Igualdad

Plan Estratégico de Seguridad de la Información – PESI 2025

MINISTERIO DE IGUALDAD Y EQUIDAD

Francia Elena Márquez Mina
Ministra de Igualdad y Equidad

Ligia Galvis Amaya
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.
Oficina de Tecnologías de la Información - Grupo de Transformación Digital

Edwin Sánchez R.
Natalia Bayona A.
Rafael Coronado B.
Joan Daniel Barragán R.
Santiago Andrés Díaz M
Kevin Santiago Sabogal H.
Iván Andrés Cardona M.
Oficina de Tecnologías de la Información - Grupo Servicios Tecnológicos

Estructuración visual del documento realizada por: Oficina Asesora de Planeación

Fecha de Aprobación Versión 1: 30-01-2025

Contenido

I. PRESENTACIÓN

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) es una herramienta que permite garantizar, en la medida de su desarrollo, a la protección de los activos de información del Ministerio de Igualdad y Equidad. Este documento estratégico busca reducir los riesgos asociados a la gestión de datos sensibles relacionados con poblaciones vulnerables y sujetos de especial protección constitucional, promoviendo la integridad, confidencialidad y disponibilidad de la información. En un contexto en el que el Ministerio lidera políticas inclusivas y de alto impacto, el PESI se posiciona como uno de los planes que aporta al desarrollo de uno de los habilitadores del Plan Nacional de Desarrollo 2022-2026 en materia de seguridad humana y justicia social, el cual se define como : "*2.A.8: Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas*", asegurando una infraestructura digital confiable y segura que respalde las funciones misionales del Ministerio.

El PESI articula estrategias como el liderazgo en seguridad de la información, la gestión de riesgos, la concientización organizacional, la implementación de controles efectivos y la gestión de incidentes. Estas estrategias no solo fortalecen la cultura institucional en torno a la seguridad digital, sino que también garantizan la capacidad de respuesta ante amenazas emergentes, destacando la importancia de integrar prácticas seguras en la digitalización de servicios y programas dirigidos a comunidades históricamente excluidas.

En última instancia, el PESI no solo cumple un rol técnico, sino que es un componente esencial para consolidar la confianza en el Ministerio y garantizar el acceso seguro a los servicios públicos digitales de acuerdo con los lineamientos de la política de gobierno digital y los habilitadores que establece. Su implementación refuerza el compromiso del Ministerio con la transparencia, la protección de datos y el respeto por los derechos fundamentales. Asimismo, el

plan promueve una sinergia entre colaboradores, ciudadanos y normativas nacionales, convirtiéndose en un ejemplo de cómo la seguridad digital puede ser un pilar para la transformación social y tecnológica en Colombia.

II. Glosario

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocio de la entidad y que, en consecuencia, debe ser protegido. Esto incluye bases de datos, archivos, sistemas de información, documentación física y digital, infraestructura tecnológica y el conocimiento de los funcionarios.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Estas pueden ser de origen interno o externo, e incluyen amenazas cibernéticas, desastres naturales, errores humanos, entre otros.

Análisis de riesgos: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo asociado a los activos de información. Este proceso implica la identificación de vulnerabilidades, la evaluación de la probabilidad e impacto de las amenazas, y la determinación del nivel de riesgo resultante.

Arquitectura de Seguridad: Descripción detallada de todos los aspectos de seguridad en una organización, incluyendo principios, políticas, modelos, controles y procedimientos de seguridad.

Ciberseguridad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados. Implica garantizar que solo las personas autorizadas tengan acceso a la información según su nivel de clasificación. Esto se logra mediante la implementación de controles de acceso, políticas de seguridad, cifrado de datos y concientización del personal sobre el manejo adecuado de la información sensible.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Asegura que solo aquellos con los permisos adecuados puedan acceder a la información.

Control: Medida que modifica el riesgo. Estos pueden ser de naturaleza técnica (como firewalls o sistemas de detección de intrusos), administrativa (como políticas y procedimientos) o física (como controles de acceso a instalaciones).

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Esto implica implementar medidas como sistemas de respaldo, planes de continuidad del negocio, redundancia de infraestructura y políticas de mantenimiento preventivo.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables. Ayuda a priorizar los riesgos y determinar las acciones necesarias.

Gestión de incidentes: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. Esto incluye la implementación de un equipo de respuesta a incidentes, procedimientos de escalamiento, análisis forense digital y mecanismos para la mejora continua basada en las lecciones aprendidas de incidentes pasados.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Implica la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos.

Integridad: Propiedad de la información relativa a su exactitud y completitud. Esto se logra mediante la implementación de controles como firmas digitales, checksums, control de versiones y políticas de gestión de cambios.

MSPI: Modelo de Seguridad y Privacidad de la Información, definido por el MinTIC para las entidades del Estado colombiano. Proporciona lineamientos para la implementación de un sistema de gestión de seguridad de la información.

MGGTI: Modelo de Gestión y Gobierno de TI, parte del Marco de Referencia de Arquitectura Empresarial del Estado colombiano. Es una guía integral que proporciona lineamientos para la gestión estratégica de las tecnologías de la información en las entidades públicas.

MRAE: Marco de Referencia de Arquitectura Empresarial, instrumento principal para implementar la Arquitectura TI de Colombia. En relación con la seguridad de la información, el MRAE proporciona un enfoque estructurado para alinear la estrategia de TI con la estrategia institucional, incluyendo consideraciones de seguridad en todos los dominios de la arquitectura empresarial.

Plan de continuidad del negocio: Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación tras una interrupción. Incluye estrategias de recuperación, roles y responsabilidades.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. Detalla las medidas específicas que se implementarán para mitigar los riesgos identificados, asignando responsabilidades, recursos y plazos para su ejecución.

Política de seguridad: Documento de alto nivel que establece el compromiso de la alta dirección a través de la Oficina de TI, junto con quienes se considere, con la seguridad de la información, define los objetivos de seguridad y proporciona un marco para la implementación de controles.

Privacidad: Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales. Implica el control sobre la recolección, uso y divulgación de información personal.

Riesgo: Se refiere a la posibilidad de que una amenaza explote una vulnerabilidad, causando daño a los activos de información y, por ende, a los objetivos de la entidad.

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Autenticación: Proceso mediante el cual se verifica la identidad de un usuario, dispositivo o sistema antes de permitir el acceso a recursos o información protegidos.

Autorización: Proceso que determina qué acciones o recursos están permitidos para un usuario, dispositivo o sistema autenticado. Las entidades públicas deben establecer políticas y procedimientos claros para la gestión de autorizaciones, incluyendo la revisión periódica de los permisos de acceso y la revocación inmediata de privilegios cuando un empleado cambia de rol o deja la organización.

Cifrado: Proceso de convertir información legible en un formato codificado e ilegible para protegerla de accesos no autorizados.

Firewall: Sistema de seguridad que monitorea y controla el tráfico de red entrante y saliente basándose en reglas de seguridad predeterminadas.

Malware: Término general que se refiere a software malicioso diseñado para dañar, interrumpir u obtener acceso no autorizado a sistemas informáticos.

III. Objetivos

Objetivo general

Adoptar el Modelo de Seguridad y Privacidad de la Información MSPI en el Ministerio de Igualdad y Equidad para garantizar la integridad, confidencialidad y disponibilidad de la información, protegiendo los activos digitales y respaldando su misión institucional mediante estrategias integrales que promuevan la confianza, la transparencia y el cumplimiento de las normativas nacionales e internacionales en materia de seguridad digital.

Objetivos Específicos

1. Diseñar el sistema de gestión de seguridad de la información (SGSI) para el Ministerio de Igualdad y Equidad.
2. Identificar y gestionar riesgos de seguridad de la información.
3. Fortalecer la cultura organizacional en seguridad y privacidad de la información.
4. Garantizar la sostenibilidad y mejora continua de la estrategia de seguridad.
5. Creación del dominio de gestión de seguridad bajo la guía del MGGTI del MRAE.

IV. Alcance

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) del Ministerio de Igualdad y Equidad abarcará todos los procesos, activos de información, servicios tecnológicos y digitales relacionados con el cumplimiento de la misionalidad, incluyendo la protección de datos sensibles vinculados a los

sujetos de especial protección constitucional, como mujeres, jóvenes, poblaciones étnicas y campesinas, entre otros.

La implementación del PESI garantizará que todas las áreas y procesos (Estratégicos, misionales, transversales y de control) a nivel central como territorial, operen bajo un marco de seguridad digital robusto. Esto implica la gestión integral de riesgos, la promoción de una cultura de seguridad de la información y la implementación de controles tecnológicos y administrativos alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI).

El alcance también incluye el cumplimiento normativo establecido en este marco, en especial lo definido en la Resolución 500 de 2021, así como con los lineamientos del Plan Nacional de Desarrollo 2022-2026. El PESI se extenderá a la interacción con ciudadanos y aliados estratégicos (Mecanismos de Interoperabilidad), asegurando la confidencialidad, integridad y disponibilidad de la información en todos los servicios y programas ofrecidos por el Ministerio.

V. Marco de referencia

A continuación de presentan las normas relacionadas con seguridad de la información para las entidades del estado colombiano y normativas relacionadas con el tratamiento de datos personales. Para cada una de las normas relacionadas en la tabla 1, se revisa

Tabla 1. Normatividad de seguridad y privacidad de la información para el estado colombiano.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Directiva	26	25	Agosto	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
Desición Andina	351			1993	Régimen común sobre derechos de autor y derechos conexos

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Ley	2052	25	Agosto	2020	por medio de la cual se expide el código general disciplinario
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 accesi 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
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 - Se crea la Agencia Nacional de espectro y se dictan otras disposiciones.
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 de utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
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 y se dictan otras disposiciones
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	527	18	Agosto	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	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	23	28	Enero	1982	Sobre derechos de autor
Drecreto	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.
Drecreto	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 Único Reglamentario del Sector de Tecnologías de la Información y la s Comunicaciones.
Drecreto	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, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, establecie ndo los conceptos, ineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Drecreto	1287	24	Septiembre	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.
Drecreto	620			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 parágrafo 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.
Drecreto	2106			2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
					procedimientos innecesarios existentes en la administración pública.
Drecreto	1008			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.
Drecreto	612			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.
Drecreto	1499			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.
Drecreto	728			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 tra vés de la implementación de zonas de acceso público a Internet inalámbrico.
Drecreto	1078			2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Drecreto	1081			2015	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Drecreto	103			2015	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Drecreto	1068			2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
Drecreto	1074			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.
Drecreto	886			2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Drecreto	2364			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.
Drecreto	2609			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.

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
Drecreto	884			2012	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
Drecreto	1377			2012	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley	1581		Octubre	2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley	489		Diciembre	1998	Por la cuál se dictan normas sobre la organizacion 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	767		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 Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones'
Decreto	1008		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 Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto	612		Abril	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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa
Decreto	1078		Mayo	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto	1377		Junio	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015
Resolución	2339			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	2338	24	junio	2024	Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de

TIPO DE DOCUMENTO	NÚMERO DE LA NORMA	FECHA DE EMISIÓN			DESCRIPCIÓN - EPÍGRAFE DEL DOCUMENTO
		DÍA	MES	AÑO	
					Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 924 de 2020.
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	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			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 Polltica General de Seguridad y Privacidad de la Informacion, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologlas de la Informacion y las Comunicaciones y se definen lineamientos frente al uso y manejo de la informacion.

VI. Estado actual del Ministerio

La Oficina de Tecnologías de la Información tiene la responsabilidad de "desarrollar políticas, normas, lineamientos y procedimientos de protección de datos -habeas data-, reserva y sistemas de manejo de la información del Ministerio" Sin embargo, actualmente no cuenta con un marco estructurado de gestión de seguridad que cumpla con los estándares internacionales como ISO 27001, de donde se han identificado lineamientos de cumplimiento en la implementación de sistemas como firewall perimetral y soluciones SIEM, Analyzer y NAC. Aun así estas soluciones también requieren personal con

competencias específicas para lograr su integración y despliegue de forma correcta en la entidad. En este punto se define que más allá de contar con tecnología de respaldo, es importante la participación de personal calificado para su operación y evolución.

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 es de:

Tabla 2. Evaluación Efectividad de controles NTC/ISO 27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	16	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	9	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	5	100	INICIAL
A.9	CONTROL DE ACCESO	20	100	INICIAL
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	19	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	17	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100	REPETIBLE
A.18	CUMPLIMIENTO	15	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		**17**	**100**	INICIAL

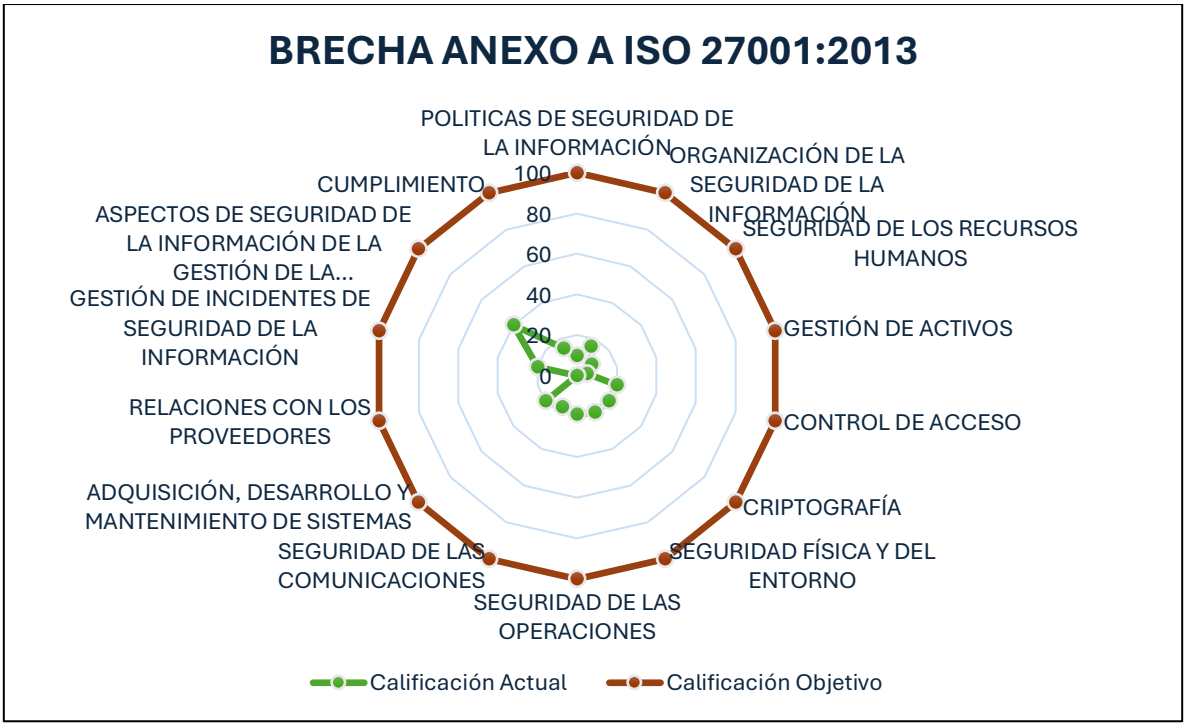

Ilustración 1. Anexo a ISO 27001:2013, brechas identificadas

Brechas identificadas

Es importante abarcar los siguientes puntos en la consolidación de brechas en atención de implementar el dominio de seguridad.

- Ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) formalmente establecido, existen actualmente dos personas encargadas de la seguridad informática y de la información, como roles adicionales a la administración de la infraestructura en general y acompañamiento técnico en otros procesos o áreas.
- Falta de políticas y procedimientos específicos de seguridad.
- Necesidad de definición clara de roles y responsabilidades en materia de seguridad.
- Carencia de procesos de gestión de riesgos de seguridad documentados.

Para el establecimiento de los proyectos se definen a continuación los componentes y actividades a considerar que de manera inicial aporten al fortalecimiento de la seguridad de la información.

Tabla 3. Brechas identificadas MIE

Actividad	Componente	Ítem
Identificación de activos críticos	Sistemas de Información Críticos	• Sistemas de información para la gestión de programas sociales. • Bases de datos de beneficiarios de programas. • Sistemas de gestión documental. • Infraestructura tecnológica de soporte a servicios misionales.
	Información Sensible	• Datos personales de poblaciones vulnerables. • Información financiera de programas sociales. • Documentación de políticas y programas estratégicos. • Información de seguimiento y evaluación de programas.
	Recursos humanos	• Directivos y tomadores de decisiones en programas y proyectos. • Especialistas en formulación y evaluación de políticas públicas. • Personal de atención directa a poblaciones vulnerables. • Profesionales de TI responsables de la gestión de sistemas ticos. • Analistas de datos e investigadores sociales.
Evaluación de amenazas y vulnerabilidades	Amenazas Identificadas	• Ciberataques dirigidos a información sensible de beneficiarios • Fuga de información confidencial • Interrupción de servicios críticos • Accesos no autorizados a sistemas de información
	Vulnerabilidades Potenciales	• Falta de controles de acceso robustos • Ausencia de políticas de seguridad documentadas • Necesidad de capacitación en seguridad para el personal • Infraestructura tecnológica en proceso de consolidación

VII. Responsables

Responsable de seguridad de la información

Cargo: Jefe de la Oficina de Tecnologías de la Información o quien sea designado por la mesa técnica de gestión de seguridad de la información que se propone más adelante, o el comité de gestión y desempeño. Las funciones principales en materia de seguridad de la información según Decreto 1075 de 2023 para la Oficina de Tecnologías de Información (OTI) en el Ministerio son:

Tabla 4. Funciones de Responsable de seguridad de la información.

Funciones	Responsables
• Desarrollar y dar lineamientos en materia de seguridad tecnológica • Definir políticas de protección de datos y sistemas de manejo de información • Establecer estándares de seguridad informática • Coordinar la implementación de controles de seguridad	• Jefe de oficina de TI • Coordinadores de GIT • Encargado de Seguridad informática • Encargado de seguridad de la información

Mesa técnica de gestión de seguridad:

La mesa técnica de Gestión de Seguridad es un grupo multidisciplinario responsable de coordinar y supervisar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en una entidad. Su objetivo principal es asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados, de acuerdo con las necesidades de cada oficina o dirección.

Tabla 5. Funciones y responsables de Mesa técnica de gestión de seguridad.

Funciones	Responsables
• Coordinar la implementación del MSPI al interior de la entidad.	• Jefe Oficina de TI (Preside).

• Revisar los diagnósticos del estado de la seguridad de la información en la entidad. • Acompañar e impulsar el desarrollo de proyectos de seguridad. • Coordinar y dirigir acciones específicas para proveer un ambiente seguro y establecer recursos de información consistentes con las metas y objetivos de la entidad. • Recomendar roles y responsabilidades específicos relacionados con la seguridad de la información. • Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. • Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. • Realizar revisiones periódicas del SGSI al menos una vez al año. • Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. • Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información.	• Jefe Oficina de Control Interno. • Coordinación de GIT Transformación Digital (Secretaría Técnica). • Jefe Oficina Asesora de Planeación. • Subdirectora Administrativa y Financiera. • Jefa Oficina de saberes y conocimientos estratégicos.

Responsables por dominios

Si bien actualmente en la entidad no se ha hecho la consolidación interna de los dominios propuestos por el MRAE, tanto por su nivel de madurez, donde aún de consolidan los procesos internos, como por la escasez de personal; a continuación, se definen algunas responsabilidades importantes de otros dominios propuestos por el MRAE, que deberán ser apoyo para el dominio de gestión de seguridad.

Tabla 6. Responsables de seguridad de la información por dominios.

Dominio	Responsable	Funciones
Sistemas de Información	Profesional Especializado en Desarrollo de Software	Implementar controles de seguridad en el ciclo de desarrollo Asegurar la integridad de las aplicaciones Gestionar accesos y roles de usuarios
Dominio de Información	Profesional en Gestión de Datos	Clasificar y proteger activos de información Implementar controles de acceso a datos Asegurar el cumplimiento normativo de protección de datos
Dominio de Servicios Tecnológicos	Profesional especializado en Infraestructura TI	Asegurar plataformas tecnológicas Gestionar seguridad perimetral Implementar controles técnicos
Dominio de Uso y Apropiación de TI	Profesional especializado en Uso y apropiación	Diseñar campañas de concienciación de seguridad y privacidad de la información Establecer protocolos de inducción a funcionarios y contratistas en el uso adecuado de servicios de TI

Responsables por áreas

Se plantea la necesidad de que, desde las diferentes oficinas y direcciones, existan personas con quien se pueda organizar el contacto desde la oficina de TI como enlaces para las diferentes socializaciones que se planteen desde Uso y Apropiación de TI, con el fin de organizar y alinear las estrategias de fomento de seguridad con las necesidades y realidades específicas de cada proceso del ministerio.

Responsables del dominio de Gestión de Seguridad de la Información

La adecuada definición de roles y responsabilidades es fundamental para la implementación efectiva del dominio de Gestión de Seguridad en La Entidad,

conforme al Modelo de Gestión y Gobierno de TI (MGGTI). Este enfoque asegura que cada actor involucrado comprenda claramente sus funciones, promoviendo una gestión eficiente y alineada con los objetivos estratégicos. Además, facilita la segregación de funciones, la rendición de cuentas y la integración transversal en todos los niveles organizacionales del ministerio. En este sentido, a continuación, se proponen las funciones y roles de los encargados desde el dominio de gestión de seguridad:

Tabla 7. Responsables del dominio de Gestión de Seguridad de la Información.

Rol	Descripción	Funciones
Especialista en Gestión de Riesgos (medio tiempo)	Asegura un enfoque proactivo frente a las amenazas potenciales. Su labor permite priorizar recursos hacia áreas críticas, minimizando impactos adversos sobre La Entidad.	• Identificar, evaluar y priorizar riesgos asociados con los activos críticos. • Diseñar planes de tratamiento para mitigar riesgos identificados. • Asegurar que los riesgos se gestionen conforme a metodologías reconocidas como ISO 31000. • Colaborar con otras áreas para integrar la gestión del riesgo en procesos institucionales.
Oficial de Seguridad de la Información (tiempo completo)	El Oficial de Seguridad actúa como el punto central para todas las iniciativas relacionadas con la seguridad, asegurando su alineación con los objetivos estratégicos y normativos. Su liderazgo es crucial para garantizar que las políticas y controles implementados sean efectivos frente a las amenazas emergentes.	• Liderar la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI). • Coordinar la gestión integral de riesgos relacionados con la seguridad de la información. • Desarrollar políticas, normas y procedimientos alineados con estándares internacionales como ISO 27001. • Supervisar el cumplimiento normativo en materia de seguridad y privacidad.
Analista de Seguridad de la Información	El Analista desempeña un papel operativo esencial al garantizar que las medidas técnicas implementadas sean	• Monitorear continuamente los sistemas para identificar vulnerabilidades y amenazas. • Realizar análisis forenses en caso de incidentes de seguridad.

Rol	Descripción	Funciones
(tiempo completo)	efectivas. Su trabajo contribuye directamente a mantener la disponibilidad, integridad y confidencialidad de los datos.	• Implementar controles técnicos para proteger los activos críticos. • Generar reportes periódicos sobre el estado de seguridad en La Entidad. • Apoyar al Oficial de Seguridad en la ejecución del plan estratégico.
Apoyo del personal de TI existente	El personal existente en TI complementa las funciones especializadas al proporcionar soporte técnico continuo y monitoreo de las herramientas de seguridad informática. Su conocimiento sobre los sistemas internos es clave para implementar soluciones efectivas y responder rápidamente ante incidentes.	• Monitoreo de las herramientas de seguridad informática. • Implementar controles técnicos definidos por el Oficial y el Analista. • Gestionar accesos a sistemas e infraestructura tecnológica. • Realizar mantenimientos preventivos y correctivos a los sistemas críticos. • Participar en simulacros y ejercicios relacionados con continuidad del negocio.

VIII. Estrategia de seguridad digital

Las estrategias de implementación se fundamentan en un enfoque sistemático que abarca aspectos técnicos, organizacionales y culturales, reconociendo que la seguridad de la información es una responsabilidad compartida que requiere el compromiso de todos los niveles de la organización. Este enfoque integral permite abordar no solo los aspectos tecnológicos, sino también los procesos, las personas y la cultura organizacional necesarios para una implementación exitosa.

Tabla 8. Estrategias de seguridad de la información.

No.	Estrategia	Actividades
1	Establecimiento del SGSI bajo el dominio de Gestión de Seguridad	• Definir el alcance del SGSI. • Obtener el compromiso de la alta dirección. • Asignar roles y responsabilidades de seguridad.

		• Desarrollar la política general de seguridad de la información.
2	Desarrollo de políticas y procedimientos	• Identificar las áreas clave que requieren políticas de seguridad. • Redactar políticas específicas (ej. control de acceso, gestión de activos, seguridad física). • Desarrollar procedimientos operativos de seguridad.
3	Creación del catálogo de servicios de seguridad	• Identificar los servicios de seguridad necesarios para la entidad. • Definir los niveles de servicio para cada componente. • Documentar y publicar el catálogo de servicios.
4	Gestión de riesgos de seguridad	• Realizar un inventario de activos de información. • Identificar y evaluar los riesgos de seguridad. • Seleccionar e implementar controles de seguridad adecuados.
5	Fomento de la cultura de seguridad	• Desarrollar un programa de concientización en seguridad. • Implementar capacitaciones regulares para todo el personal.

Descripción de las estrategias, ejes específicos

Cronograma de proyectos y actividades

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

	AÑO 2024				AÑO 2025	
Fase	**TRIMESTRE 1**	**TRIMESTRE 2**	**TRIMESTRE 3**	**TRIMESTRE 4**	**TRIMESTRE 1**	**TRIMESTRE 2**
Planificación y organización	Establecer el equipo de proyecto de seguridad.					
	Definir el alcance y los objetivos detallados del SGSI.					
	Asignar roles y responsabilidades de seguridad.					
	Desarrollar la política general de seguridad de la información.				Actualizar la política general de seguridad de la información.	
Desarrollo de políticas y procedimientos		Aprobar la Estrategia de seguridad de la información				
		Desarrollar políticas específicas y procedimientos				
	Crear el catálogo inicial de servicios de seguridad				Actualizar el catálogo de servicios de seguridad	
Análisis de riesgos, selección e implementación de controles	Realizar el inventario de activos de información.				Actualizar el inventario de activos de información.	

	Llevar a cabo el análisis de riesgos, diligenciamiento de autodiagnóstico de forma trimestral				Llevar a cabo el análisis de riesgos, diligenciamiento de autodiagnóstico de forma trimestral	
	Seleccionar los controles de seguridad apropiados de acuerdo con lo establecido en el autodiagnóstico y las necesidades de TI.				Seleccionar los controles de seguridad apropiados de acuerdo con lo establecido en el autodiagnóstico y las necesidades de TI.	
			Poner en marcha los procedimientos operativos de seguridad			
	Iniciar el programa de concientización y capacitación.				Actualizar el programa de concientización y capacitación.	
Monitoreo y mejora continua	Establecer métricas de seguridad		Establecer métricas de seguridad		Establecer métricas de seguridad	
		Realizar auditorías internas del SGSI.		Realizar auditorías internas del SGSI.		Realizar auditorías internas del SGSI.
	Implementar acciones correctivas y de mejora.				Implementar acciones correctivas y de mejora.	

Nota: Al finalizar cada vigencia, LA ENTIDAD, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

Presupuesto

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes:

<table>
<tr><th>RECURSOS</th><th colspan="3">VARIABLE</th></tr>
<tr><td rowspan="3">Humanos</td><td colspan="3">Grupos Internos de Servicios Tecnológicos y Transformación Digital</td></tr>
<tr><td colspan="3">Encargado de seguridad informática y de la información</td></tr>
<tr><td colspan="3">Líderes y gestores de procesos</td></tr>
<tr><td rowspan="2">Técnicos</td><td colspan="3">Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP</td></tr>
<tr><td colspan="3">Herramienta para la gestión de riesgos (Matriz de Riesgos SGSPI)</td></tr>
<tr><td>Logísticos</td><td colspan="3">Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.</td></tr>
<tr><td rowspan="3">Financieros</td><td colspan="3">Recursos para la adquisición de conocimiento, recursos humanos, técnicos.</td></tr>
<tr><td>Iniciativa</td><td>Proyecto</td><td>Presupuesto</td></tr>
<tr><td>Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información</td><td>Fortalecimiento institucional para la superación de brechas de desigualdad e inequidad a nivel nacional.</td><td>$1.164.500.000,00</td></tr>
</table>

Nota: La ejecución de las actividades y proyectos establecidos en este plan está sujeta a la disponibilidad presupuestal del Ministerio de Igualdad y Equidad. En caso de presentarse recortes presupuestales o reasignación de recursos por prioridades institucionales, se documentará mediante informes técnicos el impacto sobre el cumplimiento de las actividades programadas y se realizarán los ajustes pertinentes al plan, previa aprobación del Comité Institucional de Gestión y Desempeño.

IX. Referencias

- ✓ Normograma
- ✓ Manual de Gobierno Digital
- ✓ Autodiagnóstico MSPI 2024
- ✓ Matriz Gobierno Digital 2020
- ✓ Anexo A del estándar ISO/IEC 27001:2013
- ✓ Las principales nueve (9) amenazas de ciberseguridad https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

X. Control de cambios

Fecha	Versión	Descripción
20 de diciembre de 2024	1.0.	Creación

Ministerio de
Igualdad y Equidad