

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## REGIÓN ADMINISTRATIVA Y DE PLANEACIÓN ESPECIAL, RAP-E Región Central

Dirección Administrativa y Financiera

Proceso TIC

2024-2026



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

Tabla de contenido

<b>I. INTRODUCCIÓN</b> .....	3
<b>II. OBJETIVOS</b> .....	3
<b>III. ALCANCE</b> .....	3
<b>IV. DEFINICIONES</b> .....	4
<b>V. MARCO LEGAL Y/O NORMATIVO</b> .....	5
<b>VI. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN</b> .....	7
<b>Política de Organización Interna</b> .....	7
1) Roles y responsabilidades .....	7
2) Levantamiento de inventarios de activos de información .....	8
3) Plan de tratamiento de riesgos.....	8
4) Plan de socialización .....	9
<b>VII. CICLO DE OPERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI</b> 9	
<b>VIII. CONTROL DE CAMBIOS</b> .....	13



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

## I. INTRODUCCIÓN

La Región Administrativa de Planeación Especial RAP-E Región Central con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad y privacidad de los datos, el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el objetivo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

## II. OBJETIVOS

- Concientizar a los funcionarios, contratistas, y terceros sobre la implementación y adopción del Modelo de Seguridad de la Información y privacidad de la información.
- Plantear, hacer, verificar y controlar las actividades que permitan la disponibilidad, integridad y confidencialidad de los activos de información.
- Sensibilizar a los funcionarios y contratistas de la entidad, sobre la importancia de la seguridad de la información en la RAP-E Región Central.
- Evaluar el cumplimiento de los requisitos y controles de seguridad de la información para fortalecer los procesos, de la entidad.

## III. ALCANCE

Aplicar la gestión del ciclo (PHVA) de operación del modelo de seguridad y privacidad de la información (MSPI) propuesto por MINTIC, dentro de las posibilidad y recursos asignados al proceso de gestión TIC.

La seguridad de la información es un esfuerzo de equipo, se requiere la participación y apoyo de parte los funcionarios de la entidad, ya que los activos de información pueden ser bases de datos, contratos, acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Las políticas que se aplican se encuentran alineadas con el manual de políticas de seguridad de la información que se desorillara en el primer trimestre del año 2024, de acuerdo con el cronograma propuesto en dicha política, este tiene como alcance todos los funcionarios públicos, contratistas, proveedores y demás usuarios internos y externos que se relacionan con la información de la entidad.



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

Este Plan de Seguridad y Privacidad de la Información, define lineamientos que permiten la aplicación de las Políticas de Seguridad de la Información y Protección de Datos Personales.

Este documento se encuentra en fase inicial de acuerdo con los lineamientos de avance en la implementación del Modelo de Seguridad y Privacidad de la Información- MSPI, de acuerdo con lo establecido en el Decreto 1078 de 2015, además de la aplicación de los requerimientos de la norma ISO/IEC 27001:2022.

Con esta planeación se establecen algunos controles preventivos y correctivos para incidencias de seguridad de la información en temas como:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Ataques dirigidos y no dirigidos
- Pérdida o robo de la información.
- Modificación no autorizada.
- Mala gestión del conocimiento.
- Diligenciamiento errado de formatos.
- Perdida o daño de la documentación.
- Pérdida o daños sobre Activos de información
- Uso indebido de Activos de información
- Uso Indebido de Software
- Suplantación de Identidad
- Pérdidas de conectividad, contraseñas, código fuente de aplicaciones desarrolladas internamente
- Acceso físico no autorizado
- Administración de red inadecuada
- Cambio de datos intencionados o no en un sistema de información
- Copias de seguridad

#### IV. DEFINICIONES

**Activos de Información:** Es todo aquello que las entidades consideran importante o de alta validez para la misma, ya que puede contener importante información como lo puede ser Base de Datos con



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

usuarios, contraseñas, números de cuentas, etc.

**Confidencial:** Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

**Ataque de denegación de servicios:** también llamado ataque DDoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

**Disponibilidad de la información:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

**Integridad:** Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

**Inventario de activos:** Todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de los mismos.

**Seguridad de la información:** Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

## V. MARCO LEGAL Y/O NORMATIVO

ACTO ADMINISTRATIVO	OBJETO
Constitución Política de Colombia 1991	Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
Ley 527 de 1999	Por medio de 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.



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

Ley 594 de 2000	Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
LEY 603 DE 2000	Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
Ley 962 de 2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150 de 2007	Seguridad de la información electrónica en contratación en línea.
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 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 los 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 del 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. Capítulo IV, "utilización de medios electrónicos en el procedimiento 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. Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2364 de 2012	Firma electrónica.
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".



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

La Región Administrativa de Planeación Especial RAP-E, emprenderá acciones para la protección de la información que se gestiona, garantizando la confidencialidad, integridad, disponibilidad y seguridad de la información, realizando la identificación y tratamiento de los riesgos de la información a los activos críticos, estableciendo un seguimiento a las acciones acorde con la gestión de riesgos establecida a través del sistema integrado de gestión.

## VI. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

### Política de Organización Interna

La RAP-E garantiza el soporte operativo para las actividades de seguridad de la información a través de:

#### 1) Roles y responsabilidades

- a. Los funcionarios de la RAP-E, proveedores o contratistas, así como los terceros autorizados para acceder a la infraestructura de procesamiento de información, serán responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Entidad.
- b. La información almacenada en los equipos de cómputo de la Entidad es propiedad de La RAP-E y cada usuario es responsable de proteger su integridad, confidencialidad y disponibilidad.
- c. Los activos de información de La RAP-E Región Central, deben tener claramente identificado su propietario y su custodio.
- d. Los funcionarios de La RAP-E Región Central, deberán mantener especial cuidado de no divulgar información CONFIDENCIAL o RESERVADA en lugares públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la organización. Esta restricción se extiende inclusive con posterioridad a terminación del vínculo laboral o terminación de los contratos y debe estar incluida en los Acuerdos de Confidencialidad.
- e. Los líderes de los procesos estratégicos, misionales o de apoyo, de acuerdo con el mapa de procesos de la RAP-E Región Central, pueden ejercer el rol de propietarios de activos de información. En este caso el propietario es el encargado de tomar las decisiones claves sobre dicho activo y se apoya en el custodio para su protección en términos de seguridad.
- f. Los funcionarios que ejercen el rol de custodios de algún activo de información de La RAP-E Región Central, actúan como responsables de proteger el activo en términos de



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

confidencialidad, integridad y disponibilidad, por lo tanto, debe informarse acerca de las medidas necesarias para proteger el activo.

- g. Es responsabilidad de todos los funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del RAP-E, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el RAP-E, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

## 2) Levantamiento de inventarios de activos de información

Para el año 2024 se establece un plan de trabajo de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, para lo cual se realizará en el primer semestre del año el levantamiento de los activos de información, con esta actividad se espera identificar, clasificar y valorar la criticidad de los activos, tipo de información, software, hardware, servicios en los procesos.

Esta actividad se programará para actualización anual en el primer trimestre, de manera tal que se asignen por procesos gestores de activos de información que tendrán el acompañamiento del responsable de activos del proceso de Gestión de Tecnologías de la Información.

Dicha información, se plasmará en una matriz, y este consolidado deberá ser aprobado en el comité de gestión institucional y publicada en el Portal de la entidad, en el primer semestre de cada año de la vigencia.

## 3) Plan de tratamiento de riesgos

En el marco de la metodología de riesgos establecida por la Oficina Asesora de Planeación de la RAP-E Región Central, se construirán los planes de tratamiento para cada riesgo identificado, cuyo nivel de riesgo residual fuera superior a bajo.

Además se establece un Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información, para la entidad como una herramienta que proporcione las pautas necesarias para desarrollar, establecer y fortalecer los conceptos básicos y metodológicos para una adecuada administración de los riesgos de seguridad de la información, a partir de su identificación, manejo y seguimiento.



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA



4) Plan de socialización

El proceso de Gestión TIC establecerá y ejecutará un plan de sensibilización, mediante el cual generará campañas informativas enviadas masivamente desde el Área de Comunicaciones articulada con la Dirección administrativa y financiera de manera trimestral.

**VII. CICLO DE OPERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN- MSPI**

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. Este modelo inicia con el diseño del sistema de gestión de seguridad de la información (MSPI), identificando 5 fases que orientan el ejercicio para los propósitos de protección de la información de la Entidad bajo un modelo sostenible, las fases del ciclo de operación se definen de la siguiente manera:

*I. fase inicial de diagnóstico:*

Para el Diagnóstico se utiliza una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de la Entidad, según lo definido en la Estrategia de Gobierno Digital en su cuarto componente "Seguridad y Privacidad de la Información".

Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre sin fines lucrativos, por esta razón se prohíbe la comercialización y explotación de esta.



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

## DIAGNÓSTICO MSPI



### II. Fase de Planeación

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto de la entidad, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).

### III. Fase de Implementación

El desarrollo de esta fase permitirá a la entidad llevar a cabo la implementación de los aspectos y planes identificados en las fases anteriores (diagnóstico y planeación).

Un plan de control operacional establecerá las actividades y la programación para la implementación tanto de los requisitos, controles y buenas prácticas de seguridad y privacidad de la información en la RAP-E Región Central.

Como estrategia para la orientación de los propósitos de seguridad y privacidad de la información al interior de la entidad, se definen y aprueban políticas y directrices que guiarán las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

#### IV. Fase Evaluación del Desempeño del MSPI

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

#### V. Fase Mantenimiento y Mejora del MSPI

La Entidad con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tomará en cuenta los resultados de la fase anterior “Evaluación de desempeño” basada en los resultados de las actividades de seguimientos y medición (indicadores).

Tareas		Fecha de inicio	Fecha final	Días	Estado	2024		2025		2026		
						1 semestre	2 semestre	1 semestre	2 semestre	1 semestre	2 semestre	
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información	1-feb	30-mar	58	Completado						
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	1-mar	31-mar	30	En progreso						
		Validar y aceptar los activos de información por cada líder de proceso.	15-mar	1-abr	58	Sin empezar						
		Revisar los instrumentos de activos de información y realimentar a las áreas con las modificaciones.	1-abr	30-jun	90	Sin empezar						
		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.	1-jul	30/08/2024	60	Sin empezar						
		Actualizar el instrumento de Registro Activos de información	Validar nuevos activos de información en el instrumento levantado en la vigencia anterior en cada dependencia.	4/01/2025	2/12/2026	697	Sin empezar					
	Consolidar el instrumento de activos de Información.		1/06/2025	30/06/2025	29	Sin empezar						
	Reportar al área de atención al ciudadano los activos de información que contienen datos personales		1-jun	30-dic	342	Sin empezar						
	Publicar los instrumentos de activos de información consolidado en la página web	Enviar a control de legalidad el instrumento de Registro Activos de información.	2/06/2024	15/06/2024	13	Sin empezar						
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	30/06/2024	30/07/2024	30	Sin empezar						
MEJORA CONTINUA EN LA VIGENCIA 2025	Realimentación, revisión y verificación de los incidentes identificados (Ajustes) y Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	1-ene	30-dic	728	Sin empezar							
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar el documento del Plan de Gestión de Cultura Organizacional en seguridad de la información	1-mar	30-mar	29	En progreso						
		Realizar procesos de capacitación y sensibilización a los funcionarios	30-mar	30-dic	1005	En progreso						
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	5-oct	30-nov	1152	En progreso						



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos de seguridad de la información	1-jun	30-jun	29	Sin empezar									
		Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la operación	1-jul	30-jul	29	Sin empezar									
		Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	1-ago	30-ago	29	Sin empezar									
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos Identificados y planes de tratamiento	1-sep	30-sep	29	Sin empezar									
		Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	1-oct	30-oct	29	Sin empezar									
		Evaluación de riesgos residuales	1-nov	30-nov	29	Sin empezar									
	Seguimiento Fase de Tratamiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	1-dic	30-dic	29	Sin empezar									
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	15-dic	30-dic	15	Sin empezar									
		Realimentación, revisión y verificación de los incidentes identificados (Ajustes) y Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	15-jun	30-jun											
	MEJORA CONTINUA EN LA VIGENCIA 2025														

Gestión de Incidentes de Seguridad de la Información	Elaboración de procedimiento de gestión de incidentes de seguridad	Publicar y Socializar el procedimiento de incidentes de seguridad de la información	1-ene	30-ene	29	Sin empezar									
		Hacer seguimiento trimestral de los ciber incidentes materializados en la entidad	1-feb	28-feb	27	Sin empezar									
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Socializar el procedimiento a los colaboradores de la Entidad	1-mar	30-mar	29	Sin empezar									
		Gestionar los incidentes de Seguridad de la Información identificados	1-abr	30-abr	29	Sin empezar									
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno si es requerido	1-may	30-dic	243	Sin empezar									
	Eventos / vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a los activos de	1-may	30-dic	243	Sin empezar									
		Documentar resultados	1-mar	30-dic	-61	Sin empezar									
		Realimentación, revisión y verificación de los incidentes identificados (Ajustes) y Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	15-jun	30-dic	198	Sin empezar									
	MEJORA CONTINUA EN LA VIGENCIA 2025														

Continuidad de la Operación	Análisis, diseño y puesta en operación de DRP	Definir Objetivo, alcances y límites para la preparación de las TIC para la continuidad del negocio	1-ene	30-ene	29	En progreso									
		Definir Política para la preparación de las TIC para la continuidad del negocio	1-feb	28-feb	27	En progreso									
		Asignación de recurso humano competente y capacitado, comunicación de roles y responsabilidades para la preparación de las TIC para la continuidad del negocio	1-mar	30-mar	29	En progreso									
		Definición de un plan de requerimientos, categorizando las actividades para la continuidad definiendo el nivel con el cual cada actividad crítica necesita para su reanudación (RTO -RPO)	1-abr	30-abr	29	En progreso									
		Identificación de procesos alternos	1-may	30-dic	243	En progreso									
		Generación de Informe de Impacto del negocio	1-may	30-dic	243	En progreso									
		Publicación Estrategias de Continuidad de la Operación	1-jun	30-dic	212	En progreso									
		Crear Documentación del Plan de continuidad de la Operación	15-jun	30-dic	198	En progreso									
		Aprobación del Disaster Recovery Plan	1-jul	30-jul	29	En progreso									
		Realimentación, revisión y verificación de los incidentes identificados (Ajustes) y Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	30-jul	31-jul	1	En progreso									



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA

Revisión de los controles de la norma ISO 27001:2022	Revisión de los controles de la norma ISO 27001:2022	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 Formular, Implementar y actualizar los indicadores del cumplimiento del MSPI	30-mar 30-mar	30-dic 30-dic	1005 1005	En progreso En progreso								
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	1-may	30-may	29	En progreso								
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	1-jun	30-jun	29	En progreso								
	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	2-jul	30-jul	28	En progreso								

## VIII. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
Vr.1.0	22 enero 2024	MARIA DEL PILAR NIÑO CAMPOS	Versión inicial



BOGOTÁ



BOYACÁ



CUNDINAMARCA



META



TOLIMA



HUILA