COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

PLAN TRATAMIENTO DE RIEGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección Ejecutiva

Líder: Zoila Vargas Mesa.
Coordinadora Ejecutiva

Enero de 2023

CONTENIDO

1. INTRODUCCIÓN **4**
2. OBJETIVO **6**
3. ALCANCE DEL DOCUMENTO **7**
4. MARCO NORMATIVO **8**
5. RESPONSABLE DE LA ESTRATEGIA OPERACIONAL **12**
5.1. Medición de la Eficacia de los Controles. 13
6. INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DE RIESGOS Y CONTROLES **13**
6.1. Marco Teórico. 13
6.2. Activos de información. 14
6.3. Riesgos de Seguridad de la Información. 14
6.4. Identificación de controles. 15
Anexo 1. HOJA DE RUTA **16**

Historia de Actualizaciones

Fecha	Descripción	Responsable
Enero - 2021	Creación Plan Estratégico Seguridad y Privacidad de la Información	CISO
Enero - 2022	Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	CISO
Enero - 2023	Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	CISO

1. 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 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.
- ✓ 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 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, 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.

Los proyectos que componen un Plan Estratégico de Seguridad y Privacidad de la Información varían en función de diversos factores relacionados como:

- ✓ El tamaño de la Organización
- ✓ El nivel de Madurez en tecnología
- ✓ El sector al que pertenece la empresa
- ✓ El contexto legal que regula las actividades de esta
- ✓ La naturaleza de la información que manejamos
- ✓ El alcance del proyecto
- ✓ Otros aspectos organizativos

Por lo anterior, y teniendo en cuenta el mapa de ruta establecido en el Plan Estratégico de Seguridad y Privacidad 2023, se define de manera particular el Plan de Tratamiento de Riesgos de Seguridad de la Información para esta misma vigencia.

2. 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.

3. 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 2023.

4. MARCO NORMATIVO

Tabla 1. Marco normativo Plan tratamiento de riesgos de Seguridad y Privacidad de la información.

Normativa	Descripción General
Ley 527 de 1999	Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.
Decreto 103 de 2015	Reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Ley 1712 de 2014	Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1581 de 2012	Dicta disposiciones generales para la protección de datos personales.
Ley 1341 de 2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.
Decreto 1078 de 2015	Marco de Referencia de Arquitectura Empresarial para la gestión de TI (Artículo 2.2.5.1.2.2)

Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
CONPES 3854 – 2016	"Política Nacional de Seguridad Digital", se consideró que era necesario cambiar el enfoque tradicional e incluir la gestión de riesgo como uno de los elementos más importantes para abordar la temática, estableciendo como objetivo general: "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país."
Decreto 1413 del 25 de agosto de 2017	Por el cual presente reglamenta parcialmente el Capítulo IV del Título 111 de la Primera Parte de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo los lineamientos que se deben cumplir para la prestación de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administración pública a través de medios electrónicos
Decreto 612 del 4 abril de 2018	Por el cual Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011

CONPES No. 3995 de 2020	Política Nacional de Confianza y Seguridad Digital". De esta manera, el objeto es establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para alcanzar este objetivo, en primer lugar, se fortalecerán las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; en segundo lugar, se actualizará el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
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. Por el cual estable el Objeto como: Uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio

Resumen de aplicación del 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, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

En el **artículo 2.2.9.1.1.3** Principios, en este se encuentra: **Confianza**: Los sujetos obligados propenderán por que la implementación de la Política de Gobierno Digital permita el equilibrio entre las expectativas ciudadanas y el funcionamiento de las instituciones públicas. De la misma forma, los sujetos obligados cumplirán con las disposiciones que permitan la garantía de la seguridad digital, la

protección de datos, y la transparencia pública. **Resiliencia Tecnológica:** Los sujetos obligados a la aplicación de la presente Política tomarán acciones respecto de la prevención de riesgos que puedan afectar la seguridad digital y con ello propenderán por la disponibilidad de los activos, la recuperación y continuidad de la prestación del servicio ante interrupciones o incidentes.

Como Habilitadores transversales de la Política de Gobierno Digital se encuentran elementos fundamentales como Arquitectura, **Seguridad y Privacidad de la Información**, Cultura y Apropiación y Servicios Ciudadanos Digitales, que permiten el desarrollo y el logro de los propósitos de la Política de Gobierno Digital.

El propósito del habilitador de la Política de Gobierno Digital que está relacionado con la Seguridad y Privacidad de la información es: ***buscar que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.***

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)

5. 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.

5.1. Medición de la Eficacia de los Controles.

Cuando se pueda establecer un nivel de madurez en los controles, cada control deberá tener su indicador y dentro de la ficha de caracterización de estos se establece la periodicidad de medición y el método de cálculo respectivo.

Esta medición se realizará de acuerdo con la periodicidad definida para cada control, en cada componente de seguimiento de este plan.

6. INVENTARIO DE ACTIVOS DE INFORMACIÓN, IDENTIFICACIÓN DE RIESGOS Y CONTROLES

6.1. Marco Teórico.

Para el levantamiento de los activos de información de los procesos definidos se utilizó el instrumento diseñado por la entidad. El ejercicio se desarrolló basado en entrevistas con 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

6.2. Activos de información.

Los activos de información se identificaron y caracterizaron con base en los parámetros del instrumento diseñado por la entidad (Nombre, descripción, proceso al que pertenece, propietario, responsable, custodio, usuarios, tipo de activo de información, medio de conservación, ubicación, respaldo, 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 de uso interno o pública clasificada (que hace referencia a su contenido con información de datos personales protegidos por ley).

6.3. Riesgos de Seguridad de la Información.

La configuración de riesgos de seguridad de la información se establece sobre algunos activos de información identificados y se utilizó la caracterización de estos riesgos teniendo en cuenta su clasificación de tipo de riesgo (Estratégico, de imagen, de operación, de cumplimento, tecnológico o financiero), adicionalmente se caracterizó de cada riesgo sus causas – amenazas, su vulnerabilidad y consecuencias en caso de materializarse.

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.

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

Probabilidad	Impacto
Rara vez	Insignificante
Improbable	Menor
Posible	Moderado
Probable	Mayor
Casi Seguro	Catastrófico

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

6.4. Identificación de controles.

Para los riesgos que se identifican se establecen controles identificando su propósito, como se desarrolla su actividad de control, periodicidad de verificación, quien lo ejecuta y el registro que se debe llevar de este control, así como la clase de control (Preventivo o correctivo).

Anexo 1. HOJA DE RUTA

Tabla 3. Hoja de ruta tratamiento de riesgos de Seguridad y Privacidad de la Información 2023

PROYECTO	DESCRIPCIÓN PROYECTO	ACTIVIDADES	DESCRIPCIÓN ACTIVIDADES	RECURSOS	TRIMESTRE 2023			
					1	2	3	4
P1	Gestión de Riesgos de Seguridad de la información	A.01	Actualizar los lineamientos para los activos de información y la gestión de riesgos de seguridad de la información.	CISO			X	
P1	Gestión de Riesgos de Seguridad de la información	A.02	Actualización y evaluación de activos de Información	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión			X	
P1	Gestión de Riesgos de Seguridad de la información	A.03	Identificación, actualización y evaluación de Riesgos de Seguridad de Información	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión	X			
P1	Gestión de Riesgos de Seguridad de la información	A.04	Definición y evaluación de controles	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión		X		
P1	Gestión de Riesgos de Seguridad de la información	A.05	Aprobación de los riesgos de seguridad de la información	Líderes de procesos		X		
P1	Gestión de Riesgos de Seguridad de la información	A.06	Implementación y seguimiento del Plan de Tratamiento de Riesgos	Líderes de procesos Enlaces de los procesos CISO Herramienta de gestión		X	X	X

P1	Gestión de Riesgos de Seguridad de la información	A.07	Informe de ejecución de la gestión de riesgos de seguridad de la información	CISO				X