PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAPITAL

2023

TABLA DE CONTENIDO

INTRODUCCIÓN

La Política de seguridad y privacidad de la información de Capital asegura que la entidad establezca la protección de los activos de información (funcionarios, contratistas, partes interesadas, la información, los procesos, las tecnologías de información incluido el hardware y el software) dando cumplimiento a los requisitos establecidos por las partes interesadas en la gestión de la información.

Adicionalmente, tiene como propósito salvaguardar la información generada dentro de la entidad garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente, para poder realizar un Plan de Seguridad y Privacidad de la Información y con el fin de que no se presenten perdidas de información, accesos no autorizados y duplicación de información que puedan ocasionar daños a los procesos de la entidad.

Capital cumple con los tres pilares de la seguridad de la información en preservar la integridad, confidencialidad y disponibilidad de la información (ISO 27000: 2013):

- **Confidencialidad**: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (ISO 27000).
- **Disponibilidad**: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (ISO 27000).
- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (ISO 27000).

1. OBJETIVO

Definir los lineamientos y metodología a seguir para la identificación, análisis, valoración y tratamiento de riesgos de Seguridad de la Información, alineados con la política de seguridad y privacidad de la información de Capital. Con el propósito de mantener la confidencialidad, integridad, disponibilidad y privacidad de la información a través de la gestión del riesgo asociado a la información de la entidad.

2. ALCANCE

El Plan de tratamiento de riesgos de seguridad de la información es aplicable a todos los procesos de Canal Capital, con alcance a los colaboradores, contratistas y terceros; inicia desde la identificación de los riesgos de seguridad de la información que se encuentran en el nivel “Alto” en la Matriz de Activos de Información de la entidad, hasta la definición del plan de tratamiento, actividades, definición de responsables y fechas de implementación.

3. CONTEXTO

El presente plan está alineado y contribuye al logro de la misión, visión y objetivos estratégicos de Capital, los cuales se estipulan en el Plan Estratégico Institucional vigente (2023).

Articulación con el contexto estratégico	
Objetivo estratégico al que aporta:	1. Posicionar a Capital Sistema de Comunicación Pública como motor de la innovación audiovisual, a partir de un modelo de operación basado en la pluralidad, el libre acceso a la información, la generación de conocimiento y la participación de los ciudadanos de la Bogotá región. 2. Consolidar una oferta de contenidos informativos, educativos y culturales, que promuevan la participación y la inclusión de la ciudadanía. 3. Generar un proceso de transformación digital con base en el desarrollo tecnológico y humano para la optimización de los procesos internos, la creación de nuevos modelos de negocio, el relacionamiento con los clientes y ciudadanos y la producción y distribución de contenidos. 4. Consolidar a Capital como la empresa referente en el desarrollo de estrategias de comunicación pública de Bogotá región. 5. Fortalecer la capacidad institucional de Capital para ser una empresa eficiente, sostenible y transparente.
Gestión y Desempeño Institucional – MIPG	• Política Gobierno Digital • Política de Seguridad Digital • Política de Transparencia, acceso a la información pública y lucha contra la corrupción.

Establecimiento contexto

El presente plan aplica en todos los procesos de Capital donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

Son requisitos indispensables para la implementación del presente plan:

- Lograr el compromiso de la gerencia de Capital para iniciar la implementación del plan de gestión del riesgo de seguridad de la información.
- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.
- Capacitar a los servidores de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

4. DEFINICIONES

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO31000:2013.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: propiedad de exactitud y completitud.

Sistema de Gestión de Seguridad de la Información: basado en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos de la entidad. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de Contexto - Información sobre la evaluación de riesgos probabilidad y consecuencias.

5. NORMATIVIDAD

Capital ha elaborado el Plan de Seguridad y Privacidad de la Información, en cumplimiento de la siguiente normatividad:

- Ley 1474 de 2011, reglamentada por el Decreto Nacional 734 de 2012 y reglamentada parcialmente por el Decreto Nacional 4632 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales.

- Ley 1712 de 2014, reglamentada parcialmente por el Decreto Nacional 103 de 2015, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Conpes 3854 de 2016, que es la Política de Seguridad Digital para Colombia y en la cual se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

- Decreto 1413 de 2017, Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- Decreto 1008 de 2018, 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 612 de 2018, por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Norma Técnica Colombiana ISO27001:2013.

- Norma Técnica Colombiana ISO31000:2013.

6. DOCUMENTOS RELACIONADOS

- Política de Seguridad y Privacidad de la Información - AGRI-SI-PO-002.
- Manual del Sistema de Gestión de Seguridad de la Información-SGSI AGRI-SI-MN-001.
- Formato para el inventario y clasificación de activos de información- AGRI-SI-FT-038.

7. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La metodología de gestión de identificación, evaluación y gestión de riesgos de los sistemas de gestión actuales de Capital se basa en la NTC-ISO 31000, la Guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública - DAFP y la Guía de gestión de riesgos del MinTIC. Su propósito es la identificación, estimación y evaluación de los riesgos de la entidad para definir un plan de tratamiento que se ajuste a los objetivos de cada uno de los procesos.

La Gestión de Riesgos de Capital, incluyendo los Riesgos de Seguridad y Privacidad se lleva a cabo por los Líderes de cada proceso y lo gestionan para el cumplimiento de la misión, la visión y los objetivos estratégicos, con el fin de determinar el tratamiento del riesgo aceptable sobre cada uno de los riesgos identificados, teniendo en cuenta el siguiente esquema:

Contexto

Se establece un contexto del proceso con los siguientes aspectos:

- Contexto del Proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.
- Diseño del proceso: Claridad en la descripción del alcance y objetivo del proceso.
- Interrelación con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios.
- Procedimientos asociados: Pertinencia en los procedimientos que desarrollan los procesos.
- Responsables del proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

Luego se establece el tipo de proceso: Misional, Estratégicos, de Apoyo y Evaluación y Control.

Gestión de activos de información

La gestión de activos de información es una tarea de las áreas de seguridad o de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes de la entidad.

Análisis

Se realiza la identificación de causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden entorpecer el normal desarrollo de los procesos.

Valoración

El objetivo de este paso es generar una lista completa de los riesgos sobre la base de los sucesos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos de la entidad.

Tratamiento

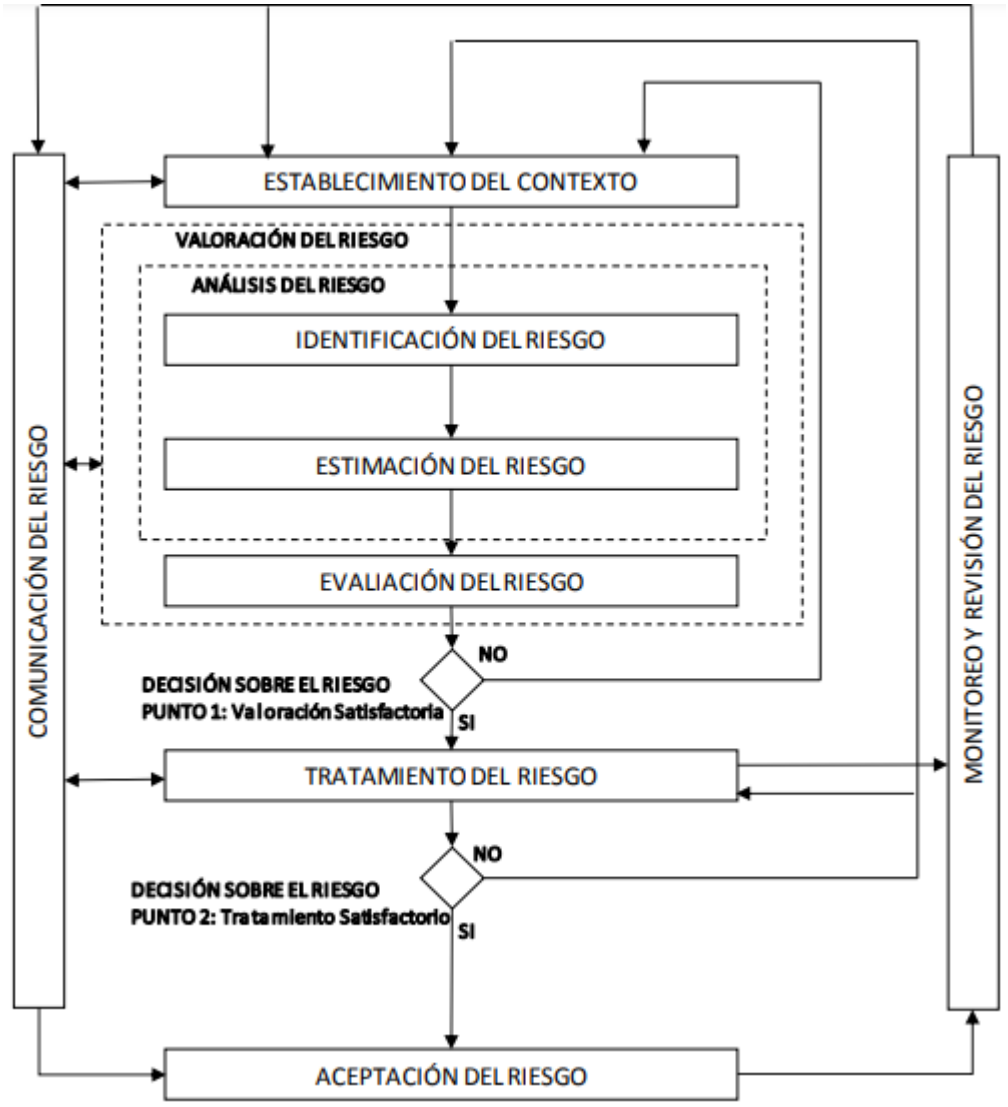
El tratamiento del riesgo consiste en seleccionar y aplicar las medidas adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños, para lo cual se definen medidas de respuesta ante los Riesgos (asumir, reducir, compartir, trasferir o evitar), luego

se definen acciones de mitigación de riesgos (actividades o tareas, responsables, plazo de ejecución y seguimiento).

El proceso de gestión de riesgo en la seguridad de la información

Consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para la administración del riesgo en seguridad de la información



Fuente tomado de la NTC-ISO/IEC27005

Así como lo ilustra la anterior imagen, el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento de este.

8. CRONOGRAMA DE ACTIVIDADES

A continuación, se presenta el esquema de actividades establecido por el Área de Sistemas:

Ítem	Actividad	Fecha de inicio	Fecha final	Responsable	Producto o resultado
Riesgos de seguridad y privacidad de la información					
1	Revisión de la matriz de activos de información acorde a la actualización realizada con las áreas.	Marzo 2023	Agosto 2023	Profesional de seguridad informática y áreas del canal	Matriz de activos de información actualizada
2	Implementación matriz de riesgos de seguridad digital	Enero 2023	Diciembre 2023	Profesional de seguridad informática	Matriz de riesgos de seguridad digital
4	Implementación de controles preventivos para el aseguramiento de los activos de información de la entidad	Enero 2023	Diciembre 2023	Equipo de sistemas	Controles implementados plataforma tecnológica
5	Implementación, seguimiento y control al plan de mejoramiento del procedimiento de copias de seguridad	Enero 2023	Diciembre 2023	Equipo de sistemas	Actividades ejecutadas plan de mejoramiento 2022.