



El futuro digital
es de todos

MinTIC

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 3.0

Ministerio de Tecnologías de la Información y las Comunicaciones

Despacho de la Ministra
Seguridad y Privacidad de la Información



POR UN
MINTIC
SEGURO

© 2021



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 DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptada mediante Resolución 2256 de 2020).....	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 DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptados mediante Resolución 2256 de 2020).....	5
5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	5
7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.....	6
8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 6	
9. DOCUMENTOS DE REFERENCIA.....	11
CONTROL DE CAMBIOS.....	14



1. INTRODUCCIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, mediante la Resolución 2306 del 7 de noviembre de 2020, -“ Por la cual se actualiza el Modelo Integrado de Gestión (MIG), se adopta el Sistema Integrado de Gestión (SIG) del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 1905 de 2019 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, Direccionamiento estratégico, Gestión jurídica, Comunicación estratégica, Gestión de recursos administrativos) y la política de Seguridad digital (Fortalecimiento organizacional, Gestión de TI, Direccionamiento estratégico, Gestión jurídica)(...), así mismo, en el artículo 9° por el cual se establecen las responsabilidades 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 de la Información en la Entidad y al Plan Estratégico de Tecnologías Información.”- 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 misma.”-. 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 # xx de comité del Modelo Integrado de Gestión – MIG del xx 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 DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptada mediante Resolución 2256 de 2020)

El Ministerio/Fondo Único 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, 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 y regulatorios, 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 DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (Adoptados mediante Resolución 2256 de 2020)

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, 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 conciencia y apropiación de la Seguridad y Privacidad de la Información y la Seguridad Digital.
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.
8. Definir, operar, 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 DE LA INFORMACIÓN.

Aplica a todos los niveles del Ministerio/Fondo Único de 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 tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por el Ministerio TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

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





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

7. 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. 2306 de 2020.

8. 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	Actualización de metodología e instrumento de levantamiento de activos de información	Equipo Activos	jun-01-2021	jun-30-2021
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	Equipo Activos	jun-01-2021	jun-30-2021
		Validar activos de información en el instrumento levantado en la vigencia anterior	Enlace de cada proceso, Equipo Activos	jul-01-2021	jul-30-2021
		Identificar nuevos activos de información en cada dependencia	Enlace de cada proceso, Equipo Activos	jul-15-2021	jul-30-2021
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Equipo Activos	ago-02-2021	ago-30-2021
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Enlaces de cada proceso	ago-23-2021	ago-30-2021
		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 cambian la criticidad del activo.	Enlaces de cada proceso	ago-20-2021	dic-29-2021
		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	sept-01-2021
	Consolidar el instrumento de activos de Información.		Equipo de Activos	oct-01-2021	oct-29-2021



		Publicar los instrumentos de activos de información consolidado en SIMIG	Oficina Asesora de Planeación	dic-01-2021	dic-20-2021
	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	oct-01-2021	oct-29-20
		Enviar a control de legalidad el instrumento de Registro Activos de información.	Equipo de Activos, Oficina Asesora Jurídica.	nov-02-2021	nov-30-20
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	Oficina Asesora Jurídica	dic-01-20	dic-20-2021
	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	sep-20-2021	sep-20-2021
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo de Gestión de Riesgos	mar-22-2021	ago-31-2021
	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	abr-19-2021	may-31-2021
	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	may-31-2021	sep-30-2021
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de Gestión de Riesgos	may-31-2021	sep-30-2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos	jun-21-2021	nov-19-2021
	Publicación	Publicación Matriz de riesgos - SIMIG	Equipo de Gestión de Riesgos	jun-21-2021	nov-19-2021
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Equipo de Gestión de Riesgos	jun-21-2021	dic-20-2021
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de Gestión de Riesgos	jun-21-2021	dic-20-2021
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de Gestión de Riesgos	jun-21-2021	dic-20-2021
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Equipo de Gestión de Riesgos	jun-21-2021	dic-20-2021



	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	jun-21-2021	dic-20-2021
Gestión de Incidentes de Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación del 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.	feb-15-2021	mar-15-2021
		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.	mar-19-2021	mar-26-2021
		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.	mar-19-2021	mar-26-2021
		Socializar el procedimiento a los colaboradores de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información	mar-19-2021	mar-26-2021
	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	ene-1-2021	dic-31-2021
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información, Encargado de Seguridad Informática y GIT de Seguridad de la Información de Gobierno Digital	ene-22-2021	dic-15-2021
	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.	ene-22-2021	dic-15-2021
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital	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	ene-18-2021	ene-29-2021



y 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	ene-29-2021	feb-12-2021
	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	feb-12-2021	dic-20-2021
	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	feb-12-2021	dic-20-2021
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	ene-22-2021	dic-22-2021
	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	jun-21-2021	dic-21-2021
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	abr-12-2021	dic-21-2021
		Publicación del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio	dic-6-2021	dic-20-2021
	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	abr-12-2021	dic-21-2021
		Publicación Valoración de Riesgos de interrupción	Equipo de Continuidad del Negocio	dic-6-2021	dic-20-2021
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	abr-12-2021	dic-21-2021
		Publicación Estrategias de Continuidad de la Operación	Equipo de Continuidad del Negocio	dic-6-2021	dic-20-2021



	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	abr-12-2021	dic-21-2021
		Aprobación del Plan de continuidad de la Operación	Equipo de Continuidad del Negocio	dic-6-2021	dic-20-2021
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	ene-18-2021	dic-20-2021
		Solicitar el cargue del análisis de causas o plan de tratamiento según sea requerido.	Planeación	ene-18-2021	dic-20-2021
	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	ene-18-2021	dic-20-2021
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	may-3-2021	may-31-2021
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Oficial de Seguridad de la Información	jun-4-2021	dic-21-2021
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	abr-15-2021	may-14-2021
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad de la Información	abr-15-2021	may-14-2021
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de Seguridad de la Información	abr-15-2021	may-14-2021
		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	abr-15-2021	may-14-2021
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de Seguridad de la Información	mar-1-2021	dic-20-2021
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	De acuerdo con programa de la OCI	De acuerdo con programa de la OCI



Enfoque sectorial	Dar lineamientos en seguridad y privacidad de la información a las entidades adscritas al sector	Realizar mesa sectorial de seguridad y privacidad de la información y seguridad digital y continuidad de los servicios	Oficial de Seguridad y Privacidad de la Información	feb-11-2021	dic-16-2021
		Generar reporte de la información histórica del cumplimiento de seguridad digital de las entidades adscritas al sector	Oficial de Seguridad y Privacidad de la Información	jul-30-2021	dic-27-2021
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	jun-4-2021	dic-21-2021
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	ene-20-2021	jun-21-2021
		Reportar indicadores	Gestores de procesos	jul-21-2021	dic-21-2021
Vulnerabilidades	Definir lineamientos para ejecutar análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Definir los lineamientos, estudios previos, anexo técnico y el alcance para la realización de análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Oficial de Seguridad, OTI	abr-5-2021	abr-30-2021
	Contratar análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Ejecutar el procesos de contratación para realizar análisis GAP, análisis de vulnerabilidades y Éthical Hacking teniendo en cuenta el alcance y metodología	Oficial De Seguridad, OTI, Contractual	may-3-2021	jul-30-2021
	Ejecución del contrato	Ejecución del contrato de análisis GAP, análisis de vulnerabilidades y Éthical Hacking de acuerdo al alcance y la metodología establecida	Proveedor	ago-9-2021	nov-30-2021
	Iniciar la ejecución del plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis GAP, análisis de vulnerabilidades y Ethical Hacking	Oficial de Seguridad, OTI	dic-1-2021	dic-31-2021
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad y Secretaría General	ene-18-2021	ene-29-2021
	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	feb-1-2021	dic-20-2021
	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	abr-22-2021	dic-20-2021

9. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** 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 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
- **Ley 1955 de 2019.** por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
- **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.
- **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.
- **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 1064 de 2020.** Por el cual se modifica la estructura del Ministerio 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 2306 de 2020.** 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
- **Resolución 1151 de 2019.** Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 0002133 del 3 de agosto de 2018
- **Resolución 924 de 2020.** Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.
- **Resolución 2256 de 2020.** 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 y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 1124 de 2020.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3905 de 2020.** Política Nacional de Confianza y Seguridad Digital.



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

Elaboró: Dayana Carbonó Carbonó – Contratista – dcarbono@mintic.gov.co, Giovanni Andrés Espitia Roa – Contratista – gespitia@mintic.gov.co, Eduardo Santiago Vanegas Galvis – Pasante Universitario – evanegasg@mintic.gov.co.

Revisó: 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 en sesión # 45 del 22 al 23 de diciembre de 2020