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

2026

Revisión histórica

Fecha	Versión	Descripción	Autor
Diciembre 2020	1.0	Creación inicial V1 del documento.	Maryury Forero Bohórquez
Diciembre 2021	2.0	Actualización V2 del documento.	Maryury Forero Bohórquez
Diciembre 2022	3.0	Actualización V3 del documento.	Maryury Forero Bohórquez
Enero 2024	4.0	Actualización V4 del documento.	Maryury Forero Bohórquez
Mayo 2025	5.0	Actualización V5 del documento. Aprobado en sesión 2 CIGD del 13/05/2025	Juan David Poveda Gomez
Enero 2026	6.0	Actualización V6 del documento. Aprobado en sesión 1 CIGD del 28/01/2026	Juan David Poveda Gomez

Contenido

INTRODUCCIÓN

La Política de Seguridad y Privacidad de la Información de Canal Capital tiene como objetivo asegurar la protección integral de los activos de información de la entidad, incluyendo funcionarios, contratistas, colaboradores, partes interesadas, información, procesos y tecnologías de la información (hardware y software). Esta política garantiza el cumplimiento de los requisitos establecidos por las partes interesadas en la gestión de la información

.

Asimismo, busca salvaguardar la información generada al interior de la entidad, asegurando la protección de los datos y el cumplimiento de la normatividad legal vigente. De esta manera, se establece el marco para la formulación y ejecución del Plan de Seguridad y Privacidad de la Información, con el fin de prevenir la pérdida de datos, accesos no autorizados y la duplicación indebida de información, eventos que podrían afectar los procesos misionales de Canal Capital.

En concordancia con el Manual de la Política de Gobierno Digital expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que promueve el uso estratégico de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanía competitivos, proactivos e innovadores, Canal Capital reafirma su compromiso con un entorno de confianza digital. La entidad garantiza el cumplimiento de los tres pilares fundamentales de la seguridad de la información, establecidos en la norma ISO 27000 integridad, confidencialidad y disponibilidad de la información:

- **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 Canal 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 funcionarios, 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 Canal Capital, los cuales se estipulan en el Plan Estratégico Institucional vigente de 2026.

Articulación con el contexto estratégico	
Objetivo estratégico al que aporta:	Cautivar y cultivar audiencias mediante una estrategia de programación de contenidos de interés, cercanos y confiables para los habitantes, visitantes y enamorados de Bogotá. Incrementar la capacidad tecnológica en toda la cadena de producción y fortalecer el patrimonio audiovisual propio para responder a las expectativas de las audiencias Establecer un modelo de negocio innovador en producción in-house, por encargo, coproducción y alianzas estratégicas, aumentando la eficiencia en la gestión para generar sostenibilidad. Fortalecer y diversificar la capacidad de producción propia, basada en la creatividad, el conocimiento de las audiencias y en estrategias de difusión y promoción de la oferta del Canal, aprovechando las oportunidades de la televisión y la convergencia

Articulación con el contexto estratégico	
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.

El presente plan aplica en todos los procesos de Canal 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:

- Compromiso de la gerencia de Canal 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 funcionarios, contratistas y colaboradores de la Entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

4. DEFINICIONES [1]

Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

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.

Eramba GRC: es una plataforma de software de código abierto para Gobernanza, Riesgo y Cumplimiento (GRC), que ayuda a las organizaciones a gestionar sus políticas, mitigar riesgos, cumplir normativas (como PCI-DSS o ISO) y gestionar auditorías e incidentes de seguridad de forma centralizada, ofreciendo versiones gratuitas (Community) y de pago (Enterprise) para controlar la seguridad y los procesos internos de forma más eficiente.[2]

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 la información que busca preservar su exactitud y completitud.

Política de Seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad 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 digital: Es la combinación de amenazas y/o vulnerabilidades que se pueden

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

[2] https://www.eramba.org/

materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

Sistema de Gestión de seguridad de la información (SGSI): Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

5. NORMATIVIDAD

Canal 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 reglamentar 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 767 de 2022, (Actualización de Política de Gobierno Digital) 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.
- 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.
- NTC ISO/IEC 27001:2022.
- NTC ISO/IEC 31000:2018.

6. DOCUMENTOS RELACIONADOS

- Política de Seguridad y Privacidad de la Información: AGRI-SI-PO-002.
- Plan de Seguridad y Privacidad de la Información: AGTIC-SI-PL-003
- Manual del Sistema de Gestión de Seguridad de la Información-SGSI: AGTIC-MN-001.
- Formato para el inventario y clasificación de activos de información: AGTIC-SI-FT-038.
- Matriz de Riesgos de Seguridad Digital: AGTIC-SI-FT-045

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 Canal Capital se basa en la NTC ISO/IEC 31000:2018, la Guía de Gestión del Riesgo del Departamento Administrativo de la Función Pública – DAFP, NTC ISO/IEC 27001:2022 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.

Para el apoyo a la gestión de los riesgos, controles y demás documentación asociada al Sistema de Gestión de Seguridad de la Información (SGSI), se utilizará la herramienta Eramba GRC, la cual permitirá administrar de manera centralizada los riesgos, controles y demás componentes relacionados con el cumplimiento de la NTC ISO/IEC 27001:2022 y los lineamientos de la Política de Gobierno Digital.

La Gestión de Riesgos de Canal 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

El análisis 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, este

proceso se lleva a cabo mediante la actualización del formato para el inventario de clasificación de activos de información y la matriz diligenciada (AGTIC-SI-FT-038).

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

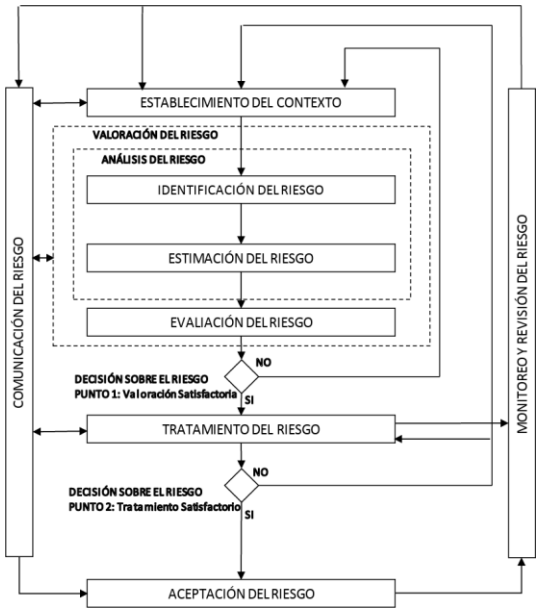
Consiste en seleccionar y aplicar las medidas adecuadas, con el fin de poder modificar el riesgo,

para evitar de este modo los daños, para lo cual se definen medidas de respuesta ante los Riesgos (asumir, reducir, compartir, transferir 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.

Mesa de crisis

Fortalecer la capacidad institucional de respuesta ante incidentes de seguridad de la información mediante la implementación de una Mesa de Crisis, articulada con el AGTIC-SI-PL-003 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION y los planes de continuidad, en cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), de la Política de Gobierno Digital.

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



Fuente: NTC-ISO/IEC 27005

8. CRONOGRAMA

NO.	ACTIVIDAD	RESPONSABLE	2026 ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1	Debilidades en los mecanismos de control para el análisis del ciclo de vida de los elementos tecnológicos que generen obsolescencia.	Gestión TIC												
1.1	Actualizar una matriz de obsolescencia y ciclo de vida para hardware y software.	Gestión TIC	■	■										
1.2	Mantener alertas preventivas para recambio y actualización tecnológica.	Gestión TIC			■	■								
2	Ausencia de mecanismos para el respaldo de datos y configuraciones de la información y equipos tecnológicos, que afectan la disponibilidad de los servicios en caso de falla	Gestión TIC												
2.1	Implementar una política de respaldo (backup y recuperación).	Gestión TIC	■											
2.2	Automatizar respaldos periódicos y generar reportes de verificación.	Gestión TIC	■											
2.3	Simulacros de recuperación.	Gestión TIC			■			■			■			■
3	Debilidad en la configuración y/o parametrización de los sistemas y controles de seguridad que puedan originar ciberataques (malware, ransomware, phishing, DoS, accesos no autorizados)	Gestión TIC												
3.1	Realizar hardening de servidores, firewalls, redes y estaciones de trabajo.	Gestión TIC	■	■	■	■	■	■	■	■	■	■	■	■
3.2	Aplicar mejores prácticas de seguridad basadas en CIS Controls o NIST.	Gestión TIC	■	■	■	■	■	■	■	■	■	■	■	■
3.3	Implementar herrmientas de ciberseguridad	Gestión TIC	■	■	■	■	■	■	■	■	■	■	■	■
4	Uso inadecuado de la información y de los recursos tecnológicos de Canal Capital, para fines internos o externos.	Gestión TIC												
4.1	Campañas de concientización sobre el uso adecuado de la información.	Gestión TIC	■	■	■	■	■	■	■	■	■	■	■	■
4.2	Implementar controles de monitoreo y trazabilidad (logs de acceso, políticas de uso aceptable).	Gestión TIC					■							