de los requisitos obligatorios de la Norma ISO 27001:2022

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

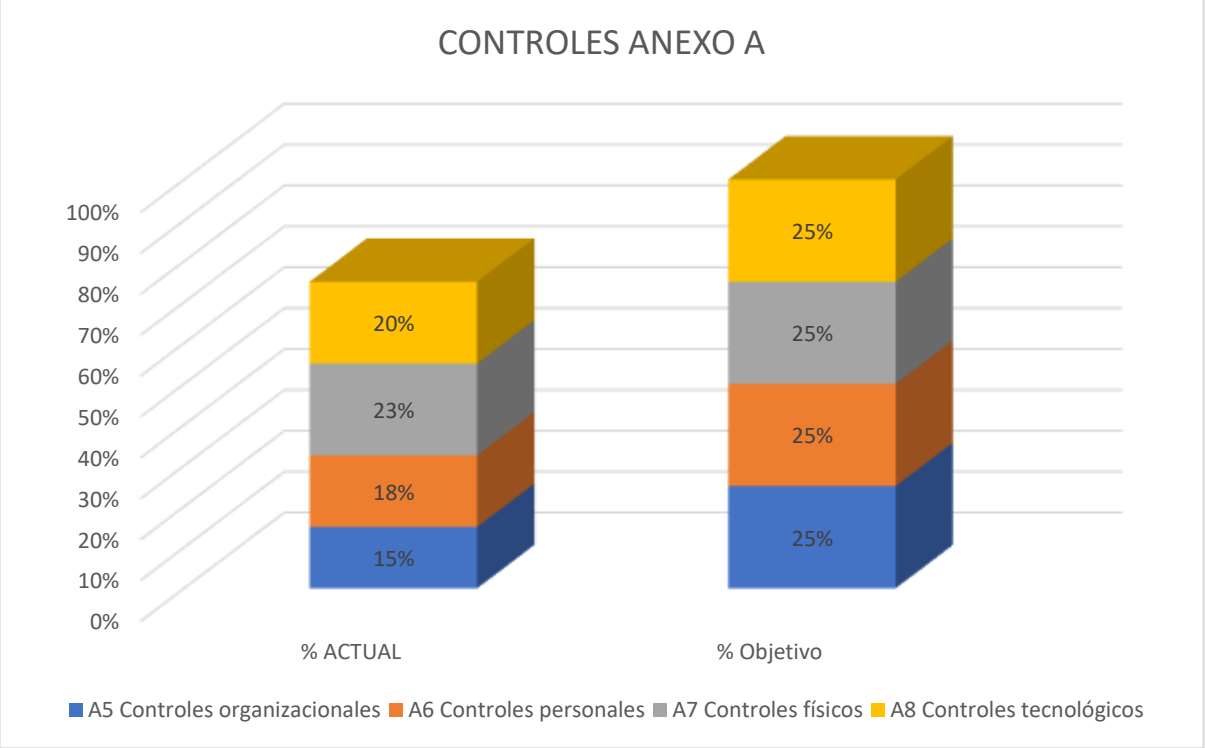


Gráfico 2. Resultado de la evaluación cuantitativa de los controles del anexo A de la Norma ISO 27001:2022

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información el porcentaje de efectividad en la implementación de los controles de la Norma de Ciberseguridad NIST CFS 2.0 es de:

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

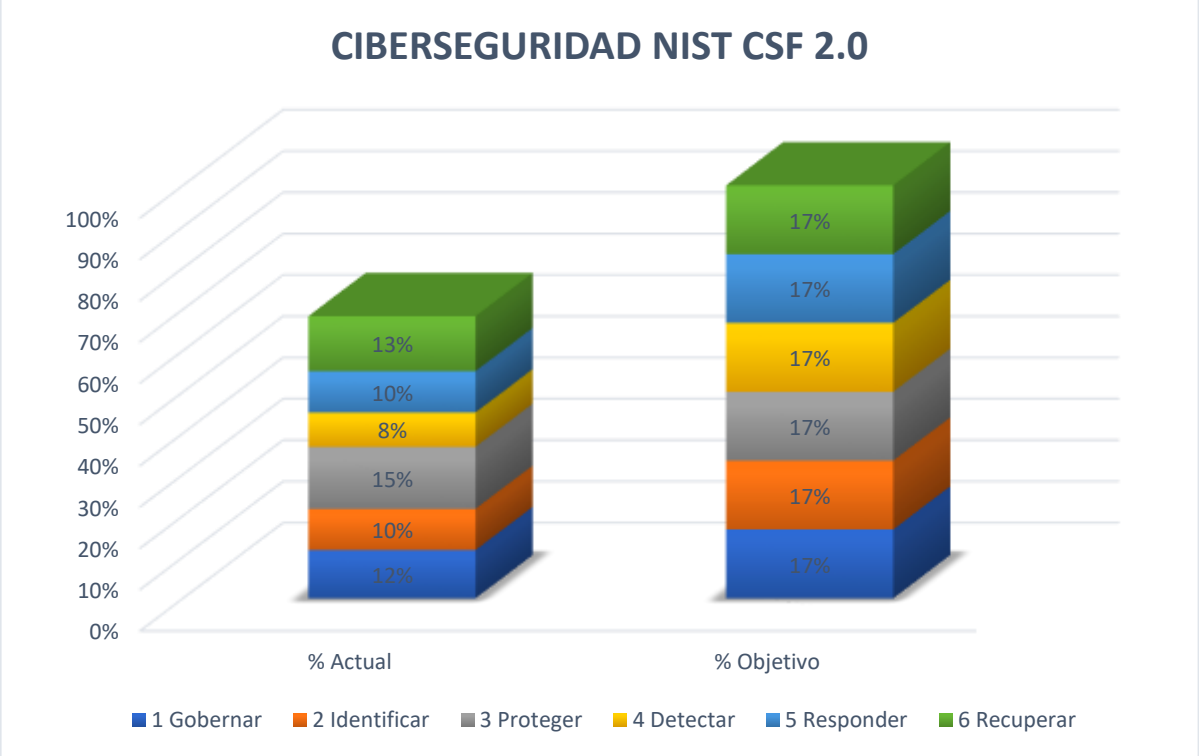


Gráfico 3. Resultado de la evaluación cuantitativa de los requisitos de ciberseguridad NIST CFS 2.0

Situación deseada

REQUISITOS OBLIGATORIOS

En cuanto a los requisitos obligatorios (71%) Se debe trabajar en los siguientes ítems:

- Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.
- "La información documentada se debe controlar para asegurar que: Esté disponible y adecuado para su uso, cuando y donde se requiere Esté protegida adecuadamente."
- Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad.
- Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
- Estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.
- Plan de auditoría interna.
- Evaluación y seguimiento a los compromisos establecidos para ejecutar el plan de tratamiento de riesgos.

- Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.
- Aprobación de la alta dirección, documentada y firmada, para la Implementación del Modelo de Seguridad y Privacidad de la Información.
- Adquisición, desarrollo y mantenimiento de los sistemas de información, datos de prueba.
- Indicadores de cumplimiento para establecer si las políticas de seguridad y privacidad de la información y las cláusulas establecidas por la organización en los contratos de trabajo, son acatadas correctamente.
- Informes del desempeño de la operación del MSPI, con la medición de los indicadores de gestión definidos.
- Pruebas y ventanas de mantenimiento (simulacro), para determinar la efectividad de los planes de respuesta de incidentes.
- Seguridad en operativa, registro de actividad y supervisión.

EFECTIVIDAD DE LOS CONTROLES

En cuanto al frente de ***Efectividad de los controles*** (75%), es necesario aumentar los indicadores relacionados con los siguientes ítems:

- Organización de la seguridad
- Gestión de activos
- Criptografía
- Seguridad de la operación y de las comunicaciones
- Desarrollo y mantenimiento de sistemas
- Incidentes de seguridad
    - Elaboración de los informes de TODOS los incidentes de seguridad y privacidad de la información. Definición de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
    - Controles y medidas identificados para disminuir los incidentes implementados
- Continuidad del negocio

MEJORES PRÁCTICAS EN CIBERSEGURIAD (NIST)

En cuanto a la calificación de las ***"mejores prácticas en ciberseguridad" (Framework de ciberseguridad NIST)***, es necesario llevar a cabo las siguientes acciones relacionadas (Calificaciones iguales o menores a 60):

- Funciones asociadas a la etapa IDENTIFICAR
- Funciones asociadas a la etapa DETECTAR

- Funciones asociadas a la etapa RECUPERAR

CRONOGRAMA

A continuación, se muestra el cronograma del plan de seguridad y privacidad para las acciones de mejora (Iniciativas o proyectos) que permitirán un avance significativo de en el porcentaje de cumplimiento de la autoevaluación del MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI):

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

ITEM	DOCUMENTO	ACTIVIDADES	DETALLE DE ACTIVIDAD	INICIO	FIN
PLANIFICACIÓN					
DOCUMENTOS	Declaración de aplicabilidad	Actualización de Declaración de aplicabilidad	Revisar el documento con los 93 controles de la norma ISO 27001:2022 y su aplicabilidad para RTVC	1-feb-25	30-jun-25
	Plan de cambio y cultura en Seguridad y Privacidad de la Información	Elaboración y Ejecución del plan de cambio y cultura en Seguridad y Privacidad de la Información para 2025	Documentar las actividades a realizar: - Oficina TIC - Ejercicios de phishing - Socialización de la Política de Seguridad de la información - Socializar el procedimiento de Gestión de incidentes - Sensibilizar vía los canales internos de RTVC - Capacitación a usuarios - Fortinet - Asistencia a capacitaciones MinTIC	1-feb-25	30-nov-25
	Política Operacional Seguridad de la Información y Seguridad Digital	Actualización de la Política Operacional Seguridad de la Información y Seguridad Digital	Elaboración de la Política Operacional Seguridad de la Información y Seguridad Digital	1-jul-25	30-sep-25
	Política de Desarrollo Seguro	Actualización de la Política de Desarrollo Seguro	Revisión y Actualización de la política de desarrollo seguro en la Política Operacional de Desarrollo e implementación de software para RTVC	1-jul-25	30-sep-25
	Contacto con autoridades y grupos de interés	Actualizar el documento Contacto con autoridades y grupos de interés	Actualizar el documento existente y actualizarlo de ser necesario	1-feb-25	30-jun-25
	Gestión de vulnerabilidades	Revisión de las Vulnerabilidades presentas	Realizar seguimiento a las Vulnerabilidades	1-feb-25	30-nov-25
ACTIVOS DE INFORMACIÓN	Guía para la Gestión y Clasificación de activos de Información	Actualización "Guía para la Gestión y Clasificación de activos de Información"	Actualización de la guía y realización de ajustes de ser necesarios	5-feb-25	18-mar-25
	Inventario y clasificación de Activos de información	Actualización del inventario de activos	Gestión de la infraestructura tecnológica	1-mar-25	30-abr-25
			Control de Asuntos disciplinarios	1-mar-25	30-abr-25
			Gestión del Talento Humano	1-mar-25	30-abr-25
			Gestión Documental	1-mar-25	30-abr-25
			Gestión de relación con grupos de interés	1-mar-25	30-abr-25
			Atención al ciudadano y gestión del cliente	1-mar-25	30-abr-25
			Direccionamiento estratégico y planeación	1-may-25	30-jun-25
			Gestión por proceso y la innovación	1-may-25	30-jun-25
			Control Interno	1-may-25	30-jun-25
			Gestión Jurídica	1-may-25	30-jun-25
			Gestión de proveedores	1-may-25	30-jun-25

ITEM	DOCUMENTO	ACTIVIDADES	DETALLE DE ACTIVIDAD	INICIO	FIN
			Gestión de infraestructura física	1-jul-25	30-jul-25
			Gestión financiera, recaudo y gasto público	1-jul-25	30-jul-25
			Aprovisionamiento para la prestación de productos y servicios convergentes	1-jul-25	30-jul-25
			Gestión de tecnologías de la información	1-jul-25	30-jul-25
RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Matrices de Riesgos de Seguridad de la información	Actualización de la matriz de riesgos y definición de plan de tratamiento de riesgos	Gestión de la infraestructura tecnológica	1-mar-25	30-abr-25
			Control de Asuntos disciplinarios	1-mar-25	30-abr-25
			Gestión del Talento Humano	1-mar-25	30-abr-25
			Gestión Documental	1-mar-25	30-abr-25
			Gestión de relación con grupos de interés	1-mar-25	30-abr-25
			Atención al ciudadano y gestión del cliente	1-mar-25	30-abr-25
			Direccionamiento estratégico y planeación	1-may-25	30-jun-25
			Gestión por proceso y la innovación	1-may-25	30-jun-25
			Control Interno	1-may-25	30-jun-25
			Gestión Jurídica	1-may-25	30-jun-25
			Gestión de proveedores	1-may-25	30-jun-25
			Gestión de infraestructura física	1-jul-25	30-jul-25
			Gestión financiera, recaudo y gasto público	1-jul-25	30-jul-25
			Aprovisionamiento para la prestación de productos y servicios convergentes	1-jul-25	30-jul-25
			Gestión de tecnologías de la información	1-jul-25	30-jul-25
IMPLEMENTACIÓN Y OPERACIÓN					
CONTROLES	Seguimiento a la implementación y ejecución de controles	Seguimiento al estado de los planes de tratamiento de riesgos identificados y verificación de evidencias de la ejecución e implementación de controles	Seguimiento ejecución de los controles (2024)	1-mar-25	30-jul-25
			Seguimiento ejecución de los controles (2024)	1-mar-25	30-jul-25
CONCIENTIZACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Ejecución del plan de cambio y cultura	Ejecutar el Plan de cambio y cultura en Seguridad de la información	Ejecutar las actividades establecidas en el Plan de cambio y cultura en Seguridad de la información	1-feb-25	30-nov-25
GESTIÓN DE VULNERABILIDADES	Gestión de vulnerabilidades	Identificación de vulnerabilidades y tratamiento	Identificación de vulnerabilidades y seguimiento a la remediación	1-feb-25	30-nov-25

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

ITEM	DOCUMENTO	ACTIVIDADES	DETALLE DE ACTIVIDAD	INICIO	FIN
SEGURIDAD INFORMÁTICA	Mejoras en la seguridad informática	Recomendaciones ajustes en el Firewall	Recomendaciones para la realización de ajustes en el Firewall	1-feb-25	30-nov-25
EVALUACIÓN					
MIPG	Documentos MIPG y FURAG	Seguimiento y reporte a MIPG y FURAG	Plan de Mejoramiento de Furag	1-abr-25	30-dic-25
SEGUIMIENTO IMPLEMENTACIÓN DEL MSPI	Herramienta de autodiagnóstico MinTIC	Seguimiento implementación del MSPI	Resultados Marzo	4-abr-25	8-abr-25
			Resultados Junio	4-jul-25	8-jul-25
			Resultados Septiembre	3-oct-25	7-oct-25
			Resultados Diciembre	28-dic-25	13-ene-25
INDICADORES	Documento registro de indicadores	Consolidar indicadores	Resultados Junio	4-jul-25	8-jul-25
			Resultados Noviembre	28-dic-25	13-ene-25
MEJORA CONTINUA					
SEGUIMIENTO IMPLEMENTACIÓN DEL MSPI	Presentación Avances de la implementación del SGSI	Socialización avances de la implementación de SGSI al Comité Institucional de Gestión y Desempeño	Socialización avances de la implementación de SGSI al Comité Institucional de Gestión y Desempeño	1-oct-25	6-dic-25
MIPG	Documentos MIPG y FURAG	Seguimiento y reporte a MIPG y FURAG	Seguimiento al Plan de Mejoramiento de Furag	1-abr-25	30-dic-25

Tabla 1: Cronograma de actividades 2025

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**
Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703

SEGUIMIENTO Y CONTROL

Indicador asociado

Nombre del indicador	Frecuencia	Meta	Tipología
Avance del plan seguridad y privacidad de la información.	Trimestral	Porcentaje	Eficacia

Tabla 2: Ficha del indicador del plan

Estado de avance	Descripción
SATISFACTORIO	80% -100%
MEDIO	60%-79%
BAJO	0-59%

Tabla 3: Escala de medición del indicador

Se realizar un seguimiento al plan de implementación el cual presentará un avance según la planeación de las actividades, este avance se presentará en forma de seguimiento del plan y se presentará en el la reunión de seguimiento de la dirección de tecnologías convergentes, de manera trimestral, la comprobación será el informe presentado.

CONTROL DE CAMBIOS

Versión	Descripción de ajuste	Fecha de publicación
01	Versión inicial	31 de enero de 2025

Javier Cerquera Dussan
Director de tecnologías convergentes

Elaboró: Javier Andrés Garzón – Coordinación de TI
Revisó: Nombre del profesional que revisó el documento técnico – Coordinación de xxxxx

Av. El Dorado Cr. 45 # 26 - 33
Bogotá D.C. Colombia - Código Postal: **111321**

Teléfonos: (+57)(601) 2200700
Línea gratuita nacional: 018000123414
Línea preferencial para personas sordas: (+57)(601) 2200703