Igualdad

Política de Seguridad y Privacidad de la Información

MINISTERIO DE IGUALDAD Y EQUIDAD

Carlos Rosero

Ministro de Igualdad y Equidad

William Alexander Duarte Vargas

Jefe Oficina de Tecnologías de la Información

Juan Diego Mallama C.

Luz Amparo Gantiva R.

Nelson Alberto Gutiérrez P.

Carlos Fredy Rey C.

Andrés Felipe Rodríguez G.

Juan Aponte Buitrago

Javier Pereira Vargas

Oficina de Tecnologías de la Información - Grupo de Transformación Digital

Edwin Sánchez R.

Natalia Bayona A.

Rafael Coronado B.

Joan Daniel Barragán R.

Kevin Santiago Sabogal H.

Iván Andrés Cardona M.

Oficina de Tecnologías de la Información - Grupo Servicios Tecnológico

Estructuración visual del documento realizada por: Oficina Asesora de Planeación

Fecha de Aprobación: 16 de Julio de 2025

Contenido

I. PRESENTACIÓN

El Ministerio de Igualdad y Equidad – MIE, como organismo principal del sector central de la Rama Ejecutiva del orden nacional, tal como lo establece la Ley 2881 de enero de 2023, y en cuyo objeto establece el artículo 3 qué, "*El Ministerio de Igualdad y Equidad tiene como objeto, en el marco de los mandatos constitucionales, de la ley y de sus competencias, diseñar, formular, adoptar, dirigir, coordinar, articular, ejecutar fortalecer y evaluar, las políticas, planes, programas, estrategias, proyectos y medidas para contribuir en la eliminación de las desigualdades económicas, políticas y sociales; impulsar el goce del derecho a la igualdad; el cumplimiento de los principios de no discriminación y no regresividad...*". Así mismo el artículo 4, numeral 9, indica la responsabilidad de, "*Establecer esquemas de seguimiento, monitoreo y evaluación a la ejecución de las políticas, planes, proyectos y oferta social de competencia del Sector de Igualdad y Equidad, en coordinación con otras entidades competentes, y rendir cuentas a la ciudadanía. Para este efecto, se promocionarán y adoptarán mecanismos participativos de control social*". En ese mismo sentido el artículo 7 establece qué, "*El Ministerio de Igualdad y Equidad tendrá como sede y domicilio la ciudad de Bogotá, DC, ejercerá sus funciones a nivel nacional y contará con direcciones departamentales a través de las cuales se adaptarán e implementarán las políticas del sector en el territorio nacional, de acuerdo con lo dispuesto en la presente Ley"*.

Para el cumplimiento de estos mandatos, el Ministerio de Igualdad y Equidad avanza firmemente con la implementación de una infraestructura tecnológica que permite habilitar sistemas de información, servicios de conectividad e interoperabilidad y equipos de seguridad digital robustos, por lo que, de manera responsable proyecta políticas de gestión que respaldan, aseguran, informan y permiten tomar decisiones acertadas para avanzar en el alcance de su misión y de sus objetivos. Por esto, el Ministerio de Igualdad y Equidad comprometido

particularmente con el trato responsable de los activos de información desarrollados, proyectados, habilitados y resguardados a lo largo de las actividades incluidas dentro de cada uno de los procesos que contribuyen en la construcción de políticas públicas, articulando los recursos financieros y materiales, así como para la transversalización de las políticas con enfoque Interseccional en todo el accionar del Estado, establece su Política de Seguridad y Privacidad de la Información, con el fin garantizar la confidencialidad, integridad y disponibilidad de los diferentes activos de información, mediante un adecuado tratamiento de riesgos de seguridad de la información y la generación de una cultura de buenas prácticas a través de la adopción del Modelo de Seguridad de la Información definido por MinTIC, que se desarrolla con base en el Sistema de Gestión de Seguridad de la Información institucional, alineado con el estándar ISO 27001.

II. OBJETIVO

Establecer los lineamientos y directrices aprobadas y apropiadas por la Alta Dirección para preservar la confidencialidad, integridad y disponibilidad de los activos de información y, fortalecer la cultura sobre la importancia de la seguridad de la información en las personas funcionarias, colaboradoras y sujetos de especial protección constitucional, orientado en el Modelo de Seguridad y Privacidad de la Información dispuesto por MINTIC para las entidades del estado, las políticas de Seguridad y Gobierno Digital y las buenas prácticas en seguridad de la información

III. DEFINICIONES

- **Activo de información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el

tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

- **Amenaza:** causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
- **Amenaza informática:** situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.
- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Contratista:** persona natural o jurídica contratada por el Ministerio para la adquisición de una obra, bien o servicio, no perteneciente al régimen laboral.
- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Copias de Seguridad:** es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla y disponerla en caso de que ocurra un fallo que afecte a esta
- **Disponibilidad:** propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Dato personal:** hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** es un activo de valor que hace parte del Ministeri, por la cual asume funciones como responsable o encargada de la misma en

cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato corporativo (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal y que no tiene restricciones de consulta o acceso.
- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.
- **Modelo Integrado de Planeación y Gestión- MIPG:** el Sistema de Gestión que deben aplicar las entidades públicas de la Rama ejecutiva, el cual integra y articula los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad con el Sistema de Control Interno.
- **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Política de Seguridad de la Información:** es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la

información. Contiene el conjunto de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información.

- **Seguridad informática:** conjunto de medidas técnicas que son implementadas para asegurar los recursos e información contenida en los componentes tecnológicos institucionales.
- **Seguridad de la información:** conjunto de medidas que buscan la protección de la información física, electrónica, digital del acceso, uso, divulgación o destrucción no autorizada.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

- **Enfoque diferencial e interseccional**: Perspectiva que reconoce que existen poblaciones con características particulares debido a su edad, género, orientación sexual, identidad de género, pertenencia étnica, situación de discapacidad, entre otras condiciones, que requieren una atención diferenciada.
- **Sujetos de especial protección constitucional**: Personas que debido a su condición física, psicológica o social particular merecen una acción positiva estatal para efectos de lograr una igualdad real y efectiva, conforme al ámbito de competencias definido en el artículo 5 de la Ley 2281 de 2023.

IV. NORMATIVIDAD

A continuación, se relaciona el marco normativo que establece los requisitos legales o reglamentarios identificados que debe cumplir el Ministerio de Igualdad y Equidad.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Ley	23	28	Enero	1982	Sobre derechos de autor.
Ley	44	5	Enero	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	1915	12	Julio	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	1755	30	Junio	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	1753	9	Junio	2015	Por la cual se expide el PND 2014 - 2018 "Todos por un nuevo país".
Ley	1712	6	Marzo	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	1581	17	Octubre	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	1474	12	Julio	2011	Por la cual se dictan normas y orientadas a fortalecer los mecanismos de la gestión pública.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Ley	1437	18	Enero	2011	Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
Ley	1341	18	Enero	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.
Ley	1266	31	Diciembre	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.
Ley	1273	5	Enero	2008	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.
Ley	1221	16	Julio	2008	Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.
Ley	962	8	Julio	2005	Sobre la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades.
Ley	850	18	Noviembre	2003	Por medio de la cual se reglamentan las veedurías ciudadanas.
Ley	594	14	Julio	2000	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.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Ley	489	29	Diciembre	1998	Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.
Decreto	338	28	Marzo	2022	Por el cual se adiciona el Titulo 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	16	Mayo	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	767	16	Mayo	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	88	24	Enero	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.
Decreto	612	4	Abril	2018	Por el cual se fijan directrices para la integración de los planes institucionales y

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
					estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto	1008	14	Junio	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	728	5	Mayo	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.
Decreto	1068	26	Mayo	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
Decreto	1074	26	Mayo	2015	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo.
Decreto	1078	26	Mayo	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto	1081	26	Mayo	2015	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Decreto	103	20	Enero	2015	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto	884	30	Abril	2012	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
Decreto	2364	22	Noviembre	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	2609	14	Diciembre	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

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
					y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto	1377	27	Junio	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto	1377	26	Junio	2012	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto	103	20	Enero	2015	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto	886	13	Mayo	2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Resolución	2339	21	Junio	2024	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 0448 de 2022.
Resolución	1838	31	mayo	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	2338	24	junio	2024	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 924 de 2020.
Resolución	4400	15	Diciembre	2019	Por medio de la cual se adopta la política pública de gobierno digital para Colombia.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Resolución	746	31	Marzo	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.
Resolución	500	10	Marzo	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.
Resolución	1519	17	Diciembre	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	512	14	Marzo	2019	Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.
Resolución	1234	3	Mayo	2018	Por medio de la cual se establecen lineamientos para la seguridad de la información en las entidades públicas.
Resolución	987	7	Marzo	2017	Por medio de la cual se adoptan medidas para el uso seguro de tecnologías en entidades estatales.
Circulares	12	20	Enero	2020	Circular sobre lineamientos en el manejo de datos personales.
Circulares	9	14	Octubre	2019	Circular que establece protocolos para la protección de información.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Comunicados	5	10	Febrero	2021	Comunicado oficial sobre actualización de políticas de privacidad.

V. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio de Igualdad y Equidad, reconoce y es consciente de la importancia que tienen sus activos de información, en los procesos de formulación, implementación, coordinación y evaluación de políticas, planes, programas y proyectos para avanzar en la garantía del derecho a la igualdad y la equidad para todas las personas, especialmente de los sujetos de especial protección constitucional, por lo cual se compromete con la adopción, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad y privacidad de la Información (SGSI), por medio del cual se establecen los lineamientos de seguridad y privacidad para generar un marco de confianza en el ejercicio de su misión, con los sujetos de especial protección constitucional y con el Estado.

VI. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección del Ministerio de Igualdad y Equidad mediante la definición de esta política se compromete a:

- Apoyar y liderar el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).
- Revisar de forma periódica el avance y la madurez del SGSI, la destinación de los recursos tecnológicos, de talento humano, entre otros necesarios para asegurar la eficacia y adecuación del SGSI,
- Incluir dentro de las decisiones y planes estratégicos, los temas necesarios para garantizar la seguridad y privacidad de la información clave del Ministerio.

VII. OBJETIVOS DE LA POLÍTICA

- Establecer el compromiso de la Alta Dirección, personas funcionarias y colaboradoras para el tratamiento seguro de la información.
- Cumplir con los principios de seguridad de la información.
- Garantizar la gestión adecuada de la información obtenida, generada o procesada en todos los procesos del Ministerio, mediante la implementación de controles de seguridad.
- Establecer los lineamientos, procedimientos, estándares y demás documentos en materia de seguridad de la información, que apoyen la gestión efectiva y transparente del ministerio.
- Proteger la información, promoviendo siempre la aplicación de las mejores prácticas de seguridad de la información de manera responsable

Establecer una cultura de seguridad de la información entre personas funcionarios y colaboradores.

VIII. DECLARACIÓNES

El Ministerio de Igualdad y Equidad por medio de la Oficina de Tecnologías de la Información insta a que todas las personas funcionarias, contratistas y proveedores cumplan con los lineamientos de seguridad de la información, con el fin de resguardar la información producida, recibida, recolectada, almacenada o transferida. Para ello se establecen las siguientes declaraciones de seguridad que soportan el Sistema de Gestión de Seguridad de la Información:

- Las responsabilidades frente a la seguridad de la información serán definidas, socializadas y publicadas por parte de la Oficina de Tecnologías de la Información - OTI y deberán ser aceptadas por cada una de las personas funcionarias, contratistas y proveedores que tengan acceso a la información de entidad.

- Vigilar el cumplimiento de los requisitos legales, reglamentarios y las obligaciones contractuales en materia de seguridad de la información y protección de datos personales que apliquen al Ministerio.
- Las personas funcionarias, contratistas y proveedores deben cumplir los lineamientos e instrucciones descritos en esta política y en los manuales, procedimientos, guías e instructivos definidos, así como los conceptos y lineamientos en materia de seguridad de la Información generados a solicitud.
- El Ministerio de Igualdad y Equidad es el responsable de la implementación de los mecanismos que permitan el tratamiento adecuado y seguro de la información y en especial los datos personales asociados a la ejecución de las estrategias transformadoras establecidas en la resolución 669 de 2024 del Ministerio y de los programas desarrollados por el mismo.

- El Ministerio de Igualdad y Equidad es el responsable de los activos de información y los administradores de estos activos son las personas funcionarias, contratistas o demás colaboradores que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología, y son los responsables de implementar los controles para su protección, de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El tratamiento de la información por parte de las personas funcionarias y colaboradoras debe ser realizado en la infraestructura tecnológica, sistemas de información o servicios otorgados por el Ministerio para el cumplimiento de sus funciones o desarrollo de sus actividades, según corresponda.
- Las personas funcionarias y contratistas tienen la obligación y responsabilidad de la identificación y notificación de cualquier incidente o evento que pudiera comprometer la seguridad de sus activos de información. Asimismo, la Entidad deberá implementar procedimientos para la correcta gestión de los incidentes detectados.
- Mantener un programa de sensibilización y transferencia de conocimiento continuo en el Ministerio relacionado con temas de seguridad de la información y protección de datos personales.
- Garantizar que las personas funcionarias, contratistas y terceros conozcan y cumplan, con las políticas, manuales, metodologías, procedimientos, formatos, actos administrativos y artefactos que hacen parte del Sistema de Seguridad y Privacidad de la Información.
- Gestionar los riesgos seguridad de la información acorde con la metodología definida.
- Con el fin de desarrollar el Sistema de Gestión de Seguridad de la Información, el Ministerio establece esta política como el documento principal junto con el Manual de políticas Específicas de Seguridad de la Información

- El Ministerio verifica que las actividades de seguridad de la información se desarrollarán considerando los enfoques de derechos, diferencial, étnico-racial, de género e interseccional, proporcionando la accesibilidad digital y la comprensión de las políticas para todas las personas, independientemente de sus condiciones particulares

IX. APLICABILIDAD

La presente política, sus objetivos, manuales, procedimientos y documentos derivados o complementarios deben ser conocidos y de obligatorio cumplimiento por las personas funcionarias y colaboradoras que se encuentran vinculados o prestan servicios al Ministerio, inclusive cuando las actividades de tratamiento de la información no sean parte de su función u obligación principal.

El Ministerio de Igualdad y Equidad se reserva el derecho de tomar las medidas administrativas, contractuales y/o actuaciones a que haya lugar ante el incumplimiento de la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados.

X. ROLES Y RESPONSABILIDADES

El Ministerio de Igualdad y Equidad, define los roles y responsabilidades para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos que hacen parte del SGSI, los cuales se relacionan a continuación:

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Alta Dirección	• Proporcionar los recursos económicos, humanos y de formación necesarios para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información. • Respaldar y promover la política general de seguridad de la información. • Establecer y aprobar la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información. • Revisar al menos una vez al año, la política general de seguridad de la información. • Revisar de forma periódica (al menos una vez por año) el avance y la madurez del SGSI, la destinación de los recursos tecnológicos, de talento humano, entre otros necesarios para asegurar la eficacia y adecuación del SGSI. • Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información. • Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

Mesa de Seguridad y privacidad de la información	• Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
	  ○ Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.
	  ○ Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	○ Aprobar acciones y mejores prácticas que en la implementación del MSPI. ○ Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información. • Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.
Oficina de Tecnologías de la Información.	• Liderar la formulación y aprobación de la política general de seguridad de la información. • Liderar la implementación y seguimiento a la política general de seguridad de la información • Implementar los controles de tipo tecnológico que ayuden al cumplimiento de la política. • Coordinar la implementación del SGSI. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades • Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
Oficial de Seguridad de la información o profesional designado por OTI	• Fomentar la implementación de la Política de Gobierno Digital • Asesorar a la entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente. • Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. • Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para las personas funcionarias, contratistas y colaboradores. • Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. • Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información. • Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente. • Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. • Apoyar la definición de políticas específicas de seguridad de la información en relación con la Entidad, personas funcionarias y colaboradoras, componente tecnológico y seguridad física de los activos de información.
Subdirección de Talento Humano	• Apoyar en la definición de estrategias de uso y apropiación relacionados con el componente de

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	seguridad de la información para las personas funcionarias y colaboradoras. • Controlar y salvaguardar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente. • Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.
Oficina de Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. • Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución.
Oficina de Control Interno Disciplinario	• Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Oficina Asesora de Comunicaciones	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información a todos los niveles de la entidad.
Subdirección de Contratación	• Verificar que se incluyan las obligaciones de seguridad de la información en la gestión con los proveedores y contratistas de la entidad.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	• Procurar la identificación de riesgos relacionados con la seguridad de la información de todos los activos de la información que puedan verse involucrados en los procesos de contratación.
Líderes de Proceso	• Implementar las políticas y lineamientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Personas funcionarias y colaboradoras	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y riesgos de seguridad de la información. • Reportar eventos o incidentes de seguridad de la información que evidencie fallas, accesos no autorizados o pérdida de información a la Oficina de Tecnologías de la Información. • Cumplir a cabalidad las políticas y lineamientos de seguridad de la información definidos y aprobados. • Aplicar los enfoques de derechos, diferencial, étnico-racial, de género e interseccional en las actividades relacionadas con seguridad de la información, promoviendo la accesibilidad y comprensión de los lineamientos para todas las personas.
Oficina Jurídica	• Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso. • Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	• Definir y documentar junto con los responsables de los activos de información, acuerdos para la transferencia segura que garantice el cumplimiento de las normas legales. • Identificar, evaluar y documentar junto con los responsables de los activos de información, los requisitos legales para los acuerdos de confidencialidad o no divulgación de la información. • Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. • Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
Subdirección Administrativa y Financiera	• Participar en la definición e implementación de políticas específicas relacionadas con los controles físicos, para la protección de las instalaciones donde se realiza tratamiento de información en el Ministerio
Subdirección Administrativa y Financiera Gestión Documental	• Liderar e implementar controles de seguridad para la información física que gestiona y mantiene el Ministerio. • Implementar estrategias de etiquetado de la información con el fin de realizar un proceso de clasificación más eficiente. • Apoyar en los procesos de articulación entre las tablas de retención documental y la identificación, clasificación y aceptación de activos de información de cada uno de los procesos de la Entidad.

XI. SANCIONES

La política de seguridad y privacidad de la información deberá ser adoptada y aplicada como una herramienta de obligatorio cumplimiento por parte de las personas funcionarias y colaboradoras. El incumplimiento de esta política y sus lineamientos será considerado como un incidente de seguridad de la información materializado que dará lugar a la aplicación de acciones disciplinarias definidas por la subdirección de Talento Humano y/o la Oficina de Control Interno Disciplinario, quienes harán cumplir la respectiva sanción administrativa, dando lugar a la imposición de sanciones.

Las acciones disciplinarias serán establecidas en el reglamento interno de trabajo del Ministerio de Igualdad y Equidad y estarán respaldas en las normas, leyes y estatutos de la ley colombiana, y las leyes regulatorias de delitos informáticos de Colombia.

XII. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

El Ministerio de Igualdad y Equidad realiza el seguimiento a la implementación y cumplimiento de la política general de seguridad y privacidad mediante la medición del avance y efectividad de Sistema de Gestión de Seguridad de la Información, esta medición está enfocada en los siguientes aspectos:

- Seguimiento al avance en la implementación y nivel de madurez del SGSI.

- Seguimiento de la ejecución de las actividades establecidas en el Plan Estratégico de Seguridad de la Información
- Seguimiento a la ejecución de las actividades establecidas en el Plan de Tratamiento de Riesgos de Seguridad de la Información.

XIII. APROBACIÓN Y REVISIONES

Esta política será efectiva desde su aprobación por la alta dirección a través del comité de Gestión y Desempeño, y su revisión o ajustes se darán bajo las siguientes condiciones:

- De forma anual, donde se revisará la efectividad de la política y sus objetivos.
- Cada vez que se requiera por cambios estructurales en el Ministerio.
- Por eventos de seguridad de la información que requieran ajustes en la política.

XIV. MANEJO DE EXCEPCIONES

Las excepciones a esta política, al manual de políticas específicas de seguridad de la información, procedimientos y controles del Sistema de Gestión de Seguridad deben ser evaluadas por la Oficina de Tecnologías de la Información y el Oficial de Seguridad de la Información o profesional designado, teniendo en cuenta:

- El evento que genera la excepción.
- Los posibles riesgos que puedan presentarse con la excepción.
- El posible impacto que pueda generar a excepción.

- Las acciones para el manejo de la excepción.

Las excepciones deben tener el visto bueno del líder de proceso y la evaluación y autorización del Oficial de Seguridad de la Información y/o mesa interna de seguridad de la información y/o el Comité institucional de Gestión y Desempeño en los casos que se requieran.

XV. REFERENCIAS

- ✓ Normograma Institucional recuperado de https://www.minigualdadyequidad.gov.co/normatividad_aplicable
- ✓ Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Manual de Gobierno Digital*. Recuperado de https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/
- ✓ International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022). ISO. Anexo A.
- ✓ Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Modelo de seguridad y privacidad de la información* (Versión 4.0). Recuperado de https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html

XVI. CONTROL DE CAMBIOS

Fecha	Versión	Descripción
16-07-2025	1.0.	Creación

Ministerio de
Igualdad y Equidad