PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAPITAL

Enero de 2024

VERSIÓN 3.0

CONTROL DEL DOCUMENTO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
VERSIÓN 3.0 ENERO 2024

ÁREA DE SISTEMAS

Historial de versiones

FECHA	VERSIÓN	AUTOR	DESCRIPCIÓN
Diciembre2020	1.0	Maryury Forero Bohórquez	Creación inicial V1 del documento. Aprobado en sesión 04 CIGD del 16-22/12/2020
Diciembre 2022	2.0	Maryury Forero Bohórquez	Actualización del documento V2
Enero 2024	3.0	Mauris Avila Velásquez	Actualización del documento v 3

TABLA DE CONTENIDO

INTRODUCCIÓN

La Política de la seguridad 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 y de acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital, 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.

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. 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 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 Capital, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI, 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

Activos de Información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Según ISO/IEC 13335-1:20041 causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Confidencialidad: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

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: Garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

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

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. 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.

- Decreto 103 de 2015, 2019 Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad

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.

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 NTC/ISO-27001, 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 85% de acuerdo con la Evaluación del Modelo de Seguridad y Privacidad para el año 2023, 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	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	98	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	89	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	98	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	88	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	85	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	87	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	88	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	GESTIONADO
A.18	CUMPLIMIENTO	89	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**85**	**100**	OPTIMIZADO

Evaluación dominios 27001 MSPI-MinTIC

De la gráfica anterior se identifican los aspectos por mejorar teniendo como precedente los cambios realizados en la medición del Formulario Único de Reporte y Avance de Gestión FURAG para la vigencia 2022 en comparación con las mediciones anteriores dado que los resultados de la vigencia no son comparables con los resultados de las mediciones de vigencias anteriores, ya que se realizaron cambios significativos a las preguntas de las políticas de Seguridad Digital y Gobierno Digital, los procesos de actualización de las temáticas y directrices; la actualización de la Norma ISO 27001 – 2022, que contempla 93 controles en contraste con la publicada en 2013 que definía 144 y los lineamientos del MIPG, el Marco de referencia de Arquitectura TI y la guía para la administración del riesgo.

a). Gestión de la continuidad del negocio.

b). Gestión de activos.

c). Apropiación organizacional de políticas y controles de seguridad de la información, almacenamiento y gestión de la información y administración del cambio.

7. 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.

Fuente: Mintic Plan de seguridad y privacidad de la información.

La iniciativa aplica para todos los niveles funcionales y organizacionales de 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.

7.1. ACTIVIDADES A DESARROLLAR

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

FASE	ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FINALIZACIÓN	PRODUCTO O RESULTADO
Implementación	Participar en las mesas de trabajo de la Alta Consejería Distrital para la articulación del Sistema de Gestión de Seguridad de la Información con respecto al plan de cumplimiento a nivel distrital	Profesional Seguridad Informática	02/01/2024	30/12/2024	Evidencias (listado de asistencia, presentaciones, citaciones, entre otros)

FASE	ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FINALIZACIÓN	PRODUCTO O RESULTADO
	Fortalecer e implementar los controles de seguridad de la información, según el análisis de brechas y la auditoría interna.	Profesional Seguridad Informática	02/01/2024	30/12/2024	Instrumento MSPI
	Implementar la matriz de riesgos de seguridad digital de la entidad.	Profesional Seguridad Informática	02/01/2024	30/12/2024	Monitoreo de riesgos de seguridad digital
	Implementar las estrategias de recuperación ante Desastres	Área de sistemas	02/01/2024	30/12/2024	Evidencias (documentos, imágenes, entre otros) de la implementación de estrategias del DRP.
	Capacitar y sensibilizar en seguridad de la información.	Profesional Seguridad Informática	02/01/2024	30/12/2024	Evidencias (listado de asistencia, actas de reunión, correos electrónicos, entre otros).
	Actualizar el instrumento MSPI para integrar los controles de la Norma ISO 27001-2022 que apliquen a la entidad según su viabilidad y pertinencia.	Profesional Seguridad Informática	02/01/2024	30/12/2024	Instrumento MSPI actualizado
Evaluación y Seguimiento	Realizar el autocontrol de las actividades a través del plan de trabajo anual del área de sistemas	Profesional Seguridad Informática	02/01/2024	30/12/2024	Plan de trabajo área de sistemas

7.2 CONTROL Y SEGUIMIENTO

En el marco de las líneas de defensa se debe realizar: Autocontrol por la primera línea de defensa (Sistemas) a través del plan de trabajo anual del área de sistemas, 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 el área de Control Interno.

Después de 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.