GOBIERNO ABIERTO DE BOGOTÁ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025

INSTITUTO DISTRITAL DE PROTECCIÓN BIENESTAR ANIMAL

CONTROL DE CAMBIOS

NO. DE ACTA DE APROBACIÓN DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	FECHA	VERSIÓN	DESCRIPCIÓN
Acta No. 1	30 de enero de 2025	1.0	Adopción

GOBIERNO ABIERTO DE BOGOTÁ

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

GOBIERNO ABIERTO DE BOGOTÁ

TABLA DE TABLAS

1. INTRODUCCIÓN.

El Instituto Distrital de Protección y Bienestar Animal, reconoce la importancia y el valor de la información con respecto a salvaguardar los niveles de seguridad de la información, entendiendo que la información no es sólo crítica para el éxito de la organización, sino estratégica para el cumplimiento de sus objetivos misionales y estratégicos a largo plazo, por esta razón, se establece el siguiente plan que regula el manejo de la información en el IDPYBA, orientado a definir los lineamientos para salvaguardar la confidencialidad, integridad y disponibilidad de la información propia del Instituto Distrital de Protección y Bienestar Animal, gestionando el acceso a la información, tomando como referencia la norma NTC/ISO 27001: 2013, adoptada por el Modelo de Seguridad y Privacidad de la Información establecido por el MinTIC.

Por lo anterior, es necesario realizar seguimiento y actividades de mejora continuas para el Modelo de Seguridad y privacidad de la información (en adelante MSPI) o también llamado Sistema de Gestión de la Seguridad de la Información (SGSI), el cual contribuya a fortalecer los niveles adecuados de seguridad para todos los activos de información de la entidad considerados relevantes, para propender por que los riesgos de la seguridad de la información sean identificados, gestionados y tratados, como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la entidad, en su estructura, sus objetivos o en alguna condición que la afecte, para asegurar que dichas políticas sigan siendo adecuadas y contribuyan a los requerimientos de la Entidad.

2. OBJETIVO.

Avanzar y fortalecer en la implementación del Modelo de Seguridad y Privacidad de la información en el Instituto Distrital de Protección y Bienestar Animal, para salvaguardar la integridad, confidencialidad y disponibilidad de la información, por medio de la actualización y adopción políticas, guías , procedimientos u otros controles técnicos y administrativos, que en conjunto con el monitoreo de los activos de información y el tratamiento de los riesgos de seguridad de la información, contribuyan a prevenir y gestionar un evento o incidente de Seguridad de la información que pueda materializarse, para velar la continuidad de los servicios tecnológicos en la entidad.

2.1. OBJETIVOS ESPECÍFICOS.

- Establecer para todo el personal del IDPYBA la necesidad de conocer y gestionar la seguridad de la información y promover la comprensión de sus responsabilidades individuales, mediante el seguimiento de controles, actividades para gestión y monitoreo de seguridad de la información, fortalecimiento de la cultura en seguridad de la información, para la concientización de funcionarios, contratistas y

terceras partes contribuyendo a minimizar la materialización de incidentes de seguridad de información.

- Fortalecer la cultura e higiene en seguridad de la información dentro del instituto.

- Determinar el acceso a los activos de información y adoptar las medidas esenciales de seguridad de la información necesarias para proteger al IDPYBA de amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando pérdida o mal uso de los activos de información. Para ello se realizará la valoración y tratamiento de Riesgos de seguridad de la información, definido en el Plan de riesgos 2023.

- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información, diligenciando y realizando seguimiento por medio de la herramienta de autodiagnóstico del MINTIC, el cual lidera la política de Gobierno Digital, apoyado por la Alta consejería para las TICS del Distrito y de conformidad con los requerimientos de las auditorías.

- Identificar y realizar la valoración de los activos de información, para determinar y evaluar los riesgos de seguridad de la información. Teniendo en cuenta las vulnerabilidades y amenazas que puede materializar el riesgo, como se establece en el plan de riesgos.

- Gestionar los riesgos de seguridad de la información, para que sean conocidos y según su impacto se realice el tratamiento de los mismos, los cuales se articulen con los cambios que se produzcan en la entidad, el entorno y la tecnología.

- Realizar el seguimiento y mejora continua de las políticas, procedimientos específicos a la política de seguridad y privacidad de la información, con el fin de velar porque estas salvaguarden los criterios de seguridad de la información, que apoyen el cumplimiento de los objetivos estratégicos de la entidad.
- Realizar el autodiagnóstico y las acciones de mejora, para fortalecer la implementación del MSPI dentro de la entidad.
- Elaborar e implementar el Plan de Recuperación de Desastres (DRP- por sus siglas en ingles) de los servicios críticos de tecnología.
- Elaborar e implementar los lineamientos concernientes a seguridad de la información, para adopción e implementación dentro de la entidad.

3. NORMATIVIDAD Y LINEAMIENTOS CONCEPTUALES Y METODOLÓGICOS.

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

Marco Normativo	Descripción
Constitución Política de Colombia. 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
Ley 1952 de 2019	Por medio de la cual se expide el código general Disciplinario
Ley 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
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 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1221 de 2008	Se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones
Decreto 680 de 2001	

	Modifica la Comisión Distrital de Sistemas y es establece el carácter de obligatoriedad en la adopción de las políticas que la CDS determine.
Decreto 053 de 15 de febrero de 2002	Por el cual se crea el Comité para la implementación del Número Único de Emergencias y Seguridad del Distrito Capital, del cual forma parte el secretario técnico de la CDS.
Decreto 397 de 17 de septiembre de 2002	Delegar en el secretario general de la Alcaldía Mayor de Bogotá las atribuciones conferidas al alcalde Mayor en el Acuerdo 57 de 2002 como presidente de la Comisión Distrital de Sistemas, y las demás funciones que se requieran en el ejercicio de esta atribución
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'
Decreto 619 del 28 de diciembre de 2007	Que el Decreto Distrital 619 de 2007 establece la estrategia de Gobierno Electrónico en el Distrito y define la necesidad de reglamentar gradualmente por parte de la Secretaría General de la Alcaldía Mayor de Bogotá la utilización de medios Electrónicos en diversos trámites, procedimientos y actuaciones de las entidades distritales.
Decreto 2106 de 2019	, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones
Decreto 612 de 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.
Decreto 460 del 1995	Registro Nacional del Derecho de Autor

Decreto 1421 de 1993	Por medio del cual se dicta el régimen especial para el Distrito Capital de Santa Fe de Bogotá, ciudad con autonomía para la gestión de sus intereses, dentro de los límites de la Constitución y la ley.
Decreto 1008 de 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 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Se establecen 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”.
Decreto 1081 de 2015	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1074 de 2015.	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 103 de 2015	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.

Decreto 1083 de 2015	Decreto Único Reglamentario de Función Pública 1083 de 2015

Decreto 1078 de 2015	Manual para la Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1.
Decreto 1080 de 2015	Se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Decreto 415 de 2016	Se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".
Directiva 005 -junio de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.
Directiva 22 de 2011	Política de estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos/as: que capturan las entidades del Distrito capital.
Directiva 005 del 12 de junio de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.

Resolución 305 de 2008	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
CONPES 3854 de 2016	Política Nacional de Seguridad digital.
CONPES 3995 de 2011	Política Nacional de confianza y seguridad digital.

4. AUTODIAGNÓSTICO.

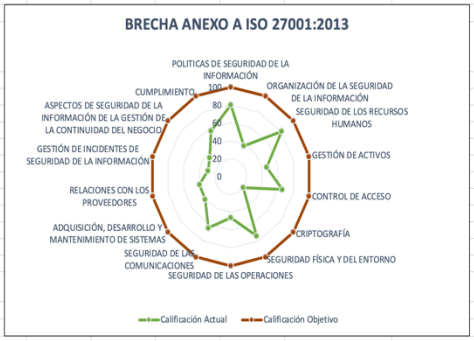
Realizando el seguimiento y diagnostico por medio del documento "Instrumento_Evaluacion_MSPI 2023" se ha evidenciado un avance significativo durante la vigencia 2023, que requieren fortalecerse para la vigencia 2025 debido a que no se ha tenido un avance fuerte en algunas actividades, las cuales ya están establecidas en el Plan de Seguridad y Privacidad de la Información para la presente vigencia.

Como se observa en la ilustración 1 de los catorce (14) dominios que comprende el MSPI se han gestionado trece (13) para una calificación de cuarenta y ocho (48) puntos de cien (100) puntos, en donde se han gestionado tres (3) dominios y un (1) optimizado, Seis (6) se encuentran en estado efectivo, cuatro (4) en estado repetible y uno (1) en estado inicial.

Ilustración 1

Reporte de autodiagnóstico del MINTIC

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	38	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	81	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	46	100	EFECTIVO
A.9	CONTROL DE ACCESO	66	100	GESTIONADO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	74	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	46	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	64	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	41	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34	100	REPETIBLE
A.18	CUMPLIMIENTO	56,5	100	EFECTIVO
	PROMEDIO EVALUACIÓN DE CONTROLES	51	100	EFECTIVO



Fuente: Herramienta de autodiagnóstico del MINTIC, diligenciada para el IDPYBA

Por lo cual al verificar el estado de avance por el ciclo PHVA (ilustración 2), se determina que el IDBYPA se encuentra la fase de planificación del 30%, Implementación 13%, Evaluación y desempeño 11% y mejora continua 12%, para un total de 65% de avance actual de la entidad. Evidenciando que se requiere fortalecer y dar continuidad con las acciones para el incremento de la fase de planeación, que contribuirán al aumento de las otras fases para alcanzar el avance esperado, según lo planteado en el autodiagnóstico del MSPI.

Ilustración 2

Reporte de autodiagnóstico del MINTIC, corte de diciembre de 2024

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	30%	40%
	Implementación	13%	20%
	Evaluación de desempeño	11%	20%
	Mejora continua	12%	20%
TOTAL		65%	100%

Fuente: Herramienta de autodiagnóstico del MINTIC, diligenciada para el IDPYBA

5. DESARROLLO DEL PLAN.

Teniendo en cuenta los anterior se hace necesario, efectuar actividades para aumentar el nivel de implementación del Modelo de Seguridad y Privacidad de la Información dentro del IDPYBA, para ello se hace necesario incrementar el componente de planificación e implementación.

Para fortalecer la fase de planificación se requiere realizar las siguientes actividades:

1. Revisar y/o actualizar u crear Políticas concernientes con la Seguridad y privacidad de la información y procedimientos para su implementación, según sea requerido por el MSPI

Esta actividad está asociada con los dominios A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN y A.9 CONTROL DE ACCESO, el cual comprende la revisión de todo el proceso de gestión tecnológica, desde la caracterización, hasta los procedimientos, guías instructivos, formatos y demás controles técnicos u administrativos, que apoyen en la gestión de la seguridad y privacidad de la información.

2. Elaborar, adoptar y/o actualizar las políticas, procedimientos y demás documentos concernientes a la protección y privacidad de la información sensible concerniente a

bases de datos de los sistemas de información, bases no formales y procesos y procedimientos para la recolección de información privada o semiprivada.

Esta actividad está asociada con el dominio A.18 CUMPLIMIENTO, la cual es necesaria para formalizar e implementar lineamientos para el fortalecimiento y adecuada gestión para la protección de datos personales.

3. Actualizar y hacer seguimiento al Autodiagnóstico de Seguridad y privacidad de la Información con la herramienta MINTIC de Gobierno Digital.

Actividad establecida para medir el avance en la implementación del MSPI con la herramienta dispuesta.

4. Realizar las mesas de trabajo con las áreas, para el seguimiento y actualización de los Activos de Información, los cuales sean posteriormente aprobados por el comité de Gestión y desempeño.

Actividad asociada con el dominio A.8 GESTIÓN DE ACTIVOS, en donde los activos de información del Instituto Distrital de Protección y Bienestar Animal han sido identificados y clasificados, para lo cual se considera dentro del presente plan, realizar la actualización y revisión al interior del Instituto para establecer su grado de criticidad. Así mismo, deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo de información como insumo principal para desarrollar las actividades y controles relacionados con la seguridad de la información.

5. Realizar seguimiento para Valoración, tratamiento y controles de los Riesgos de Seguridad de la Información.

Esta actividad está asociada con el componente de planificación y comprende que el plan de tratamiento de riesgos y la declaración de aplicabilidad cuenten con:

a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos.
b. Se determinaron todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos.
c. Compare los controles determinados en el plan de tratamiento con los del Anexo A y verifique que no se han omitidos controles, si estos han sido omitidos se debe reflejar en la declaración de aplicabilidad.
d. Revise la Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, ya sea que se implementen o no y la justificación para las exclusiones de los controles del Anexo A, y que haya sido revisado y aprobado por la alta Dirección.

e. Revise que el plan de tratamiento de riesgos haya sido revisado y aprobado por la alta Dirección.
f. Revise que exista una aceptación de los riesgos residuales por parte de los dueños de los riesgos.

6. Realizar seguimiento de las jornadas de sensibilización y/o capacitaciones establecidas en el PIC, con relación a Tecnologías de la información y Seguridad y privacidad de la información

Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

La anteriores Actividades contribuirán en el avance del componente de planificación en un 10% y pasar al 40% de avance esperado en el MSPI.

Para fortalecer la fase de implementación, se hace necesario realizar las siguientes actividades:

Igualmente se establecerán controles técnicos, para realizar seguimiento de la infraestructura tecnológica, velando por que estos cuenten con los principios de confidencialidad, integridad y disponibilidad de la información.

a. Estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.

Esta actividad comprende la estrategia de planificación y control operacional para seguimiento del MSPI.

b. Porcentaje de avance en la ejecución de los planes de tratamiento

Esta actividad comprende la medición del desarrollo y cumplimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información.

La anteriores Actividades contribuirán en el avance del componente de implementación en un 5% y pasar al 18% aproximándose al avance esperado en el MSPI

6. ALCANCE DE LA ESTRATEGIA DE SEGURIDAD DE INFORMACIÓN

Los contenidos del presente plan son aplicables a todos los activos de información de todos los procesos del Instituto Distrital de Protección y Bienestar Animal, consta de las

políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con el plan para el tratamiento de riesgos 2025.

7. CRONOGRAMA

Para hacer realizables las estrategias, estas son materializadas en actividades de acuerdo con su complejidad; el IDPYBA tiene previsto realizar las siguientes actividades para el desarrollo y cumplimiento del Plan de Seguridad y Privacidad de la Información, el cual se encuentra en la matriz adjunta al presente documento.

8. EVALUACIÓN Y SEGUIMIENTO

Tabla 2

Indicadores de seguimiento del PSPI

N°	ACTIVIDAD	META ESPERADA	PRODUCTO O ENTREGABLE	MES DE EJECUCIÓN		RESPONSABLE
				FECHA INICIO	FECHA FINAL	
1	Revisar y/o actualizar u crear Políticas concernientes con la Seguridad y privacidad de la información y procedimiento para su implementación, según sea requerido por el MSPI	100	documentos actualizados o elaborados referente a Políticas, procedimientos, guías, instructivos y/o formatos concernientes al modelo de Seguridad de la Información	Febrero	Diciembre	Lider del Proceso Gestión TIC/ profesional del proceso
2	Elaborar, adoptar y/o actualizar las política , procedimientos y demás documentos concernientes a la protección y privacidad de la información sensible concerniente a	1	Politicas y/o procedimientos y/o documentos concernientes a la protección de Información personal	Febrero	Diciembre	

	bases de datos de los sistemas de información, bases no formales y procesos y procedimientos para la recolección de información privada o semiprivada.				
3	Actualizar y hacer seguimiento al Autodiagnóstico de Seguridad y privacidad de la Información con la herramienta MINTIC de Gobierno Digital	1	Documento de informe de Autodiagnóstico	Febrero	Diciembre
4	Realizar las mesas de trabajo con las áreas, para el seguimiento y actualización y de los Activos de Información, los cuales sean posteriormente aprobados por el comité de Gestión y desempeño	1	Mesas de Trabajo con las áreas y matriz de inventarios de Activos de Información actualizada y aprobada	Abril	Agosto
5	Realizar seguimiento para Valoración, tratamiento y controles de los Riesgos de Seguridad de la Información y la declaración de aplicabilidad	1	Documento Riesgos de seguridad y privacidad de la información y la declaración de aplicabilidad, consolidados y actualizados	Abril	Diciembre
6	Realizar seguimiento de las jornadas de sensibilización y/o capacitaciones establecidas en el PIC, con relación a Tecnologías de la información y	1	Capacitaciones y/o sensibilizaciones brindadas a personal del IDPYBA	Febrero	Noviembre

	Seguridad y privacidad de la información				
7	Participar, elaborar y desarrollar del plan de mejoramiento definido	1	Plan de Recuperación de Desastres	Abril	Diciembre
8	Desarrollar la estrategia que se debe ejecutar con las actividades para lograr la implementación y puesta en marcha del MSPI de la entidad.	1	documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Marzo	Diciembre
9	Elaborar e implementar el Plan de Recuperación de Desastres (DRP- por sus siglas en ingles) de los servicios críticos de tecnología, en coordinación con todo el equipo de gestión tecnológica	1	documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Febrero	Diciembre

Fuente: Elaboración propia Gestión Tecnológica

9. REFERENCIAS Y BIBLIOGRAFÍA.

Listado maestro del Modelo de Seguridad y Privacidad de la información -MSPI https://gobiernodigital.mintic.gov.co/692/articles-237872_maestro_mspi.pdf

Manual de implementación Gobierno Digital del MinTIC
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/