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 2022

CONTENIDO

Historia de Actualizaciones

Fecha	Descripción	Responsable
Enero -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

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, 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 lo 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:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema integral de gestión en el aparte de seguridad de la información
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Comisión de Regulación de Comunicaciones. (Política General de Seguridad de la Información de la CRC)

De acuerdo con el estado actual en la Comisión de Regulación de comunicaciones, existe la necesidad de actualizar el 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, la Coordinación de Tecnologías y Sistemas de Información de la Comisión de Regulación de Comunicaciones plantea 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 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 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.

La Comisión de Regulación de comunicaciones, en adopción del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo "2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales 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". Por lo anterior, el presente documento se actualiza como plan de acción de cumplimiento 2022, dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de implementación de Seguridad y Privacidad de la Información en la CRC.

1. OBJETIVO

Formular del Plan Estratégico De Seguridad y Privacidad de la información de la Comisión de Regulación de Comunicaciones (CRC) para la vigencia 2022, el cual se enmarca en los siguientes objetivos:

- Realizar un diagnóstico de la situación actual de la seguridad y privacidad de la información en la Entidad.
- Definir los proyectos e iniciativas.
- Clasificar y priorizar los proyectos a realizar.
- Aprobar el plan de Seguridad y privacidad de la información

2. ALCANCE DEL DOCUMENTO

Este documento incorpora la definición estratégica de la Seguridad y Privacidad de la información para la Coordinación de Tecnologías de Información y Comunicaciones, estableciendo el plan de implementación de los proyectos y servicios que se proponen ejecutar en el año 2022, definidos a través del plan de acción de la entidad para los diferentes ámbitos en el Modelo de Seguridad y privacidad de la información.

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

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.

3. 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 1008 de 14 de junio de 2018 por el Ministerio de tecnologías de la información y las comunicaciones, en el **artículo 2.2.9.1.1.1** Objeto. 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.

En los propósitos de la Política de Gobierno Digital que están relacionados con seguridad de la información son los siguientes:

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad
- Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información. (Comunicaciones, M. de T. de la I. y las. (2018). Decreto 1008 14jun 2018 MinTIC, 1–7).

La elaboración del Plan Estratégico de Seguridad y Privacidad de la Información se construirá siguiendo los principales marcos de referencia en materia de seguridad (ISO 27001, 27002, MSPI de Ministerio de tecnologías de información y comunicaciones) y lineamientos establecidos en Gobierno Digital. (ICONTEC. (2013). Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (Sgsi). Requisitos Ntc-Iso/Iec 27001. Icontec, 37)

4. 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. 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.

No.	Evaluación de Efectividad de controles	
	DOMINIO	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	OPTIMIZADO
A.9	CONTROL DE ACCESO	GESTIONADO
A.10	CRIPTOGRAFÍA	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	GESTIONADO
A.18	CUMPLIMIENTO	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**GESTIONADO**

5. CONSOLIDADO DE BRECHAS.

Análisis de Brechas

En el presente capítulo se desarrolla lo siguiente:

a. Se toman las brechas identificadas por componente de Gobierno digital
b. Se establecen posibles soluciones.
c. Se determinan las entregas de valor.
d. Se identifican los interesados claves.

6. 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.

ANEXO 01. ANALISIS Y PRIORIZACIÓN DE INICITIVAS

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.

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	Actualización de Instrumentos de gestión de la información pública	Febrero	Junio	Todos los procesos	Matrices de activos
1.2	Publicación Instrumentos de gestión de la información pública	junio	Agosto	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	Marzo	Junio	SGSI – SGD - SGC	Documentación con los lineamientos institucionales
1.4	Implementación de las estrategias definidas para el etiquetado de los activos de tipo información en medio físico y electrónico	Junio	Diciembre	Todos los procesos	Informe de actividades realizadas
2. Riesgos de Seguridad y Privacidad de la Información					
2.1	Identificación y Análisis de Riesgos Seguridad de la información	Abril	Junio	Todos los procesos	Matrices de riesgos aprobadas
2.2	Definición del Tratamiento de Riesgos Seguridad de la Información	Abril	Junio	Todos los procesos	Plan de Tratamiento de Riesgos de Seguridad de la Información
2.3	Seguimiento a la implementación de los planes de tratamiento	Julio	Diciembre	CISO	Informe de seguimiento de los planes de tratamiento

2.4	*Actualización de la Declaración de Aplicabilidad*	*Julio*	*Diciembre*	*CISO*	*Informe de seguimiento de los planes de tratamiento*
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
3.1	*Actualización del Plan de Uso y Apropiación incluyendo los temas Seguridad y Privacidad*	*Enero*	*Febrero*	*CISO - Comunicaciones*	*Documento Plan de Concienciación en Seguridad y Privacidad*
3.2	*Ejecución del Plan de Concienciación en Seguridad y Privacidad.*	*Febrero*	*Diciembre*	*CISO - Comunicaciones*	*Informe de ejecución.*
3.3	*Entrenamientos y/o Sensibilizaciones en temas Seguridad y Privacidad de la información.*	*Febrero*	*Diciembre*	*CISO*	*Listado de asistencia, videos Informe de las acciones realizadas.*
3.4	*Análisis de 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	*Revisión de la Política de Protección de Datos Personales de la entidad*	*Junio*	*Agosto*	*CISO – AJSC - GAF*	*Política de Protección de Datos Personales*
4.2	*Actualización del Manual de Protección de Datos Personales*	*Junio*	*Agosto*	*CISO – AJSC - GAF*	*Manual de Protección de Datos Personales*
4.3	*Divulgación de la política y manual de Protección de Datos Personales*	*Febrero*	*Diciembre*	*CISO*	*Listado de asistencia, videos Informe de las acciones realizadas.*

4.4	*Implementación de los lineamientos definidos en el Manual de Protección de Datos Personales*	*Agosto*	*Diciembre*	*Todos los procesos*	*Listado de asistencia, videos Informe de las acciones realizadas.*
4.5	*Seguimiento a la implementación del Manual de Protección de Datos Personales*	*Marzo*	*Diciembre*	*CISO*	*Informe de Seguimiento y Recomendaciones.*
5. Sistema de Gestión de Seguridad de la Información					
5.1	*Revisión de la Política, Manual de Políticas de Seguridad y Privacidad de la Información*	*Enero*	*Marzo*	*CISO - CIGyD*	*Manual y Política de Seguridad de la Información.*
5.2	*Apoyar en la definición y/o actualización de la documentación asociada a Seguridad y Privacidad de la Información*	*Marzo*	*Diciembre*	*TSI*	*Documentos, procedimientos guías.*
5.3	*Definición de lineamientos de seguridad como apoyo a la ejecución de los procesos*	*Febrero*	*Diciembre*	*CISO*	*Documentos, procedimiento guías, correos.*
5.4	*Definición de la Matriz RACI de Seguridad y Privacidad de la Información*	*Agosto*	*Septiembre*	*CISO*	*Matriz RACI*
5.5	*Revisión de los controles de la norma ISO 27001:2013*	*Junio*	*Diciembre*	*TSI*	*Herramienta de medición y autodiagnóstico del MSPI semestral*
5.6	*Apoyo en la definición, socialización y apropiación de los lineamientos de cifrado, copias de respaldo,*	*Febrero*	*Diciembre*	*TSI*	*Documentación, registros de asistencias, Informes de resultado de las revisiones*

	gestión de vulnerabilidades, usuarios privilegiados, gestión de accesos, desarrollo seguro, seguridad física, entre otros.				
5.7	*Revisión por la Dirección*	*Junio*	*Diciembre*	*CISO – Coordinación de planeación estratégica*	*Acta de Revisión por la Dirección*
5.8	*Gestionar auditoría interna al Sistema de Gestión de Seguridad de la Información*	*Septiembre*	*Octubre*	*Oficina de Control Interno*	*Plan Anual de Auditoria*
5.9	*Identificación y Reporte de cumplimiento de los indicadores de seguridad de la Información*	*Enero*	*Diciembre*	*Equipo Seguridad de la Información*	*Indicadores de Seguridad y Privacidad de la información*
6. Continuidad del Negocio					
6.1	*Realizar el análisis de impacto al negocio – BIA para los servicios críticos de la entidad*	*Junio*	*Agosto*	*CISO*	*Documento de análisis de impacto al negocio – BIA*
6.2	*Definir los Escenarios de afectación para los servicios críticos de la entidad*	*Agosto*	*Octubre*	*CISO*	*Riesgos de Continuidad del Negocio*
6.3	*Definición del Plan de Continuidad del Negocio*	*Octubre*	*Noviembre*	*CISO*	*Plan de Continuidad del Negocio*
6.4	*Realizar la planeación y ejecución de las pruebas definidas en el Plan de Continuidad del Negocio*	*Noviembre*	*Diciembre*	*CISO*	*Informe de resultados de las pruebas realizadas*

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*