COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLAN ESTRATÉGICO 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

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 estratégico 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.

El presente plan estratégico 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.

El plan 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 presenta 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 del Plan Estratégico de Seguridad y Privacidad de la Información de la Comisión de Regulación de Comunicaciones (CRC) para la vigencia 2025, 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 el año 2025, 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 el 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 de MinTIC, resultados del FURAG y los controles de la NTC-ISO 27001. Este análisis permite conocer el estado actual o línea base a partir de 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

No.	DOMINIO	Calificación Actual	Evaluación de efectividad de control
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	72	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	93	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	57	**EFECTIVO**
A.9	CONTROL DE ACCESO	67	**GESTIONADO**
A.10	CRIPTOGRAFÍA	60	**EFECTIVO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	76	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	61	**GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	64	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	60	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	49	**EFECTIVO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67	**GESTIONADO**
A.18	CUMPLIMIENTO	76	**GESTIONADO**
Promedio evaluación de controles		**69**	**GESTIONADO**

Resultado Autodiagnóstico de controles MSPI

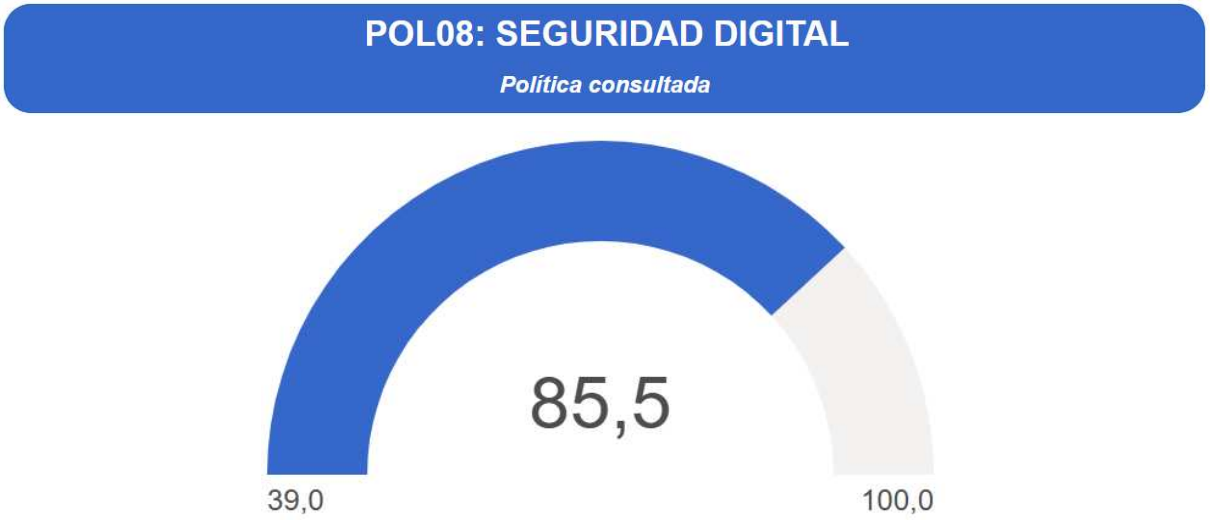
Para la medición, este instrumento se divide en componentes, los cuales involucran Planificación, Implementación, Evaluación de Desempeño y Mejora Continua, cada uno con una respectiva medición y porcentaje esperado de implementación, lo que permite identificar las brechas que tienen:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	33%	40%
	Implementación	14%	20%
	Evaluación de desempeño	15%	20%
	Mejora continua	18%	20%
TOTAL		80%	100%

Resultado Autodiagnóstico de componentes MSPI

Con respecto a la medición del FURAG 2023, se obtuvo un porcentaje de cumplimiento del 85,5, lo que evidencia una relación en las valoraciones realizadas con la herramienta del Autodiagnóstico de 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.



Resultado FURAG Política de Seguridad Digital

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

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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.

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 información, 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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1. Activos de información					
1.1.	Publicar los Instrumentos de gestión de la información pública	Enero	Febrero	TSI	Registro de Activos de Información. Índice de Información Clasificada y Reservada
1.2.	Implementar de las estrategias definidas para el etiquetado de los activos de tipo información en medio físico y electrónico	Abril	Diciembre	Todos los procesos	Informe de actividades realizadas
2. Riesgos de Seguridad y Privacidad de la Información					
2.1.	Actualizar en la Política de Administración de Riesgos de la entidad	Febrero	Junio	PyG	Política de Administración de Riesgos actualizada.
2.2.	Identificar y/o actualizar los Riesgos Seguridad de la información	Enero	Marzo	Todos los procesos	Matrices de riesgos aprobadas
2.3.	Actualizar el Tratamiento de Riesgos Seguridad de la Información	Enero	Marzo	Todos los procesos	Plan de Tratamiento de Riesgos de Seguridad de la Información
2.4.	Hacer seguimiento a la implementación de los planes de tratamiento	Febrero	Diciembre	PyG	Informe de seguimiento de los planes de tratamiento
2.5.	Actualizar la Declaración de Aplicabilidad	Febrero	Junio	PyG	Declaración de aplicabilidad
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
3.1.	Actualizar el Plan de Uso y Apropiación.	Enero	Febrero	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.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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.	*Definir el responsable con el rol de Oficial de Datos Personales*	*Enero*	*Marzo*	*Dirección Ejecutiva*	*Comunicación de designación.*
4.2.	*Actualizar el Registro Nacional de Base de Datos Personales antes la SIC.*	*Marzo*	*Mayo*	*Oficial de protección de datos personales*	*Registro actualizado por parte de la SIC.*
4.3.	*Realizar un plan cierre de brechas identificadas en el 2024*	*Abril*	*Abril*	*Oficial de protección de datos personales*	*Plan de cierre de brechas*
4.4.	*Realizar un informe de la ejecución del plan.*	*Diciembre*	*Diciembre*	*Oficial de protección de datos personales*	*Informe de la ejecución del plan.*
5. Sistema de Gestión de Seguridad de la Información					
5.1.	*Revisar la Política y el Manual de Políticas de Seguridad y Privacidad de la Información y actualizar en caso de ser necesario.*	*Febrero*	*Agosto*	*PyG*	*Manual y/o Política de Seguridad de la Información revisados.*
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*	*Acta de Revisión por la Dirección*
5.5.	*Reportar de cumplimiento de los indicadores de seguridad de la Información*	*Enero*	*Diciembre*	*PyG*	*Indicadores de Seguridad y Privacidad de la información*

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

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 las pruebas de vulnerabilidades – Ethical Hacking*	*Junio*	*Diciembre*	*CISO - TSI*	*Informe de resultados de las pruebas realizadas*
6.3.	*Realizar seguimiento al cierre de brechas de las vulnerabilidades encontradas.*	*Marzo*	*Diciembre*	*TSI*	*Seguimiento al cierre de brechas*