PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

Revisión histórica

Fecha	Versión	Descripción	Autor
Diciembre 2020	1.0	Creación inicial V1 del documento. Aprobado en sesión 04 CIGD del 1622/12/2020	Maryury Forero Bohórquez
Diciembre 2022	2.0	Actualización del documento V2	Maryury Forero Bohórquez
Enero 2024	3.0	Actualización del documento V3	Mauris Avila Velásquez
Mayo 2025	4.0	Actualización del documento V4 - Aprobado en sesión 2 CIGD del 13/05/2025	Juan David Poveda Gomez
Enero 2026	5.0	Actualización del documento (Se incluye mesa de crisis) V5 - Aprobado en sesión 1 CIGD del 28/01/2026	Juan David Poveda Gomez

INTRODUCCIÓN

La Política de la seguridad de la información de Canal 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 y de acuerdo con lo estipulado en el lineamiento del numeral 8.1 del documento maestro del MSPI[1], el Plan de seguridad y privacidad de la información, tiene como propósito establecer los detalles de cómo se realizará la implementación y mejora de la seguridad de la información en la Entidad para cada vigencia, estipulando directrices, tiempos y responsables con el fin de mitigar los riesgos asociados a la pérdida de información, seguridad e indisponibilidad de los servicios TI de la entidad.

Canal Capital propende por cumplir con los tres pilares de la seguridad de la información y con ello preservar la integridad, confidencialidad y disponibilidad de la información (ISO 27000: 2022):

- **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] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

1. OBJETIVO

Formular la estrategia para diseñar e implementar las políticas, controles, lineamientos, y procedimientos con los cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de Canal Capital a través de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Contribuyendo con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de los activos de información de la entidad.

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos de Canal Capital, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información, contemplando los controles definidos y aplicables a la entidad en la Norma Técnica Colombiana ISO IEC 27001:2022, mediante el cual se implementan buenas prácticas para salvaguardar los activos de información de Canal Capital.

3. DEFINICIONES[2]

Activos de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

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.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

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.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del

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

Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo de seguridad digital: Es la combinación de amenazas y/o vulnerabilidades que se pueden 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.

Seguridad de la Información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC27001:2022).

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas. (Decreto 338 de 2022). Para el caso de estandarización de lenguaje este concepto se asocia al aceptado internacionalmente como ciberseguridad.

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.

Tecnología de la Información: Las tecnologías de la información se centra en el tratamiento y la gestión de datos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

Vulnerabilidad de seguridad digital: Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización. (Decreto 338 de 2022).

4. 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 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 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.
- Decreto 1081 de 2015, Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
- 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.
- Resolución 0277 de 2025, con la cual se actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), contenido en el Anexo 1 de la Resolución 500 de 2021, y se derogan disposiciones anteriores que resultaban contrarias a los nuevos estándares internacionales en esta materia.

5. INSTRUMENTO DE MEDICIÓN

A través del instrumento: Modelo de Seguridad y Privacidad de la Información (MSPI), iniciando con la fase de diagnóstico de Seguridad y Privacidad de la información se define como la fase inicial del MSPI establecido por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC) para todas aquellas entidades que pertenecen al ámbito gubernamental y permite identificar el estado actual de las entidades con respecto a los requerimientos del MSPI. Esta fase pretende alcanzar metas tales como:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles implementados de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la Normatividad vigente relacionada con protección de datos personales e identificación del uso de buenas prácticas en seguridad de la información.
- Identificar el nivel de madurez en materia de Ciberseguridad.

Los activos de información son lo más importante en la Entidad que deben ser gestionados para proteger y garantizar la continuidad del negocio. A través de la implementación del Sistema de Gestión de seguridad de la Información-SGSI, se garantiza la gestión y protección eficiente de la información al interior de la entidad que desea asegurar la integridad, confidencialidad y disponibilidad de la misma, siendo esto los tres pilares más importantes de la seguridad de la información.

Según la ISO/IEC 27001:2022, la seguridad de la información preserva la confidencialidad, integridad, disponibilidad y privacidad, pero para poder considerar que, si es de gran valor, la información debe poseer ciertas características tales como:

- El ser relevante

- Estar siempre actualizada
- Ser altamente confiable
- Poseer un alto nivel de calidad
- Siempre debe ser completa

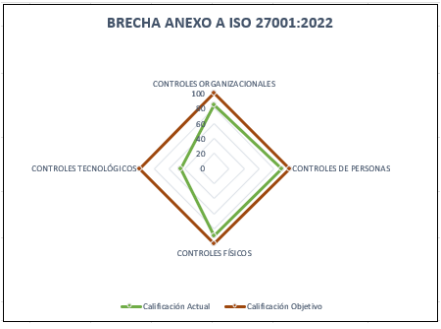
Lo anterior le permite cumplir eficientemente con el objetivo por el cual fue creada, por ello se hace necesario implementar medidas que permitan salvaguardar de la mejor manera y que al hacerlo cumpla con los tres grandes pilares de la seguridad, evitando que sea usada para fines distintos y pueda afectar de gran manera la operación en la entidad y el cumplimiento de los objetivos institucional.

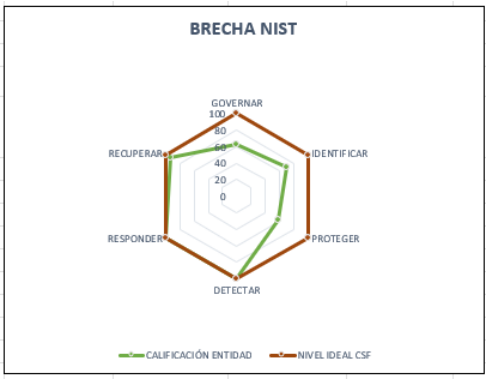
Ciclo de operación del MSPI

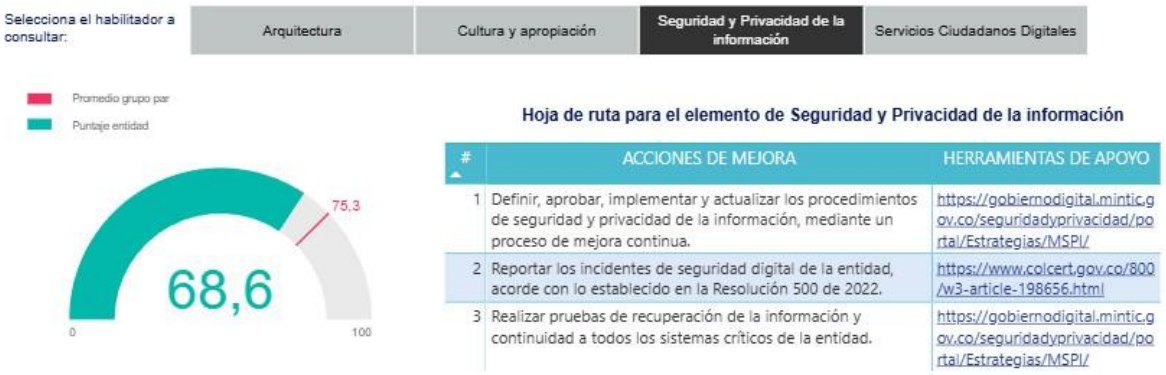
6. ESTADO ACTUAL

De acuerdo con los resultados promedio del 86% como resultado a la Evaluación del Modelo de Seguridad y Privacidad para el año 2025, se describen los ítems con la calificación actual, con el fin de que se adelanten las acciones para el fortalecimiento de la estrategia de seguridad digital de la Entidad: Evaluación de efectividad de controles:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	84	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	90	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	90	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	44	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		77	100	GESTIONADO







Fuente: Resultados de FURAG https://gobiernodigital.mintic.gov.co/portal/Mediciones/

7. MESA DE CRISIS

7.1 PROPÓSITO

Establecer el marco organizacional para la gestión de incidentes de seguridad y privacidad de la información, incluyendo la conformación y operación de la Mesa de Crisis, con el fin de responder eficazmente a eventos que comprometan la confidencialidad, integridad y disponibilidad de la información, que aplicará a todos los procesos, activos de información, sistemas de información, funcionarios, contratistas y terceros que gestionen información de Canal Capital.

7.2 CRITERIOS DE ACTIVACIÓN DE LA MESA DE CRISIS

La Mesa de Crisis será activada ante incidentes que cumplan al menos uno de los siguientes criterios:

- Compromiso de información clasificada como confidencial o reservada.

- Afectación significativa a servicios misionales.
- Violación de datos personales.
- Riesgo reputacional o legal relevante.
- Incidentes con impacto alto o crítico que puedan llegar a afectar la operación o la misionalidad de Canal Capital.

7.3 CONFORMACIÓN DE LA MESA DE CRISIS

- **Líder de la Mesa de Crisis**
  Responsable de Seguridad de la Información: Gestión TIC.

  Responsabilidades:

  - Activar y desactivar la Mesa de Crisis.
  - Dirigir la gestión del incidente.
  - Clasificar el incidente según impacto y severidad.
  - Coordinar con equipos técnicos, jurídicos y directivos.
  - Validar decisiones estratégicas de contención y recuperación.
  - Garantizar el cumplimiento de la NTC ISO/IEC 27001:2022 y normativa aplicable.

- **Líder técnico (TI / Infraestructura / Firewall)**
  Gestión TIC.

  Responsabilidades:

  - Analizar técnicamente el incidente.
  - Ejecutar acciones de contención, erradicación y recuperación.
  - Preservar evidencias técnicas.
  - Reportar avances y riesgos técnicos a la Mesa de Crisis.

  - Coordinar con proveedores tecnológicos si aplica.

- **Asesoría jurídica**
  Oficina Jurídica.

  Responsabilidades:

  - Evaluar impactos legales, contractuales y regulatorios.
  - Definir obligaciones de notificación a autoridades (SIC, MinTIC, entes de control).
  - Asesorar sobre responsabilidades legales y sanciones.
  - Validar comunicaciones externas desde el punto de vista legal.

- **Responsable de Comunicaciones**
  Gestión de Comunicaciones.

  Responsabilidades:

  - Gestionar la comunicación interna y externa del incidente.
  - Preparar comunicados oficiales.
  - Coordinar mensajes con Gerencia y la Oficina Jurídica.
  - Evitar divulgación no autorizada de información sensible.

- **Representante de la Alta Dirección**
  Gerente o quien designe en representación.

  Responsabilidades:

  - Aprobar decisiones estratégicas y excepcionales.
  - Autorizar uso de recursos extraordinarios.
  - Asegurar alineación con los objetivos institucionales.
  - Respaldar las acciones de la Mesa de Crisis.

- **Custodio del activo de información afectado**
  Propietarios de la información o activo. Responsabilidades:
  - Aportar conocimiento del activo impactado.
  - Apoyar la evaluación de impacto operativo.
  - Validar procesos de recuperación funcional.

7.4 RESPONSABILIDADES GENERALES

- Coordinar la respuesta integral al incidente.
- Asegurar la toma de decisiones informadas y oportunas.
- Proteger los activos de información y los datos personales.
- Garantizar el cumplimiento normativo y contractual.
- Documentar el incidente y promover el aprendizaje organizacional.
- Comunicar asertivamente.

8. PLAN

De acuerdo con la evaluación realizada en el instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI), se demuestra que la entidad ha tenido avances significativos frente a la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio de las TIC, sin embargo, se deben definir algunas actividades que garanticen el cumplimiento del total de los

lineamientos establecidos en dicho instrumento.

Con lo cual se plantea la iniciativa del fortalecimiento institucional para la seguridad y privacidad de la información que propenderá por implementar estrategias para garantizar la seguridad de los datos, la privacidad, su arquitectura y administración como se representa en la gráfica.

Asimismo, establecer la conformación de la Mesa de Crisis con el fin de responder eficazmente a eventos que comprometan la confidencialidad, integridad y disponibilidad de la información.

Fuente propia

La iniciativa aplica para todos los niveles funcionales y organizacionales de Canal Capital, involucrando funcionarios, contratistas, personal en misión, operadores y proveedores, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolectan, procesan, intercambien o consulten su información, al igual que a las entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

8.1 ACTIVIDADES A DESARROLLAR

				2026											
NO.	ACTIVIDAD	RESPONSABLE	RESULTADO	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1	Fortalecer e implementar los controles de seguridad de la información, según el análisis de brechas y la auditoría interna.	Profesional Seguridad Informática	Instrumento MSPI - Gestión en Eramba GRC												
2	Actualizar la matriz de riesgos de seguridad digital de la entidad.	Profesional Seguridad Informática	Monitoreo de riesgos de seguridad digital												
3	Actualizar las estrategias de recuperación ante Desastres	Gestión TIC	Evidencias (documentos, imágenes, entre otros) de la implementación de estrategias del DRP y ejecución de pruebas												
4	Ejecución del plan de sensibilización del SGSI	Profesional Seguridad Informática	Evidencias (listado de asistencia, actas de reunión, correos electrónicos, entre otros).												
5	Actualización del instrumento MSPI para integrar los controles de la norma ISO 27001 que apliquen a la entidad seguún viabilidad y pertinencia	Profesional Seguridad Informática	Instrumento MSPI actualizado												
6	Evaluación y seguimiento Realizar el autocontrol de las actividades a través del plan de trabajo anual de Gestión TIC	Profesional Seguridad Informática	Plan de trabajo de Gestión TIC												

8.2 CONTROL Y SEGUIMIENTO

En el marco de las líneas de defensa se debe realizar: Autocontrol por la primera línea de defensa (Gestión TIC) a través del plan de trabajo anual de Gestión TIC, Autoevaluación o monitoreo por la segunda línea de defensa (Planeación) se realiza con lo formulado en el Plan de Acción Institucional y evaluación independiente por la tercera línea de defensa por la Oficina de Control Interno.

Posterior a su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el plan de seguridad y privacidad de la información, en este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.