COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección Ejecutiva
Líder: Zoila Vargas Mesa
Coordinadora Ejecutiva

Enero de 2026

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

INTRODUCCIÓN

En el contexto actual, la seguridad y privacidad de la información se han convertido en aspectos fundamentales para el desarrollo tecnológico, la protección de datos personales e institucionales, y el cumplimiento de regulaciones en Colombia. Ante un panorama digital en constante evolución, es crucial garantizar la confidencialidad, integridad y disponibilidad de la información, así como protegerla de amenazas cibernéticas cada vez más sofisticadas.

El presente plan estratégico tiene como objetivo establecer un marco integral que aborde los desafíos actuales y futuros en materia de ciberseguridad y protección de datos. Este plan busca promover una cultura de seguridad y privacidad que involucre a entidades públicas y privadas en un esfuerzo colaborativo por proteger la información sensible.

Además, este plan estratégico reconoce la importancia de la formación continua y la concienciación en temas de seguridad informática, así como el fomento de buenas prácticas para mitigar riesgos y responder eficazmente a incidentes de seguridad. Asimismo, se propone establecer mecanismos de supervisión y evaluación que permitan medir el impacto del plan y adaptarlo a los cambios tecnológicos y legislativos.

Este plan representa un compromiso con la protección de la información en Colombia, con miras a fortalecer la confianza en el entorno digital y garantizar el respeto a los derechos individuales. Es un paso fundamental hacia una sociedad más segura, resiliente y preparada para enfrentar los desafíos del mundo digital.

Así mismo, tiene como propósito principal establecer directrices claras y efectivas para garantizar el respeto a la privacidad, la integridad y la confidencialidad de los datos en cumplimiento con las regulaciones colombianas, así como con los estándares de protección de datos.

Adicionalmente, busca no solo fortalecer las medidas técnicas y organizativas para proteger la información, sino también fomentar una cultura de privacidad y transparencia en el tratamiento de los datos. Además, se propone una estrecha colaboración con las entidades reguladoras para asegurar el cumplimiento normativo y adaptarse a las cambiantes leyes y normativas relacionadas con la privacidad y protección de datos en Colombia.

Actualmente, la Comisión de Regulación de Comunicaciones tiene el propósito de fortalecer la protección de los activos de información que soportan los procesos de la Entidad. Para asegurar la dirección estratégica de la Entidad, establece la política de seguridad de la información con los siguientes objetivos:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en la CRC.
2. Identificar, clasificar y mantener actualizado el inventario de los activos de información de la CRC de acuerdo con los requisitos legales y regulatorios.
3. Administrar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación tecnológica que puedan afectar los activos de información.
4. Gestionar los eventos e incidentes de seguridad de la información que afecten o puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información reduciendo su impacto y propagación.
5. Implementar las estrategias de continuidad para los servicios tecnológicos que soporten los requerimientos de continuidad del negocio.

Teniendo en cuenta lo anterior, las coordinaciones de Tecnologías y Sistemas de Información y Planeación y Gestión de la Comisión de Regulación de Comunicaciones presentan el análisis de la información referente a temas de seguridad y privacidad de la información, diseñando un plan estratégico de seguridad y privacidad de la información basado en los estándares ISO 27001, ISO 27701, el Modelo de Seguridad y Privacidad de la Información del MinTIC y los lineamientos de Gobierno Digital con el fin de proporcionar una solución a los requerimientos de seguridad y protección de la información en la Entidad fortaleciendo así las políticas de seguridad existentes, prevenir posibles daños o pérdida de información y afianzando la cultura de seguridad de la información entre los funcionarios.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

OBJETIVO

Formular el Plan Estratégico de Seguridad y Privacidad de la Información de la Comisión de Regulación de Comunicaciones (CRC) para la vigencia 2026, el cual se enmarca en los siguientes objetivos:

- Definir los proyectos e iniciativas.
- Clasificar y priorizar los proyectos a realizar.
- Aprobar el plan estratégico de seguridad y privacidad de la información.

ALCANCE DEL DOCUMENTO

Este documento incorpora la definición estratégica de la seguridad y privacidad de la información para la CRC, estableciendo el plan de implementación de los proyectos y servicios que se proponen ejecutar en la vigencia 2026, definidos a través del plan de acción de la entidad para los diferentes ámbitos en el Modelo de Seguridad y Privacidad de la Información.

El documento describe las definiciones realizadas sobre la estrategia, objetivos, marco normativo, situación actual, entendimiento estratégico, modelo de gestión y el respectivo modelo de planeación definiendo el portafolio de proyectos y la hoja de ruta de implementación.

ANÁLISIS DE LA SITUACIÓN ACTUAL

En este apartado se describe la situación actual de la seguridad y privacidad de la información de la Entidad en relación con los dominios del Modelo de Seguridad y Privacidad de la Información del MinTIC, resultados del FURAG y los controles de la NTC-ISO 27001. Este análisis permite conocer el estado actual o línea base con la cual se debe partir para proyectar la visión de lo que se espera en materia de gestión de seguridad de la información en la Entidad.

Los resultados de cada análisis muestran el estado en cuanto al cumplimiento del modelo y un análisis cualitativo representado porcentualmente, que indica a su vez las brechas a cerrar y que son determinantes para el modelo de planeación y la inclusión dentro del portafolio de proyectos.

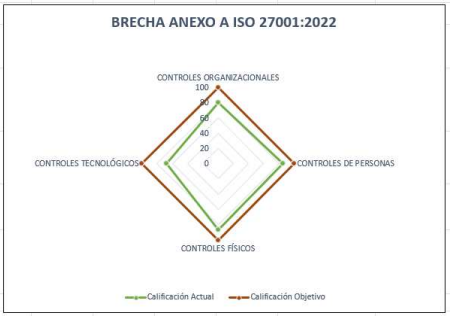
Respecto a la cuantificación y a los criterios de calidad definidos, y de acuerdo con el autodiagnóstico de los componentes de Gobierno Digital para el componente habilitador de Seguridad y Privacidad de la información como se presenta a continuación.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Figura 1. Resultado Autodiagnóstico de controles MSPI

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	80	100	GESTIONADO
A.6	CONTROLES DE PERSONAS	85	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	87	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	68	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		80	100	GESTIONADO



FUENTE: Autodiagnóstico MSPI CRC

Para la medición, este instrumento se divide en componentes, los cuales involucran Planificación, Implementación, Evaluación de Desempeño y Mejora Continua, cada uno con una respectiva medición y porcentaje esperado de implementación, lo que permite identificar las brechas que tienen:

Figura 2. Resultado Autodiagnóstico de componentes MSPI

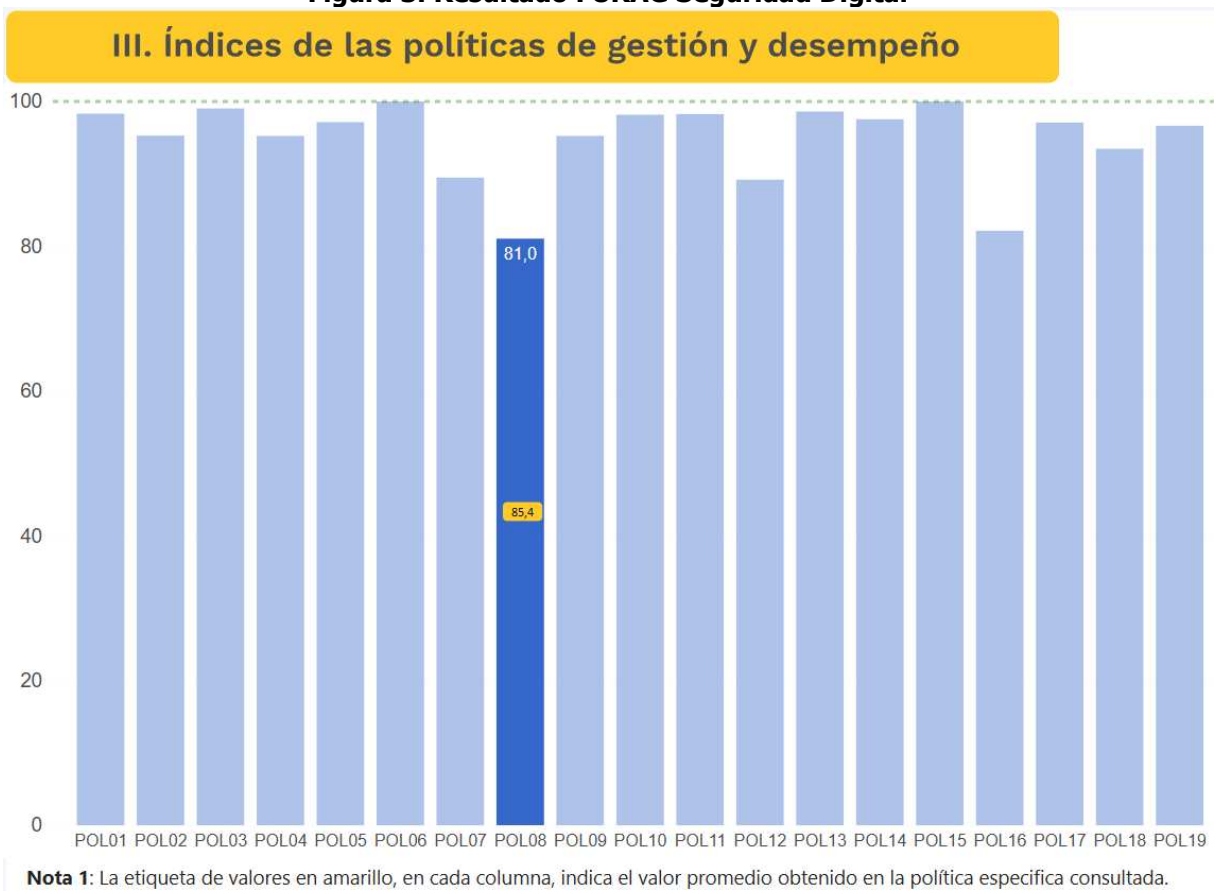
AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	12%	14%
		Liderazgo	14%	14%
		Planificación	14%	14%
		Soporte	13%	14%
	Implementación	Operación	14%	16%
	Evaluación de Desempeño	Evaluación del desempeño	12%	14%
	Mejora Continua	Mejora	11%	14%
TOTAL			91%	100%

FUENTE: Autodiagnóstico MSPI CRC

Con respecto a la medición del FURAG 2024, se obtuvo un porcentaje de cumplimiento del 81.0, lo que evidencia una relación en las valoraciones realizadas con la herramienta del Autodiagnóstico del MinTIC y un compromiso de la CRC para con el cumplimiento de esta política en la Entidad gracias a que su resultado sobresale y es referente para el Sector en el que se encuentra.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Figura 3. Resultado FURAG Seguridad Digital



Nota 1: La etiqueta de valores en amarillo, en cada columna, indica el valor promedio obtenido en la política especifica consultada.

FUENTE: Resultados FURAG CRC

Asimismo, durante la vigencia 2024 se realizó la primera auditoría interna al proceso de Gestión De Tecnologías y Sistemas de Información que incluyó al SGSI bajo el enfoque de la ISO 27001:2013, dejando los siguientes hallazgos:

0	42	55
Fortalezas	Observaciones	No conformidades

Cabe resaltar que el alcance de la auditoría incluyó FURAG, Gobierno Digital, Seguridad Digital, Accesibilidad de la Página WEB, entre otras, por lo que no todas corresponden a hallazgos del SGSI bajo la NTC-ISO 27001:2013. Durante el 2025 se realizaron los respectivos planes de mejoramiento.

PRESUPUESTO ASIGNADO

De acuerdo con los planes establecidos para la vigencia 2026, se contempla invertir presupuesto para el fortalecimiento de las capacidades administrativas, técnicas y humanas relacionadas con la seguridad y privacidad de la información en la CRC de acuerdo con su Plan Estratégico Institucional[1], así:

Actividad Proyecto de Inversión	Pilar	Objetivo	Descripción	Valor
A1. Desarrollar proyectos de Infraestructura Tecnológica requerida para la gestión institucional	P4. Fortalecimiento Estratégico Institucional	O12. Impulsar y fortalecer la transformación digital de la entidad mediante iniciativas tecnológicas y el cumplimiento de los lineamientos de la política de gobierno digital para mejorar la eficiencia y efectividad de sus procesos.	Servicios de Firewall, WAF, Access Point, Switches, Fortianalyzer y SOAR que permitan garantizar la seguridad informática de la CRC, así como las mejoras en los accesos de conectividad. (Incluye Monitoreo IPV6)	$338.057.000

[1] https://crcom.gov.co/sites/default/files/Transparencia/planes_institucionales/Plan-Estrategico-Institucional-2025-2029-VF.pdf

Actividad Proyecto de Inversión	Pilar	Objetivo	Descripción	Valor
A1. Desarrollar proyectos de Infraestructura Tecnológica requerida para la gestión institucional	P4. Fortalecimiento Estratégico Institucional	O12. Impulsar y fortalecer la transformación digital de la entidad mediante iniciativas tecnológicas y el cumplimiento de los lineamientos de la política de gobierno digital para mejorar la eficiencia y efectividad de sus procesos.	Renovar el licenciamiento del servicio de Backup que permiten garantizar las copias de respaldo de los servidores que alojan los servicios tecnológicos de la CRC.	$261.354.000
A3. Contar con la asesoría y herramientas tecnológicas necesarias para toma de decisiones basadas en datos	P4. Fortalecimiento Estratégico Institucional	O11. Optimizar la gestión de la Entidad mediante la apropiación y mejora de los instrumentos de gestión que permitan el fortalecimiento de los procesos para contribuir a un mejor desempeño organizacional.	Suscripción, soporte, actualización y mantenimiento de una herramienta consolidada integral para el seguimiento del Sistema Integrado de Gestión, en modalidad SAAS para la Comisión de Regulación de Comunicaciones – CRC por un año.	$185.715.170
A4. Diseñar e implementar procesos que soporten el fortalecimiento del Gobierno Digital	P4. Fortalecimiento Estratégico Institucional	O12. Impulsar y fortalecer la transformación digital de la entidad mediante iniciativas tecnológicas y el cumplimiento de los lineamientos de la política de gobierno digital para mejorar la eficiencia y efectividad de sus procesos.	Apoyo Gestión Seguridad y Privacidad de la Información y continuidad del negocio	$172.500.000
A4. Diseñar e implementar procesos que soporten el fortalecimiento	P4. Fortalecimiento Estratégico Institucional	O11. Optimizar la gestión de la Entidad mediante la apropiación y mejora de los instrumentos de gestión que permitan el fortalecimiento de los	Adquisición/Renovación Certificados firmas digitales Suministrar catorce (14) certificados de firma digital para el sistema SIIF Nación.	$16.995.000

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Actividad Proyecto de Inversión	Pilar	Objetivo	Descripción	Valor
del Gobierno Digital		procesos para contribuir a un mejor desempeño organizacional.		
A4. Diseñar e implementar procesos que soporten el fortalecimiento del Gobierno Digital	P4. Fortalecimiento Estratégico Institucional	O12. Impulsar y fortalecer la transformación digital de la entidad mediante iniciativas tecnológicas y el cumplimiento de los lineamientos de la política de gobierno digital para mejorar la eficiencia y efectividad de sus procesos.	Adquisición de servicios de Centro de Seguridad de Operaciones SOC.	$840.511.063
A4. Diseñar e implementar procesos que soporten el fortalecimiento del Gobierno Digital	P4. Fortalecimiento Estratégico Institucional	O12. Impulsar y fortalecer la transformación digital de la entidad mediante iniciativas tecnológicas y el cumplimiento de los lineamientos de la política de gobierno digital para mejorar la eficiencia y efectividad de sus procesos.	Contratación de los servicios de Ethical Hacking	$40.500.000
			Total asignado 2026	$1.855.632.233

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

HOJA DE RUTA

Se presenta la hoja de ruta elaborada a partir de brechas agrupadas en paquetes de trabajo que generan la misma capacidad a la Entidad.

ANÁLISIS Y PRIORIZACIÓN DE INICIATIVAS

Se identifican las iniciativas de seguridad y privacidad de la información, las cuales están alineadas con el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI), conforme al resultado del diagnóstico realizado con respecto al cumplimiento y nivel de madurez del modelo de seguridad y privacidad de la información, resultados de auditoría interna e iniciativas propias de la CRC.

Las iniciativas están enmarcadas dentro de los controles sugeridos para buscar una adecuada arquitectura de seguridad y privacidad de la información, utilizando soluciones de tecnología y las nuevas tendencias de seguridad de la información, así:

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1. Activos de información					
1.1.	Implementar la herramienta para la identificación y valoración de los activos de información	Febrero	Mayo	PyG	Herramienta configurada.
1.2.	Diligenciar los activos de información en la herramienta	Mayo	Julio	Todos los procesos	Matrices de activos de información por proceso.
1.3.	Publicar los Instrumentos de gestión de la información pública	Agosto	Septiembre	PyG	Registro de Activos de Información. Índice de Información Clasificada y Reservada.
2. Riesgos de Seguridad y Privacidad de la Información					
2.1.	Actualizar la Política de Administración de Riesgos de la Entidad.	Febrero	Marzo	PyG - CICCI	Política de Administración de Riesgos actualizada.
2.2.	Implementar la herramienta para la gestión de los riesgos del SGSPI.	Febrero	Mayo	PyG	Herramienta configurada.

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
2.3.	Diligenciar los Riesgos del SGSPI en la herramienta.	Mayo	Julio	Todos los procesos	Matrices de riesgos aprobadas.
2.4.	Actualizar el tratamiento de Riesgos de Seguridad de la Información.	Febrero	Abril	Todos los procesos	Plan de tratamiento de Riesgos de Seguridad de la Información.
2.5.	Hacer seguimiento a los controles y a los planes de tratamiento.	Febrero	Diciembre	PyG	Informe de seguimiento de los planes de tratamiento.
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
3.1.	Actualizar el Plan de Uso y Apropiación.	Febrero	Marzo	TSI - PyG	Documento plan de concienciación en seguridad y privacidad.
3.2.	Ejecutar el Plan de concienciación en seguridad y privacidad.	Febrero	Diciembre	PyG	Informe de ejecución del plan.
3.3.	Analizar los resultados del Plan de concienciación en seguridad y privacidad.	Noviembre	Diciembre	PyG	Informe de resultados Plan de concienciación en seguridad y privacidad.
4. Protección de Datos Personales					
4.1.	Actualizar el Registro Nacional de Base de Datos - RNBD Personales antes la SIC.	Marzo	Mayo	Oficial de protección de datos personales	Registro actualizado por parte de la SIC.
4.2.	Actualizar la política de tratamiento de información de datos personales.	Febrero	Abril	Oficial de protección de datos personales	Política actualizada y formalizada.
4.3.	Divulgar la política de tratamiento de datos personales.	Abril	Mayo	Oficial de protección de datos personales	Piezas de divulgación.
4.4.	Sensibilizar a todos los procesos sobre los nuevos	Mayo	Noviembre	Oficial de protección de datos personales	Registros de asistencia, actas, grabaciones, entre otros.

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
	lineamientos de Privacidad de la Información.				
4.5.	*Revisión de la documentación asociada al tratamiento de datos personales*	*Abril*	*Diciembre*	*Oficial de protección de datos personales*	*Propuestas de documentos actualizados.*
5. Sistema de Gestión de Seguridad de la Información					
5.1.	*Revisar y actualizar la Política y el Manual de Políticas Específicas de Seguridad y Privacidad de la Información.*	*Febrero*	*Abril*	*PyG*	*Política y Manual de Políticas Específicas de Seguridad y Privacidad de la Información actualizados y formalizados.*
5.2.	*Realizar seguimiento a la implementación de los controles del MSPI.*	*Junio*	*Diciembre*	*PyG*	*Herramienta de medición y autodiagnóstico del MSPI semestral.*
5.3.	*Hacer seguimiento a los planes de mejoramiento producto de la auditoría interna.*	*Enero*	*Diciembre*	*PyG*	*Reporte de planes de mejoramiento.*
5.4.	*Presentar la Revisión por la Dirección.*	*Enero*	*Marzo*	*PyG*	*Documento de Revisión por la Dirección.*
5.5.	*Preparación y acompañamiento en la auditoría interna al SGSPI.*	*Marzo*	*Agosto*	*PyG - TSI*	*Informe de auditoría interna al SGSPI.*
5.6.	*Reportar el cumplimiento de los indicadores de seguridad de la Información.*	*Enero*	*Diciembre*	*PyG*	*Resultado de indicadores de Seguridad y Privacidad de la Información.*
5.7.	*Fortalecer el uso de la seguridad y privacidad de la Inteligencia Artificial en la CRC*	*Abril*	*Noviembre*	*PyG - TSI*	*Charlas, sensibilizaciones, piezas gráficas.*

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
6. Seguridad informática / Ciberseguridad					
6.1.	Hacer seguimiento a la ejecución del SOC-NOC.	Enero	Diciembre	CISO - TSI	Informe mensual de seguimiento.
6.2.	Gestionar la contratación del contrato de ciberseguridad.	Febrero	Diciembre	CISO - TSI	Contrato adjudicado.
6.3.	Gestionar las pruebas de vulnerabilidades – Ethical Hacking.	Junio	Diciembre	CISO - TSI	Informe de resultados de las pruebas realizadas.
6.4.	Realizar seguimiento al cierre de brechas de las vulnerabilidades encontradas.	Enero	Diciembre	TSI	Seguimiento al cierre de brechas.