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 2024

CONTENIDO

Historial de actualizaciones

Fecha	Descripción	Responsable
Enero de 2021	Creación Plan Estratégico Seguridad y Privacidad de la Información	CISO
Enero de 2022	Actualización Plan Estratégico Seguridad y Privacidad de la Información vigencia 2022	CISO
Enero de 2023	Actualización Plan Estratégico Seguridad y Privacidad de la Información vigencia 2023	CISO
Enero de 2024	Actualización Plan Estratégico Seguridad y Privacidad de la Información vigencia 2024	CISO

1. 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 en la CRC. Este plan busca promover una cultura de seguridad y privacidad en un esfuerzo colaborativo por proteger la información sensible de la Entidad.

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 al interior de la CRC para mitigar riesgos y responder eficazmente a incidentes de seguridad.

Este plan estratégico representa un compromiso con la protección de la información, 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 plan busca no solo fortalecer las medidas técnicas y organizativas para proteger la información de la CRC, sino también fomentar una cultura de privacidad y transparencia en el tratamiento de los datos.

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:

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, la Coordinación de Tecnologías y Sistemas de Información 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 perdida de información y afianzando la cultura de seguridad de la información entre los funcionarios.

2. OBJETIVO

Formular del Plan Estratégico de Seguridad y Privacidad de la Información de la Comisión de Regulación de Comunicaciones (CRC) para la vigencia 2024, 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

3. 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 2024, 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 y el modelo de planeación definiendo la hoja de ruta de implementación.

4. MARCO NORMATIVO

Resolución No. 003484 de 2012 por la cual se crea el Sistema de Información integral del sector TIC-Colombia TIC, en el artículo 2° Entidades públicas de conforman el sistema Colombia TIC y sus responsabilidades. La Comisión de Regulación de comunicaciones hace parte del sistema Colombia TIC. (Comunicaciones, M. de T. de la I. y las (2012). Resolución 003484 MinTIC. Retrieved from https://www.mintic.gov.co/portal/604/articles-3789_documento.pdf).

De acuerdo con lo dispuesto en **el artículo 4 de la Ley de 2009**, es función del estado invertir en el sector de las Tecnologías de la información y las comunicaciones TIC, para promover condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red, así como la seguridad informática y de redes.

Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". El presente capitulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las Comunicaciones para consolidad un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

En el **artículo 2.2.9.1.1.3 Principios**, en este se encuentra Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riegos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades de Estado, y de los servicios que presentan al ciudadano.

Como Habilitadores transversales de la **Política de Gobierno Digital**: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y servicios ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

5. 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 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, los anterior 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.

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	77	GESTIONADO
A.7	Seguridad de los recursos humanos	97	OPTIMIZADO
A.8	Gestión de activos	69	GESTIONADO
A.9	Control de acceso	74	GESTIONADO
A.10	Criptografía	90	OPTIMIZADO
A.11	Seguridad física y del entorno	92	OPTIMIZADO
A.12	Seguridad de las operaciones	71	GESTIONADO
A.13	Seguridad de las comunicaciones	71	GESTIONADO
A.14	Adquisición, desarrollo y mantenimiento de sistemas	72	GESTIONADO
A.15	Relaciones con los proveedores	80	GESTIONADO
A.16	Gestión de incidentes de seguridad de la información	74	GESTIONADO
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	80	GESTIONADO
A.18	Cumplimiento	76	GESTIONADO
Promedio evaluación de controles		**80**	**OPTIMIZADO**

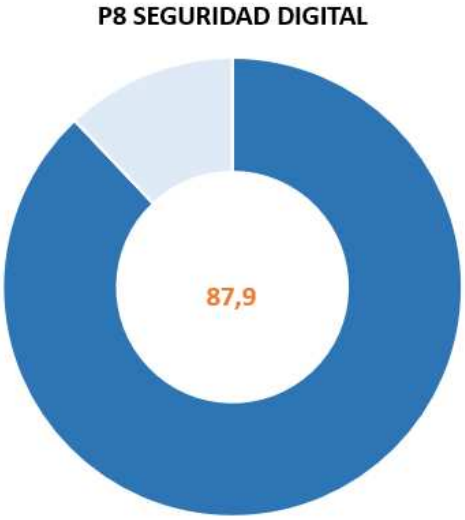
Resultado Autodiagnóstico de controles MSPI

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:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	36%	40%
	Implementación	17%	20%
	Evaluación de desempeño	11%	20%
	Mejora continua	14%	20%
TOTAL		**77%**	**100%**

Resultado Autodiagnóstico de componentes MSPI

Con respecto a la medición del FURAG 2022, se obtuvo un porcentaje de cumplimiento del **87,9** 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.



NO. INDICE	POLITICA SEGURIDAD DIGITAL	PUNTAJE
I21	ASIGANCIÓN DE RECURSOS	59,4
I22	IMPLEMENTACIÓN LINEAMIENTOS DE POLÍTICA	94,7
I23	DESPLIEGUE DE CONTROLES	100,0

Resultado FURAG Seguridad Digital

6. HOJA DE RUTA.

Se presenta la hoja de ruta elaborada a partir de brechas identificadas de acuerdo con la capacidad de la Entidad.

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.

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.

ANEXO 01. HOJA DE RUTA SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

No	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado esperado
1. Activos de información					
1.1.	Actualizar los Instrumentos de gestión de la información pública	Febrero	Junio	Todos los procesos	Matrices de activos
1.2.	Publicar los Instrumentos de gestión de la información pública	Julio	Septiembre	TSI	Registro de Activos de Información. Índice de Información Clasificada y Reservada
1.3.	Establecer los lineamientos y estrategias para el etiquetado de los activos de tipo información en medio físico y electrónico	Febrero	Marzo	SGSI – SGD - SGC	Documentación con los lineamientos institucionales
1.4.	Implementar 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.	Identificar y/o actualizar los Riesgos Seguridad de la información	Junio	Octubre	Todos los procesos	Matrices de riesgos aprobadas
2.2.	Actualizar el Tratamiento de Riesgos Seguridad de la Información	Junio	Octubre	Todos los procesos	Plan de Tratamiento de Riesgos de Seguridad de la Información
2.3.	Hacer seguimiento a la implementación de los planes de tratamiento	Noviembre	Diciembre	CISO	Informe de seguimiento de los planes de tratamiento
2.4.	Actualizar la Declaración de Aplicabilidad	Octubre	Diciembre	CISO	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	CISO - Comunicaciones	Documento Plan de Concienciación en Seguridad y Privacidad
3.2.	Ejecutar el Plan de Concienciación en Seguridad y Privacidad.	Febrero	Diciembre	CISO - Comunicaciones	Informe de ejecución.

3.3.	*Analizar los resultados del Plan de Concienciación en Seguridad y Privacidad.*	*Noviembre*	*Diciembre*	*CISO*	*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 Personales antes la SIC.*	*Marzo*	*Mayo*	*CISO*	*Registro actualizado por parte de la SIC.*
4.2.	*Realizar seguimiento semestral al cumplimiento de la política de Protección de Datos Personales*	*junio*	*Diciembre*	*CISO*	*Informe de Seguimiento y Recomendaciones.*
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*	*Febrero*	*Agosto*	*CISO - CIGyD*	*Manual y/o Política de Seguridad de la Información.*
5.2.	*Realizar seguimiento a la implementación de los controles del MSPI y de la norma ISO 27001 versión 2013 y 2022*	*Junio*	*Diciembre*	*TSI*	*Herramienta de medición y autodiagnóstico del MSPI semestral*
5.3.	*Presentar la Revisión por la Dirección*	*Enero*	*Febrero*	*CISO – Coordinación de planeación estratégica*	*Acta de Revisión por la Dirección*
5.4.	*Gestionar auditoría interna al Sistema de Gestión de Seguridad de la Información basada en la NTC-ISO 27001:2013 y el MSPI.*	*Marzo*	*Junio*	*Comité Institucional de Control Interno*	*Plan Anual de Auditoria*
5.5.	*Reportar de cumplimiento de los indicadores de seguridad de la Información*	*Enero*	*Diciembre*	*CISO - TSI*	*Indicadores de Seguridad y Privacidad de la información*
6. Continuidad del Negocio					
6.1.	*Actualizar el análisis de impacto al negocio – BIA para los servicios críticos de la entidad*	*Abril*	*Junio*	*CISO*	*Documento de análisis de impacto al negocio – BIA*
6.2.	*Actualizar los Escenarios de afectación para los servicios críticos de la entidad*	*Junio*	*Septiembre*	*CISO*	*Riesgos de Continuidad del Negocio*
6.3.	*Actualizar del Plan de Continuidad del Negocio*	*Septiembre*	*Octubre*	*CISO*	*Plan de Continuidad del Negocio*
6.4.	*Realizar la planeación y ejecución de las pruebas*	*Junio*	*Diciembre*	*CISO*	*Informe de resultados de las pruebas realizadas*

	definidas en el Plan de Continuidad del Negocio				
6.5.	*Analizar los resultados de la aplicación de la estrategia de Continuidad del Negocio y gestionar las acciones de mejora identificadas con el fin de fortalecer los planes y documentación*	*Noviembre*	*Diciembre*	*CISO*	*Informe de resultados de las pruebas realizadas*
7. Seguridad informática / Ciberseguridad					
7.1.	*Hacer seguimiento a la ejecución del SOC-NOC*	*Enero*	*Diciembre*	*CISO - Infraestructura*	*Informe mensual de seguimiento*
7.2.	*Gestionar las pruebas de vulnerabilidades – Ethical Hacking*	*Junio*	*Diciembre*	*CISO*	*Informe de resultados de las pruebas realizadas*
7.3.	*Realizar seguimiento al cierre de brechas de las vulnerabilidades encontradas.*	*Junio*	*Diciembre*	*TSI*	*Seguimiento al cierre de brechas*