Plan de Seguridad y Privacidad de la Información

Código SG/MIPG	127-PPPGI-05
Vigencia desde	27/01/2021
Versión	4

Proceso Gestión de la Información de la Tecnología

ALCALDÍA MAYOR DE BOGOTÁ D.C.
DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO
BOGOTÁ

Tabla de Contenido

1. Introducción 3
2. Elementos Estratégicos 3
2.1 Misión 3
2.2 Visión 2024 3
2.3 Objetivos Estratégicos 2020 - 2024 3
3. Generalidades del Plan 4
3.1. Diagnóstico 4
3.1 Formulación 6
3.2 Objetivos 6
3.3 Objetivos específicos 6
3.4 Alcance del Plan 6
3.5 Recursos 6
3.6 Metodología de seguimiento y publicación 6
4. Actividades del Plan 7
5. Riesgos asociados al Plan 9
6. Indicadores 11
7. Normatividad 11

1. Introducción

El Departamento Administrativo de la Defensoría del Espacio Público - DADEP ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones, y acorde con las políticas establecidas por el Gobierno Nacional, la entidad implementa el SGSI, siguiendo los lineamientos del MSPI dictados por MinTic.

El MSPI del DADEP adopta la guía para la identificación y valoración de los activos de información, la guía para la evaluación y tratamiento de los riesgos y la guía para la definición y maduración del MSPI definidas por el MINTIC. Así mismo, el MSPI del DADEP define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoria y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la madurez del MSPI.

De esta forma, por medio de este plan, el modelo del MSPI es adoptado por la entidad de acuerdo al ciclo PHVA (planear, hacer, verificar y actuar), con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada.

2. Elementos Estratégicos

2.1 Misión

Contribuir al mejoramiento de la calidad de vida en Bogotá, por medio de una eficaz defensa del espacio público, de una óptima administración del patrimonio inmobiliario de la ciudad y de la construcción de una nueva cultura del espacio público, que garantice su uso y disfrute colectivo y estimule la participación comunitaria.

2.2 Visión 2024

En 2024, el Departamento Administrativo de la Defensoría del Espacio Público será una entidad reconocida a nivel distrital y nacional como líder en la protección integral del espacio público y del patrimonio inmobiliario distrital, la gestión del conocimiento urbanístico de los bienes de uso público y fiscales del nivel central de Bogotá, y por promover la participación ciudadana, la corresponsabilidad y la coordinación interinstitucional.

2.3 Objetivos Estratégicos 2020 - 2024

Contribuir al incremento del uso, goce y disfrute del patrimonio inmobiliario distrital y el espacio público, con acceso universal a la ciudadanía.

Aumentar la oferta cuantitativa, cualitativa y la equidad territorial del patrimonio inmobiliario distrital y el espacio público.

Mejorar la coordinación interinstitucional con todas las entidades que tienen competencia en materia de espacio público, así como la comunicación con los grupos de interés y de valor.

Fortalecer la capacidad institucional en el marco del Modelo Integrado de Planeación y Gestión, bajo los enfoques de una gestión orientada a resultados, la eficiencia en el manejo de recursos, la transparencia, el gobierno abierto y la participación de los grupos de interés.

3. Generalidades del Plan

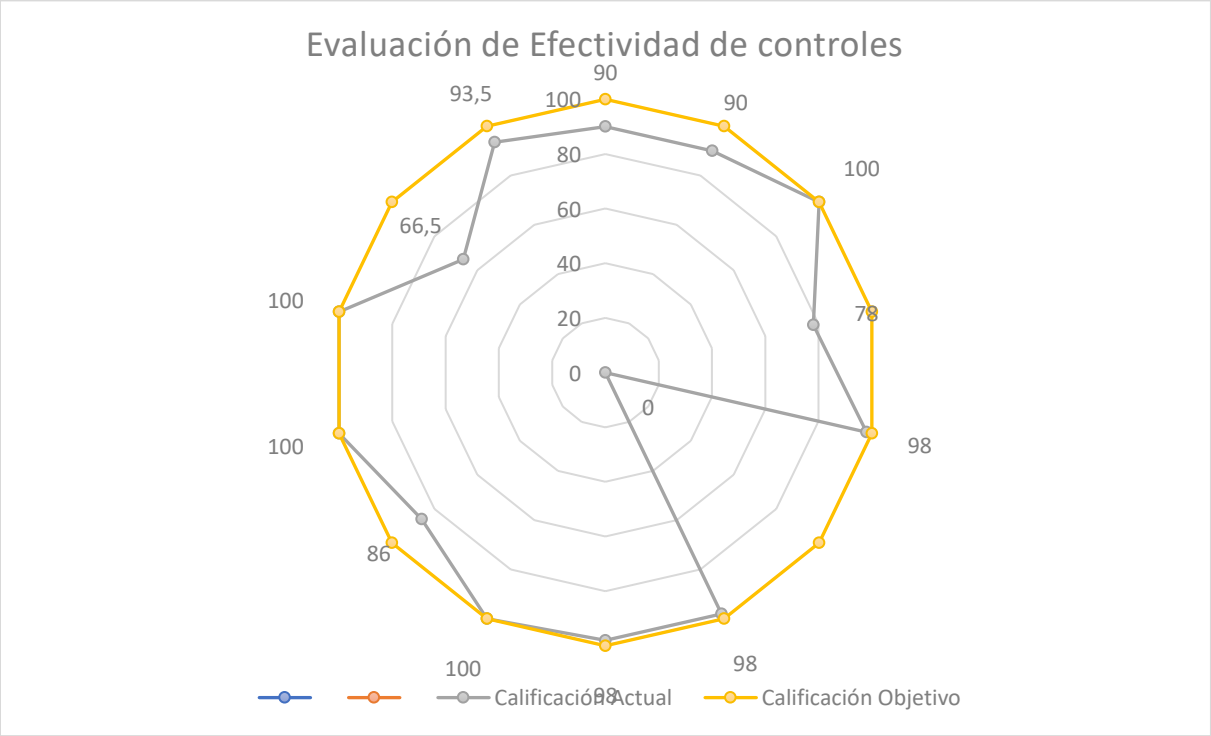
3.1. Diagnóstico

Para poder realizar el Plan de Seguridad y Privacidad de la Información es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios con el fin de plantear prioridades sobre su implementación. Los resultados se muestran a continuación:

No.	Evaluación de Efectividad de controles			
	DOMINIO ISO 27001	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	78	100	GESTIONADO
A.9	CONTROL DE ACCESO	98	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	98	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	98	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	66,5	100	GESTIONADO
A.18	CUMPLIMIENTO	93,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		86	100	OPTIMIZADO

Tabla 1: Resultado valoración de madurez del MSPI de la ISO 27001:2013

Los resultados obtenidos se ilustran en la siguiente gráfica



Gráfica 1: Brechas de la evaluación de efectividad de controles 2020

Lo cual determinó el porcentaje de avance actual de la Entidad en los diferentes componentes del PHVA, de acuerdo con la siguiente tabla:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	22%	40%
	Implementación	10%	20%
	Evaluación de desempeño	13%	20%
	Mejora continua	14%	20%
TOTAL		59%	100%

Tabla 2: Resultado del porcentaje de maduración alcanzado por la Entidad en el ciclo PHVA año 2020

3.1 Formulación

Este plan se realizó con la participación del responsable de Seguridad de la Información de la Entidad, quien hace parte de la oficina de sistemas. Adicionalmente y como ya se mencionó se siguieron los lineamientos y aplicación de las guías y formatos, establecidos para tal fin por el MINTIC.

3.2 Objetivos

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 del Sistema de Gestión de Seguridad de la Información, adoptado por el DADEP, 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).

3.3 Objetivos específicos

1. Comunicar e implementar la estrategia de seguridad de la información.
2. Incrementar el nivel de madurez en la gestión de la seguridad de la información.
3. Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
4. Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
5. Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

3.4 Alcance del Plan

Aplica a todos los niveles del DADEP, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación.

3.5 Recursos

ECONÓMICO: Los recursos financieros para la implementación del presente plan se determinaron en el documento del Mapa de Ruta PETI 2020-2024.

HUMANO: La Oficina de Sistemas, los líderes de proceso, Oficina de Control Interno y un profesional de apoyo especializado en seguridad informática.

FÍSICO: Infraestructura tecnológica y controles de acceso físico.

3.6 Metodología de seguimiento y publicación

El seguimiento y monitoreo a la ejecución de las actividades, se realizará trimestralmente en cabeza del encargado del MSPI contratado por la Oficina de Sistemas. Para realizar el seguimiento, las actividades definidas en este plan serán trasladadas a la herramienta Project Online para registrar el avance y la trazabilidad de las mismas, así mismo se contará con el formato de plan de acción que definirá las acciones a que haya lugar en caso de que las desviaciones superen el porcentaje permitido. Las desviaciones permitidas para este plan se establecen en 5% (SPI[1] mayor al 95%)

4. Actividades del Plan

Actividades	Meta	Producto	Fecha programada	Presupuesto
Fase. Planeación				
Actualizar la Política general de la Seguridad de la Información y Resolución de Seguridad de la Información.	Política de Seguridad y Privacidad de la Información actualizada al menos una vez al año	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Diciembre 2021	
Actualizar Manual Políticas de Seguridad de la Información.	Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Diciembre 2021	
Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)			Abril 2021	
Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información.	Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Marzo 2021	
Actualizar los Roles y responsabilidades de seguridad y privacidad de la información.	Roles y responsabilidades de seguridad y privacidad de la información.	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	Mayo 2021	

[1] SPI índice de desempeño del cronograma de acuerdo a lo establecido en la guía PMBOK del PMI

Actividades	Meta	Producto	Fecha programada	Presupuesto
		la información dentro de la entidad.		
Definir lineamientos para el levantamiento de activos de información.	Inventario de activos de información.	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	Junio 2021	
Actualización de Activos de Información.			Julio 2021	
Publicación de Activos de Información.			Julio 2021	
Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Marzo 2021	
Actualización de lineamientos de riesgos	Identificación, Valoración y tratamiento de riesgo.	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 la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Agosto 2021	
Sensibilización			Alineado con el plan de sensibilización	
Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación			Agosto 2021	
Elaborar el Plan de Comunicaciones.	Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y	Mayo 2021	

Actividades	Meta	Producto	Fecha programada	Presupuesto
Ejecutar el Plan de Comunicaciones.		capacitación para la entidad.	Alineado con el plan de sensibilización	
Analizar el Plan de Comunicaciones.			Alineado con el plan de sensibilización	
Fase. Implementación				
Aceptación de Riesgos Identificados	Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Septiembre 2021	
Publicación			Septiembre 2021	
Seguimiento Fase de Tratamiento	Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Trimestral	
Evaluación de riesgos residuales			Trimestral	
Mejoramiento			Trimestral	
Monitoreo y Revisión			Trimestral	
Formular, Implementar y actualizar los indicadores del SGSI	Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Abril 2021	
Reportar indicadores			Trimestral	
Fase. Evaluación del Desempeño				
Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad.	Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	trimestral	
Participación en las auditorías internas y externas de la norma ISO 27001:2013	Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	De acuerdo a programación OCI	
Fase. Mejora Continua				
	Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	10/12/2021	

5. Riesgos asociados al Plan

Una vez definido el plan, se identificaron los siguientes riesgos y su respectivo plan de respuesta:

Área de Riesgo	Riesgo	Valoración final del riesgo (impacto * Probabilidad)	Estrategia	Plan de Respuesta
Tiempo	En razón a no contar con el profesional experto en el tiempo establecido para su contratación, podrían afectarse las fechas planeadas, trayendo como consecuencia la modificación de la fecha de finalización del plan.	Alto	Mitigar - Impacto	Realizar un control de cambios al tiempo y/o alcance del plan
Costos	A causa de la ejecución de las actividades el plan, podría identificarse la adquisición de un software o análisis de vulnerabilidades adicionales lo que traería como consecuencia la afectación en los costos del plan	Bajo	Mitigar - Impacto	Escalar al comité Directivo para buscar los recursos. Realizar el proceso de contratación, según aplique, si el comité lo ha aprobado
Calidad	Debido a la desactualización, inexactitud de la información y poca participación de los interesados, podrían generarse productos que no cumplan los requerimientos establecidos lo que generaría reprocesos	Medio	Mitigar Probabilidad	Solicitar la información a fuentes confiables Validar la exactitud y actualización de la información entregada antes de realizar los productos Definir un plan de comunicación a los interesados
Alcance	A raíz de cambios en las guías, procedimiento y regulaciones se podría afectar el alcance del plan y sus actividades trayendo como consecuencia el replanteamiento de todo el plan de MSPI	Bajo	Aceptar	Realizar el ajuste al plan

Tabla 3: Identificación de los riesgos del plan y el respectivo plan de respuesta

6. Indicadores

Nombre	Indicador	Meta	Frecuencia	Responsable
Índice de desempeño del cronograma (SPI)	Actividades ejecutadas/actividades planeadas	≥ 95%	Trimestral	Gerente Proyecto
Reprocesos	Sumatoria de devoluciones de cumplimiento de requisitos de los productos	≤2	Por producto	Gerente Proyecto
Involucramiento de los interesados	Número de asistentes a las sensibilizaciones/ Número de convocados	≥90%	Con cada Sensibilización	Apoyo Técnico - MSPI

Tabla 4: Indicadores del plan

7. Normatividad

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 2093. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 2099. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo 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.
- 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 de espectro y se dictan otras disposiciones. • Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 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. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1712 de 2014. 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.
- Ley 2015 de 2018. Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario
- Ley 2055 de 2020. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- 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 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- 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.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2034 de 2016. Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC. • Resolución 2133 de 2018. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.

- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- Resolución 2005 de 2019. Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

Elaboró: Guiomar Pilar Cortes Ávila – Gerente de proyectos Oficina de Sistemas
Aprobó: Claudia Liliana Paipa – Jefe Oficina de Sistemas
Código de archivo: 140

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
4	27/01/2021	Se actualiza para la vigencia 2021, conforme a lo dispuesto en el el Decreto 612 de 2018.