COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección Ejecutiva
Coordinadora Ejecutiva
Líder: Zoila Vargas Mesa.

Diciembre de 2024

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

Historia de Actualizaciones

Fecha	Descripción	Responsable
Diciembre de 2024	Inclusión de la Privacidad en el SGSI de acuerdo con la propuesta en la Revisión por la Dirección.	CISO
Enero de 2022	Actualización Política de Seguridad y Privacidad de la Información vigencia 2022	CISO
Diciembre de 2016	Creación Política de Seguridad y Privacidad de la Información	CISO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. OBJETIVO

Establecer y formalizar la política de seguridad y privacidad de la información tendiente a garantizar la integridad, confidencialidad, disponibilidad y privacidad de los activos de información con el fin de actualizar y mejorar continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI de la Comisión de Regulación de Comunicaciones.

2. ALCANCE

El Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI y la presente Política de seguridad y privacidad de la información aplican a todos los procesos de la Comisión de Regulación de Comunicaciones – CRC, y es de obligatorio complimiento para las personas naturales y jurídicas que tengan vínculos laborales o contractuales con esta.

3. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Comisión de Regulación de Comunicaciones - CRC, en cumplimiento de los requisitos legales y regulatorios, se compromete a mantener la integridad, confidencialidad, disponibilidad y privacidad los datos personales y de los activos de información, fortaleciendo y mejorando continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, el cual fomenta la cultura de seguridad de los colaboradores, realiza la gestión integral de riesgos e incidentes cibernéticos, de seguridad digital, privacidad y de la información reduciendo así el impacto negativo en la continuidad de la prestación de los servicios que soportan los procesos en la comisión, buscando apoyar la regulación los mercados de comunicaciones bajo criterios de mejora normativa para proteger los derechos de la ciudadanía, promover la competencia, la inversión, la calidad de los servicios y el pluralismo informativo.

4. OBJETIVOS

I. Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en la CRC

II. Identificar, clasificar y mantener actualizado el inventario de los activos de información de la CRC de acuerdo con los requisitos legales y regulatorios.

III. 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.

IV. Gestionar los eventos e incidentes de privacidad y seguridad de la información que afecten o puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información reduciendo su impacto y propagación.

V. Implementar las estrategias de continuidad para los servicios tecnológicos que soporten los requerimientos de continuidad del negocio.

5. GOBIERNO DE SEGURIDAD.

5.1. El Comité Institucional de Gestión y Desempeño

De acuerdo con la Resolución No. 067 de 2021 "Por medio de la cual se derogan las Resoluciones CRC 429 de 2017, 004 de 2020, se subroga la Resolución CRC 262 de 2020 y, se dictan otras disposiciones", establece en su **ARTÍCULO SEGUNDO**, entre otras, las siguientes funciones del comité:

(…)

7. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información

11. Dar directrices al Interior de la Entidad para la implementación de la estrategia de Gobierno Digital, de acuerdo con los lineamientos y metas propuestas para las entidades de orden nacional.

12. Asignar roles y responsabilidades específicos que se relacionen con el desarrollo de la estrategia de Gobierno Digital.

13. Participar activamente en la formulación y evaluación de planes de acción para el desarrollo de la estrategia de Gobierno Digital.

(…)

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5.2. Oficial de seguridad de la información

Es el rol que debe desarrollar todas las actividades de coordinación de la seguridad y privacidad de la información, seguridad digital y ciberseguridad de forma estratégica, táctica y operativa en la CRC como segunda línea de defensa de acuerdo con el MIPG, asimismo es el encargado de:

- Presentar y hacer seguimiento a las actividades propuestas en el Plan Estratégico de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Brindar apoyo en liderar el proyecto de implementación del modelo de seguridad de la información en la Entidad, de acuerdo con los lineamientos de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Definir y gestionar de manera estratégica y táctica las políticas, lineamientos, estándares, guías y demás relacionadas con seguridad de la información que se definan en la entidad de acuerdo con el Plan Estratégico de Seguridad y Privacidad de la Información de la CRC.
- Apoyar en la formulación y liderazgo de los proyectos y planes de acción de seguridad digital y de la información según las necesidades de la Entidad.

5.3. Oficial de Protección de Datos Personales

Es el rol que debe desarrollar todas las actividades relacionadas con la privacidad de la información y el manejo de datos personales, asimismo es el encargado entre otras de:

- Establecer e implementar los controles para la protección de datos personales.
- Ser Enlace y coordinación con las demás áreas de la CRC.
- Promover una cultura de protección de datos personales.
- Registrar las bases de datos ante la Superintendencia de Industria y Comercio a través del Registro Nacional de Bases de Datos.
- Revisar y adaptar los protocolos de respuesta en el manejo de eventos e incidentes que involucren datos personales e implementar mejoras.

5.4. Líder de proceso

Liderar los temas como primera línea de defensa para la implementación de las políticas que integran en MIPG especialmente las de *Gobierno Digital* y *Seguridad Digital* para los temas de Seguridad y privacidad de la información.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

5.5. CIO

Es el líder de la gestión estratégica de Tecnologías de Información y de la transformación digital de la CRC, encargado de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI.

5.6. Colaboradores

Los colaboradores de la CRC son responsables de conocer, apropiar, divulgar y cumplir con las políticas, procedimientos y lineamientos que apliquen a su trabajo, rol o función respecto a Seguridad y Privacidad de la Información.

5.7. Control interno

Tiene la función de auditoría interna, a través de un enfoque basado en el riesgo, proporcionado aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.

6. REVISIÓN.

La presente política debe ser revisada anualmente, con el fin de evaluar su pertinencia y aplicabilidad de acuerdo con los cambios significativos y de gran impacto en el contexto externo o interno que afecten al SGSPI.