PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1.0

Ministerio de Tecnologías de la Información y las Comunicaciones

Despacho de la Ministra
Seguridad y Privacidad de la Información

Ministerio de Tecnologías de la Información y las Comunicaciones
Edificio Murillo Toro, Carrera 8a, entre calles 12A y 12B
Código Postal: 111711 . Bogotá, Colombia
T: +57 (1) 3443460 Fax: 57 (1) 344 2248
www.mintic.gov.co

TABLA DE CONTENIDO

1. INTRODUCCIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, mediante resolución 911 del 26 de marzo de 2018, -*"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 3174 de 2014, la Resolución 3021 de 2016 y la Resolución 453 de 2016"-,* artículo 9° por el cual se establecen las responsabilidades del Comité MIG, espáticamente en los numerales 7 –"*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información*"- y 15 -"*Aprobar y hacer seguimiento a la implementación de la Estrategia de Gobierno Digital y Seguridad de la Información en la Entidad y al Plan Estratégico de Tecnologías Información.*"-. además, el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de implementación de Seguridad y Privacidad de la Información al interior del Ministerio de Tecnologías de la Información y las Comunicaciones, aprobado mediante acta # 30 de comité del Modelo Integrado de Gestión – MIG del 3 de abril de 2019.

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

3. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptada mediante Resolución 512 de 2019)

El Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

3.1. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptados mediante Resolución 512 de 2019)

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.
3. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información del Ministerio.
5. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
6. Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal del Ministerio.
7. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Aplica a todos los niveles del Ministerio/Fondo de las TIC, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio 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 archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el Ministerio TIC, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

5. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI

Modelo de Operación por Gestiones del Dimensión de Seguridad de la Información

6. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información son asumidas por el Comité del Modelo Integrado de Gestión (MIG) mediante Resolución No. 911 de 2018.

7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información	Equipo Activos	2-may-19	24-may-19
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	Equipo Activos	27-may-19	31-may-19
		Validar activos de información en el instrumento levantado en la vigencia anterior	Enlace de cada proceso, Equipo Activos	4-jun-19	14-jun-19
		Identificar nuevos activos de información en cada dependencia	Enlace de cada proceso, Equipo Activos	17-jun-19	27-jun-19
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo Activos	2-jul-19	12-jul-19
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Enlaces de cada proceso	15-jul-19	26-jul-19
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Enlaces de cada proceso	30-jul-19	31-dic-19
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en SIMIG por cada líder de proceso.	Enlace de cada proceso, Equipo Activos	1-ago-19	14-ago-19
		Consolidar el instrumento de activos de Información.	Equipo de Activos	15-ago-19	23-ago-19
		Publicar los instrumentos de activos de información consolidado en SIMIG	Oficina Asesora de Planeación	26-ago-19	28-ago-19

	Registros activos de información ley 1712	Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información.	Equipo de Activos	2-sep-19	13-sep-19
		Enviar a control de legalidad el instrumento de Registro Activos de información.	Equipo de Activos, Oficina Asesora Jurídica.	16-sep-19	20-sep-19
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	Oficina Asesora Jurídica	27-sep-19	27-sep-19
	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos .	Equipo de Activos	30-sep-19	30-sep-19
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo de Gestión de Riesgos	1-mar-19	30-mar-19
	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	1-abr-19	9-abr-19
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	29-abr-19	30-sep-19
		Realimentación, revisión y verificación de los riesgos identificados(Ajustes)	Equipo de Gestión de Riesgos	29-abr-19	30-sep-19
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	29-jun-19	30-nov-19
	Publicación	Publicación Matriz de riesgos - SIMIG	Equipo de Gestión de Riesgos	29-jun-19	30-nov-19
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Equipo de Gestión de Riesgos	29-jun-19	1-dic-19
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de Gestión de Riesgos	29-jun-19	31-dic-19
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de Gestión de Riesgos	29-jun-19	31-dic-19
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Equipo de Gestión de Riesgos	29-jun-19	31-dic-19
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	29-jun-19	31-dic-19
Gestión de Incidentes de	Elaboración de procedimiento de gestión de incidentes de seguridad	Elaboración del procedimiento de gestión de incidentes basados en la ISO 27035	Equipo Incidente	2-may-19	31-may-19

Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Publicar el procedimiento de gestión de incidentes de Seguridad de la Información en SIMIG	Encargado de la Gestión de Incidentes de Seguridad de la Información.	4-jun-19	7-jun-19
		Socializar el procedimiento a los especialistas de la OTI, indicando los cambios en el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información.	10-jun-19	14-jun-19
		Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información.	10-jun-19	14-jun-19
		Socializar el procedimiento a los colabores de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información	17-jun-19	21-jun-19
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Especialistas OTI - Gestión de la Información	1-jul-19	31-dic-19
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información, Encargado de Seguridad Informática y Equipo de trabajo Interno de Seguridad de la Información de Gobierno Digital	1-mar-19	27-dic-19
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Profesional de la OTI, encargado de la Gestión de Incidentes de Seguridad de la Información.	1-mar-19	27-dic-19
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	1-abr-19	12-abr-19

Continuidad de la Operación		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	11-abr-19	12-abr-19
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Gestor de procesos	2-may-19	31-dic-19
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	1-jun-19	31-dic-19
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	2-may-19	30-may-19
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	4-jun-19	31-dic-19
Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
		Publicación del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
	Documentación de Valoración de Riesgos de Interrupción	Actualización del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
		Publicación Valoración de Riesgos de interrupción	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
		Publicación Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19

	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
		Aprobación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	1-jul-19	31-dic-19
Acciones correctivas y Notas de mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM en SIMIG	Planeación	11-feb-19	31-dic-19
		Solicitar el cargue del análisis de causas o plan de tratamiento según sea requerido.	Planeación	11-feb-19	31-dic-19
	Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Planeación	11-feb-19	31-dic-19
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Oficial de Seguridad de la Información	4-feb-19	30-abr-19
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Oficial de Seguridad de la Información	1-may-19	31-dic-19
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Oficial de Seguridad de la Información	7-feb-19	28-feb-19
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad de la Información	1-mar-19	30-mar-19
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de Seguridad de la Información	1-mar-19	30-mar-19
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Oficial de Seguridad de la Información	1-mar-19	31-dic-19
	CCOC	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de Seguridad de la Información	7-feb-19	31-dic-19
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el PAAI	Todos los procesos	1-oct-19	31-dic-19

Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013,	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Oficial de Seguridad de la Información	7-feb-19	31-dic-19
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Oficial de Seguridad de la Información	15-mar-19	30-jun-19
		Reportar indicadores	Gestores de procesos	2-jul-19	31-dic-19
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de Seguridad, OTI	11-mar-19	22-mar-19
	Contratar Análisis de Vulnerabilidades y Pentest	Definir estudios previos y procesos de contratación para realizar el pentes y análisis de vulnerabilidades teniendo en cuenta el alcance y mitología	Oficial De Seguridad, OTI, Contractual	2-jul-19	30-jul-19
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	Pentester	1-sep-19	30-sep-19
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest	Oficial De Seguridad, OTI	1-oct-19	31-dic-19
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	Oficial De Seguridad y Secretaría General	25-feb-19	28-feb-19
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial De Seguridad y Gestor de procesos	4-mar-19	31-dic-19
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oficial de Seguridad	1-abr-19	31-dic-19

8. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** 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 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario
- **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.
- **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 911 de 2018.** Por la cual se actualiza el Modelo Integrado de Gestión del MinTIC.
- **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
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
28/02/2019	Versión 1	Elaboración del Plan

Elaboró: Andrés Díaz Molina – Asesor del Despacho de la Ministra de TIC, con funciones de Oficial de Seguridad de la información – adiazm@mintic.gov.co
Aprobó: Comité MIG de acuerdo a acta # 30 del 3 de abril de 2019