FEDERACIÓN COLOMBIANA DE MUNICIPIOS

simit

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021 – 2025

BOGOTÁ, D.C. ENERO 2021

REGISTRO Y CONTROL DE CAMBIOS		
Fecha	**Descripción de la actualización**	**Versión**
01/06/2016	Versión Inicial Plan Estratégico de Seguridad y Privacidad de la Información	1.0
13/06/2017	Revisión y actualización de los avances del MSPI en el Plan Estratégico de Seguridad y Privacidad de la Información	2.0
19/12/2018	Revisión y actualización de los avances del MSPI en el Plan Estratégico de Seguridad y Privacidad de la Información	3.0
31/01/2020	Revisión y actualización de los avances del MSPI en el Plan Estratégico de Seguridad y Privacidad de la Información	4.0
31/01/2021	Revisión y actualización de los avances del MSPI en el Plan Estratégico de Seguridad y Privacidad de la Información	5.0

Elaboró	**Revisó**	**Aprobó**
Harol Méndez Collo – Dirección de Tecnologías de la Información	Alejandro Murillo Pedroza – Dirección de Tecnologías de la Información	Alejandro Murillo Pedroza – Dirección de Tecnologías de la Información

TABLA DE CONTENIDO

Pág.

Introducción 5
1. Objetivo 6
2. Objetivos Específicos 6
3. Alcance 6
4. Marco Legal 7
5. Conocimiento de la Entidad 8
5.1. Aspectos Generales de la Organización 8
5.2. Reseña Histórica 10
5.3. Nuestra Declaración – Misión 13
5.4. Nuestro Propósito Superior – Visión 13
5.5. Nuestra Identidad 13
5.6. Objetivos y Funciones 13
5.7. Nuestros Valores 14
5.8. Nuestros Principios 14
5.9. Estructura Organizacional 15
5.10. Mapa de Procesos 16
6. Estructura Organizacional del PESI 17
7. Funciones y Roles del MSPI 17
7.1. Director Ejecutivo – Dirección Ejecutiva 17
7.2. Comité de Gobierno Digital y Seguridad de la Información 18
7.3. Director Técnico – Dirección de Tecnologías de la Información 20
7.4. Profesional Oficial de Seguridad Informática 22
8. Metodología para Análisis y Evaluación de Riesgos 26
9. Contexto para el Análisis y Evaluación de Riesgos 28
10. Plan Proyecto de Inversión y Presupuesto del MSPI 28
11. Implementación Plan de Proyectos y Actividades del MSPI 31
11.1. Proyecto de adopción de IPv4 a Ipv6 en la FCM 31
11.2. Campaña de Capacitación e Ingeniería Social en la FCM 32
11.3. Análisis de Vulnerabilidades y Ethical Hacking en la FCM 32
11.4. Plan de Trabajo y Actividades de mejora Continua para el MSPI 32
12. Descripción y Entregables de las Fases del MSPI 42

TABLA DE ILUSTRACIONES

Pág.

Ilustración 1 Estructura Organizacional 15
Ilustración 2 Mapa de Procesos 16
Ilustración 3 Estructura Organizacional del PESI 17
Ilustración 4 Metodología DAFP 27
Ilustración 5 Metodología Magerit 27
Ilustración 6 Estado actual del MSPI en la FCM 29
Ilustración 7 Nivel de Madurez del MSPI en la FCM 29
Ilustración 8 Proyección del nivel de madurez en la FCM 30
Ilustración 9 Brechas Principales de Implementación 30

TABLAS

Pág.

Tabla 1 Marco Legal..... 8
Tabla 2 Reseña histórica de la Federación Colombiana de Municipios 13
Tabla 3 Plan de trabajo transición IPv4 a IPv6 32
Tabla 4 Plan de Trabajo – MSPI..... 41
Tabla 5 Fase Diagnóstico 42
Tabla 6 Fase de Planificación..... 43
Tabla 7 Fase de Implementación 44
Tabla 8 Fase de Evaluación 45
Tabla 9 Fase de Mejora Continua 46

DERECHOS DE AUTOR

A menos que se indique de forma contraria, el copyright (traducido literalmente como derecho de copia y que, por lo general, comprende la parte patrimonial de los derechos de autor) del texto incluido en este documento es de la Federación Colombiana de Municipios.

El presente documento PESI (Plan Estratégico de Seguridad y Privacidad de la Información) corresponde a la función pública de la Federación Colombiana de Municipios, es un documento que se puede acceder sin restricción alguna desde el portal del web del Simit cuya dirección es: www.simit.org.co, debido a que es un documento clasificado como público.

El PESI, se puede reproducir gratuitamente en cualquier formato o medio sin requerir un permiso expreso para ello, bajo las siguientes condiciones:

- ✓ El texto particular no se ha indicado como excluido y por lo tanto no puede ser copiado o distribuido.
- ✓ La copia no se hace con el fin de ser distribuida comercialmente.
- ✓ Los materiales se deben reproducir exactamente y no se deben utilizar en un contexto engañoso.
- ✓ Las copias serán acompañadas por las palabras "copiado/distribuido con permiso de la Federación Colombiana de Municipios. Todos los derechos reservados".
- ✓ El título del documento debe ser incluido al ser reproducido como parte de otra publicación o servicio.

Si se desea copiar o distribuir el documento con otros propósitos, debe solicitar el permiso entrando en contacto con la Dirección de Tecnologías de la Información de la Federación Colombiana de Municipios de la República de Colombia.

Introducción

El Plan Estratégico de Seguridad y Privacidad de la Información, se elaboró con la recopilación de las guías de seguridad y privacidad de la información del programa de la Política de Gobierno Digital, mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información – MSPI de la Política de Gobierno Digital.

La Política de Gobierno Digital, liderada por la Dirección de Tecnologías de la Información de la Federación Colombiana de Municipios, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de ofrecer servicios de tecnología con altos estándares de seguridad y privacidad de la información, de tal manera que contribuye con la construcción de un Estado más participativo, más eficiente y más transparente, hacia las autoridades de tránsito y municipios del País.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Federación Colombiana de Municipios, está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos estratégicos, misionales, apoyo, control y evaluación; y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, en la Federación Colombiana de Municipios, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la Política de Gobierno Digital.

Decreto 1008 del 14 de junio 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 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Así mismo, el Modelo de Seguridad y Privacidad de la Información en la Federación Colombiana de Municipios, se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los componentes de la Política de Gobierno Digital: TIC para el Estado y TIC para Sociedad.

El Modelo de Seguridad y Privacidad de la Información, pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la Federación Colombiana de Municipios, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Objetivo

Establecer, apropiar y presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad según el modelo de Seguridad y Privacidad de la Información, en adelante MSPI emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, adoptado por la Federación Colombiana de Municipios; este documento expone las prioridades de implementación de los controles en relación a seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

2. Objetivos Específicos

- ✓ Promover el uso de las mejores prácticas de seguridad y privacidad de la información en la FCM.
- ✓ Definir las responsabilidades relacionadas con la seguridad y privacidad de la información.
- ✓ Comunicar e implementar la estrategia de seguridad y privacidad de la información.
- ✓ Identificar el nivel de madurez en la gestión de la seguridad y privacidad de la información.
- ✓ Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MPSI, con el objetivo de proteger la información y los sistemas de información.

3. Alcance

El objetivo que se busca con la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI es mejorar los niveles de seguridad de la información y la protección de los activos de información, para lograrlo es indispensable implementar los controles según lo señalado por el estándar ISO/IEC 27001:2013 y la normatividad vigente aplicable.

Por la razón expuesta anteriormente, los funcionarios, contratistas y terceros que interactúen con los activos de información de la FCM, deberán conocer y cumplir las políticas, procesos y procedimientos que hacen parte del Modelo de Seguridad y Privacidad de la Información – MSPI, salvaguardando ante todo los principios de confidencialidad, integridad y disponibilidad que los protegen frente a cualquier tipo de tratamiento.

4. Marco Legal

Norma	Descripción
Decreto 1008 del 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 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.[1]
Ley 1928 de 2018	Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.
Ley 1978 de 2019	Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones (tic), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
Ley 1955 de 2019	Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad"; Art. 147
Copes 3975 de 2019	Política nacional para la transformación digital e inteligencia artificial
Conpes 3920 de 2019	Política nacional de explotación de datos (big data)
Conpes 3968 de 2019	Declaración de importancia estratégica del proyecto de desarrollo, masificación y acceso a internet nacional, a través de la fase II de la iniciativa de incentivos a la demanda de acceso a internet
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.[2]
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Resolución 2405 de 2016	Por el cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité
Conpes 3701 de 2011	"Lineamientos de la política para la Ciberseguridad y Ciberdefensa"[3]
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Ley 1273 de 2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Circular No. 058 de 2009	Cumplimiento Decreto 1151 del 14 de abril de 2008

[1] Decreto 1008. Ministerio de Tecnologías de la Información y las Comunicaciones, Bogotá, Colombia, 14 de junio de 2018.

[2] Resolución 2710. Ministerio de Tecnologías de la Información y las Comunicaciones, Bogotá, Colombia, 03 de octubre de 2017

[3] Consejo Nacional de Políticas Económica y Social. República de Colombia. Bogotá, 14 de julio de 2011

Norma	Descripción
Decreto 1151 de 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Directiva 02 de 2000	Plan de Acción de la estrategia de Gobierno en Línea
Conpes 3072 de 2000	Agenda de Conectividad
NTC/ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.[4]
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.[4]

Tabla 1 Marco Legal

5. Conocimiento de la Entidad

5.1. Aspectos Generales de la Organización

La Federación Colombiana de Municipios es una persona jurídica de carácter privado, sin ánimo de lucro, creada mediante el concurso y consenso de los entes territoriales en ejercicio del derecho constitucional de asociación. A ella pertenecen por derecho propio todos los municipios, distritos y asociaciones de municipios del país y tiene como finalidad la defensa de sus intereses. En este sentido, la Federación Colombiana de Municipios se rige por el derecho privado, salvo en lo que concierne a la función pública asignada según los artículos 10 y 11 de la Ley 769 de 2002, cuyo fundamento constitucional se esgrime en el artículo 209 de la Constitución Política.

Luego, si bien es cierto que la Federación Colombiana de Municipios se rige por las normas del derecho privado, en lo concerniente a la función pública delegada por disposición legal, se encuentra sometida a las normas propias del derecho público, siendo aplicable entonces para el presente proceso de contratación, los procedimientos contemplados en la Ley 80 de 1993, modificada por la Ley 1150 de 2007, Ley 1474 de 2011 y el Decreto Reglamentario 1082 de 2015.

La Federación Colombiana de Municipios por expreso mandato legal, ha requerido desde sus inicios, contar con una infraestructura tecnológica suficiente que garantice un adecuado y permanente funcionamiento, y que sea susceptible de perfeccionamiento a través de la implementación de nuevas tecnologías aplicadas siempre al logro del fin perseguido, con métodos de control y calidad de la información.

[4] ISO International Organization for Standardization e IEC International Electrotechnical Commission. ISO / IEC 27001: 2013. (2013). [PDF file]. Bogotá, DC: Autor. Recuperado de: https://www.iso.org/standard/54534.html

En el marco del cumplimiento de dicha función pública delegada y teniendo en cuenta que la Dirección Nacional Simit, administra un sistema de información que está disponible en internet y a pesar de las implementaciones en seguridad puede llegar a ser objeto de intentos de sabotaje o ataques cibernéticos, se hace necesario para la entidad prepararse en la protección del sistema y de sus activos de información contra posibles ataques y amenazas, la protección debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Información) que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia de Gobierno en Línea y en cumplimiento de lo señalado en el artículo 5 del decreto 2573 del 2014 y lo expresado en el Decreto 1078 de 2015.

Así mismo, la Federación Colombiana de Municipios dentro de la administración y actualización del sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito debe garantizar la integridad de la información almacenada en el Sistema y blindar la infraestructura asegurando su disponibilidad para la consulta del estado de cuenta, cargue de información de las autoridades de tránsito a nivel nacional y por supuesto, la generación de paz y salvos que permitan, a los ciudadanos, realizar los trámites de tránsito.

Dado esto se hace necesario buscar un apoyo que le permita a la Federación Colombiana de Municipios tomar las decisiones correctas, apropiadas y oportunas en cuanto a la seguridad de la información, acordes a la rápida evolución de los sistemas de información a nivel mundial y por lo tanto volviéndose un insumo indispensable para proteger el sistema y los procesos, basándose en las mejores prácticas existentes en la actualidad. Para suplir esta necesidad la Federación Colombiana de Municipios requiere contar con asesorías sobre los modelos de seguridad informática, las cuales deben incluir las revisiones y mejoras de políticas, normas, procedimientos y estándares, así como divulgaciones y capacitaciones para todos los usuarios de la entidad.

Atendiendo a que las actividades propias de seguridad y privacidad de la información demandan conocimientos especializados en donde predomina el factor intelectual, se asigna al Profesional Oficial de Seguridad Informática, quien, a través de su conocimiento y experiencia en implementación de soluciones de tecnología, experiencia en la Gerencia de Proyectos de TI, consultoría y auditoría en la norma ISO 27001 y en la Interventoría de Proyectos, se encuentran enfocados y especializados en la Seguridad de la Información.

El Profesional Oficial de Seguridad Informática, como responsible de Seguridad de la Información para la Federación Colombiana de Municipios, busca mantener vigentes los requerimientos de la entidad en los procesos que serán analizados para posteriormente complementar, ajustar e implementar la seguridad y privacidad de la información con las mejores prácticas, para administrar y mitigar razonablemente los riesgos informáticos relacionados con pérdida de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Por estas razones, dada la necesidad de acceder a la información cualificada en el marco de las funciones encomendadas por expreso mandato legal; se hace necesario dirigir, coordinar y gestionar a través del Profesional Oficial de Seguridad Informática, el logro de objetivos estratégicos y tácticos en materia de

confidencialidad, integridad y disponibilidad de los sistemas y activos de información con los que cuenta la Federación Colombiana de Municipios.

Descripción de la Entidad con Función Pública Delegada

Razón social: Federación Colombiana de Municipios
Dirección: Kra 7a, No. 74-56 Bogotá D.C
Teléfono: (57+1) 593 40 20
Responsable: Dr. Gilberto Toro Giraldo
Teléfono Responsable: (57+1) 593 40 20
Cargo: Director Ejecutivo.

Descripción y Actividad Comercial: La Federación Colombiana de Municipios, es una entidad privada sin ánimo de lucro, mediante el cual; el congreso de la república mediante un acto administrativo de estado, le delego un órgano de gobierno para su administración pública, con el fin de fortalecer la gestión y necesidades estratégicas de los municipios de Colombia y el sistema de información sobre multas y sanciones por infracciones de tránsito del País, el órgano de gobierno que le fue delegado es la Dirección Nacional Simit.

Como actividad comercial, realiza convenios y contrataciones a nivel nacional e internacional, con el fin de apoyar las necesidades estratégicas y tácticas que poseen las alcaldías y las autoridades de transito del país, de tal manera que materializa la estrategia hacia una operación de negocio a nivel nacional en varios ámbitos, como: político, tecnológico, gestión social, infraestructura, entre otros.

5.2. Reseña Histórica

Los alcaldes del país sentían la necesidad de tener una mayor interlocución con el Gobierno Central y tener una representatividad donde se aunarán esfuerzos para conquistar objetivos comunes.

Por iniciativa de los primeros alcaldes elegidos por voto popular de los municipios de Santiago de Cali, Carlos Holmes Trujillo; Cartagena de Indias, Manuel Domingo Rojas Salgado; y Bogotá Distrito Especial, Andrés Pastrana Arango, se organizó el Primer Congreso Nacional de Municipios los días 16 y 17 de febrero de 1989.

Allí se suscribió el Acta de Constitución de la Federación Colombiana de Municipios y los primeros estatutos, que tuvieron como consideraciones importantes, impulsar el proceso de descentralización política, administrativa y fiscal en el país; fortalecer la capacidad de gestión administrativa en los entes locales; vigorizar la autonomía de los municipios de Colombia; enfrentar en conjunto los problemas comunes; incrementar la participación de los entes locales en el proceso de toma de decisiones del país; fomentar la integración, asistencia y colaboración entre los municipios.

Se iniciaron entonces las labores con el apoyo de la Federación Española de Municipios y Provincias (FEMP) y de la Fundación Friedrich Ebert en Colombia (Fescol).

De esta forma se comenzaba a abrir paso para una de las reformas más importantes del siglo XX en el país: el inicio del proceso de descentralización con una nueva forma de política a nivel local que permitía incrementar la participación ciudadana, cerrarle el paso a la corrupción y promover formas de desarrollo local.

La creación de la Federación no sólo era una buena idea, era una necesidad de los alcaldes agremiarse, por cuanto en este nuevo marco institucional, eran autónomos y responsables de una gran cantidad de competencias nuevas que implicaban un gran reto para los municipios y una gran responsabilidad política.

El éxito o fracaso del nuevo modelo de Estado, dependería en buena medida de la gestión de las nuevas administraciones locales que tendrían por primera vez alcaldes elegidos popularmente.

Así nació la Federación Colombiana de Municipios. Inicialmente se cobró $100.000 de inscripción por cada municipio y por cada asociación de municipios para un total de 181 municipios y 6 asociaciones, con lo cual se obtuvo un capital inicial social de $21 millones 860 mil.

Por su parte, la Alcaldía Mayor de Bogotá Distrito Especial reconoció la personería jurídica de la nueva Federación con la resolución 0759 de 11 de diciembre de 1.989.

En sus inicios la Federación fue considerada como una entidad pública debido a que estaba compuesta por las entidades territoriales del nivel local. Pero posteriormente, a través de la jurisprudencia de la Corte Constitucional y el Consejo de Estado, se avanzó hacia la concepción de la Federación como una entidad gremial de naturaleza asociativa, de derecho privado y sin ánimo de lucro. (Sentencias C-671/99, C305/03. Consejo de Estado. Sala de Consulta de Servicios Civil. Magistrado Ponente Susana Montes Echeverría. 15 de agosto de 1.999).

Como en las etapas iniciales de todo proceso, se requirió el esfuerzo y la voluntad de muchos para emprender su consolidación. Fue especialmente destacable su papel en algunos aspectos de la vida local que fueron los retos del momento: apoyo a la creación de centros de conciliación, cultura de prevención de desastres, construcción de vivienda de interés social, búsqueda de recursos financieros y mejoramiento de la prestación de servicios públicos.

Los primeros años sirvieron para registrar cada vez más municipios y consolidar la estructura organizativa de la entidad. También se lograron facilidades para el desplazamiento de los mandatorios locales de Bogotá para realizar gestiones ante organismos nacionales y capacitación para alcaldes y funcionarios municipales.

	Poco a poco la búsqueda de cooperación con instituciones iberoamericanas y europeas se constituyó en un elemento fundamental para el desarrollo de la Federación, no sólo por el aporte económico sino la transferencia de conocimientos y capacitación que sigue siendo pilar de la entidad.
	Han sido 25 años llenos de esfuerzos, luchas y grandes logros, que son reconocidos nacional e internacionalmente y que le han permitido a los mandatarios locales fortalecerse en su gestión de forma democrática.

Tabla 2 Reseña histórica de la Federación Colombiana de Municipios[5]
Nota: Recuperado de "Historia" de "La Federación Colombiana de Municipios"., Recuperado de https://www.fcm.org.co/historia/

5.3. Nuestra Declaración – Misión

Somos la entidad que cataliza el desarrollo territorial y el empoderamiento municipal, siendo voceros y representantes de los gobiernos locales, generando conocimiento, innovación y oportunidades de desarrollo sostenible, para lograr el desarrollo integral del país desde los municipios.[6]

5.4. Nuestro Propósito Superior – Visión

Hacemos posible el desarrollo integral del país desde las regiones, empoderando municipios capaces de generar bienestar a sus comunidades.[7]

5.5. Nuestra Identidad

Somos referentes del empoderamiento y desarrollo municipal.[7]

5.6. Objetivos y Funciones

Valor Social – Aliados en el Desarrollo Municipal

- ✓ Objetivo: Incrementar el valor que entregamos a los municipios mediante nuevas líneas de soluciones que faciliten el empoderamiento de los municipios.

[5] Federación Colombiana de Municipios. Historia de la FCM. Tomado de https://www.fcm.org.co/?page_id=726
[6] Federación Colombiana de Municipios. Misión y Visión. Tomado de https://simit.org.co/mision-y-vision
[7] Federación Colombiana de Municipios. Misión y Visión. Tomado de https://simit.org.co/mision-y-vision

- ✓ Objetivo: Fortalecer la estrategia de consecución de recursos para la generación de proyectos de impacto en el territorio.
- ✓ Objetivo: Gestionar con efectividad el Sistema Integral de Información sobre Multas y Sanciones por Infracciones de Tránsito.

Presencia y cercanía - Vocería y Representación

- ✓ Objetivo: Ampliar y afianzar la presencia de la FCM en el territorio de manera permanente.
- ✓ Objetivo: Fortalecer el posicionamiento estratégico de la FCM como la entidad especializada en el desarrollo municipal.
- ✓ Objetivo: Incidir en la instancias Gubernamentales en los temas claves de descentralización, siendo voceros de los gobiernos locales.

Capital Humano

- ✓ Objetivo: Facilitar la transformación cultural de la FCM.

Referente de Conocimiento

- ✓ Objetivo: Facilitar la operación de la FCM como "Laboratorio de innovación y aprendizaje municipal"[8]

5.7. Nuestros Valores

- ✓ Integridad
- ✓ Responsabilidad
- ✓ Lealtad
- ✓ Respeto
- ✓ Solidaridad
- ✓ Compromiso
- ✓ Confianza
- ✓ Excelencia en la gestión.[7]

5.8. Nuestros Principios

- ✓ Autonomía Municipal
- ✓ Pluralismo Ideológico
- ✓ Respeto DDHH
- ✓ Defensa y Fortalecimiento Democracia

[8] Federación Colombiana de Municipios. Objetivos Estratégicos. Tomado de https://simit.org.co/objetivos-y-funcionalidades.

- ✓ Desarrollo Integral Municipios

5.9. Estructura Organizacional

Ilustración 1 Estructura Organizacional[9]

[9] Federación Colombiana de Municipios. Estructura Organizacional. Tomado de https://simit.org.co/estructura-organizacional

5.10. Mapa de Procesos

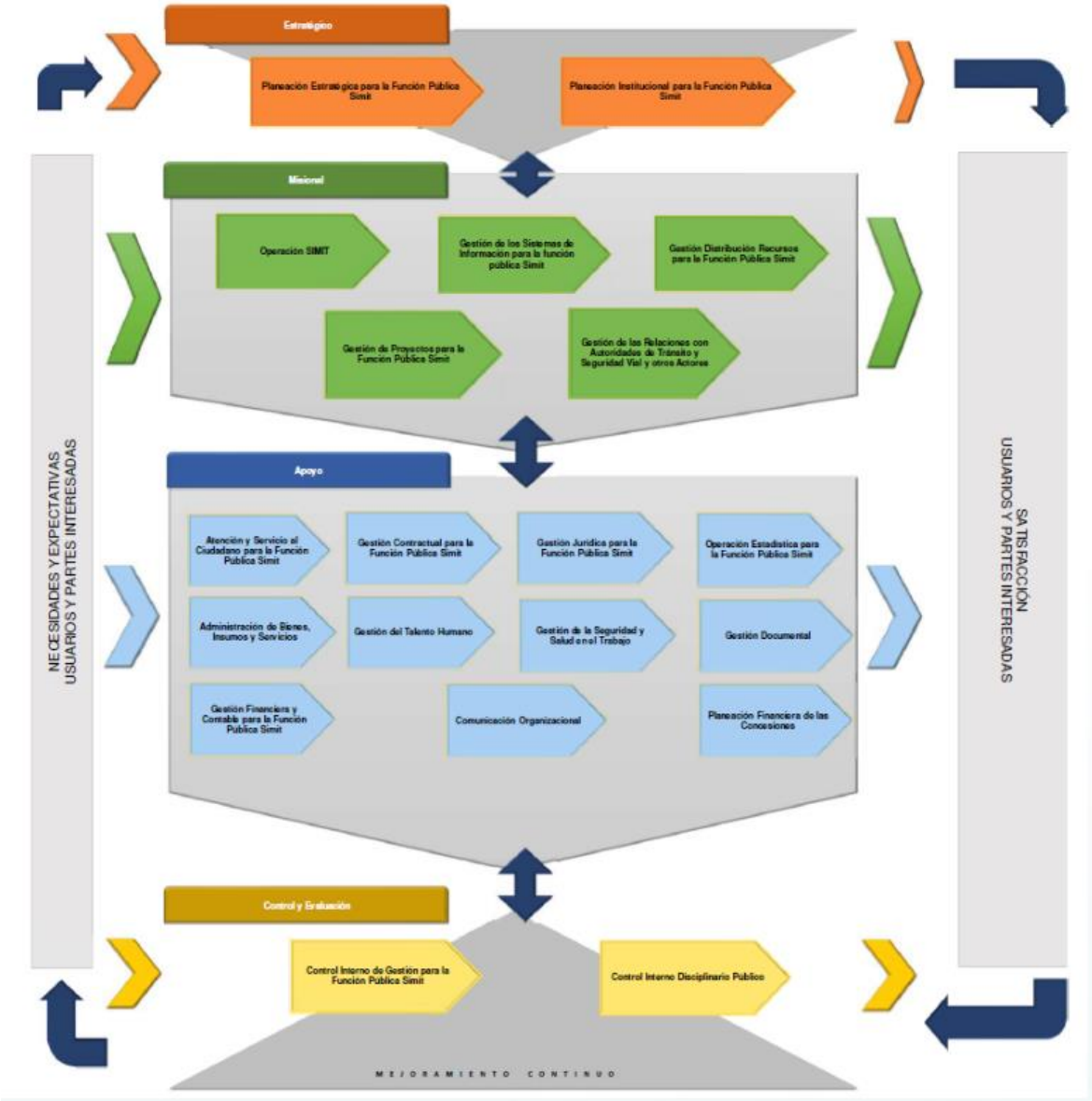


Ilustración 2 Mapa de Procesos[10]

[10] Federación Colombiana de Municipios. Mapa de Procesos. Tomado de https://simit.org.co/mapa-de-procesos

6. Estructura Organizacional del PESI

Ilustración 3 Estructura Organizacional del PESI

7. Funciones y Roles del MSPI

7.1. Director Ejecutivo – Dirección Ejecutiva

Las responsabilidades y funciones del Director Ejecutivo en el marco de la Política de Gobierno Digital y Seguridad de la Información son las siguientes:

- ✓ Orientar, planificar y articular la planeación estratégica de la Federación y sus diferentes áreas.
- ✓ Representar, defender, y promover los intereses de los municipios, distritos y asociaciones de municipios del país.
- ✓ Direccionar, articular y controlar los procesos estratégicos, misionales, de apoyo, de control y evaluación.

- ✓ Realizar el seguimiento al cumplimiento de los objetivos y metas institucionales de la Federación y sus diferentes áreas.[11]

7.2. Comité de Gobierno Digital y Seguridad de la Información

Las responsabilidades y funciones del Comité de Gobierno Digital y Seguridad de la Información son las siguientes:

- ✓ Ser el responsable directo de la gestión, cumplimiento y éxito de ejecución de la Política de Gobierno Digital y de Seguridad de la Información.
- ✓ Definir los mecanismos para dar cumplimiento a la normatividad relacionada con la Política de Gobierno Digital y de Seguridad de la Información y las demás disposiciones que sobre la materia se establezcan.
- ✓ Apoyar en el proceso de racionalización y simplificación de trámites aprovechando el uso de las Tecnologías de la información y las Comunicaciones.
- ✓ Hacer seguimiento a los lineamientos para la implementación de políticas y estándares relacionados con la Política de Gobierno Digital y de Seguridad de la Información.
- ✓ Definir y generar estrategias para el acercamiento de los ciudadanos al uso de los trámites y servicios en línea establecidos por la entidad.
- ✓ Hacer seguimiento al proceso de implementación de los componentes de la Política de Gobierno Digital, en coordinación con los miembros del Comité y las diferentes delegaciones de la Federación Colombiana de Municipios.
- ✓ Garantizar la participación de funcionarios de la entidad en procesos de sensibilización, capacitación y formación, que se desarrollen bajo el liderazgo de la Dirección de Tecnologías de Información y el Grupo Administrativo – Gestión Humana.
- ✓ Gestionar y verificar cada año los avances en la implementación de la Política de Gobierno Digital y Seguridad de la Información conforme a los proyectos aprobados por la entidad.
- ✓ Hacer seguimiento a la correcta implementación de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información dispuesto por el Ministerio de las Tecnologías de la Información y las Comunicaciones al interior de la Federación Colombiana de Municipios.
- ✓ Revisar los diagnósticos del estado de la seguridad de la información.
- ✓ Acompañar e impulsar el desarrollo de proyectos de la Política de Gobierno Digital y de seguridad y privacidad de la Información.
- ✓ Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.
- ✓ Recomendar roles y responsabilidades específicos que se relacionen con la Política de Gobierno Digital ty de seguridad y privacidad de la información.
- ✓ Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos, contribuyendo al cumplimiento de la Política de Gobierno Digital y de Seguridad de la Información.

[11] Federación Colombiana de Municipios. Tomado de: Resolución 22 de 2019.

- ✓ Supervisar, evaluar y aprobar las auditorías realizadas por la Jefatura de Control Interno de Gestión a la Política de Gobierno Digital y Seguridad de la Información, para todas las áreas de la entidad (como mínimo una vez al año) y de acuerdo con los resultados de la auditoria se deben definir las acciones pertinentes con el apoyo del Comité y del Profesional Oficial de Seguridad Informática.
- ✓ Promover la difusión y sensibilización de la Política de Gobierno Digital y Seguridad de la Información dentro de la entidad.
- ✓ Poner en conocimiento de la entidad, los documentos generados al interior del Comité de Gobierno Digital y de Seguridad de la Información que impacten de manera transversal a la misma.
- ✓ Proponer y revisar periódicamente las Políticas de Gobierno Digital y de Seguridad de la Información para que sean implementadas en la Federación Colombiana de Municipios.
- ✓ Formular las recomendaciones para incrementar la seguridad de la información.
- ✓ Conocer e informar al Director Ejecutivo sobre los activos de información de la organización y su criticidad para el cumplimiento de la misión de la entidad.
- ✓ Validar y ratificar los activos claves que se quieren proteger y los niveles de protección.
- ✓ Proponer las responsabilidades generales en materia de la Política de Gobierno Digital y Seguridad de la Información.
- ✓ Garantizar que la Política de Gobierno Digital y Seguridad de la Información sea parte del proceso de planificación y desarrollo de proyectos de sistemas de información y arquitectura empresarial.
- ✓ Promover la difusión y apoyo de la Política de Gobierno Digital y de seguridad de la información dentro de la organización.
- ✓ Acordar y aprobar metodologías y procesos específicos en la Política de Gobierno Digital y Seguridad de la Información.
- ✓ Evaluar y coordinar la implementación de controles específicos en seguridad de la información.
- ✓ Avalar el plan de continuidad del negocio (Business Continuity Plan - BCP) el cual debe estar alineado con la misión de la entidad.
- ✓ Monitorear cambios significativos en los riesgos.
- ✓ Realizar y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información.
- ✓ Revisar y monitorear las acciones y medidas preventivas y correctivas derivadas de los incidentes de seguridad de la información.
- ✓ Revisar periódicamente el estado general de la Política de Gobierno Digital y Seguridad de la Información, mediante el análisis a los informes presentados por las aéreas de la entidad.
- ✓ Supervisar y verificar que se realicen los llamados de atención o se impongan las sanciones por el incumplimiento a las políticas y normas establecidas en la Política de Gobierno Digital y Seguridad de la Información, por parte del Grupo Administrativo – Talento Humano de la Secretaría General.
- ✓ Recomendar las modificaciones o nuevas políticas de Gobierno Digital y Seguridad de la Información para que sean aprobadas por el Director Ejecutivo.
- ✓ Presentar un informe de gestión semestral sobre las actividades que se adelanten en materia de la Política de Gobierno Digital y Seguridad de la Información.
- ✓ Revisar los planes de gestión que se elaboren en relación con los proyectos o actividades de la Política de Gobierno Digital y Seguridad de la Información y realizar las recomendaciones o ajustes que se requieran.

- ✓ Revisar y/o proponer que los proyectos y actividades de la Política de Gobierno Digital y Seguridad de la Información sean incluidos en el presupuesto anual de la entidad y que exista disponibilidad de recursos para su ejecución.
- ✓ Realizar las demás actividades relacionadas con la Política de Gobierno Digital y Seguridad de la Información en la Federación Colombiana de Municipios.
- ✓ Supervisar que el Profesional Oficial de Seguridad Informática, como responsable de Seguridad y Privacidad de la Información cumpla su papel teniendo en cuenta el marco de referencia de arquitectura empresarial dispuesto por el Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia de Gobierno en Línea / Política de Gobierno Digital.

7.3. Director Técnico – Dirección de Tecnologías de la Información

Para el fortalecimiento institucional en el marco de la Política de Gobierno Digital, el Director de la Dirección de Tecnologías de la Información, deberá:

- ✓ Apropiar la Política de Gobierno Digital en las aéreas y procesos de la entidad.
- ✓ Fortalecer la autonomía en la entidad en virtud de la descentralización, incorporando el uso de TI en la prestación de sus servicios.
- ✓ Articular la Política de Gobierno Digital con los modelos integrados de planeación y gestión para mejorar la eficiencia de la gestión administrativa y pública institucional.
- ✓ Incrementar el Índice de Gobierno Digital para medir la incorporación del uso de TI en la gestión institucional.
- ✓ Informar un reconocimiento del alcance y los beneficios de la Política de Gobierno Digital para la entidad.
- ✓ Identificar el estado actual de la implementación de la Política de Gobierno Digital, desde los objetivos estratégicos y procesos de la entidad, y las políticas del Modelo Integral de Planeación y Gestión.
- ✓ Generar apropiación y valor a la entidad con la implementación de la Política de Gobierno Digital.
- ✓ Promover los servicios en línea en la entidad, el cual corresponde a los requisitos de calidad que deben cumplir los trámites y servicios en línea disponibles. Dentro de estos requisitos se encuentra la disponibilidad, seguridad, soporte, acceso, usabilidad, multicanalidad e interoperabilidad frente al ciudadano.
- ✓ Promover la implementación del Gobierno Abierto, el cual se establecen los requisitos de calidad con lo que deben contar los conjuntos de datos abiertos y las plataformas de participación que favorecen a la construcción de un gobierno transparente, abierto y participativo.
- ✓ Promover las capacidades de gestión de TI, el cual establece las capacidades institucionales en gestión de TI que debe desarrollar la entidad, para demostrar su habilidad de aprovechar adecuadamente la tecnología al interior de la institución y para proporcionar servicios que se ofrecen a los ciudadanos, asociados y alcaldes, y demás grupos de interés bajo esquemas de eficiencia, seguridad y calidad, conforme a los lineamientos establecidos en el componente de "TIC para la Estado" de la Política de Gobierno Digital.

- ✓ En el marco de la Política de Gobierno Digital, liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado.
- ✓ En el marco de la Política de Gobierno Digital, liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad y/o sector en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información y las Comunicaciones (TIC) del Estado, la Política de Gobierno Digital y según la visión estratégica, las necesidades de transformación y marco legal específicos de su entidad o sector.
- ✓ En el marco de la Política de Gobierno Digital, desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia.
- ✓ En el marco de la Política de Gobierno Digital, liderar la gestión, seguimiento y control de la ejecución de recursos financieros asociados al portafolio de proyectos y servicios definidos en el plan estratégico de Tecnologías y Sistemas de información de toda la Entidad.
- ✓ En el marco de la Política de Gobierno Digital, identificar oportunidades para adoptar nuevas tendencias tecnológicas que generen impacto de transformación digital en la entidad.
- ✓ En el marco de la Política de Gobierno Digital, coordinar las actividades de definición, seguimiento, evaluación y mejoramiento a la implementación de la cadena de valor y procesos del área de tecnologías de la información. Así mismo, atender las actividades de auditorías de gestión de calidad que se desarrollen en la entidad y liderar la implementación y seguimiento a los planes de mejoramiento en materia de tecnología que se deriven de las mismas.
- ✓ En el marco de la Política de Gobierno Digital, liderar los procesos de adquisición de bienes y servicios de tecnología, mediante la definición de criterios de optimización y métodos que direccionen la toma de decisiones de inversión en tecnologías de la información buscando el beneficio económico y de los servicios de la entidad.
- ✓ En el marco de la Política de Gobierno Digital, adelantar acciones que faciliten la coordinación y articulación entre entidades del sector y del Estado en materia de integración e interoperabilidad de información y servicios, creando sinergias y optimizando los recursos para coadyuvar en la prestación de mejores servicios al ciudadano.
- ✓ En el marco de la Política de Gobierno Digital, generar espacios de articulación con otros actores institucionales, la academia, el sector privado y la sociedad civil para contribuir en aspectos inherentes a la formulación y ejecución de planes, programas y proyectos que incorporen tecnologías y sistemas de la información y las comunicaciones (TIC) en la entidad.
- ✓ En el marco de la Política de Gobierno Digital, proponer y desarrollar programas de formación para fortalecer las competencias del talento de TI en virtud de las necesidades de la gestión de TI y

adelantar acciones con el fin de garantizar la óptima gestión del conocimiento sobre los proyectos, bienes y servicios de TI.

- ✓ En el marco de la Política de Gobierno Digital, desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la entidad.
- ✓ En el marco de la Política de Gobierno Digital, proponer e implementar acciones para impulsar la estrategia de gobierno abierto mediante la habilitación de mecanismos de interoperabilidad y apertura de datos que faciliten la participación, transparencia y colaboración en el Estado.
- ✓ En el marco de la Política de Gobierno Digital, designar los responsables de liderar el desarrollo, implementación y mantenimiento de los sistemas de información y servicios digitales de la entidad, de lo establecido en el Plan Estratégico de Tecnologías de la Información, así como las necesidades de información de los servicios al ciudadano y grupos de interés.
- ✓ En el marco de la Política de Gobierno Digital, señalar los responsables de liderar la definición, adquisición y supervisión de las capacidades de infraestructura tecnológica, servicios de administración, operación y soporte y velar por la prestación eficiente de los servicios tecnológicos necesarios para garantizar la operación de los sistemas de información y servicios digitales según criterios de calidad, oportunidad, seguridad, escalabilidad y disponibilidad.
- ✓ En el marco de la Política de Gobierno Digital, propender y facilitar el uso y apropiación de las tecnologías, los sistemas de información y los servicios digitales por parte de los colaboradores y/o a quienes están dirigidos en la entidad.
- ✓ En el marco de la Política de Gobierno Digital, promover el uso efectivo del derecho de acceso de todas las personas a las tecnologías de la información y las comunicaciones, dentro de los límites establecidos por la Constitución y la Ley.

7.4. Profesional Oficial de Seguridad Informática

De las actividades de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital (antes Gobierno en Línea), el Profesional Oficial de Seguridad Informática de la Federación Colombiana de Municipios, deberá:

Funciones y Deberes

- ✓ Aplicar conocimientos, habilidades, herramientas y técnicas, dirigiendo y coordinando las actividades de los proyectos de seguridad de la información e informática, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- ✓ Identificar la brecha entre la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información dispuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones y la situación de seguridad de la Información de la Federación Colombiana de Municipios.
- ✓ Generar el cronograma de la implementación de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información.

- ✓ Dirigir, Coordinar, Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido para Implementar la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información.
- ✓ Gestionar los proyectos de gobierno digital, de seguridad y privacidad de la información de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- ✓ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo.
- ✓ Encaminar los proyectos que se desarrollen en la entidad hacia el adecuado cumplimiento de la implementación de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información para la entidad.
- ✓ Trabajar de manera integrada los temas de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información con todos los grupos de trabajo que componen todas las direcciones. áreas y asesorías de la Federación Colombiana de Municipios.
- ✓ Asegurar el adecuado cumplimiento y seguimiento de métricas de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información
- ✓ Velar por el mantenimiento de la documentación de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información en la Federación Colombiana de Municipios
- ✓ Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información en cuanto a la documentación de las lecciones aprendidas.
- ✓ Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información
- ✓ Liderar en la entidad las implementaciones de sistemas de información y plataformas tecnológicas para que cuenten con estándares de seguridad y privacidad de la información en coordinación con los grupos, áreas, direcciones y/o autoridades pertinentes.
- ✓ Definir, conjuntamente con los grupos, áreas y/o direcciones, una estrategia de seguridad y privacidad de la información desde la perspectiva de la tecnología, procesos, procedimientos, estándares en las dimensiones de la protección de bienes, activos, servicios, derechos y libertades dependientes de la FCM y que coordine las agencias y convenios público-privadas relacionadas con la seguridad y privacidad de la información en el Marco de la Arquitectura Empresarial de Gobierno Digital.
- ✓ Definir los lineamientos de política y estándares de protección de la información pública, para su preservación en situaciones de desastre.
- ✓ Promover en la dinámica de la FCM según Gobierno Digital y el Ministerio de las Tecnologías de la Información y las Comunicaciones una cultura de la ciberresponsabilidad, basada en la concientización y formación continua en ciberseguridad.
- ✓ Promover la investigación, el desarrollo y la innovación en la entidad, en materia de la ciberseguridad, que proporcione soluciones de tecnologías de la información requeridas por la FCM.
- ✓ Formular y Gerenciar proyectos para identificar fortalezas y debilidades relacionadas con la estructura de la información tales como la innovación, adaptación y obsolescencia tecnológica para

garantizar estándares de calidad y seguridad de la información en coordinación con las demás direcciones, áreas y grupos de la entidad.

- ✓ Proponer y Coordinar con la Dirección de Tecnologías de la Información, el diseño e implementación de las políticas de Tecnologías de la Información que modernicen y transformen las plataformas tecnológicas de la Federación Colombiana de Municipios, buscando garantizar la efectividad de la gestión y la interoperabilidad entre los sistemas de Tecnologías de la Información con seguridad y privacidad de la información.
- ✓ Analizar y proponer directrices de Tecnologías de la Información que cumplan los parámetros requeridos en materia de información estatal y/o de gobierno, de seguridad y protección de la información, coordinando con los colaboradores, áreas, grupos y direcciones pertinentes en los temas de su competencia.
- ✓ Coordinar y promover acuerdos institucionales que permitan la interoperabilidad de las Tecnologías de la Información estatal y privada para el manejo compartido de las mismas entre entidades y sectores.
- ✓ Promover alianzas público-privadas para mejorar los procesos de adopción de Tecnologías de la Información, en las estrategias fijadas para el funcionamiento efectivo de la Federación Colombiana de Municipios.
- ✓ Formular y presentar a la Dirección de Tecnologías de la Información planes de acción para incorporar los estándares y los parámetros de arquitectura de seguridad requeridos en la Federación Colombiana de Municipios.
- ✓ Formular, en coordinación con la Dirección de Tecnologías de la Información, programas y planes de adopción de Tecnologías de la Información que modernicen y transformen las plataformas tecnológicas y garanticen la efectividad de la gestión y la interoperabilidad entre los sistemas de Tecnologías de la Información con seguridad y privacidad de la información, e incorporarlos en las estrategias de Gobierno Corporativo de TI y de la Federación Colombiana de Municipios.
- ✓ Formular y presentar a la Dirección de Tecnologías de la Información planes de fortalecimiento del talento humano requerido para impulsar y gestionar proyectos de diseño y adopción de Tecnologías de la Información en la Federación Colombiana de Municipios.
- ✓ Coordinar el diseño y la implementación de una gestión de riesgos asociada a la seguridad y privacidad de la información bajo los lineamientos de la Política de Gobierno Digital y las mejores prácticas de las entidades dedicadas a ciberseguridad y ciberdefensa en el país.
- ✓ Liderar el diseño e implementación de las estrategias, procesos y procedimientos para la seguridad y privacidad de la información acorde con los lineamientos de políticas vigentes de la Federación Colombiana de Municipios y la Política de Gobierno Digital.
- ✓ Elaborar informes de avances sobre la implementación, actualización y mejora continua de la Política de Gobierno Digital, para la Federación Colombiana de Municipios en materia de Tecnologías de la Información, con el fin de retroalimentar el cumplimiento de las políticas y normatividad pública.
- ✓ Identificar la brecha entre la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información y la situación de la entidad.
- ✓ Generar el cronograma de las mejoras de implementación de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información.

- ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido en los proyectos de la Política de Gobierno Digital y Seguridad de la Información.
- ✓ Gestionar el equipo de proyectos de seguridad de la información de la entidad, definiendo roles, responsabilidades, entregables y tiempos.

Funciones en el Marco de Arquitectura Empresarial de TI de la Federación Colombiana de Municipios.

Dominio Servicios Tecnológicos

- ✓ Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución.
- ✓ Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
- ✓ Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
- ✓ Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
- ✓ Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
- ✓ Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.

Dominio Estrategia TI

Ayudar a definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de apoyar y guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.

Dominio Gobierno TI

Apoyar el ejercicio de seguimiento y control de la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI.

Dominio Sistemas de Información

- ✓ Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.
- ✓ Apoyar la implementación segura de los sistemas de información, de acuerdo con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información del estado colombiano.

- ✓ Coordinar, programar y desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
- ✓ Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
- ✓ Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

Dominio de Información

- ✓ Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.
- ✓ Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

Dominio Uso y Apropiación

- ✓ Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles.
- ✓ Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora.
- ✓ Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

8. Metodología para Análisis y Evaluación de Riesgos

La metodología de análisis y evaluación de riesgos para los activos de información y de Tecnología, en la Federación Colombiana de Municipios, se opta manejar principalmente la metodología de riesgos del Departamento Administrativo de la Función Pública, sin embargo se combina el ejercicio de manera integral a través de la metodología MAGERIT, con el fin de fortalecer la Valoración de Riesgos de los activos de Información en cuanto a confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad.

A continuación, se presenta la Metodología para la valoración de riesgos que se utiliza de manera integral en la entidad conforme a la metodología el Departamento Administrativo de la Función Pública y MAGERIT.

Metodología DAFP

MATRIZ DE INVENTARIO, CLASIFICACIÓN Y RIESGO DE ACTIVOS DE INFORMACIÓN
FEDERACIÓN COLOMBIANA DE MUNICIPIOS
DIRECCIÓN NACIONAL SIMIT

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN

PROBABILIDAD DEL RIESGO

	Categoría	Valoración
Probabilidad	Raro (puede ocurrir excepcionalmente)	1
	Improbable (puede ocurrir excepcionalmente)	2
	Posible (puede ocurrir en cualquier momento futuro)	3
	Probable (probablemente va a ocurrir)	4
	Casi cierto, ocurre en la mayoría de las circunstancias)	5

IMPACTO

	Valoración
Insignificant	1
Menor	2
Moderado	3
Mayor	4
Catastróficc	5

VALORACIÓN DEL RIESGO

PROBABILIDAD \ IMPACTO (VALORACIÓN)	1	2	3	4	5
Raro (puede ocurrir excepcionalmente)	2	3	4	5	6
Improbable (puede ocurrir excepcionalmente)	3	4	5	6	7
Posible (puede ocurrir en cualquier momento futuro)	4	5	6	7	8
Probable (probablemente va a ocurrir)	5	6	7	8	9
Casi cierto, ocurre en la mayoría de las circunstancias)	6	7	8	9	10

CATEGORÍA DEL RIESGO

VALORACIÓN DEL RIESGO	CATEGORÍA
8, 9 y 10 (MA)	Riesgo Extremo (MA)
6 y 7 (A)	Riesgo Alto (A)
5 (M)	Riesgo Medio (M)
2,3 y 4 (B)	Riesgo Bajo (B)

El resultado final de la valoración del riesgo al que está expuesto cada activo depende de la suma de la probabilidad VS el impacto de la tabla anterior. Nuestro cálculo se basa en todo lo recogido durante las entrevistas y el cómputo de la pestaña "Inventario y Valoración de Activos" contra la tabla de valoración del riesgo.

Ilustración 4 Metodología DAFP

Metodología Magerit

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO \ PROBABILIDAD	MA	A	M	B	MB
MA	5	10	15	20	25
A	4	8	12	16	20
M	3	6	9	12	15
B	2	4	6	8	10
MB	1	2	3	4	5
RIESGO	MB	B	M	A	MA

VALORACIÓN DEL RIESGO

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	25
	A	Importante	16 a 20
	MA	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Ilustración 5 Metodología Magerit

9. Contexto para el Análisis y Evaluación de Riesgos

Para realizar el análisis y evaluación de riesgos según la metodología del Departamento administrativo de la Función Pública y Metodología Magerit, hacia los activos de información y de tecnología de la Federación Colombiana de Municipios, se aborda en el marco de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad; los siguientes criterios:

- ✓ Determinación de las vulnerabilidades, amenazas y riesgos de seguridad.
- ✓ Valoración Cualitativa según Dominios Magerit
- ✓ Atributos de Clasificación de la Información
- ✓ Valoración Cuantitativa de los Riesgos según Dominios Magerit
- ✓ Probabilidad de vulneración
- ✓ Calculo del riesgo neto
- ✓ Criticidad neta
- ✓ Calificación de Gestión
- ✓ Riesgo residual
- ✓ Criticidad residual
- ✓ Niveles de aceptación del riesgo
- ✓ Controles de Seguridad según Norma ISO27001:2013 e ISO27002:2013
- ✓ Plan de Tratamiento de Riesgos.

10. Plan Proyecto de Inversión y Presupuesto del MSPI

El Profesional Oficial de Seguridad Informática; es el Oficial de Seguridad de la Información de la entidad, encargado de dirigir, coordinar y definir la estrategia e implementación de la Seguridad y Privacidad de la Información, con base a los lineamientos, instrumentos, artefactos y guías que dispone la Política de Gobierno Digital.

Por lo tanto, el proyecto de Inversión y Presupuesto para el Modelo de Seguridad y Privacidad de la Información será realizado con los recursos propios de la Dirección de Tecnologías de la Información, y demás actores de la entidad que se involucren en el desarrollo de actividades para la Implementación del Modelo de Seguridad y Privacidad de la Información en la Federación Colombiana de Municipios.

En la proactividad y eficiencia administrativa de la entidad, en el año 2020 se logran avances significativos en la implementación del Modelo de Seguridad y Privacidad de la Información que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones, para las entidades de la administración pública; esto conforme a los lineamientos de la Política de Gobierno Digital.

Por lo anterior, se resumen en alto nivel; el estado actual del Modelo de Seguridad y Privacidad de la Información en la FCM.

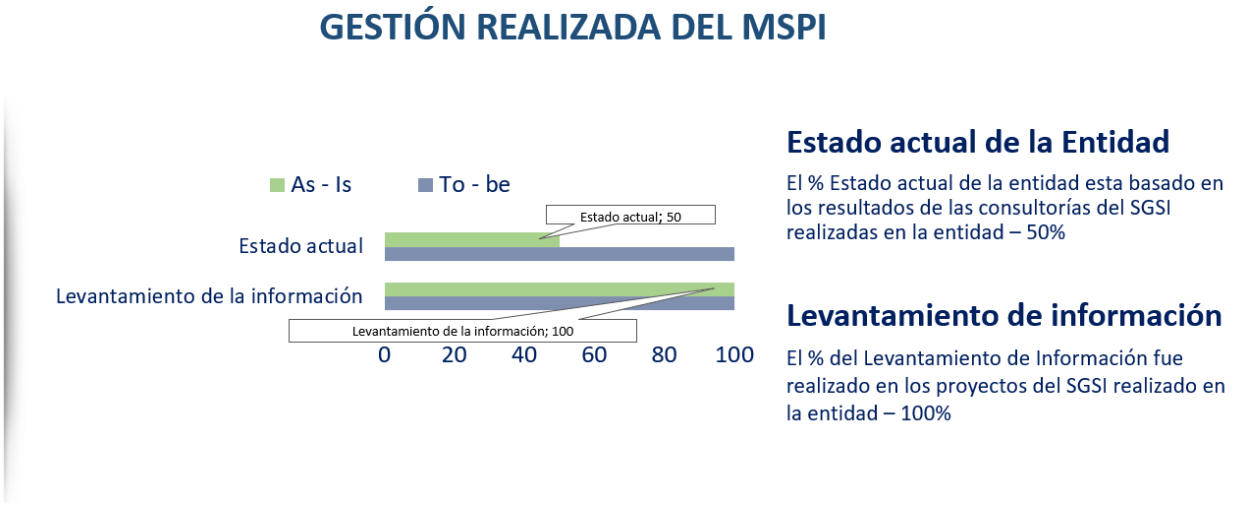


Ilustración 6 Estado actual del MSPI en la FCM

En la siguiente ilustración se identifica el nivel de madurez del MSPI en la FCM

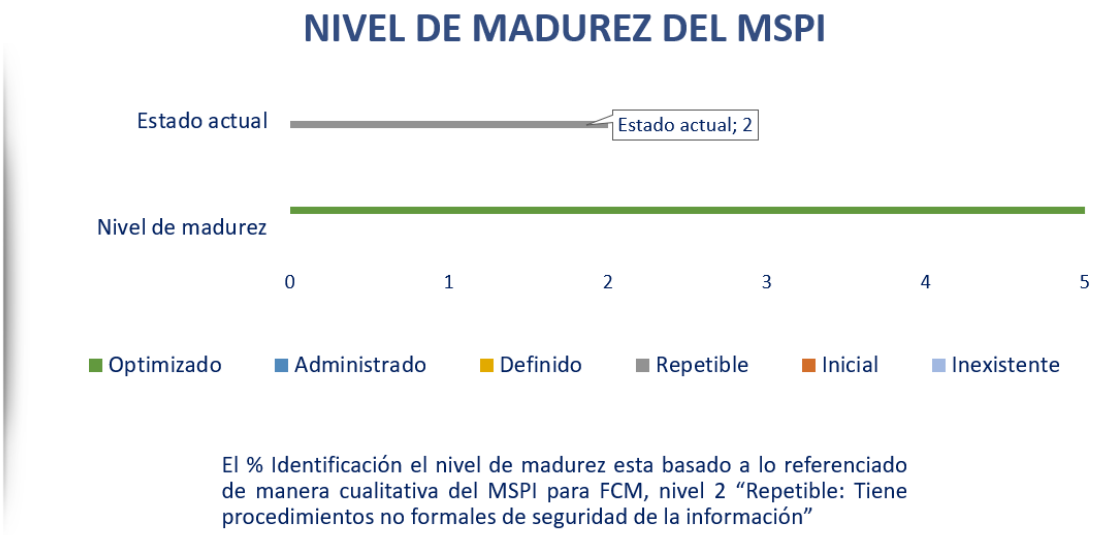


Ilustración 7 Nivel de Madurez del MSPI en la FCM

A continuación, se visualiza la proyección del nivel de madurez del Modelo de Seguridad y Privacidad de la Información en la FCM.

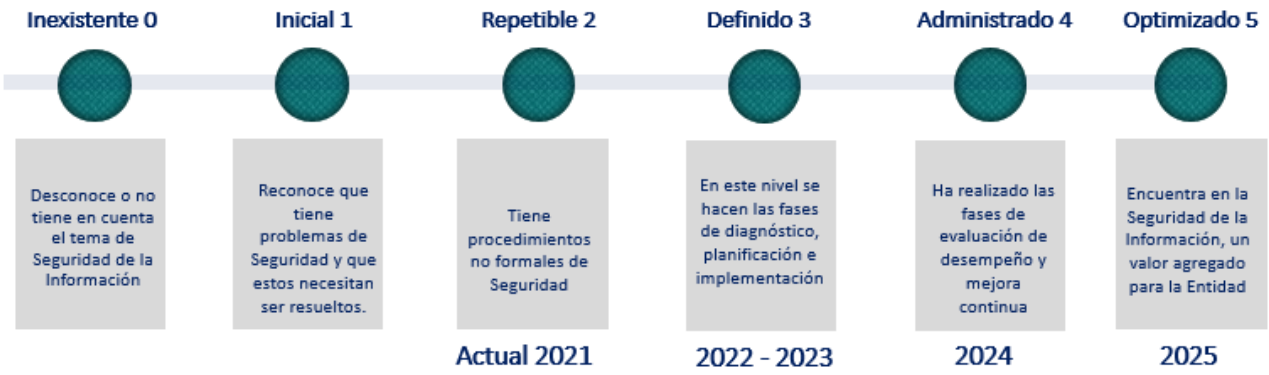


Ilustración 8 Proyección del nivel de madurez en la FCM

Los resultados del Modelo de Seguridad y Privacidad de la Información – MSPI como se observa en las gráficas anteriores, tenemos un nivel de implementación del 50% y un nivel 2 de madurez "Repetible", por lo tanto, se han identificado las brechas principales de Implementación, para avanzar con la gestión del MSPI cubriendo todos sus componentes de seguridad y ciberseguridad para la entidad.

Con base a los resultados del Diagnóstico realizado en la Federación Colombiana de Municipios con el Instrumento "Autodiagnóstico del MSPI" que dispuso el Ministerio de Tecnologías de Información y las Comunicaciones – Min TIC, para definir el Plan Estratégico de Seguridad y Privacidad de la Información – PESI, se identifican las brechas requeridas para avanzar con la implementación y operación del MSPI:

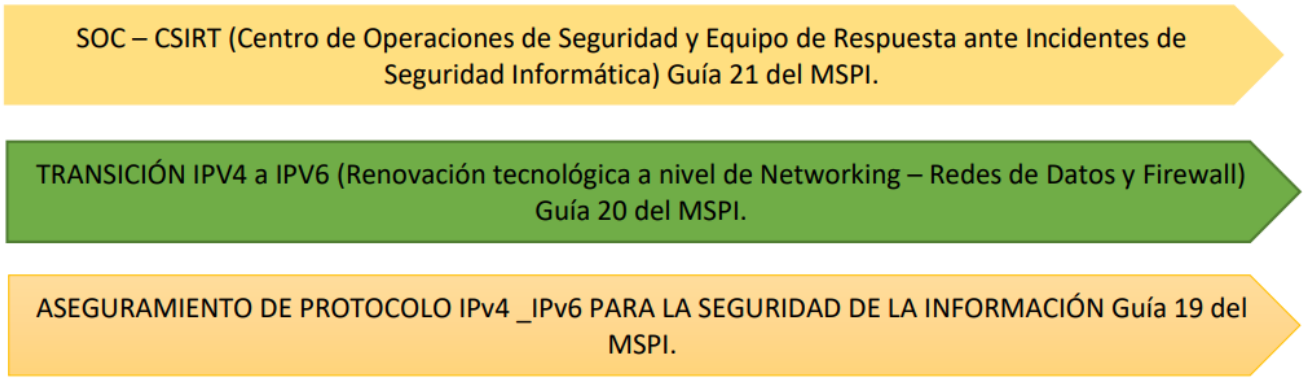


Ilustración 9 Brechas Principales de Implementación

11. Implementación Plan de Proyectos y Actividades del MSPI

Las actividades y/o proyectos de inversión del Modelo de Seguridad y Privacidad de la Información – MSPI para su ejecución están definidos durante el periodo (2021 – 2025), la cual dichas actividades y/o proyectos pertenecientes al año 2021, se encuentran a continuación.

11.1. Proyecto de adopción de IPv4 a Ipv6 en la FCM

11.1.1 Objetivo

Diseñar e implementar el plan de Transición del protocolo IPv4 a IPv6 en redes de datos, acorde a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC).

11.1.2. Fases del Proyecto

A continuación, se describen las fases que se van a llevar acabo para la implementación y adopción de IPv4 a IPv6 en la infraestructura tecnológica de la Federación Colombiana de Municipios, alineado al Modelo de Seguridad y Privacidad de la Información, dando cumplimiento a la Política de Gobierno Digital. El proyecto busca proponer un "plan para la transición" de IPv4 a IPv6 en redes de datos, teniendo en cuenta las instrucciones brindadas por MinTIC en la "*Guía No.20 de transición de IPv4 a IPv6 y Guía No. 19 Aseguramiento de protocolo IPv4 a IPv6 para Colombia*" y sus directrices específicas al momento de hacer la planeación de la transición en la Federación Colombiana de Municipios; según estas guías, se deben realizar actividades concretas para obtener un plan de diagnóstico que incluya el inventario de activos de información, un informe de la infraestructura de red de comunicaciones y sugerencias con respecto a los dispositivos que no soportan el nuevo protocolo, además de una propuesta con el plan del proceso de transición, ver tabla 2 "Plan de trabajo transición IPv4 a IPv6".

Las actividades para la implementación de la transición de IPv4 a IPv6 se realizará en el año 2021, como se muestra en la siguiente tabla.

Fases	Actividades
Diagnóstico situación actual	Construcción del Plan de Diagnóstico
	Inventario TI (Hardware y Software)
	Análisis de la nueva topología de la ingraestructura actual y su funcionamiento
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos
	Planeación de la transición de los servicios tecnológicos de la Entidad
	Validación del estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes
	Identificación de esquemas de seguridad de la información y las comunicaciones

Fases	Actividades
	Hito de Entregables Fase I
Desarrollo del plan de implementación	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.
	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.
	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.
	Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.
	Hito de Entregables Fase II
Pruebas de funcionalidad de IPv6	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.
	Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.
	Hito de Entregables Fase III

Tabla 3 Plan de trabajo transición IPv4 a IPv6

11.2. Campaña de Capacitación e Ingeniería Social en la FCM

11.2.1 Objetivo

Realizar campaña de concientización e Ingeniería Social en seguridad de la información dirigida a usuarios finales para la mitigación del riesgo sobre la información de la Federación Colombiana de Municipios de función pública delegada.

11.3. Análisis de Vulnerabilidades y Ethical Hacking en la FCM

11.3.1 Objetivo

Llevar acabo análisis de seguridad informática mediante la aplicación de dos instrumentos: análisis de vulnerabilidades y Ethical Hacking, teniendo en cuenta la ISO 27001 del 2013 con el fin de fortalecer y asegurar la disponibilidad de los servicios tecnológicos de información de la Federación Colombiana de Municipios de función pública delegada

11.4. Plan de Trabajo y Actividades de mejora Continua para el MSPI

11.4.1 Objetivo Modelo de Seguridad y Privacidad de la Información – MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) hace parte del sistema integrado de gestión de la Federación Colombiana de Municipios, se basa en un enfoque de gestión de riesgos de seguridad de la información de los procesos, en el contexto de los riesgos globales de la Entidad, para: establecer, implementar, operar, hacer seguimiento, mantener y mejorar la seguridad de la información. La gestión de la seguridad de la información es una tarea continua que se realiza con el fin de preservar las propiedades de confidencialidad, integridad y disponibilidad en los activos de información que manejan los procesos de la Federación Colombiana de Municipios, con base en su nivel de riesgo. El MSPI permite a la entidad identificar, implementar, mantener y mejorar los controles que requiere para tratar los riesgos de seguridad de la información y llevarlos a niveles aceptables, de tal forma que estos controles sean suficientes para proporcionar un ambiente de control y seguridad adecuados. Los lineamientos del Modelo de Seguridad y Privacidad de la Información son aplicables a cualquier proceso de la Federación Colombiana de Municipios, sin importar su tamaño o función, dado que la implementación del sistema debe ser proporcional a la criticidad de los activos de información que maneja y los riesgos identificados en los mismos.

MSPI en la Federación Colombiana de Municipios

El MSPI de la Federación Colombiana de Municipios, establece un sentido general de dirección, gestión y principios con relación a la seguridad de la información, orientados en su totalidad al cumplimiento de la política de seguridad de la información de la Federación Colombiana de Municipios, teniendo en cuenta los requisitos normativos internos, los legales o reglamentarios, y las obligaciones contractuales. Este documento hace referencia a diferentes documentos que serán presentados como anexos del mismo y que se puede clasificar en los siguientes cinco grandes grupos:

- ✓ Roles y Responsabilidades del MSPI
- ✓ Políticas de Seguridad de la Información
- ✓ Procedimientos que integran el MSPI
- ✓ Declaración de Aplicabilidad
- ✓ Medición del MSPI

Línea base de plan de trabajo y actividades para la implementación del MSPI

A continuación, se estructura el ponderado de los avances de actividades del proyecto que se han realizado a la fecha, como también identificando como brecha la ejecución de actividades que no están al 100%, de los cuales se tiene que desarrollar para los próximos (5) años (2021 al 2025), esto alineado conforme a las fases del proyecto de Implementación del Modelo de Seguridad y Privacidad de la Información para la Federación Colombiana de Municipios, las cuales son: Diagnóstico, Planificación, Implementación, Mejoramiento continuo y la Evaluación de desempeño.

La siguiente es la línea base del plan de trabajo y actividades para la implementación del MSPI en la Federación Colombiana de Municipios para los próximos 4 años:

	PROCESO	MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO	PLN-APY-12-05-02-15	
			VERSIÓN	01	
	FORMATO	PLAN DE TRABAJO	PÁGINA	1 de 8	
			VIGENTE DESDE	30/08/2017	

ACTIVIDADES DEL PLAN DE TRABAJO

FASE	ACTIVIDADES	RECURSO HUMANO	AVANCES ESTIMADOS						TIEMPO		DOCUMENTO	OBSERVACIONES
			0	20	40	60	80	100	FECHA INICIAL	FECHA FINAL		
DIAGNÓSTICO	Manifestar la intención de incluir el MSPI en el SGC por parte de la Alta Dirección.	Profesional Oficial de Seguridad Informática / Dirección TI / Dir. Ejecutiva / Planeación y Calidad				60						
	Conformar Comité de Seguridad de la Información	Profesional Oficial de Seguridad Informática						100			Acta No. 001 de 2019 del Comité de Gobierno Digital y Seguridad de la Información	
	Aprobar Comité de Seguridad de la Información	Dirección Ejecutiva						100			Resolución 123 de 11 de Noviembre 2019	
	Aplicar el autodiagnóstico de Seguridad de la Información	Profesional Oficial de Seguridad Informática						90				

ACTIVIDADES DEL PLAN DE TRABAJO

FASE	ACTIVIDADES	RECURSO HUMANO	AVANCES ESTIMADOS						TIEMPO		DOCUMENTO	OBSERVACIONES
			0	20	40	60	80	100	FECHA INICIAL	FECHA FINAL		
	Desarrollar Plan de Proyecto para implementar el MSPI	Profesional Oficial de Seguridad Informática					80					
	Aprobar el plan de proyecto para iniciar el proyecto MSPI	Comité MSPI				60						
	Divulgar el plan de Trabajo para estandarizar el MSPI con los procesos construidos, manifestar las auditorias que se planearan con el propósito de la mejora continua al MSPI.	Profesional Oficial de Seguridad Informática				60						
	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la FCM	Profesional Oficial de Seguridad Informática					80					
	Identificar el nivel de madurez de seguridad y privacidad de la información en la FCM	Profesional Oficial de Seguridad Informática						100				
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Profesional Oficial de Seguridad Informática						100				
	Hito de Entregables Fase Diagnostico	Profesional Oficial de Seguridad Informática				60						

ACTIVIDADES DEL PLAN DE TRABAJO

FASE	ACTIVIDADES	RECURSO HUMANO	AVANCES ESTIMADOS						TIEMPO		DOCUMENTO	OBSERVACIONES
			0	20	40	60	80	100	FECHA INICIAL	FECHA FINAL		
PLANIFICACIÓN	Definir el alcance del MSPI (contexto, liderazgo, planeación, interesados, limites, aplicabilidad, soporte)	Profesional Oficial de Seguridad Informática / Comité MSPI					80					
	Aprobar alcance del MSPI, límites de acuerdo a la estructura de la organización	Comité MSPI					80					
	Definir roles y responsabilidades de seguridad de la información	Profesional Oficial de Seguridad Informática / Comité MSPI						100			Resolución No. 123	
	Aprobar roles y responsabilidades de seguridad de la información	Comité MSPI						100			Resolución No. 123	
	Definir la política general, manual de políticas y política por documento, teniendo encuentra los objetivos.	Profesional Oficial de Seguridad Informática					80					
	Aprobar la políticas y objetivos del MSPI	Profesional Oficial de Seguridad Informática / Comité MSPI					80					
	Definir los instrumentos para la identificación y clasificación de activos de información	Profesional Oficial de Seguridad Informática			40							
	Aprobar los instrumentos para la identificación y clasificación de activos de información (documento y formato)	Profesional Oficial de Seguridad Informática			40							
	Identificar y clasificar los activos de información por proceso de acuerdo con el alcance del MSPI definido.	Profesional Oficial de Seguridad Informática					80					
	Aplicar la metodología de gestión de riesgos alineada a control interno	Profesional Oficial de Seguridad Informática / Control Interno de Gestión				60						

ACTIVIDADES DEL PLAN DE TRABAJO

FASE	ACTIVIDADES	RECURSO HUMANO	AVANCES ESTIMADOS						TIEMPO		DOCUMENTO	OBSERVACIONES
			0	20	40	60	80	100	FECHA INICIAL	FECHA FINAL		
	Aprobar la metodología de gestión de riesgos	Profesional Oficial de Seguridad Informática / Comité MSPI					80					
	Realizar la identificación, valoración y evaluación de riesgos de seguridad de la información por proceso según la metodología aprobada.	Profesional Oficial de Seguridad Informática					80					
	Aprobar matriz de riesgos del MSPI	Profesional Oficial de Seguridad Informática					80					
	Establecer el plan de tratamiento de riesgos	Profesional Oficial de Seguridad Informática					80					
	Aprobar plan de tratamiento de riesgos	Profesional Oficial de Seguridad Informática / Comité MSPI					80					
	Definir documento de declaración de aplicabilidad	Profesional Oficial de Seguridad Informática						100				
	Aprobar documento de declaración de aplicabilidad	Profesional Oficial de Seguridad Informática / Comité MSPI					80					
	Elaborar Procedimiento del MSPI	Profesional Oficial de Seguridad Informática				60						
	Socializar Procedimientos a los miembros del Comité MSPI	Profesional Oficial de Seguridad Informática / Comité MSPI			40							
	Entregar copia de los Procedimientos a Planeación y Calidad para su integración a los sistema de gestión institucional	Profesional Oficial de Seguridad Informática	0									

ACTIVIDADES DEL PLAN DE TRABAJO

FASE	ACTIVIDADES	RECURSO HUMANO	AVANCES ESTIMADOS						TIEMPO		DOCUMENTO	OBSERVACIONES
			0	20	40	60	80	100	FECHA INICIAL	FECHA FINAL		
	Integrar los documentos de seguridad de la información al Manual SGC	Profesional Oficial de Seguridad Informática / Planeación y Calidad										
	Aprobar el Manual SGC con la integración del MSPI	Profesional Oficial de Seguridad Informática / Planeación y Calidad										
	Definir la estrategia y adoptar la Integración del MSPI con el Sistema de Gestión Documental de la entidad	Profesional Oficial de Seguridad Informática / Coord. Gestión Documental			40							
	Aprobar la estrategia y adopción de la Integración del MSPI con el Sistema de gestión documental	Profesional Oficial de Seguridad Informática / coord. Gestión documental										
	Implementación de la Integración del MSPI con el sistema de gestión documental	Profesional Oficial de Seguridad Informática / coord. Gestión documental										
	Plan de Diagnostico de IPV4 a IPV6	Profesional Oficial de Seguridad Informática						10			Estamos en la Fase 2 Implementación	
	Incluir dentro de los planes de concienciación y sensibilización, capacitación y entrenamiento del SGC de la FCM, los aspectos de seguridad de la información.	Profesional Oficial de Seguridad Informática / Planeación y Calidad / Recursos Humanos					80					
	Definir mecanismos (qué, quién, cuándo) para la evaluación del cumplimiento de las políticas declaradas.	Profesional Oficial de Seguridad Informática			40							
	Ajustar y/o definir y planificar el programa de auditorías internas incluyendo aspectos de seguridad de la información.	Profesional Oficial de Seguridad Informática / Control Interno de Gestión			40							

ACTIVIDADES DEL PLAN DE TRABAJO												
FASE	**ACTIVIDADES**	**RECURSO HUMANO**	**AVANCES ESTIMADOS**						**TIEMPO**		**DOCUMENTO**	**OBSERVACIONES**
			0	**20**	**40**	**60**	**80**	**100**	**FECHA INICIAL**	**FECHA FINAL**		
	Aprobar el programa de auditorías internas incluyendo aspectos de seguridad de la información.	Profesional Oficial de Seguridad Informática / Control Interno de Gestión / Comité MSPI										
	Establecer indicadores de eficacia para el MSPI en general	Profesional Oficial de Seguridad Informática			40							
	Aprobar indicadores de eficacia para el MSPI en general	Profesional Oficial de Seguridad Informática										
	Hitos de Entregables de Planificación y Plan de Seguridad y Privacidad de la Información	Profesional Oficial de Seguridad Informática										
IMPLEMENTACIÓN	Desarrollar las actividades incluidas en los planes de concienciación y sensibilización, entrenamiento y capacitación a la FCM que hacen referencia al MSPI.	Profesional Oficial de Seguridad Informática						100				
	Implementar controles del plan de tratamiento de riesgos de acuerdo a los riesgos encontrados	Profesional Oficial de Seguridad Informática										
	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Profesional Oficial de Seguridad Informática										
	Planificación y Control Operacional: Actualizar la declaración de aplicabilidad	Profesional Oficial de Seguridad Informática										

ACTIVIDADES DEL PLAN DE TRABAJO

FASE	ACTIVIDADES	RECURSO HUMANO	AVANCES ESTIMADOS						TIEMPO		DOCUMENTO	OBSERVACIONES
			0	20	40	60	80	100	FECHA INICIAL	FECHA FINAL		
	Describir en documento la Evaluación del MSPI conforme a los Indicadores de Gestión definidos	Profesional Oficial de Seguridad Informática										
	Plan de Transición de IPv4 a IPv6	Profesional Oficial de Seguridad Informática / Grupo de Gestión de Infraestructura Tecnológica				60						
	Aprobación del plan con la estrategia de implementación de IPv6 en la entidad, aprobado por TI.	Profesional Oficial de Seguridad Informática / Grupo de Gestión de Infraestructura Tecnológica					80					
EVALUACIÓN	Evaluar el cumplimiento de las políticas/procedimientos implementados y Plan de revisión y seguimiento a la Implementación del MSPI	Profesional Oficial de Seguridad Informática			40							
	Ejecutar el programa de auditorías internas.	Auditores Control Interno de Gestión/ Profesional Oficial de Seguridad Informática										
	Revisar y analizar el nivel del riesgo residual, implementación del plan de riesgos, revisión y aprobación de la declaración de aplicabilidad actualizada e indicadores	Profesional Oficial de Seguridad Informática										
	Realizar la revisión por la Alta Dirección de la FCM dentro del marco del SGC	Comité MSPI										

ACTIVIDADES DEL PLAN DE TRABAJO												
FASE	**ACTIVIDADES**	**RECURSO HUMANO**	**AVANCES ESTIMADOS**						**TIEMPO**		**DOCUMENTO**	**OBSERVACIONES**
			0	**20**	**40**	**60**	**80**	**100**	**FECHA INICIAL**	**FECHA FINAL**		
MEJORANMIENTO	Generar el plan de mejoramiento del MSPI y auditorias (acciones correctivas y mejora continua) de acuerdo con los resultados de las revisiones dadas.	Profesional Oficial de Seguridad Informática / Control Interno de Gestión / demás áreas de la entidad		20								
	Aprobar el plan de mejoramiento del MSPI y de las auditorias (acciones correctivas y mejora continua) de acuerdo con los resultados de las revisiones dadas.	Profesional Oficial de Seguridad Informática / Control Interno de Gestión										
	Ejecutar el plan de mejoramiento del MSPI.	Profesional Oficial de Seguridad Informática / Control Interno de Gestión		20								

Tabla 4 Plan de Trabajo – MSPI

12. Descripción y Entregables de las Fases del MSPI

FASE DIAGNOSTICO	
GESTION A REALIZAR	**ENTREGABLES**
En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas: 1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. 2. Determinar el nivel de madurez de los controles de seguridad de la información. 3. Identificar el avance de la implementación del ciclo de operación al interior de la entidad. 4. Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales. 5.Identificación del uso de buenas prácticas en ciberseguridad. Para ello se recomienda utilizar los siguientes instrumentos: 1. Herramienta de diagnóstico 2. Instructivo para el diligenciamiento de la herramienta 3. Guía No 1 - Metodología de Pruebas de Efectividad Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.	Documento de identificación del nivel de madurez de la entidad. Herramienta de diagnóstico Diligenciada. Documento con los hallazgos encontrados en las pruebas de vulnerabilidad Macroprocesos de Gestión de la Seguridad y Privacidad de la Información y la Caracterización de Procesos, integrado al SGC - Sistema de Gestión de Calidad.

Tabla 5 Fase Diagnóstico

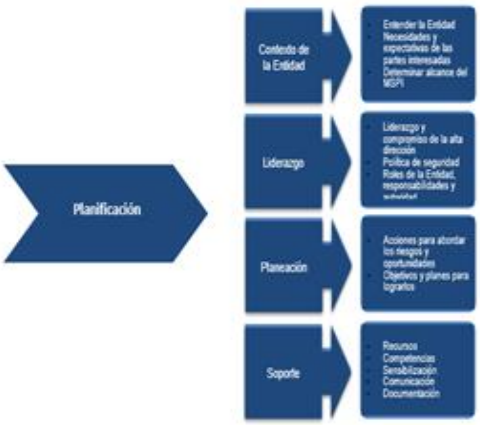
FASE PLANIFICACIÓN	
GESTION A REALIZAR	**ENTREGABLES**
Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad. Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.  Figura 3 - Fase de planificación	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad. Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad. Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional. Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6. Integración del MSPI, con el sistema de gestión documental de la entidad. Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección. Documento con el plan de comunicación, sensibilización y capacitación para la entidad. Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

Tabla 6 Fase de Planificación

FASE IMPLEMENTACION	
GESTION A REALIZAR	**ENTREGABLES**
Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI. Figura 4 - Fase de implementación[2] Plan de Transición de IPv4 a IPv6 | Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

Tabla 7 Fase de Implementación

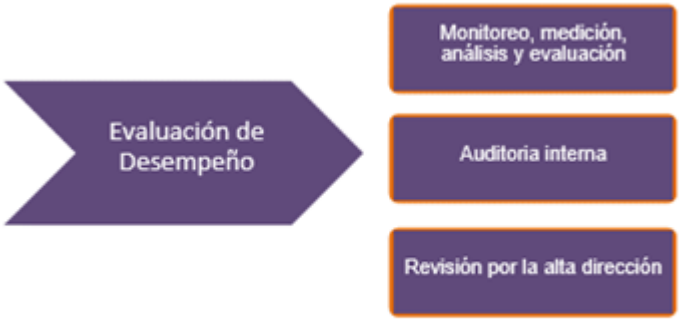
FASE EVALUACIÓN	
GESTION A REALIZAR	**ENTREGABLES**
El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.  Figura 5 - Fase de Evaluación de desempeño[3]	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

Tabla 8 Fase de Evaluación

FASE MEJORA CONTINUA	
GESTION A REALIZAR	**ENTREGABLES**
En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas. Figura 6 - Fase de mejoramiento continúo[4] En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye: · Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. · Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Utilizando los insumos anteriores, la entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados. Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Tabla 9 Fase de Mejora Continua