



El futuro digital  
es de todos

MinTIC

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

*Versión 6.0*

Ministerio de Tecnologías de la Información y las Comunicaciones

Despacho de la Ministra  
Seguridad y Privacidad de la Información



**POR UN  
MINTIC  
SEGURO**

© 2022



Pública

Ministerio de Tecnologías de la Información y las Comunicaciones  
Edificio Murillo Toro, Carrera 8a, entre calles 12A y 12B  
Código Postal: 111711 . Bogotá, Colombia  
Teléfono Conmutador: +57601344346  
Línea Gratuita: 01-800-0914014  
[www.mintic.gov.co](http://www.mintic.gov.co)



SPI-TIC-DI-003  
V 6.0



## TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	3
2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	3
3. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	4
4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptada mediante Resolución 0448 de 2022).....	4
4.1. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptados mediante Resolución 0448 de 2022).....	5
5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. ....	5
7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	6
8. DOCUMENTOS DE REFERENCIA .....	14
9. CONTROL DE CAMBIOS .....	17





## 1. INTRODUCCIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, mediante la Resolución 1092 del 11 de mayo de 2021, - “Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2306 del 2020 y sus modificatorias”, artículo 4. *Alineación MIG con otros modelos y sistemas de gestión.* Expresa que (...) *La implementación del MIG, a través de sus dimensiones y eje articulador señalados en los artículos 2 y 3 de este acto administrativo, responden a los requisitos y lineamientos normativos, a la dinámica organizacional y a mecanismos que facilitan la articulación de modelos y sistemas como lo son el MIPG, Responsabilidad social institucional, modelo de seguridad y privacidad de la información, entre otros.(...),* e indica los procesos relacionados con la alineación de las políticas del MIG, indicando que (...) *La política de Gobierno digital (en donde se encuentra como habilitador el Modelo de Seguridad de la Información) los Procesos (Fortalecimiento organizacional, Gestión de TI, Seguridad y privacidad de la Información) y la política de Seguridad digital (Fortalecimiento organizacional, Gestión de TI, Seguridad y privacidad de la Información)(...),* así mismo, en el artículo 18° por el cual se establecen las funciones del Comité MIG, especialmente en los numerales 14 –*“Aprobar y hacer seguimiento a la implementación de políticas de gestión y directrices en materia de Estrategia de Gobierno Digital y Seguridad y privacidad de la Información y al Plan Estratégico de Tecnologías Información de la Entidad.”-* y 15 –*“Aprobar y apoyar la implementación del plan de continuidad de la operación del Ministerio, con el fin de mitigar los riesgos asociados a una posible interrupción de la operación.”-* 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, de igual manera el 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, en el parágrafo del artículo 16 indica que (...) *Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.(...)*

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 de la sesión # 52 de comité del Modelo Integrado de Gestión – MIG del 29 de diciembre de 2021.

## 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. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones adopta en su modelo de procesos, el proceso de Seguridad y Privacidad de la Información en el nivel estratégico que permitirá garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en el Ministerio, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.



Ciclo PHVA del proceso de Seguridad y Privacidad

### 4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptada mediante Resolución 0448 de 2022)

El Ministerio/Fondo Único de TIC, 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, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.





#### 4.1. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL MINISTERIO/FONDO ÚNICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptados mediante Resolución 0448 de 2022)

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios.
3. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.
4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información del Ministerio/Fondo Único de TIC.
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 un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.
7. Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
8. Definir, operar y mantener el Plan de Continuidad de la Operación de los servicios del Ministerio/Fondo Único de TIC

#### 5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones.

#### ÁMBITO DE APLICACIÓN

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Ministerio/Fondo Único de TIC, aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a la entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, esta política aplica a toda la información creada, procesada o utilizada por el Ministerio/Fondo Único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre.





## 6. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI



Modelo de Operación por Gestiones de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la Operación

## 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	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique	Equipo Activos	Documentación actualizada en SIMIG	1-jun-22	30-jun-22
	Levantamiento Activos de Información	Socializar la metodología de activos de Información.	Equipo Activos	Listado de asistencia	1-jun-22	5-jul-22
		Validar activos de información en el instrumento levantado en la vigencia anterior	Enlace de cada proceso, Equipo Activos	Acta de Reunión	5-jul-22	30-jul-22





Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
		Identificar nuevos activos de información en cada dependencia	Enlace de cada proceso, Equipo Activos	Acta de Reunión, Formato GDO-TIC-FM-032 diligenciado	18-jul-22	5-ago-22
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo Activos	Correos electrónicos	1-ago-22	31-ago-22
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Enlaces de cada proceso	Formato GDO-TIC-FM-032 diligenciado	8-ago-22	31-ago-22
		Actualización del inventario de 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.	Gestores de cada proceso	Correo electrónico, Formato GDO-TIC-FM-032 diligenciado	3-oct-22	30-dic-22
	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	Memorando de aceptación	1-sep-22	30-sep-22
		Consolidar el instrumento de activos de Información.	Equipo de Activos	GDO-TIC-DI-020 Consolidado activos de la información MinTIC	3-oct-22	31-oct-22
		Publicar los instrumentos de activos de información consolidado en SIMIG	Equipo de Activos, Oficina Asesora de Planeación y Estudios Sectoriales, GIT de Grupos de Interés y Gestión Documental	GDO-TIC-DI-020 Consolidado activos de la información MinTIC publicado en SIMIG	1-dic-22	19-dic-22







Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
	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	Documento Registro Activos de Información	3-oct-22	31-oct-22
		Enviar a control de legalidad el instrumento de Registro Activos de información.	Equipo de Activos, Oficina Asesora Jurídica.	Correo electrónico	1-nov-22	30-nov-22
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	Equipo de Activos, Oficina Asesora de Prensa, Oficina de TI	Correo electrónico con la solicitud	1-dic-22	19-dic-22
Reporte Datos Personales	Reportar al Oficial de Protección de Datos personales la información recolectada en el instrumento de activos, correspondiente a bases de datos con datos personales.	Equipo de Activos, Oficial de Protección de Datos personales	GDO-TIC-DI-020 Consolidado activos de la información MinTIC publicado en SIMIG	1-dic-22	19-dic-22	
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Equipo de Gestión de Riesgos	Correos electrónicos, Documentación actualizada en SIMIG	1-feb-22	30-nov-22
	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	Listas de asistencia, Correos electrónicos	1-mar-22	31-may-22
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Equipo de Gestión de Riesgos	Correos electrónicos Mapas de riesgos	1-mar-22	31-may-22
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de Gestión de Riesgos	Correos electrónicos Mapas de riesgos	1-mar-22	31-may-22
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	Memorandos de aceptación mapas de riesgos	2-may-22	15-jun-22
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Equipo de Gestión de Riesgos	Mapas de riesgos publicados en SIMIG	1-jun-22	30-jun-22
	Seguimiento Fase de Tratamiento	Seguimiento controles y planes de tratamiento de riesgos los	Equipo de Gestión de Riesgos	Seguimiento mapas de riesgos, seguimiento plan operativo	17-ene-22	23-dic-22







Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
		identificados (verificación de evidencias)				
	Seguimiento valoración de riesgos residuales	Seguimiento a la valoración de los riesgos residuales	Equipo de Gestión de Riesgos	Seguimiento mapas de riesgos	17-ene-22	23-dic-22
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de los planes de tratamiento y al seguimiento de la valoración de los riesgos residuales	Equipo de Gestión de Riesgos	Correos electrónicos	17-ene-22	23-dic-22
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Equipo de Gestión de Riesgos	Correos electrónicos, Documentación actualizada	1-jul-22	23-dic-22
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	Correos electrónicos reporte indicador	17-ene-22	30-dic-22
Gestión de Incidentes de Seguridad y Privacidad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación cuando se requiera el procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035	Encargado de la Gestión de Incidentes de Seguridad de la Información.	Documentación actualizada en SIMIG	14-feb-22	30-jun-22
		Socializar cuando se requiera el procedimiento a los especialistas de la OTI, soportes en sitio, Mesa de Servicios indicando los cambios en el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información.	Correos electrónicos, listados de asistencia	14-feb-22	30-jun-22
		Socializar el procedimiento a los colaboradores de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información	Correo electrónico	14-feb-22	30-jun-22
	Gestionar los incidentes de Seguridad de la Información identificados	Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo a lo establecido en el procedimiento definido	Especialistas OTI - Gestión de la Información	Correos electrónicos, seguimiento al reporte de incidentes	1-ene-22	31-dic-22
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad y Privacidad de la Información, Encargado de Seguridad Informática y	Boletines publicados en el Micrositio	22-ene-22	15-dic-22





Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
			Equipo de trabajo Interno de Seguridad de la Información de Gobierno Digital			
	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.	correos electrónicos	22-ene-22	15-dic-22
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Actualizar la documentación del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital, en el caso que aplique	Oficial de Seguridad y Privacidad de la Información	Documentación actualizada en SIMIG	17-ene-22	11-feb-22
		Publicar y Divulgar el Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital con los gestores de procesos, en el caso que aplique	Oficial de Seguridad y Privacidad de la Información	Correo electrónico	31-ene-22	11-feb-22
	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 Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Oficial de Seguridad y Privacidad de la Información, Gestor de procesos	Correo electrónico, listados de asistencia	14-feb-22	23-dic-22
	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 Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Oficial de Seguridad y Privacidad de la Información	Informe de medición	14-feb-22	23-dic-22
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Actualizar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Actualización la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficial de Seguridad y Privacidad de la Información, Oficina Asesora de Planeación y Estudios Sectoriales	Documentación actualizada en SIMIG	17-ene-22	23-dic-22





Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas		
					Fecha Inicio	Fecha Final	
	Revisar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Solicitar las evidencias del cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficial de Seguridad y Privacidad de la Información	Correo electrónico, MIG-TIC-DI-023 Matriz Identificación de Requisitos Legales y de Otra índole actualizado y publicado en SIMIG	17-ene-22	23-dic-22	
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	Documento actualizado en SIMIG	12-jun-22	30-dic-22	
		Publicación del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio	Publicación en SIMIG del documento	18-jul-22	30-dic-22	
	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	Documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación actualizado en SIMIG	15-jun-22	30-dic-22	
		Publicación Valoración de Riesgos de interrupción	Equipo de Continuidad del Negocio	Publicación en SIMIG del documento	30-jun-22	30-dic-22	
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	Documento Estrategias de Continuidad de la Operación actualizado en SIMIG	21-jun-22	30-dic-22	
		Publicación Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	Publicación en SIMIG del documento	5-jul-22	30-dic-22	
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	Documentación del Plan de continuidad de la Operación	4-jun-22	30-dic-22	
		Aprobación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	Memorando de aprobación	24-ago-22	30-dic-22	
	Oportunidades de mejoras SGSI	Reporte del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM en SIMIG	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Informe del estado actual de las AC y OM del proceso	17-ene-22	23-dic-22
			Solicitar y/o realizar el cargue del análisis de causas y plan de tratamiento según sea requerido.	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Correo electrónico, Documento Análisis de Causa y plan de tratamiento	17-ene-22	23-dic-22





Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Correos electrónicos	17-ene-22	23-dic-22
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar cuando se requiera los Manuales, Políticas, Resoluciones, documentación del SGSPI y la documentación estratégica del proceso de Seguridad y privacidad de la Información.	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Documentación actualizada en SIMIG y Página Web	17-ene-22	23-dic-22
		Actualizar el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos.	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Documentación actualizada en SIMIG y Página Web	15-nov-21	31-ene-22
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 y Privacidad de la Información y equipo implementador	Documento de Diagnostico de MINTIC para Medición del MSPI	15-abr-22	14-may-22
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad y Privacidad de la Información	Documentación actualizada y alineada al MSPI	15-abr-22	14-may-22
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de Seguridad y Privacidad de la Información	Herramienta de diagnóstico del MinTIC	15-abr-22	14-may-22
		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 y Privacidad de la Información	Actas de reuniones	15-abr-22	14-may-22
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de Seguridad y Privacidad de la Información	Diligenciamiento y/o Actualización de la Matriz de ICC, correo electrónico de lo enviado por las entidades de la mesa sectorial	1-mar-22	20-dic-22
Enfoque sectorial	Dar lineamientos en seguridad y privacidad de la	Realizar mesa sectorial de seguridad y privacidad de la	Oficial de Seguridad y	correo electrónico	11-feb-22	23-dic-22





Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
	información a las entidades adscritas al sector	información y seguridad digital y continuidad de los servicios	Privacidad de la Información			
		Realizar seguimiento a la implementación del MSPÍ en las entidades adscritas al sector	Oficial de Seguridad y Privacidad de la Información	Presentaciones entidades adscritas, grabación, lista de asistencia	11-feb-22	23-dic-22
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	Listado de asistencia, informes de auditorías	11-feb-22	23-dic-22
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 y Privacidad de la Información	Herramienta diligenciada	7-feb-22	23-dic-22
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Oficial de Seguridad y Privacidad de la Información	Correos electrónicos, Hoja de vida indicadores	17-ene-22	30-nov-22
		Reportar indicadores	Gestores de procesos	Correos electrónicos, Reporte indicadores SIMIG, ASPA	17-ene-22	30-dic-22
Vulnerabilidades	Definir lineamientos para ejecutar las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de Seguridad y Privacidad de la Información, OTI	Anexo Técnico	11-ene-22	20-ene-22
	Contratar Análisis de Vulnerabilidades y Pentest	Definir estudios previos y procesos de contratación para realizar el pentest y análisis de vulnerabilidades teniendo en cuenta el alcance y metodología	Oficial de Seguridad y Privacidad de la Información, OTI, Contractual	Documentación contractual	20-ene-22	14-abr-22
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo con el alcance y la metodología establecida	Pentester	Informe Ejecución de Pruebas	11-may-22	30-nov-22
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pentest	Oficial de Seguridad y Privacidad de la Información, OTI	Seguimiento Remediación de vulnerabilidades	11-may-22	30-nov-22
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de	Oficial de Seguridad y Privacidad de	Memorando Firmado y enviado por el Oficial de	22-ene-22	5-feb-22





Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
		datos personales de acuerdo con los estándares emitidos por la SIC	la Información y Secretaría General	Seguridad y Privacidad de la Información		
	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 Privacidad de la Información y Gestor de procesos	Formatos y listados de asistencia	1-feb-22	20-dic-22
	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 y Privacidad de la Información	Certificado del registro de BD que expide la SIC	22-abr-22	20-dic-22

## 8. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia.** Artículos 15, 20, 23 y 74.
- **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 23 de 1982.** Sobre derechos de autor
- **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).
- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos
- **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.
- **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
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas
- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **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 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **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 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 1450 de 2011.** Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- **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 1753 de 2015.** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”.
- **Ley 1755 de 2015.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **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 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.
- **CONPES 3854 de 2017.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020.** Confianza y Seguridad Digital
- **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 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1287 de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Directiva 26 de 2020.** Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario
- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- **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.
- **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 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 1068 de 2015.** por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **Decreto 620 de 2020.** por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del párrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 884 de 2012.** por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **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.
- **Ley 2088 de 2021.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones
- **Resolución 1838 de 2022.** Por la cual se reglamentan las modalidades de teletrabajo, se establecen las condiciones de trabajo en casa y se definen los lineamientos de desconexión laboral en el MINTIC, y se deroga la resolución 1151 del 16 de mayo de 2019.
- **Resolución 0448 de 2022.** Por la cual se actualiza 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, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.
- **Resolución 924 de 2020.** Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2007 de 2018.
- **Resolución 1519 de 2020.** “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **Resolución 500 de 2021.** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- **Decreto 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- **Decreto 338 de 2022.** Por el cual se adiciona el Título 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 767 de 2022.** 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 746 de 2022.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021





- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.

## 9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
28/02/2019	Versión 1	Elaboración del Plan
26/12/2019	Versión 2	Actualización del Plan por cambio a vigencia 2020
13/08/2020	Versión 2.1	Actualización documentos de referencia.
22/12/2020	Versión 3.0	Actualización del Plan por cambio a vigencia 2021
29/12/2021	Versión 4.0	Actualización del Plan por cambio a vigencia 2022
15/02/2022	Versión 5.0	Actualización del Plan por entrada en vigor de la nueva Resolución 0448 de 2022. Actualización de los documentos de referencia.
01/08/2022	Versión 6.0	Se actualizan y amplían las fechas de las actividades finales de ejecución del Plan de Continuidad de la Operación relacionadas, dicha ampliación fue aprobada por todos los miembros del comité MIG en la sesión virtual No. 58 llevada a cabo del 25/07/2022 al 27/07/2022.  Se actualiza la sección 8. DOCUMENTOS DE REFERENCIA

Elaboró: Rosa Lucia Ortega –Funcionaria– [rlortega@mintic.gov.co](mailto:rlortega@mintic.gov.co), Giovanni Andrés Espitia Roa – Contratista – [gespitia@mintic.gov.co](mailto:gespitia@mintic.gov.co), Sergio Andrés Ramos P- Contratista – [sramos@mintic.gov.co](mailto:sramos@mintic.gov.co).

Revisó: Andrés Díaz Molina – Asesor del Despacho de la Ministra de TIC, con funciones de Oficial de Seguridad y Privacidad de la información – [adiazm@mintic.gov.co](mailto:adiazm@mintic.gov.co)

Aprobó: Comité MIG en sesión #52 del 29 de diciembre de 2021

