AQUÍ SÍ PASA BOGOTÁ MI CIUDAD MI CASA

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2026

BOGOTÁ

## CONTROL DE CAMBIOS

| NO. DE ACTA DE APROBACIÓN | FECHA | VERSIÓN | DESCRIPCIÓN |
|---|---|---|---|
| Acta de aprobación No 02 de 2026 del Comité Institucional de Gestión y Desempeño | 29/01/2026 | 1.0 | Adopción |

CONTENIDO

## 1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información - MSPI, es el instrumento a través del cual el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, establece los lineamientos que deben seguir las entidades públicas en cumplimiento de la política de gobierno digital en su habilitador transversal “Seguridad de la información”, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de las Políticas de Gobierno Digital y Seguridad Digital.

El Instituto Distrital de Protección y Bienestar Animal - IDPYBA como Entidad Pública Distrital se adhiere a las iniciativas del Modelo de Seguridad y Privacidad de la Información - MSPI y demás lineamientos del gobierno distrital y nacional, por lo cual ha establecido y mejorado continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI; el cual a través del Plan de Seguridad y Privacidad de la Información define a alto nivel las actividades a desarrollar durante la vigencia, enfocado en cubrir todos los procesos del IDPYBA; y con ello determinar las actividades para la implementación y mejora continua que permitan alcanzar el estado de madurez deseado en materia de seguridad y privacidad de la Información. Esta estrategia se encuentra alineada a los objetivos estratégicos, la misión y visión de la Entidad con el fin de apoyar el logro y cumplimiento de los objetivos, programas y proyectos de la entidad.

Con respecto a lo anterior desde la Subdirección de Gestión Corporativa y en colaboración con todas las subdirecciones y jefaturas, implementa, mantiene y mejora el modelo de gestión de la seguridad de la información que permita alcanzar y mantener dentro de las diferentes áreas y colaboradores una cultura y conciencia en el acceso y uso adecuado de la información en la Entidad.

Este Plan se ha definido con base en las mejores prácticas de seguridad de los principales marcos de referencia de la materia como lo son: ISO 27001, ISO 27002, ISO 31000, ISO 27701, el Manual de Política de Gobierno Digital y del Modelo de Privacidad y Seguridad de la Información; aplicando el ciclo de mejora continua y lo establecido para la gestión de seguridad y privacidad de la información en la vigencia 2026 de manera efectiva.

## 2. OBJETIVOS

### *2.1 Objetivo general*

Incrementar el nivel de madurez en seguridad de la información, privacidad y ciberseguridad del Instituto Distrital de Protección y Bienestar Animal - IDPYBA durante la vigencia 2026, fortaleciendo la gestión de riesgos, las capacidades de prevención, detección y respuesta a incidentes, y la implementación de controles alineados con estándares, políticas y disposiciones legales vigentes, con el fin de garantizar la confidencialidad, integridad, disponibilidad, privacidad de los activos de información y la continuidad y confiabilidad de los servicios institucionales.

### *2.2 Objetivos específicos*

- Definir las actividades que darán cumplimiento a las (5) cinco fases del Modelo de Seguridad y Privacidad de la Información tales como: Diagnóstico, Planificación, Operación, Evaluación de desempeño y Mejoramiento continuo.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital, ciberseguridad y protección de la información personal.
- Asegurar la protección de los activos de información del IDPYBA, a través de la identificación, clasificación y/o actualización de los activos de información y sus riesgos asociados.
- Gestionar de manera oportuna los eventos e incidentes de seguridad de la información que pongan en riesgo la integridad, confidencialidad, disponibilidad y privacidad, reduciendo su impacto y propagación.
- Fortalecer la cultura, el conocimiento y las habilidades de los funcionarios y contratistas en los temas de seguridad y privacidad de la información en el IDPYBA.
- Incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en el Instituto Distrital de Protección y Bienestar Animal – IDPYBA.

## 3. ALCANCE

El Plan de Seguridad y Privacidad de la Información y Seguridad Digital, aplica para todos los procesos del IDPYBA y es de obligatorio complimiento para los funcionarios, contratistas, pasantes y terceros que tengan vínculos laborales o contractuales con la entidad y que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten su información de forma interna o externa, independientemente de su ubicación. De igual forma, esta política aplica a toda la información creada, procesada, transmitida y gestionada por la entidad, sin importar el medio, formato, presentación o lugar en la cual se encuentre.

## 4. MARCO NORMATIVO

El diseño e implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI del Instituto Distrital de Protección y Bienestar Animal - IDPYBA se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC y demás entidades que regulan en la materia:

- **Ley 1266 de 2008.** "Por la cual se dictan las disposiciones generales del Habeas 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."
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **Ley 1581 de 2012.** "Por la cual se dictan disposiciones generales para la protección de datos personales."
- **Decreto 1377 de 2013.** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012."
- **Ley 1712 de 2014.** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."
- **Decreto 886 de 2014**. "Por el cual se reglamenta el Registro Nacional de Bases de Datos."
- **Decreto 103 de 2015.** "Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones."
- **Decreto 1083 de 2015** del Departamento Administrativo de la Función Pública, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital.
- **Decreto 1499 de 2017.** "Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión."
- **Decreto 728 de 2017.** "Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico."
- **Decreto 1008 del 2018.** "Por el cual se establecen los lineamientos generales de la

política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

- **CONPES 3975 DE 2019.** Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **Resolución 1519 del 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 en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos."
- **CONPES 3995 de 2020** - Política Nacional de Confianza y Seguridad Digital.
- **Resolución 500 de 2021.** "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
- **Resolución 746 de 2022.** "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
- **Decreto 338 de 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 de 2022.** "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- **NTC-ISO/IEC 27001:2022.** Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de seguridad de la información. Requisitos.
- **Decreto 472 de 2024 – Gobernanza de Ciberseguridad Distrital:** Por el cual se adopta el Modelo de Gobernanza de Seguridad Digital para el Distrito, se modifica el artículo 5 del Decreto Distrital 025 de 2021 y se dictan otras disposiciones.
- **Directiva 002 de 2025 – Alcaldía Mayor de Bogotá, D.C.:** Reconoce la seguridad de la información como un componente para proteger datos, TIC y garantizar la privacidad, según lineamientos distritales de seguridad digital. Objetivo: Integrar la seguridad digital en procesos distritales.
- **Resolución 2277 de 2025.** Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- **Decreto Distrital 640 de 2025:** Establecer la obligación de realizar Evaluaciones de Impacto en la Privacidad (PIA) en las entidades del Distrito Capital, con el fin de identificar, evaluar y mitigar riesgos asociados al tratamiento de datos personales en soluciones tecnológicas.

## 5. DESARROLLO DEL PLAN

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC definió el Modelo de Seguridad y Privacidad -MSPI, el cual fue facilitado a las entidades del Estado colombiano con el fin de que estos lo adopten e incrementen el nivel de madurez en los temas de seguridad y privacidad de la información. De acuerdo con lo anterior, la metodología de implementación del Plan de Seguridad y Privacidad del IDPYBA está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el MSPI y se ejecuta a través del mapa de ruta definido a continuación:


*Ilustración 1 - Ciclo del Modelo de Seguridad y Privacidad de la Información (Tomado de MinTIC)*

### *5.1 **Fase de Diagnostico***

Esta fase permite por medio del uso de herramientas de diagnóstico, actividades de reconocimiento y valoración de controles de seguridad de la información, identificar cual es el estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este de diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad de la información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.

#### *5.1.1 Estado Actual*

Teniendo en cuenta la calificación de FURAG, el IDPYBA se encuentra en un puntaje de 58,9 en la política de seguridad digital, esto refleja que el Instituto tiene brechas significativas frente a su implementación, siendo además la política con menor resultado

en el Instituto, por lo que se requiere de mayor esfuerzo y capacidades para incrementar el nivel de implementación de la política:

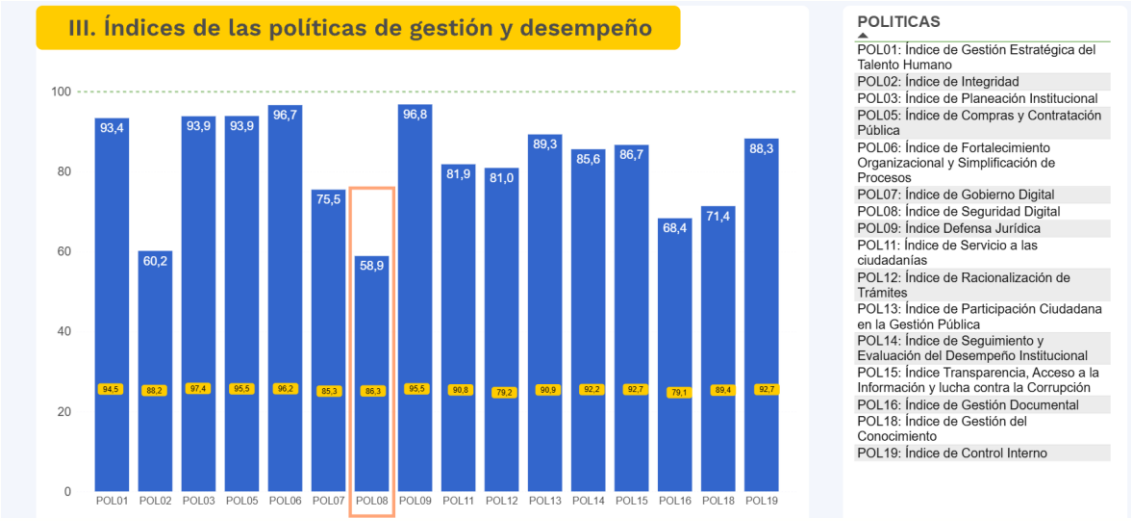


*Ilustración 2 - Resultado Medición FURAG 2024*

El nivel de implementación del MSPI permitirá al IDPYBA establecer la estrategia a desarrollar para la que en la vigencia 2026 se prioricen las brechas a implementar y mejorar en los procesos (17 procesos) misionales, estratégicos, de apoyo y de evaluación de la Entidad y toda la infraestructura que los soporte. Se realizó la medición del MSPI según el instrumento actualizado por MINTIC, obteniendo los siguientes resultados:

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | Nivel de Madurez |
| A.5 | CONTROLES ORGANIZACIONALES | 36 | 100 | REPETIBLE |
| A.6 | CONTROLES DE PERSONAS | 45 | 100 | EFECTIVO |
| A.7 | CONTROLES FÍSICOS | 40 | 100 | REPETIBLE |
| A.8 | CONTROLES TECNOLÓGICOS | 33 | 100 | REPETIBLE |
| PROMEDIO EVALUACIÓN DE CONTROLES | | 39 | 100 | REPETIBLE |

*Ilustración 3 - Resultado Medición MSPI 2025*

### *5.2 Fase de Planificación*

De acuerdo con el resultado de la fase de diagnóstico, se definen las necesidades y objetivos de seguridad y privacidad de la información basados en el contexto estratégico,

el modelo de operación del IDPYBA, los recursos disponibles y su articulación con el Plan Estratégico Institucional, entre otros, los cuales permiten definir los lineamientos para asegurar el cumplimiento de los requisitos de Modelo de Seguridad y Privacidad de la Información.

### *5.3 **Fase de Implementación u Operación***

Es necesario la actualización e implementación de la política y manual de políticas de seguridad y privacidad de la información a través de la estructuración y puesta en marcha de los controles de seguridad de la información que ayudan a mitigar el impacto de los riesgos definidos en la etapa de Planificación que hacen parte del Modelo de Seguridad y Privacidad de la Información.

Esta fase dará paso a que el IDPYBA lleve a cabo la implementación de los requisitos base presentados el Modelo de Seguridad y privacidad de la información – MSPI y la norma ISO/IEC 27001; de la misma forma llegar a la implementación de los controles, que por normativa o por resultado de la identificación de riesgos deban ser implementados.

Dentro de la estrategia de la Entidad se encuentra la definición de los propósitos de seguridad y privacidad de la información, y por ende se definirán e implementarán políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad. Por lo que para la vigencia 2026 estaremos centralizados en la implementación y mejora de los controles focalizado en dominio por lo que se requiere del liderazgo y apoyo de las áreas responsables de estos controles.

## 6. SEGUIMIENTO Y EVALUACIÓN

La evaluación del desempeño del Modelo de Seguridad y Privacidad de la información se realiza a través de la medición y monitoreo de los indicadores de gestión, el seguimiento de la eficacia de los controles para determinar su efectividad, la revisión por la Alta Dirección del IDPYBA para determinar las acciones necesarias que permitan mejorar la implementación del SGSPI.

Con la revisión periódica se debe asegurar que las mejoras realizadas cumplan con los objetivos dispuestos en la Política de Seguridad y Privacidad de la Información y Seguridad Digital.

Dado que la seguridad y privacidad de la Información es un proceso transversal a toda la Entidad, el anterior mapa de ruta establecer las acciones necesarias para implementar, gestionar, realizar seguimiento, medición y cumplimiento con respecto al objetivo de la entidad de mejorar el nivel de madurez frente al MSPI, que permitan el cumplimiento de los objetivos estratégicos de la entidad, lo anterior se mediara a través de la definición de indicadores para el SGSPI.

### *6.1 Mejoramiento Continuo*

El mejoramiento continuo del Modelo de Seguridad y Privacidad de la información es el resultado del seguimiento y revisión de todo el sistema de seguridad y privacidad de la información, donde se evalúa el alcance, la metodología de riesgo y la eficacia de los controles, que como resultado se identifican mejoras al sistema a través de planes de mejoramiento (acciones correctivas) y de esta manera mejorar continuamente el desempeño institucional del citado Modelo.

Resultado del mejoramiento continuo, se retroalimentan los planes de seguridad, políticas, procedimientos y controles, que impacta de manera positiva, en el desempeño del sistema.

En las actividades definidas en el mapa de ruta se contemplan varias que aportarán al mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en el IDPYBA por lo que el objetivo de este plan es la incorporación de los temas de seguridad y privacidad de la información en todos los procesos de la entidad.

## 7. CRONOGRAMA

| COMPONENTE O ETAPA O EJE | ACTIVIDAD | RESPONSABLE | P/E | PRIMER TRIMESTRE DE ENERO A MARZO | | | SEGUNDO TRIMESTRE DE ABRIL A JUNIO | | | TERCER TRIMESTRE DE JULIO A SEPTIEMBRE | | | CUARTO TRIMESTRE DE OCTUBRE A DICIEMBRE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **Activos de Información** | Realizar la identificación y actualización de los activos de información para los procesos que quedaron pendientes en 2025. | Gestión Tecnológica | P | | 30% | 30% | 40% | | | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Socialización y acompañamiento de los lineamientos para la identificación y actualización de activos de información | Gestión Tecnológica | P | | | | | | 25% | 25% | 25% | 25% | | | |
| | | | E | | | | | | | | | | | | |
| | Identificación y Actualización de Instrumentos de gestión de la información pública | Todos los procesos con el apoyo del proceso de Gestión Tecnológica | P | | | | | | 25% | 25% | 25% | 25% | | | |
| | | | E | | | | | | | | | | | | |
| | Publicación Instrumentos de gestión de la información pública | Gestión Tecnológica | P | | | | | | | | | 30% | 70% | | |
| | | | E | | | | | | | | | | | | |
| | Definir los lineamientos y ejecutar las estrategias para la clasificación y etiquetado de los activos de tipo información en medio físico y electrónico | Subdirección de Gestión Corporativa (Gestión Documental, Gestión Tecnológica)<br><br>Fortalecimiento de la Gestión Institucional | P | | | 25% | 25% | | | 25% | | | | 25% | |
| | | | E | | | | | | | | | | | | |
| | Definir y socializar los lineamientos y controles sobre áreas seguras | Todos los procesos con el apoyo de la Subdirección de Gestión Corporativa (Gestión Tecnológica Gestión Administrativa, Gestión Documental y Gestión del Talento Humano) | P | | | | | | 25% | 25% | 25% | 25% | | | |
| | | | E | | | | | | | | | | | | |

| COMPONENTE O ETAPA O EJE | ACTIVIDAD | RESPONSABLE | P/E | PRIMER TRIMESTRE DE ENERO A MARZO | | | SEGUNDO TRIMESTRE DE ABRIL A JUNIO | | | TERCER TRIMESTRE DE JULIO A SEPTIEMBRE | | | CUARTO TRIMESTRE DE OCTUBRE A DICIEMBRE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **Identificación y Valoración** | Definición del Plan de Concienciación en Seguridad y Privacidad | Gestión Tecnológica | P | 40% | 60% | | | | | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Ejecución del Plan de Concienciación en Seguridad y Privacidad | Gestión Tecnológica con el apoyo de Gestión del Talento Humano y Gestión de Comunicaciones | P | | 10% | 10% | 10% | 10% | 10% | 10% | 10% | 10% | 10% | 10% | |
| | | | E | | | | | | | | | | | | |
| | Análisis de resultados del Plan de Concienciación en Seguridad y Privacidad. | Gestión Tecnológica | P | | | | | | | | | | | | 100% |
| | | | E | | | | | | | | | | | | |
| **Protección de Datos Personales** | Actualización de la política de protección de datos personales | Subdirección de Gestión Corporativa (Gestión Tecnológica Gestión Jurídica, Servicio a la Ciudadanía) | P | | | 25% | 25% | 25% | 25% | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Reporte y actualización del inventario de bases de datos de información de tipo personal del IDPYBA en el Registro Nacional | Subdirección de Gestión Corporativa (Gestión Tecnológica Gestión Jurídica) | P | | 50% | 50% | | | | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Gestión para la incorporación de lineamientos de protección de datos en la documentación y sistemas de información del IDPYBA | Subdirección de Gestión Corporativa (Gestión Tecnológica Gestión Jurídica) | P | | | | | | | 30% | | 30% | | 40% | |
| | | | E | | | | | | | | | | | | |
| **Implementación y mejora del Sistema de Gestión de Seguridad y Privacidad de la Información** | Actualización y socialización del Manual de Políticas de Seguridad y Privacidad de la Información | Gestión Tecnológica | P | | | 20% | 30% | 30% | 20% | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Definición del plan de cierre de brechas según la medición del MSPI por dominio | Gestión Tecnológica | P | 25% | 75% | | | | | | | | | | |
| | | | E | | | | | | | | | | | | |

| COMPONENTE O ETAPA O EJE | ACTIVIDAD | RESPONSABLE | P/E | PRIMER TRIMESTRE DE ENERO A MARZO | | | SEGUNDO TRIMESTRE DE ABRIL A JUNIO | | | TERCER TRIMESTRE DE JULIO A SEPTIEMBRE | | | CUARTO TRIMESTRE DE OCTUBRE A DICIEMBRE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| | Revisión de los controles de la norma ISO 27001:2022 | Gestión Tecnológica | P | | | | | | | | | 20% | 40% | 40% | |
| | | | E | | | | | | | | | | | | |
| | Revisión por la Dirección | Gestión Tecnológica<br>Fortalecimiento de la Gestión Institucional | P | | | | | | | | | | 50% | 50% | |
| | | | E | | | | | | | | | | | | |
| | Acompañamiento y ejecución de las actividades de los planes de mejoramiento y planes de cierre de brechas correspondientes al SGSPI | Todos los procesos de la entidad donde aplique | P | | 9% | 9% | 9% | 9% | 9% | 9% | 9% | 9% | 9% | 9% | 10% |
| | | | E | | | | | | | | | | | | |
| | Medición del nivel de implementación de la política de seguridad digital | Gestión Tecnológica | P | | | 30% | 40% | 30% | | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Seguimiento a la gestión y cierre oportuno de los incidentes y eventos de seguridad de la Información | Gestión Tecnológica | P | | | | 33% | | | | 33% | | | | 34% |
| | | | E | | | | | | | | | | | | |
| | Gestionar la ejecución de análisis de vulnerabilidades | Gestión Tecnológica | P | | | | 30% | 30% | 40% | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Seguimiento a la remediación de las vulnerabilidades | Gestión Tecnológica | P | | | | | | | | 50% | | | | 50% |
| | | | E | | | | | | | | | | | | |
| | Seguimiento a la Implementación, afinamiento y gestión de las herramientas de seguridad | Gestión Tecnológica | P | | | | 33% | | | | 33% | | | | 34% |
| | | | E | | | | | | | | | | | | |

| COMPONENTE O ETAPA O EJE | ACTIVIDAD | RESPONSABLE | P/E | PRIMER TRIMESTRE DE ENERO A MARZO | | | SEGUNDO TRIMESTRE DE ABRIL A JUNIO | | | TERCER TRIMESTRE DE JULIO A SEPTIEMBRE | | | CUARTO TRIMESTRE DE OCTUBRE A DICIEMBRE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| | Realizar ejercicios y simulaciones para fortalecer el reporte y gestión de incidentes de seguridad y privacidad de la información | Gestión Tecnológica | P | | | | | 50% | 50% | | | | | | |
| | | | E | | | | | | | | | | | | |
| **Continuidad Tecnológica** | Formalizar y socializar el Plan de Recuperación de Desastres - DRP | Gestión Tecnológica | P | | | 30% | 30% | 40% | | | | | | | |
| | | | E | | | | | | | | | | | | |
| | Gestionar las pruebas a los escenarios definidos en el Plan de Recuperación de Desastres – DRP en la medida de los recursos disponibles | Gestión Tecnológica | P | | | | | | | 20% | 20% | 20% | 20% | 20% | |
| | | | E | | | | | | | | | | | | |

## REFERENCIAS Y BIBLIOGRAFÍA

Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI – 2025. Ministerio de tecnologías de la información y las comunicaciones.