COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLAN TRATAMIENTO DE RIEGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección Ejecutiva
Líder: Ingrid Picón Carrascal
Coordinadora de Tecnologías y Sistemas de Información

Enero de 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

INTRODUCCIÓN **3**
OBJETIVO **6**
ALCANCE DEL DOCUMENTO **6**
RESPONSABLE DE LA ESTRATEGIA OPERACIONAL **6**
INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DE RIESGOS Y CONTROLES **7**
INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DE RIESGOS Y CONTROLES **8**
Activos de información. 9
Riesgos de Seguridad de la Información. 9
HOJA DE RUTA. **14**

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 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, confidencialidad e 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.

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 de 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 perdida 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

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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 2025, 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 la Información SGSI.

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 2025.

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 SGSI.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DE RIESGOS Y CONTROLES

De acuerdo con la Política de Administración de Riesgos 2023 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.

INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DE RIESGOS Y CONTROLES

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, Activos de información previos, procesos y procedimientos, lineamientos de operación de cada dependencia y el conocimiento de los responsables de cada proceso cumpliendo como alcance:

- 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 actuales.
- Definición de controles aplicables a la mitigación y gestión de riesgos identificados

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

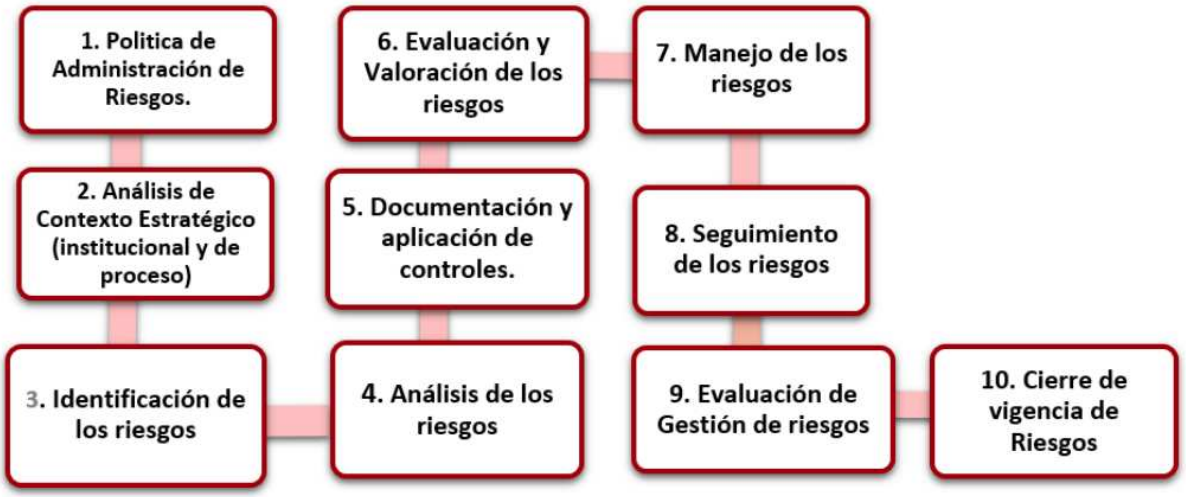
Activos de información

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 el 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:



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 el instrumento diseñado por la CRC.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 1. Clasificación de probabilidad de riesgos de seguridad de la información.

Nivel	Descriptor	Histórico	Prospectiva
1	Rara vez	En los últimos cinco (5) años no se ha materializado el riesgo	Se espera que el evento de riesgo se materialice en los próximos cinco (5) años.
2	Improbable	En los últimos cinco (5) años se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice más de una vez en los próximos cinco (5) años.
3	Posible	En los últimos dos (2) años se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice al menos una vez en los próximos dos (2) años.
4	Probable	En el último año se ha materializado el riesgo al menos una vez	Se espera que el evento de riesgo se materialice una vez en el próximo año
5	Casi seguro	En el último año se ha materializado el riesgo más de una vez	Se espera que el evento de riesgo se materialice más de una vez en el próximo año

Fuente: Elaboración Propia CRC.

La combinación de esta calificación de probabilidad e impacto define el nivel de riesgo.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 2. Clasificación de impacto de riesgos de seguridad de la información.

Nivel	Descriptor	Consecuencias Cuantitativas	Consecuencias Cualitativas
1	**Insignificante**	• No hay pérdidas económicas. • Afectación Imagen a nivel de grupo o equipo. • Llamados de atención a nivel grupo o equipo. • No hay daño medioambiental. • Indisponibilidad de los servicios menor a una hora. • Afectación a datos personales públicos.	• No hay interrupción de las operaciones de la entidad. • No se generan observaciones por entes de regulación o control. • Pérdida de información clasificada como baja. • No se Incumplen las metas y objetivos institucionales. • No se afecta la imagen institucional de forma significativa.
2	**Menor**	• Pérdidas económicas hasta de 10 SMMLV. • Afectación Imagen nivel de área • Sanciones o llamados de atención a nivel área. • Daño ambiental menor a un día recuperación. • Indisponibilidad de los servicios menor a un día. • Afectación a datos personales semiprivados.	• Interrupción de las operaciones de la entidad hasta por 24 horas. • Se generan observaciones administrativas por entes de regulación o control. • Pérdida de información clasificada como media. • Atrasos de actividades del plan de acción Institucional. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
3	**Moderado**	• Pérdidas económicas entre 10.1 y 100 SMMLV. • Afectación Imagen del proceso • Sanciones o llamados de atención a nivel de proceso. • Daño ambiental menor a una semana de recuperación. • Indisponibilidad de los servicios menor a una semana. • Afectación a datos personales privados o sensibles.	• Interrupción de las operaciones de la entidad entre 24 y 48 horas. • Se generan observaciones administrativas con incidencia disciplinaria por entes de regulación o control. • Pérdida de información clasificada como alta. • Incumplimiento o atrasos en un proyecto estratégico de la CRC. • Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4	**Mayor**	• Pérdidas económicas entre 100.1 y 200 SMMLV. • Afectación Imagen a Nivel Nacional. • Sanciones o llamados de atención a toda la entidad. • Daño ambiental menor a un mes de recuperación. • Indisponibilidad de los servicios menor a un mes. • Afectación a datos personales vulnerables o sensibles.	• Interrupción de las operaciones de la entidad por más de dos (2) días. • Se generan observaciones administrativas con incidencia fiscal o penal por entes de regulación o control. • Pérdida parcial y recuperable de la información clasificada como crítica de la entidad. • Incumplimiento o atraso en los objetivos estratégicos de la CRC. • Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos. También por envío de información errónea y exposición de un vocero no autorizado.
5	**Catastrófico**	• Pérdidas económicas mayores a 300 SMMLV. • Afectación Imagen a Nivel internacional. • Sanciones de Contraloría, Procuraduría y/o Fiscalía. • Daño ambiental mayor a un mes de recuperación. • Indisponibilidad de los servicios mayor a un mes. • Afectación a datos personales vulnerables.	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Se genera intervención por parte de un ente de regulación o control. • Pérdida total de la información clasificada como crítica de la entidad. • Incumplimiento en la misión de la CRC. • Imagen institucional afectada en el orden nacional o regional por actos, hechos de corrupción comprobados o equivocación en el cargue de resultados.

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.

Casi seguro	0	0	0	0	0
Probable	0	0	0	0	0
Posible	0	0	0	0	0
Improbable	0	0	0	0	0
Rara vez	0	0	0	0	0
Probabilidad (R)/Impacto (R)	*Insignificante*	*Menor*	*Moderado*	*Alto*	*Catastrófico*

Fuente: Elaboración propia CRC

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

HOJA DE RUTA

ACTIVIDAD	DESCRIPCIÓN	RECURSOS	TRIMESTRE 2025			
			1	2	3	4
1.	Actualizar en la Política de Administración de Riesgos de la entidad	PyG	X	X		
2.	Publicación de activos de Información	Líderes de procesos Enlaces de los procesos Herramienta de gestión	X			
3.	Identificación, actualización y evaluación de Riesgos de Seguridad de Información	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión	X			
4.	Definición, actualización y/o evaluación de controles	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión	X	X		
5.	Revisión y aprobación de los riesgos de seguridad de la información	Líderes de procesos		X		
6.	Implementación y seguimiento del Plan de Tratamiento de Riesgos	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión		X	X	X
7.	Informe de ejecución de la gestión de riesgos de seguridad de la información	CISO				X