COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLAN TRATAMIENTO DE RIESGOS 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

La seguridad y privacidad de la información en las entidades busca afrontar los retos que impone el negocio, la incursión de nuevas infraestructuras digitales modernas, robustas y seguras.

Teniendo en cuenta el acelerado avance de las tecnologías de información y comunicaciones, genera preocupación e incertidumbre el manejo de los riesgos de la información que estén asociados con las debilidades en la seguridad de las tecnologías de la información, vulnerabilidades que puedan afectar a los activos de información, los cuales pueden ocasionarse por el manejo de una ciberseguridad inadecuada afectando la triada de la seguridad de la información como lo son: la disponibilidad, la confidencialidad y la integridad.

Con el fin de garantizar la seguridad de la información en las entidades públicas y privadas, se deben desarrollar capacidades que les permita estar un paso adelante de las amenazas y vulnerabilidades latentes que a diario atentan en contra de los activos de información, infraestructuras críticas y los usuarios, estos como agentes del ciberespacio.

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 y apoyan la implementación del modelo de seguridad y privacidad de la información (MSPI).

La Comisión de Regulación de Comunicaciones, para asegurar la dirección estratégica de la Entidad, establece la política de seguridad de la información con los siguientes objetivos de seguridad de la información:

- ✓ Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en la CRC.
- ✓ Identificar, clasificar y mantener actualizado el inventario de los activos de información de la CRC de acuerdo con los requisitos legales y regulatorios.
- ✓ 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.
- ✓ 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.
- ✓ Implementar las estrategias de continuidad para los servicios tecnológicos que soporten los requerimientos de continuidad del negocio.

De acuerdo con el estado actual en la Comisión de Regulación de Comunicaciones, existe la necesidad de diseñar un Plan Estratégico de Seguridad y Privacidad de la Información que fortalezca las políticas de seguridad de la información y su gestión antes de posibles fallas en los procesos y la responsabilidad

en el manejo de los procedimientos al interior de la entidad, minimizando las potenciales amenazas que pueden ser introducidas accidental o deliberadamente.

Teniendo en cuenta lo anterior, las coordinaciones de Tecnologías y Sistemas de Información y Planeación y Gestión de la Comisión de Regulación de Comunicaciones plantean presentar 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 de la ISO 270001, el Modelo de Seguridad y Privacidad de la Información por MinTIC y 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.

La importancia del apoyo de la alta dirección para la implementación del componente de Seguridad y Privacidad de la Información y la gestión de los riesgos de Seguridad de la información en la Entidad con respecto a lo indicado, toma relevancia al formular un Plan Estratégico de Seguridad y Privacidad de la Información para que de forma estructurada se establezcan las iniciativas y proyectos que garanticen el cumplimiento del objetivo de seguridad de la información que es proteger, asegurar y minimizar el daño en el que pueda incurrir la entidad y que afecte sus activos de información.

Por lo anterior, y teniendo en cuenta el mapa de ruta establecido en el Plan Estratégico de Seguridad y Privacidad de la Información 2026, se define de manera particular el Plan de Tratamiento de Riesgos de Seguridad de la Información para esta misma vigencia.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

OBJETIVO

Formular el Plan de Tratamiento de Riegos de Seguridad y Privacidad de la Información de la Comisión de Regulación de Comunicaciones (CRC) que se enmarca en los siguientes objetivos:

- Realizar un diagnóstico de la situación actual de la seguridad y privacidad de la información en la Entidad.
- Actualizar y realizar seguimiento del levantamiento de activos de información y gestión de riesgos.
- Aprobar el plan de tratamiento de Riegos de Seguridad y Privacidad de la Información.

ALCANCE DEL DOCUMENTO

En el presente documento se indica la metodología para implementar las medidas de seguridad definidas en el Plan de Tratamiento de Riesgos para los Activos de Información que apoyan los procesos internos de la Comisión de Regulación de Comunicaciones, estableciendo las actividades a realizar, la duración estimada y las prioridades para gestionar los riesgos. Se plantea un control operacional que pueda ser aplicado a los procesos de la CRC que ingresan al Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Adicionalmente, como resultado de los ejercicios incorpora el plan de acción a través de la definición de la hoja de ruta de ejecución para el año 2026.

RESPONSABLE DE LA ESTRATEGIA OPERACIONAL

Es responsabilidad del Comité Institucional de Gestión y Desempeño liderar y hacer seguimiento a cada uno de los componentes de éste, que operen y generen las salidas requeridas para garantizar la operación del SGSPI.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DERIESGOS Y CONTROLES

De acuerdo con la Política de Administración de Riesgos 2025 de la CRC, la cual Establece el marco general y la metodología para la administración de los riesgos en la Comisión de Regulación de Comunicaciones – CRC mediante la ejecución de un proceso ordenado y continuo, que contribuya al mejoramiento constante de las actividades y al cumplimiento de los objetivos de la Entidad. Asimismo, planteó los siguientes objetivos institucionales:

- ✓ Formalizar al interior de la CRC una metodología para administrar los riesgos de toda naturaleza a los que se enfrenta la entidad: gestión, corrupción, seguridad digital y fiscales.
- ✓ Establecer pautas para la identificación de los factores que representan amenazas u oportunidades para el cumplimiento de los objetivos.
- ✓ Definir los roles y responsabilidades en marco de la administración de riesgos y el Sistema de Control Interno, bajo el esquema de las líneas de Defensa en la CRC.
- ✓ Establecer desde el direccionamiento estratégico el análisis del entorno externo e interno de la entidad, que sirve de base para la identificación de los posibles riesgos, así como los factores de riesgo.
- ✓ Fijar las escalas de valoración para la probabilidad de ocurrencia y el impacto de cada factor de riesgo identificado, a partir de las metodologías establecidas por el Departamento Administrativo de la Función Pública.
- ✓ Establecer los lineamientos para el diseño de los controles.
- ✓ Establecer los seguimientos y la periodicidad que deben realizar las líneas de defensa, así como los seguimientos a los mapas de riesgos por parte de la segunda línea de defensa (Coordinación de Planeación Estratégica).
- ✓ Establecer los lineamientos para la gestión de incidentes (materialización de los riesgos) su manejo, análisis conducentes a la toma de decisiones.
- ✓ Estipular las reglas para la identificación de las actividades de control que minimicen la ocurrencia e impacto de los factores de riesgo.
- ✓ Caracterizar el instrumento para la administración del riesgo de acuerdo con los requisitos establecidos en la Guía vigente para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.
- ✓ Cumplir con los principios del Modelo Integrado de Planeación y Gestión – MIPG, Modelo Estándar de Control Interno y el Sistema Integrado de Gestión de la CRC.
- ✓ Establecer un mecanismo y periodicidad para la difusión y apropiación de la política de riesgos por parte de todo el equipo de la CRC.
- ✓ Establecer responsabilidades en el marco del Sistema de Control Interno Institucional.
- ✓ Definir el ciclo metodológico de la administración de riesgos institucional.

Para la actualización de los activos de información de los procesos de la CRC se utilizó la herramienta institucional para el registro y aprobación. El ejercicio se desarrolló basado en las Tablas de Retención Documental – TRD vigentes, activos de información previos, procesos y procedimientos, lineamientos

de operación de cada coordinación y el conocimiento de los responsables de cada proceso cumpliendo como alcance, así:

- Conocimiento de gestión del proceso.
- Identificación de activos de información con base en los principios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad.
- Identificación de riesgos configurados para los procesos con base en los activos vigentes.
- Definición de controles aplicables a la mitigación y gestión de riesgos identificados.

Activos de información.

Los activos de información se identificaron y caracterizaron con base en los parámetros solicitados por la Ley de Transparencia y Acceso a la Información Pública y sus decretos reglamentarios (Nombre, descripción, proceso al que pertenece, propietario, responsable, custodio, usuarios, tipo de activo de información, medio de conservación, ubicación y características de su contenido que permiten un entendimiento y calificación del mismo) y se calificaron de acuerdo con las propiedades de la información (Confidencialidad, Integridad, Disponibilidad) respecto de su seguridad.

Dentro del levantamiento de los activos de información es importante resaltar que, respecto de la Confidencialidad, toda la información inherente a estos activos en los procesos evaluados es pública, pública clasificada o pública reservada (De acuerdo con los Art. 18 y 19 de la Ley 1712 de 2014 respectivamente).

Riesgos de Seguridad de la Información.

Los riesgos de seguridad de la información siguen el ciclo metodológico para la administración de los riesgos de la CRC como se muestra a continuación:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Figura 1. Metodología de administración de riesgos CRC

Fuente: Elaboración propia CRC

Para identificar los riesgos de seguridad digital se debe iniciar con la identificación de los activos de información, y la redacción se debe dar por la combinación de:
Pérdida de confidencialidad, integridad y/o disponibilidad + Activo(s) de información afectado(s) + Vulnerabilidad(es) + Amenaza(s).

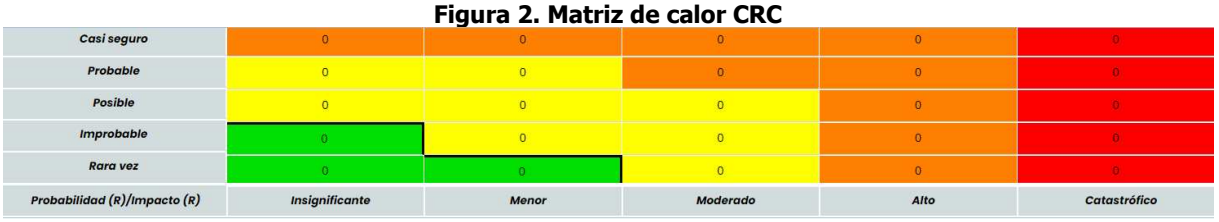
Se califica el riesgo con base en su probabilidad de ocurrencia y el impacto de éste, teniendo en cuenta los parámetros de medición establecidos en la metodología para la administración del riesgo de la CRC.

Para el 2025, la CRC actualizó la metodología de riesgos adaptando la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7, asimismo, para el SGSPI se tuvo en cuenta el numeral 3 *Gestión De riesgos De Seguridad De La Información Para Entidades Públicas* de los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del Modelo de Seguridad y Privacidad de la Información del MinTIC.

Finalmente, se presenta la matriz de calor que se tiene en la CRC para definir la evaluación de los riesgos de seguridad y privacidad de la información; los riesgos en las zonas moderada, alta y extrema deben contar con planes de tratamiento.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Figura 2. Matriz de calor CRC



Fuente: Elaboración propia CRC

HOJA DE RUTA.

ACTIVIDAD	DESCRIPCIÓN	RECURSOS	TRIMESTRE 2026			
			1	2	3	4
1.	Actualizar la Política de Administración de Riesgos de la entidad.	PyG	x	x		
2.	Implementar la herramienta para la identificación y valoración de los activos de información.	PyG	x	x		
3.	Diligenciar los activos de información en la herramienta.	Líderes de procesos Enlaces de los procesos Herramienta de Gestión		x	x	
4.	Publicación de activos de Información.	Líderes de procesos Enlaces de los procesos Herramienta de Gestión	x			
5.	Implementar la herramienta para la gestión de los riesgos del SGSPI.	PyG	x	x		
6.	Diligenciar los riesgos del SGSPI en la herramienta de Gestión.	Líderes de procesos Enlaces de los procesos CISO Herramienta de Gestión		x	x	
7.	Actualizar el tratamiento de riesgos de Seguridad de la Información.	Líderes de procesos Enlaces de los procesos CISO Herramienta de Gestión	x	x		
8.	Hacer seguimiento a los controles y a los planes de tratamiento.	CISO		x	x	x
9.	Informe de ejecución de la gestión de riesgos de Seguridad y Privacidad de la Información.	CISO				x