

2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



**ALCALDÍA MAYOR
DE BOGOTÁ D.C.**

SECRETARÍA DE SALUD

TABLA DE CONTENIDO

1	OBJETIVO	1
1.1	Objetivos Específicos.....	1
2	ALCANCE	1
3	MARCO NORMATIVO	1
4	DOCUMENTOS DE REFERENCIA	4
5	ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	4
6	ESTRATEGIAS	5
6.1	Descripción de las Estrategias.....	6
6.2	Portafolio de Proyectos / Actividades	7
6.3	Cronograma de Actividades / Proyectos	9
6.4	Presupuesto.....	12
7	INDICADORES	12
8	SEGUIMIENTO	13
9	ANEXOS	15
10	CONTROL DE CAMBIOS.....	15

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	1
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1 OBJETIVO

Fortalecer la seguridad y privacidad de la información en la Secretaría Distrital de Salud de Bogotá, mediante la implementación de las actividades establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Política de Gobierno Digital del MinTIC, en alineación con la NTC ISO/IEC 27001, la Política Pública de Seguridad Digital y los criterios de continuidad de la operación de los servicios. Este plan se enfoca en la protección de la información que circula en los procesos de la entidad, asegurando su confidencialidad, integridad y disponibilidad, en cumplimiento con las normativas y mejores prácticas internacionales.

1.1 Objetivos Específicos

- Definir y establecer la estrategia de seguridad digital de la Entidad.
- Identificar y gestionar los riesgos asociados a la información.
- Implementar controles y medidas de protección adecuadas.
- Sensibilizar y capacitar al personal en buenas prácticas de seguridad.
- Evaluar y monitorear la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).

2 ALCANCE

Este plan aplica a todos los procesos, sistemas de información, usuarios y activos tecnológicos de la Entidad, incluyendo datos sensibles y confidenciales manejados en el marco de sus funciones.

3 MARCO NORMATIVO

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- Ley 2088 de 2012. Por la cual se regula el trabajo en casa y se dictan otras disposiciones
- Ley 2052 de 2020. 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.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- 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 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan 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 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- Ley 527 de 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.
- Decreto 338 de 2022. Por el cual se adiciona el Título 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.
- Decreto 88 de 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, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

- 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.
- 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 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- 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 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 2609 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.
- Resolución 1838 de 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 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.
- Resolución 1519 de 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.
- CONPES 3995 de 2020. Confianza y Seguridad Digital
- CONPES 3854 de 2017. Política Nacional de Seguridad digital.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Resolución 1569 de 2024. “Por la cual se crea el Comité Institucional de Gestión y Desempeño y se establecen disposiciones para la operación del Modelo Integrado de Planeación y Gestión en la Secretaría Distrital de Salud de Bogotá D.C.”

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

4 DOCUMENTOS DE REFERENCIA

El Plan de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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”
- 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”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC, incluidos los controles basados en el Anexo A de la norma NTC/ISO 27001:2013.
- Estándar ISO/IEC 27001:2022, incluido el Anexo A.

5 ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con base en el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), establecido en la Política Nacional de Gobierno Digital, se ha evaluado el nivel de implementación de los controles de seguridad de la Norma NTC/ISO 27001:2013 en la Secretaría Distrital de Salud de Bogotá.

No.	Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	44	100	EFFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	74	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	44	100	EFFECTIVO
A.9	CONTROL DE ACCESO	49	100	EFFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	47	100	EFFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	57	100	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	43	100	EFFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	31	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	84	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		46	100	EFFECTIVO

El análisis de efectividad refleja un porcentaje de implementación de los controles de seguridad de 46%, evidenciando el estado actual de madurez del sistema y permitiendo identificar brechas críticas en la gestión de la seguridad de la información

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

A continuación, se presenta una visualización de la brecha general identificada, la cual permitirá orientar las estrategias y acciones necesarias para fortalecer la seguridad y privacidad de la información en la entidad:



Este diagnóstico se empleó como base para la priorización de actividades dentro del Plan de Seguridad y Privacidad de la Información, con el fin de avanzar en el cierre de las brechas detectadas y asegurar el cumplimiento.

6 ESTRATEGIAS

La Secretaría Distrital de Salud – SDS adopta una estrategia integral de seguridad basada en el MSPI y alineada con los lineamientos de la Política de Gobierno Digital del MinTIC, la NTC ISO/IEC 27001, la Política Pública de Seguridad Digital y los criterios de continuidad de la operación de los servicios.

Esta estrategia establece un marco de referencia para la gestión de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos en todos los procesos institucionales. Para ello, se definen acciones, controles y mecanismos que permitan fortalecer la protección de los activos de información, mitigar riesgos, asegurar el cumplimiento normativo y fomentar una cultura de seguridad en la entidad.

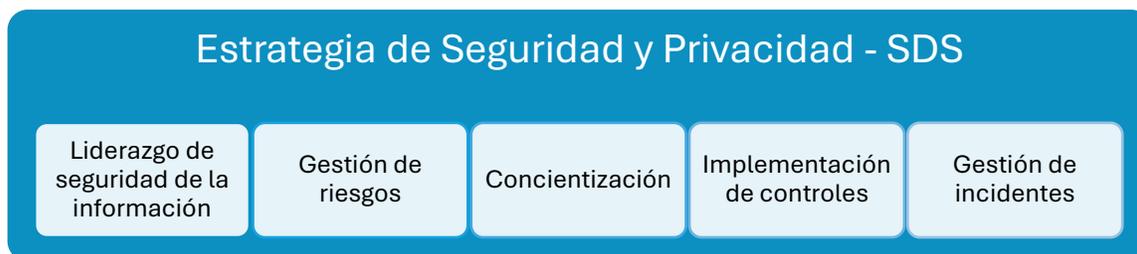
La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

6.1 Descripción de las Estrategias

Para asegurar una gestión efectiva de la seguridad y privacidad de la información, la SDS ha definido un conjunto de estrategias alineadas con el MSPI, la resolución 500 de 2021 y las mejores prácticas establecidas en la NTC ISO/IEC 27001.

Cada estrategia aborda un eje fundamental en la protección de la información y está orientada a mitigar riesgos, fortalecer la resiliencia institucional y asegurar la continuidad de los servicios. Estas estrategias incluyen liderazgo en seguridad, gestión de riesgos, concienciación y capacitación, implementación de controles y gestión de incidentes.



A continuación, se presentan las estrategias específicas con su respectiva descripción y objetivos, las cuales permitirán consolidar un entorno seguro para la gestión de la información en la entidad:

ESTRATEGIA / EJE	DESCRIPCIÓN	OBJETIVO
Liderazgo de Seguridad de la Información	Asegura el compromiso de la alta dirección y la integración de la seguridad de la información en la gestión estratégica de la Entidad, estableciendo políticas, roles y responsabilidades para cada una de las líneas de defensa.	Asegurar la gobernanza y liderazgo en seguridad de la información mediante la aprobación y aplicación de políticas, alineadas con la NTC ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información (MSPI).
Gestión de Riesgos	Identifica, analiza y trata los riesgos de seguridad de la información para minimizar vulnerabilidades y fortalecer la resiliencia de la entidad frente a amenazas internas y externas.	Asegurar la identificación y gestión de riesgos, permitiendo su tratamiento efectivo para prevenir incidentes y optimizar la seguridad de los procesos y servicios de la entidad.
Concientización y Capacitación	Fomenta una cultura organizacional en seguridad y privacidad de la información a través de programas de sensibilización, formación y transferencia de conocimiento para todos los funcionarios y colaboradores.	Concientiar y capacitar a los funcionarios en seguridad y privacidad de la información, promoviendo el cumplimiento de normativas y buenas prácticas en la gestión de la información.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

ESTRATEGIA / EJE	DESCRIPCIÓN	OBJETIVO
Implementación de Controles	Implementa medidas de seguridad administrativas, técnicas y físicas alineadas con la NTC ISO/IEC 27001, asegurando la protección de los activos de información y la mitigación de riesgos.	Aplicar controles adecuados para proteger la información contra accesos no autorizados, alteraciones, pérdida o destrucción, cumpliendo con los estándares de seguridad requeridos.
Gestión de Incidentes	Establece procedimientos para la identificación, análisis, respuesta y recuperación ante incidentes de seguridad de la información, reduciendo su impacto y mejorando la capacidad de respuesta.	Establecer un enfoque estructurado para la gestión de incidentes, asegurando una respuesta oportuna y eficiente para minimizar impactos y mejorar la seguridad de la entidad.

A partir de las anteriores estrategias, se establecieron las acciones y proyectos específicos que permitirán su implementación efectiva, con un enfoque basado en la mejora continua y la alineación con las normativas y mejores prácticas en materia de seguridad de la información.

6.2 Portafolio de Proyectos / Actividades

Para asegurar la implementación efectiva de la estrategia de seguridad y privacidad de la información, la SDS ha definido un conjunto de proyectos y actividades alineados con las estrategias establecidas en este plan.

Este portafolio tiene como objetivo traducir las estrategias en acciones concretas, permitiendo la ejecución de iniciativas orientadas a fortalecer la gobernanza en seguridad, la gestión de riesgos, la concienciación, la implementación de controles y la respuesta ante incidentes. Cada proyecto y actividad contribuirá al desarrollo y consolidación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Entidad, asegurando su alineación con la NTC ISO/IEC 27001 y los lineamientos del MSPI.

A continuación, se presentan los proyectos y actividades clave, organizados según los ejes estratégicos de seguridad definidos en este plan:

ESTRATEGIA / EJE	PROYECTO / ACTIVIDAD	PRODUCTOS
Liderazgo de Seguridad de la Información	ACTIVIDAD LSI 1: Actualizar e implementar la política de seguridad de la información conforme a los requisitos de la NTC ISO/IEC 27001:2022 y el MSPI.	Política de Seguridad actualizada, formalizada e Implementada.
	ACTIVIDAD LSI 2: Actualizar los Roles y Responsabilidades de Seguridad de la Información.	Establecer los roles, responsabilidades y autoridades para la Seguridad de la Información

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
	Código:	SDS-DFO-PL-001	Versión:	1	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda					

ESTRATEGIA / EJE	PROYECTO / ACTIVIDAD	PRODUCTOS
		formalizados. Establecer las competencias para el SGSI.
	ACTIVIDAD LSI 3: Desarrollar o actualizar documentos requeridos por el SGSI.	Reporte de estado y avance de implementación del SGSI.
	ACTIVIDAD LSI 4: Realizar el seguimiento y evaluación de los indicadores.	Reporte de los indicadores de desempeño de seguridad de la información.
Gestión de Riesgos	ACTIVIDAD GR 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información	Matriz de riesgos de seguridad para la seguridad de la información.
	ACTIVIDAD GR 2: Definir e implementar planes de tratamiento de riesgos de seguridad.	Planes de tratamiento de riesgos de Seguridad de la Información.
Concienciación y Capacitación	ACTIVIDAD CC 1: Establecer la planeación anual de sensibilización.	Plan de Sensibilización
	ACTIVIDAD CC 2: Realizar jornadas de sensibilización a todo el personal.	Evidencias de las actividades desarrolladas.
	ACTIVIDAD CC 3: Medir el grado de sensibilización a toda la Entidad.	Resultado de las encuestas de medición.
Implementación de Controles	ACTIVIDAD IC 1: Establecer metodologías, mecanismos y documentación para la gestión de la seguridad en la nube.	Reporte de estado de la seguridad de los activos alojados en la nube.
	ACTIVIDAD IC 2: Realizar análisis de vulnerabilidades técnicas a los activos de información.	Reporte de priorización de las vulnerabilidades técnicas.
	PROYECTO IC 1: Desplegar soluciones tecnológicas de seguridad.	Catálogos actualizados de servicios e infraestructura de seguridad. Reportes de operación de los servicios de seguridad.
	PROYECTO IC 2: Implementación del instrumento para el ejecución y seguimiento del SGSI.	Herramienta para el ejecución y seguimiento implementada.
Gestión de Incidentes	ACTIVIDAD GI 1: Actualizar y formalizar la gestión de Incidentes de seguridad de la información.	Procedimiento de gestión de incidentes de seguridad formalizado
	ACTIVIDAD GI 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	Sesiones de capacitación desarrolladas.

A través de estas iniciativas, la Entidad asegura la protección de sus activos de información, optimizará la gestión de riesgos y consolidará una cultura organizacional basada en la seguridad de la información y la mejora continua.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

6.3 Cronograma de Actividades / Proyectos

Para una implementación estructurada y eficiente de las estrategias de seguridad y privacidad de la información, la SDS ha establecido un cronograma de actividades y proyectos. Este cronograma detalla la planificación temporal de las acciones definidas en el portafolio de proyectos y actividades, estableciendo plazos, líderes y dependencias clave para su ejecución. Su propósito es asegurar el cumplimiento de los objetivos estratégicos en seguridad de la información, optimizando recursos y garantizando un seguimiento efectivo de los avances.

A continuación, se presenta la planificación de las actividades y proyectos a desarrollar, organizada en períodos estratégicos para su implementación.

ESTRATEGIA / EJE	ID	PROYECTO / ACTIVIDAD	TAREA(S) CLAVE	LIDER EJECUCION	PROGRAMACIÓN *	
					INICIA	FINALIZA
Liderazgo de Seguridad de la Información	A_LSI 1	Actualizar y divulgar la política de seguridad	Actualizar Diagnóstico de Seguridad	Referente de seguridad de la información (DPI&C), Equipo Seguridad Informática (DTIC)	1/2/2025	28/2/2025
			Formalizar de la Política de Seguridad conforme a los requisitos de la NTC ISO/IEC 27001:2022 y el MSPI.	Referente de seguridad de la información (DPI&C), comité de gestión institucional	1/2/2025	28/2/2025
			Divulgar nueva de la Política de seguridad de la Información.	Referente de seguridad de la información (DPI&C)	1/3/2025	31/12/2025
		Implementar la política de seguridad	Planificar las acciones determinadas en el plan de tratamiento de riesgos	Equipo Seguridad Informática (DTIC), Gestores de procesos	1/3/2025	31/11/2025
			Realizar reuniones de socialización de los avances de la implementación.	Referente de seguridad de la información (DPI&C)	1/4/2025	31/4/2025
	A_LSI 2	Actualizar los Roles y Responsabilidades	Establecer los roles, responsabilidades y autoridades.	Referente de seguridad de la información (DPI&C)	1/2/2025	15/2/2025
			Establecer las competencias para el SGSI	Referente de seguridad de la información (DPI&C)	1/2/2025	15/2/2025
	A_LSI 3	Desarrollar o actualizar documentos requeridos	Actualizar Manuales, Políticas, Resoluciones y documentación del SGSI	Referente de seguridad de la información (DPI&C)	1/2/2025	31/12/2025
			Actualizar el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos.	Referente de seguridad de la información (DPI&C), Equipo Seguridad Informática (DTIC)	15/11/2025	31/1/2026

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
	Código:	SDS-DFO-PL-001	Versión:	1	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda					

ESTRATEGIA / EJE	ID	PROYECTO / ACTIVIDAD	TAREA(S) CLAVE	LIDER EJECUCION	PROGRAMACIÓN *	
					INICIA	FINALIZA
			Actualizar documentación de cumplimiento requerimientos infraestructuras críticas del gobierno.	Referente de seguridad de la información (DPI&C), Equipo Seguridad Informática (DTIC)	1/4/2025	31/12/2025
			Actualizar el Análisis de Impacto de la Operación	Referente de seguridad de la información (DPI&C)	1/4/2025	31/5/2025
			Actualizar y documentar la valoración de riesgos de interrupción, estrategia y plan de continuidad de la operación TIC	Equipo de Continuidad Operativa TIC (DTIC)	1/6/2025	31/12/2025
			Actualizar la gestión de datos personales	Referente de seguridad de la información (DPI&C), Gestores de procesos	1/2/2025	31/12/2025
	A_LSI 4	Realizar el seguimiento y evaluación	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información y Seguridad Digital.	Referente de seguridad de la información (DPI&C)	1/3/2025	15/12/2025
			Formular, Implementar y actualizar los indicadores del SGSI	Referente de seguridad de la información (DPI&C)	1/3/2025	31/7/2025
			Reportar indicadores	Gestores de procesos	1/2/2025	31/12/2025
			Participar en las auditorías internas (primera y segunda parte)	Referente de seguridad de la información (DPI&C)	1/2/2025	31/12/2025
			Planificar la realización de auditorías externas	Referente de seguridad de la información (DPI&C)	1/7/2025	31/12/2025
			Reportar del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora	Referente de seguridad de la información (DPI&C)	1/2/2025	31/12/2025
Gestión de Riesgos	A_GR 1	Identificar, valorar y clasificar los riesgos	Actualizar e identificar nuevos activos de información en cada dependencia	Gestores de procesos	1/2/2025	31/3/2025
			Validar, consolidar y publicar los activos de información	DPI&C, Gestión documental	1/9/2025	15/12/2025
			Actualización y sensibilización de lineamientos de riesgos	Equipo de gestión de riesgos	1/2/2025	31/3/2025
			Realizar la Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Gestores de procesos	1/5/2025	30/6/2025
	A_GR 2		Definir de planes de tratamiento de riesgos los identificados	Gestores de procesos	1/7/2025	30/9/2025

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL				
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
	Código:	SDS-DFO-PL-001	Versión:	1	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda					

ESTRATEGIA / EJE	ID	PROYECTO / ACTIVIDAD	TAREA(S) CLAVE	LIDER EJECUCION	PROGRAMACIÓN *	
					INICIA	FINALIZA
		Definir e implementar planes de tratamiento de riesgos	Realizar el seguimiento implementación de controles	Referente de seguridad de la información (DPI&C)	1/7/2025	31/12/2025
Concienciación y Capacitación	A_CC 1	Establecer la planeación anual de sensibilización	Actualizar la documentación del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad	Referente de seguridad de la información (DPI&C)	1/2/2025	28/2/2025
	A_CC 2	Realizar jornadas de sensibilización	Implementar las estrategias del Plan de Cambio, Cultura y Apropiación	Referente de seguridad de la información (DPI&C)	1/3/2025	31/12/2025
	A_CC 3	Medir el grado de sensibilización	Analizar los resultados de los instrumentos de medición del Plan de Cambio, Cultura y Apropiación	Referente de seguridad de la información (DPI&C)	1/3/2025	31/12/2025
Implementación de Controles	A_IC 1	Establecer la gestión de la seguridad en la nube	Establecer metodologías, mecanismos y documentación para la gestión de la seguridad de la información alojada en la nube	Equipo Seguridad Informática (DTIC)	1/3/2025	31/12/2025
	A_IC 2	Realizar análisis de vulnerabilidades técnicas	Descubrir falencias técnicas en los sistemas y aplicaciones.	Equipo Seguridad Informática (DTIC)	1/2/2025	30/6/2025
			Ejecutar el plan de remediación de acuerdo con las vulnerabilidades identificadas	Equipo Seguridad Informática (DTIC), Dirección TIC.	1/7/2025	15/12/2025
	P_IC 1	Desplegar soluciones tecnológicas de seguridad	Implementar soluciones tecnológicas de seguridad	Equipo Seguridad Informática (DTIC)	1/3/2025	31/12/2025
	P_IC 2	Implementación del instrumento del SGSI	Planificar de la selección de la instrumentalización	Referente de seguridad de la información (DPI&C)	1/3/2025	31/3/2025
Desplegar la herramienta SGSI			Referente de seguridad de la información (DPI&C)	1/4/2025	31/12/2025	
Gestión de Incidentes	A_GI 1	Actualizar y formalizar la gestión de Incidentes	Revisar, actualizar y publicar del procedimiento de incidentes de seguridad	Referente de seguridad de la información (DPI&C)	1/5/2025	31/5/2025
			Gestionar los incidentes de Seguridad	Equipo Seguridad Informática (DTIC), Referente de seguridad de la información (DPI&C)	1/2/2025	31/12/2025
	A_GI 2	Capacitar al personal en la gestión de incidentes	Socializar el procedimiento a los especialistas TIC, soportes en sitio, Mesa de Servicios TIC	Referente de seguridad de la información (DPI&C)	1/4/2025	31/12/2025
			Socializar el procedimiento a los colaboradores de la Entidad	Referente de seguridad de la información (DPI&C)	1/4/2025	31/12/2025

Nota: * Formato estándar de fecha día/mes/año

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

6.4 Presupuesto

El presente plan contempla la inversión en infraestructura tecnológica, capacitación, adquisición de herramientas de seguridad, implementación de controles y gestión de riesgos, a través de los recursos del *Proyecto 8108*, asegurando la sostenibilidad y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) de la Entidad.

7 INDICADORES

Para medir la efectividad de la implementación de las estrategias de seguridad y privacidad de la información, la SDS ha definido un conjunto de indicadores. Estos indicadores permitirán evaluar el cumplimiento de los objetivos del MSPI, la norma NTC ISO/IEC 27001 y otros lineamientos normativos aplicables.

A través del monitoreo y análisis de estos indicadores, la entidad podrá identificar oportunidades de mejora, optimizar la gestión de riesgos y asegurar la madurez continua del SGSI.

A continuación, se presentan los indicadores seleccionados para la medición del desempeño de este plan.

ESTRATEGIA / EJE	ID P/A	INDICADOR	META
Liderazgo de Seguridad de la Información	A_LSI 1	Porcentaje de avance en la actualización e implementación de la política de seguridad.	100% de la política actualizada e implementada.
	A_LSI 2	Porcentaje de roles y responsabilidades formalizados en la política de seguridad.	100% de roles y responsabilidades documentados y aprobados.
	A_LSI 3	Número de documentos SGSI actualizados o desarrollados.	100% de documentos del SGSI actualizados o desarrollados.
	A_LSI 4	Porcentaje de cumplimiento en el seguimiento y evaluación de indicadores.	100% de los indicadores de seguridad evaluados trimestralmente.
Gestión de Riesgos	A_GR 1	Porcentaje de activos de información evaluados en la matriz de riesgos.	100% de los activos de información registrados en la matriz de riesgos.
	A_GR 2	Porcentaje de riesgos con planes de tratamiento implementados.	90% de los riesgos críticos con planes de tratamiento implementados.
Concienciación y Capacitación	A_CC 1	Número de planes de sensibilización elaborados y aprobados.	1 plan anual de sensibilización elaborado y aprobado.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

ESTRATEGIA / EJE	ID P/A	INDICADOR	META
	A_CC 2	Número de jornadas de sensibilización realizadas.	Mínimo 4 jornadas de sensibilización al año.
	A_CC 3	Porcentaje de personal capacitado y sensibilizado en seguridad de la información.	90% del personal capacitado anualmente.
Implementación de Controles	A_IC 1	Porcentaje de mecanismos implementados para la gestión de seguridad en la nube.	100% de los mecanismos de seguridad implementados.
	A_IC 2	Número de análisis de vulnerabilidades técnicas realizados.	Mínimo 2 análisis de vulnerabilidades técnicas por año.
	P_IC 1	Porcentaje de soluciones tecnológicas de seguridad desplegadas.	100% de las soluciones tecnológicas de seguridad desplegadas.
	P_IC 2	Grado de implementación del instrumento de ejecución y seguimiento del SGSI.	100% de implementación del instrumento de ejecución y seguimiento del SGSI.
Gestión de Incidentes	A_GI 1	Porcentaje de cumplimiento en la actualización del procedimiento de gestión de incidentes.	100% de cumplimiento en la actualización del procedimiento de gestión de incidentes.
	A_GI 2	Número de sesiones de capacitación en gestión de incidentes realizadas.	Mínimo 2 sesiones de capacitación en gestión de incidentes por año.

8 SEGUIMIENTO

El seguimiento se realizará a través de indicadores de desempeño, auditorías internas, revisiones periódicas y reportes de avances, permitiendo la identificación de oportunidades de mejora y la toma de decisiones informadas para fortalecer la seguridad y privacidad de la información en la Entidad.

A continuación, se presentan los mecanismos y herramientas utilizados para el seguimiento y control del plan.

ESTRATEGIA / EJE	ID P/A	SEGUIMIENTO	RESPONSABLE
Liderazgo de Seguridad de la Información	A_LSI 1	Revisión trimestral del cumplimiento y aplicación de la política de seguridad.	Referente de seguridad de la información (DPI&C)
	A_LSI 2	Verificación semestral de la documentación de roles y responsabilidades.	Referente de seguridad de la información (DPI&C) / Talento Humano.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

ESTRATEGIA / EJE	ID P/A	SEGUIMIENTO	RESPONSABLE
	A_LSI 3	Supervisión mensual del avance en la actualización de documentos del SGSI.	Referente de seguridad de la información (DPI&C) / Dirección PI&C.
	A_LSI 4	Revisión trimestral de los reportes de indicadores de desempeño en seguridad.	Referente de seguridad de la información (DPI&C) / Alta Dirección.
Gestión de Riesgos	A_GR 1	Evaluación semestral de la matriz de riesgos y actualización de registros.	Líder de Gestión de Riesgos / Referente de seguridad de la información (DPI&C).
	A_GR 2	Seguimiento mensual a la implementación de los planes de tratamiento de riesgos.	Líder de Gestión de Riesgos, Gestores de cada proceso
Concienciación y Capacitación	A_CC 1	Supervisión anual de la planeación de sensibilización y su implementación.	Área de Capacitación y Sensibilización / Referente de seguridad de la información (DPI&C).
	A_CC 2	Control trimestral sobre la ejecución de las jornadas de sensibilización.	Área de Capacitación y Sensibilización / Talento Humano. Referente de seguridad de la información (DPI&C)
	A_CC 3	Monitoreo semestral del nivel de sensibilización del personal.	Área de Capacitación y Sensibilización / Referente de seguridad de la información (DPI&C).
Implementación de Controles	A_IC 1	Revisión anual del estado de seguridad de activos en la nube y mejoras necesarias.	Responsable de Infraestructura Tecnológica / Referente de seguridad de la información (DPI&C).
	A_IC 2	Supervisión trimestral de la ejecución de análisis de vulnerabilidades.	Grupo de Seguridad Informática / Referente de seguridad de la información (DPI&C).
	P_IC 1	Seguimiento trimestral del despliegue de soluciones tecnológicas de seguridad.	Grupo de Seguridad Informática / Infraestructura Tecnológica.
	P_IC 2	Monitoreo mensual del estado de implementación del instrumento del SGSI.	Referente de seguridad de la información (DPI&C) / Dirección PI&C.
Gestión de Incidentes	A_GI 1	Evaluación semestral del procedimiento de gestión de incidentes y su aplicación.	Grupo de Seguridad Informática. Referente de seguridad de la información (DPI&C).
	A_GI 2	Supervisión semestral de la capacitación y nivel de conocimiento en gestión de incidentes.	Referente de seguridad de la información (DPI&C) / Dirección PI&C.

El seguimiento continuo mantiene su efectividad y evolución, permitiendo la identificación de mejoras y la optimización de las estrategias implementadas.

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE SALUD	DESARROLLO Y FORTALECIMIENTO INSTITUCIONAL DIRECCION DE PLANEACION INSTITUCIONAL Y CALIDAD SISTEMA DE GESTIÓN CONTROL DOCUMENTAL			
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Código:	SDS-DFO-PL-001	Versión:	
Elaborado por: Luis G. Barrera / Revisado por: Luz A. Manquillo - Jaime A. Pineda/ Aprobado por: Luz A. Manquillo - Jaime A. Pineda				

9 ANEXOS

- El Modelo de Seguridad y Privacidad de la Información, el cual puede ser consultado en línea y descargar las guías pertinentes, en la dirección: <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>
- Los lineamientos y estándares para la estrategia de seguridad digital y el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital pueden ser consultados en línea y descargar las guías pertinentes, en la dirección: https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_0500_2021.htm

10 CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE ACTUALIZACIÓN	CRÉDITOS
1	31/01/2025	Se crea con el propósito establecer la estrategia para proteger la información y los activos digitales respondiendo a la necesidad de cumplir con normativas vigentes.	Luis Guillermo Barrera

La impresión de este documento se considera **COPIA NO CONTROLADA** y no se garantiza que esta corresponda a la versión vigente, salvo en los procesos que usan sello. Esta información es de carácter confidencial y propiedad de la Secretaría Distrital de Salud (SDS); está prohibida su reproducción y distribución sin previa autorización del proceso que lo genera, excepto en los requisitos de ley.