PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAJA DE LA VIVIENDA POPULAR

Oficina de Tecnologías de la Información y las Comunicaciones

Bogotá D.C., enero de 2021
Versión 3.0

Liliana Morales
lmorales@cajaviviendapopular.gov.co

TABLA DE CONTENIDO

1. OBJETIVO

Establecer la estrategia para diseñar e implementar las políticas, controles, lineamientos, procedimientos y buenas practicas que coadyuve a salvaguardar la disponibilidad, integridad y confidencialidad de los activos de información, con el propósito de garantizar la continuidad en los procesos misionales de La Caja de la Vivienda Popular, el Plan de Seguridad y Privacidad de la Información está alineado a los requisitos de la Política de Gobierno Digital, Seguridad Digital y la aplicación de la norma NTC-ISO:27001:2013.

2. ALCANCE

La Caja de la Vivienda Popular produce, recibe, maneja, intercambia y divulga información clasificada, reservada y pública, relacionada con la población de estratos 1 y 2 que habita en barrios de origen informal o en zonas de riesgo, así como la de sus funcionarios, contratistas y/o terceros.

Este Plan de Seguridad y Privacidad de la Información, facilita el fortalecimiento de la seguridad de la información en la Caja de la Vivienda Popular, con el fin de garantizar la protección de esta y la privacidad de los datos de los ciudadanos y servidores públicos de la entidad, dando cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la Política de Gobierno Digital y Seguridad Digital.

El Plan de Seguridad y Privacidad de la Información inicia con la definición y adopción de la política de seguridad de la información, la clasificación de los activos de información que hacen parte de los procesos, la identificación y tratamiento de los riesgos de seguridad de la información y finaliza con la definición de procedimientos, controles además de buenas prácticas de seguridad de la información que permitan proteger los activos de información de la Caja de la Vivienda Popular.

3. RESPONSABLES

El Responsable por la actualización del Plan es la Oficina de Tecnología de Información y las Comunicaciones – TIC.

4. DEFINICIONES

A continuación, se relacionan los conceptos y definiciones aplicables al presente plan:

- ***Acceso a la Información Pública:*** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- ***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.
- ***Confidencialidad***: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- ***Dato Abierto***: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- ***Dato Privado***: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- ***Dato Sensible***: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de

partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- ***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.
- ***Información Clasificada***: Es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a ciertos derechos, contemplados en la misma ley.
- ***Información Reservada***: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- ***Integridad***: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- ***No repudio***: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ***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 [Según ISO 27000]:*** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de

información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias

- ***Seguridad de la Información***: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad.
- ***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.
- ***Tratamiento de Datos Personales***: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- ***Vulnerabilidad***: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. DOCUMENTOS DE REFERENCIA

La Caja de la Vivienda Popular 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.

6. INSTRUMENTO DE MEDICION

Modelo de Seguridad y Privacidad de la Información (MSPI)

La fase de diagnóstico de Seguridad y Privacidad de la información se define como la fase inicial del Modelo de Seguridad y Privacidad de la información (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 de seguridad de la información

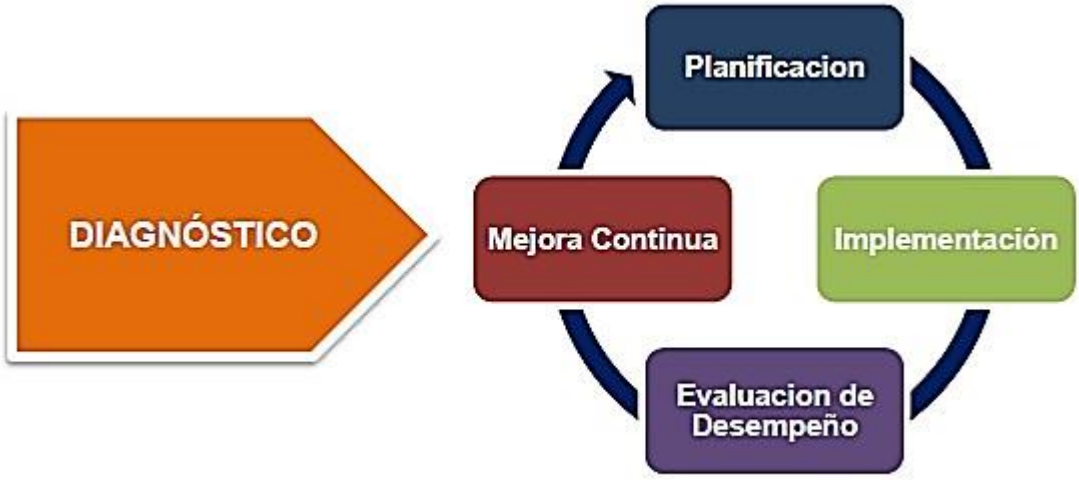
- ✓ Identificar el avance de la implementación del ciclo de operación al interior de la entidad
- ✓ Identificar el nivel de cumplimiento con la Normatividades vigente relacionada con protección de datos personales e identificación del uso de buenas prácticas en seguridad de la información.

Los activos de información son lo más importantes en la Entidad que deben ser gestionados para proteger y garantizar la continuidad del negocio. A través de la implantación de un 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 integridad, confidencialidad y disponibilidad, 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.



Fases del Modelo de Seguridad y Privacidad de la Información-MSPI

Objetivos de la Fase Diagnostico-MSPI

7. DIAGNÓSTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el primer semestre del año en curso, se recolectó información mediante el diligenciamiento de la herramienta (Instrumento Evaluación-MSPI) proporcionada por el Ministerio de las TIC para determinar el estado actual de

gestión de seguridad y privacidad de la información al interior de la Entidad. Para el diligenciamiento de este instrumento (MSPI), se usó como guía el "Instructivo para el Diligenciamiento de la herramienta de Diagnóstico de Seguridad y Privacidad de la Información" el cual proporcionó de manera precisa los pasos a seguir para recolectar toda la información posible y determinar si se cumplen y en qué calificación se encuentran los objetivos.

De acuerdo a esto:

- ✓ Con el diligenciamiento de la herramienta (Instrumento Evaluación MSPI), permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de la Caja de la Vivienda Popular, según lo definido en la Política de Seguridad Informática establece como lineamiento y estándar la "Seguridad y Privacidad de la Información".

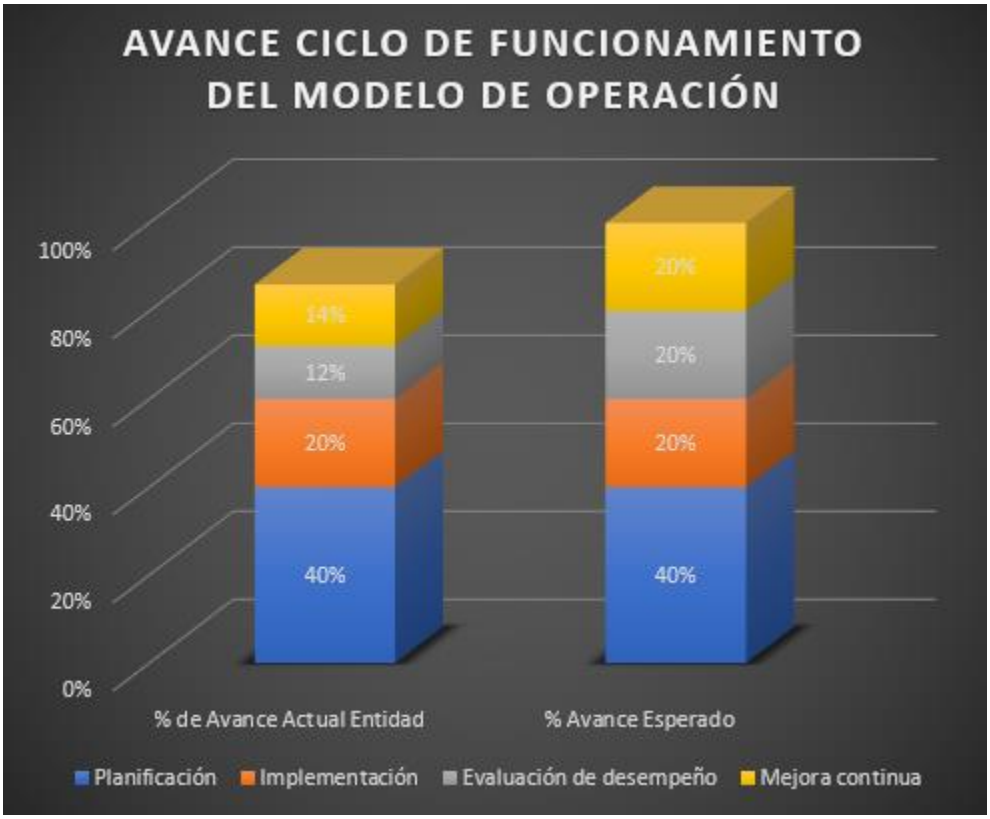
- ✓ Se realizó levantamiento de información a nivel de procedimientos, formatos, guías y controles técnicos de acuerdo a los requisitos planteados en el instrumento.

Brecha Anexo A ISO 27001:2013: En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la Información.

A continuación, se desglosa de manera precisa el proceso realizado y los resultados obtenidos para cada aspecto evaluado e identificado mediante el diagnóstico de seguridad y privacidad de la información.

En la siguiente gráfica se puede evidenciar la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo correspondiente, estipulada en el MSPI:

Avance PHVA: Este componente permite evidenciar el avance en el ciclo del modelo de seguridad definido en el Modelo de Seguridad y Privacidad de la Información, el cual está alineado con los plazos para la implementación de las actividades que se establecieron en la Política de Gobierno Digital, y a través del Decreto 1008 del 14 de junio de 2018 de MinTIC : *"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"*



Como se puede observar, en la medición realizada en el mes de diciembre de 2019, se obtuvo un promedio total de 86% en la evaluación de los controles, lo cual evidencia la gestión del equipo de seguridad de la información durante la vigencia.

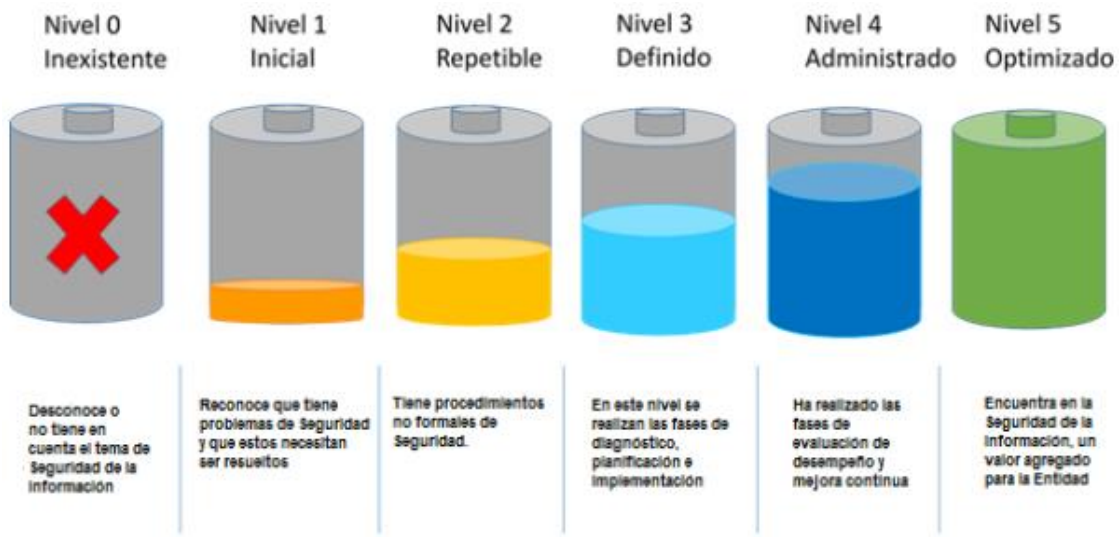
De acuerdo con la anterior gráfica los dominios que más incrementaron fueron políticas de seguridad de la información, control de acceso, seguridad física y del entorno y seguridad de las comunicaciones. El dominio que no presentó avance fue criptografía, y finalmente los que requieren mayor trabajo fueron desarrollo y mantenimiento de sistemas, y finalmente gestión de incidentes de seguridad de la información.

8. PLAN

De acuerdo con lo evidenciado en los capítulos anteriores, se demuestra que la Caja de la Vivienda Popular ha tenido avances significativos frente a la implementación del Modelo de Seguridad y Privacidad de la Información, sin embargo, se deben definir ciertas actividades que garanticen el cumplimiento del total de los lineamientos establecidos en dicho modelo.

Es importante tener en cuenta el Modelo de Madurez de Seguridad y Privacidad de la Información, establecido por el Ministerio de las TIC, el cual mide la brecha entre el nivel actual de la entidad y el nivel optimizado.

La figura a continuación muestra los diferentes niveles que hacen parte de este modelo de madurez:



En la siguiente tabla se presentan las características de cada uno de los niveles de madurez con una descripción general:

NIVEL	DESCRIPCION
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.

NIVEL	DESCRIPCION
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información. • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. • La entidad genera tráfico en IPv6

A continuación, se presenta el esquema de actividades establecido por la Oficina TIC de la Entidad:

PLAN DE TRABAJO DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN - PERIODO: FEBRERO A DICIEMBRE DE 2020

FASE	DESCRIPCIÓN META	MAGNITUD PROGRAMADA	No.	DESCRIPCIÓN ACTIVIDAD	META	PRODUCTO (ENTREGABLE)	RESPONSABLE ACTIVIDAD	ALINEACIÓN MARCO DE	% PONDERACIÓN ACTIVIDAD	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Implementación	Implementar el 100% del Sistema de Gestión de Seguridad de la información en la Caja de Vivienda Popular	100%	1	Revisar la documentación vigente del MSPI(Alcance, Objetivos, Políticas, Manual, Procedimientos, etc.)	Verificar el 100% de los documentos vigentes	Evaluación y Diagnóstico de -Matriz de cumplimiento de requisitos de la norma INTD SIG y MSPI	Profesional Seguridad de la información	LI.ES.01 LI.ES.02 LI.ES.06 LI.ES.08 LI.GO.01 LI.GO.04 LI.GO.09 LI.GO.07	6,0%											
			2	Desarrollar acciones para garantizar la implementación y mantenimiento de los requisitos de la Política de Gobierno Digital aplicables al MSPI.	Implementar el 100% de los requisitos de Gobierno Digital aplicables al MSPI.	Cumplimiento de requisitos MSPI	Profesional Seguridad de la información		8,0%												
			3	Participar en las actividades 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	Participar en al menos (1) actividad	Asistencia an las actividades	Profesional Seguridad de la información		8,0%												
			4	Actualizar el plan de tratamiento de riesgos de seguridad de la información	Actualizar el Plan de tratamiento de riesgos de SI de acuerdo a la guia del DAFP	Plan de tratamiento de riesgos de SI	Profesional Seguridad de la información	LI.ES.07 LI.ES.09 LI.ES.10 LI.GO.01	10,0%												
			5	Establecer el plan de contingencias de los sistemas de información y servicios de TI	Plan de contingencias de sistemas de información y servicios de TI	Plan de Contingencia	Profesional Seguridad de la información	LI.GO.04 LI.GO.07 LI.GO.08	8,0%												
			6	Documentar políticas,procedimientos, lineamientos, instructivos, etc. Asociados al MSPI, MPGy Gobierno Digital	Publicar la documentación referente al MSPI, MPG y Gobierno Digital	Documentación en cumplimiento a MSPI, MPG y Gobierno Digital	Profesional Seguridad de la información	LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02	10,0%												
			7	Implementar transición Protocolo IPV4 - IPV6	Publicar el manual de seguridad de información	Manual de seguridad de información elaborado y publicado	Profesional Seguridad de la información	LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23	10,0%												
			8	Elaborar y publicar procedimiento de gestión de cambios	(1) un procedimiento de gestión de cambios	Procedimiento de gestión de cambios publicado y aprobado	Profesional Seguridad de la información		10,0%												
			9	Implementar la herramienta de medición de la política de gobierno digital	Diligenciamiento de la herramienta de GD	Herramienta diligenciada	Profesional Seguridad de la información	LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13	10,0%												
Evaluación del desempeño	Hacer seguimiento y medición a la implementación del MSPI.	100%	1	Realizar seguimiento y revisión de la efectividad de la implementación del MSPI.	Seguimiento y revision del MSPI	Seguimiento al MSPI	Profesional Seguridad de la información	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08	5,0%												
			2	Revisar las acciones de los riesgos identificados de SI	Seguimiento a las acciones de riesgos de SI	Seguimiento a l plan de tratamiento de riesgos de SPI	Profesional Seguridad de la información		10,0%												
Mejora Continua	Determinar los factores y/o aspectos a mejorar que hacen parte del MSP	100%	1	Diseñar el plan de mejoramiento de acuerdo a revisiones realizadas por Control Interno	Plan de mejoramiento	Plan de mejoramientp	Profesional Seguridad de la información		5,0%												
TOTAL									100,0%											

La metodología definida, establece tres (3) fases: implementación, evaluación del desempeño y mejora continua, con actividades en cada una. En cada fase se busca avanzar en los diferentes Niveles de Madurez, con el propósito de llegar al nivel Optimizado, que es el más alto del modelo y en el cual la Entidad se encontraría en una búsqueda constante de la mejora continua.

Para cada macro actividad se deben definir los tiempos, recursos y entregables esperados, sin embargo.

9. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mm-aaaa)	Cambios	(Nombre y Cargo) Revisó
1	27-07-2018	Creación del documento	Diana Carolina Donoso Casas Jefe Oficina TIC
2	30-01-2020	Actualización del contenido del documento.	Andrés Orlando Briceño Díaz. Jefe Oficina TIC
3	28-01-2021	Actualización del contenido del documento.	Liliana Morales Jefe Oficina TIC