Control de cambios

Versión	Fecha	Descripción de la modificación
01	13 de febrero de 2020	Se aprueba el Plan de Seguridad y Privacidad de la Información de la Secretaría Distrital de Gobierno.
02	13 de febrero del 2021	Se ajusta las metas para la vigencia 2021

Método de Elaboración	Revisa	Aprueba
El documento se elabora de acuerdo con las indicaciones de la Oficina Asesora de Planeación y el grupo de trabajo de la Dirección de Tecnología e Información.	**Jorge Bernardo Gomez** Proceso Gerencia de TIC Director de Tecnologías e Información **Liliana Casas** Profesional de revisión por normalización de la OAP	**Ana María Aristizábal Osorio** Líder del Macroproceso Gerencia de la Información Subsecretario de Gestión Institucional **Jorge Bernardo Gomez** Director de Tecnologías e Información El documento fue revisado y aprobado mediante caso en aplicativo Hola No. 155123

1. INFORMACIÓN GENERAL

1.1 Propósito

Definir las actividades necesarias para implementar el Modelo de Seguridad y Privacidad de la Información, siguiendo la metodología sugerida por el MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, el Departamento Administrativo de Función Pública y la Alta Consejería Distrital TIC con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

1.2 Responsable

El responsable de la Seguridad y Privacidad de la información es el Comité Institucional de Gestión y Desempeño-CIGD, creado mediante la Resolución 783 de 2018 y modificado por la Resolución 236 de 2018.

La Dirección de Tecnologías e Información coordinará el equipo técnico de la seguridad y privacidad de la información que direccione el CIGD.

1.3 Glosario[1]

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

Integridad: Propiedad de exactitud y completitud.

No repudio: El no repudio en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor en el envío de la información a través de una red. Tiene como objetivo certificar que la información o datos provengan realmente de la fuente que dice ser.

[1] Diciembre 2018. Consultoría "Guardianes de la Información". Alta Consejería Distrital de las Tics. http://ticbogota.gov.co/documentos/guardianes-la-informaci%C3%B3n

1.4 Siglas

- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **CSIRT:** Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
- **DTI:** Dirección de Tecnologías e Información.
- **ISO**: Organización Internacional de Estandarización.
- **MINTIC**: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **PETI:** Plan Estratégico de Tecnologías e Información.
- **PHVA:** Planear, Hacer, Verificar, Actuar.
- **SIC:** Superintendencia de Industria y Comercio.
- **TIC:** Tecnologías de la Información y las Comunicaciones.

2. ESTRUCTURA DEL PLAN

2.1 Introducción

La Secretaría Distrital de Gobierno mediante Resolución 783 de 2018, modificada por la Resolución 236 de 2018 creo el Comité Institucional de Gestión y Desempeño como órgano rector y articulador de las acciones y estrategias que se desarrollen para la correcta implementación, operación, seguimiento y fortalecimiento del Modelo Integrado de Planeación y Gestión MIPG, como marco de referencia del Sistema de Gestión Institucional.

Esta resolución, estableció las responsabilidades para cada una de las dimensiones y políticas de MIPG en la cual la Subsecretaría de Gestión Institucional quedó a cargo de las Políticas de Gobierno Digital y Seguridad digital de la dimensión de Gestión con Valores para Resultados. De acuerdo con esta responsabilidad, la Dirección de Tecnologías e Información define la política de Seguridad, privacidad de la Información y Seguridad digital, la cual se encuentra establecida en el manual de Gestión de Seguridad y el Plan Estratégico de Tecnología de Información, PETI, en el cual se fundamentan los propósitos y objetivos de este documento mediante la iniciativa estratégica 12, mejorar la prestación de los servicios tecnológicos y el proyecto 14, seguridad y privacidad de la información.

Igualmente se tienen en cuenta las directrices establecidas en materia de servicios ciudadanos detalladas en el Decreto 2106 de 2019 y el marco metodológico basado en las buenas prácticas de la norma ISO 27001, así como los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones, garantizando la evolución y permanencia de su implementación.

La implementación de este plan ayudará a identificar las responsabilidades en materia de seguridad y privacidad de la información, así como el desarrollo de las actividades necesarias para la identificación y

clasificación de los activos de información con el fin de aplicar los controles de confidencialidad, integridad y disponibilidad bajo un entorno de mejora continua dentro del ciclo PHVA.

En cuanto al estado actual de los controles establecidos en la norma ISO 27001:2013 (Anexo A), la Secretaría Distrital de Gobierno levantó en el año 2019 el autodiagnóstico definido por la Alta Consejería Distrital TIC obteniendo los siguientes resultados:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	19	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	33	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	8	100	INICIAL
A.9	CONTROL DE ACCESO	36	100	REPETIBLE
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	55	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	37	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	44	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	36	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	11	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	10	100	INICIAL
	PROMEDIO EVALUACIÓN DE CONTROLES	28	100	REPETIBLE

Ilustración 1 Autodiagnóstico 2019

Como se puede observar en el autodiagnóstico, es imperativo generar una estrategia para la concientización de la seguridad de la información en el año 2020, para lo cual en el primer trimestre se debe replantear la estrategia enfocada a todas las dependencias de la Entidad.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	29	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	42	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	23	100	REPETIBLE
A.9	CONTROL DE ACCESO	37	100	REPETIBLE
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	48	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	41	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	44	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	37	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	31	100	REPETIBLE
	PROMEDIO EVALUACIÓN DE CONTROLES	34	100	REPETIBLE

Ilustración 2 Autodiagnóstico 2020

Con respecto a la vigencia anterior se ve un leve aumento en la calificación promedio, eso se ve reflejado en el aumento de la evaluación algunos controles. Sin embargo, llegar al 100% de la calificación objetivo plantea un plan de trabajo a mediano plazo.

De acuerdo con el reporte FURAG, las recomendaciones en lo relacionado con la Seguridad y Privacidad de la información a tener en cuenta en el desarrollo de este plan son las siguientes:

- Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
- Elaborar el plan operacional de seguridad y privacidad de la información de la entidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
- Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.

Como una de las actividades principales a desarrollar para la implementación de este plan, es necesario contar con un perfil idóneo que cumpla las obligaciones de oficial de seguridad de la información para el manejo adecuado de la gestión de incidentes en materia de seguridad y privacidad de la información, para esto se debe concientizar a la Alta Dirección de la obligatoriedad e importancia de contar con este profesional.

2.2 Alcance

La Secretaría Distrital de Gobierno adoptará el Modelo de Seguridad y Privacidad de la Información -MSPI propuesto por MINTIC y basado en la norma ISO 27001:2013, mediante la ejecución de planes de trabajo independientes para los temas de seguridad y de privacidad de la información, por lo cual se segmentan las dependencias de la Entidad para la aplicación de los cronogramas de trabajo.

Las dependencias involucradas en cada grupo son:

PRIMER GRUPO	SEGUNDO GRUPO
• Dirección Tecnologías e Información • Oficina Asesora de Planeación • Dirección de Gestión del Talento Humano • Subsecretaría para la Gobernabilidad y Garantía de Derechos • Dirección de Derechos Humanos • Dirección de Convivencia y Diálogo Social • Subdirección de Asuntos Étnicos • Subdirección de Libertad Religiosa y de Conciencia	• Subsecretaría de Gestión Local • Dirección para la Gestión de Desarrollo Local • Dirección para la Gestión Policiva • Despacho • Oficina Asesora de Comunicaciones • Dirección para la Gestión Administrativa Especial de Policía • Dirección de Relaciones Políticas
TERCER GRUPO	**CUARTO GRUPO**
• Alcaldías Locales	• Oficina Asuntos Disciplinarios • Oficina Asesora de Control Interno

	• Dirección de Contratación • Dirección Jurídica • Subsecretaría de Gestión Institucional • Dirección Financiera • Dirección Administrativa

Tabla 1 Grupos de implementación del MPSI

2.3 Plan de Trabajo

A continuación, se detallan las actividades específicas que se deben realizar de manera general para toda la Entidad y luego de manera específica para cada uno de los grupos, siguiendo la metodología del ciclo PHVA en el cual se enmarca el Sistema de Gestión de la entidad.

En el primer cronograma detallado en el numeral 2.3.1, se definen las actividades correspondientes a la temática de seguridad de la información de manera general como el levantamiento de activos de hardware, software, personas etc., y otras específicas para cada uno de los grupos definidos en el alcance.

2.3.1 Detalle de actividades del plan de trabajo según alcance y vigencia

ETAPA	ACTIVIDADES	ALCANCE	Año 2020				Año 2021				Año 2022				Año 2023			
			Trimestre				Trimestre				Trimestre				Trimestre			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ACTIVIDADES TRANSVERSALES																		
PLANEAR	a) Diagnóstico con herramienta MSPI del MINTIC	Toda la Entidad																
	b) Autodiagnóstico con herramienta MINTIC de Gobierno Digital																	
	c) Generar indicadores de medición interna																	
	d) Verificación y planeación estratégica de uso y apropiación seguridad y privacidad de la información																	
	e) Solicitud auditorías internas																	
	f) Valoración activos de la información (Cronograma 2 - Levantamiento de Activos de Información)																	
	g) Planeación y solicitud de permisos para desarrollar pruebas de intrusión, pruebas phising, revisión seguridad de la información de la red y/o Ethical Hacking																	
HACER	a) Implementación estrategia de uso y apropiación seguridad y privacidad de la información	Toda la Entidad																
	b) Análisis de acceso físico a áreas críticas y sensibles																	
	c) Análisis de aspectos ambientales para áreas críticas																	
	d) Gestión de riesgos de seguridad del centro de datos																	
	e) Implementación pruebas de seguridad, según los permisos concedidos																	
	b) Identificar riesgos activos de información																	
	c) Análisis del riesgo activos de información																	
	d) Evaluación y tratamiento del riesgo activos de información																	
VERIFICAR	a) Verificación vigencia y reestructuración de plan de seguridad	Toda la Entidad																
	b) Revisión Política de seguridad y plan de manejo de su implementación																	
	c) Verificación compromiso de la Alta Dirección																	
	d) Revisión de indicadores de seguridad																	
ACTUAR	a) Plan de mejoramiento	Toda la Entidad																
	b) Revisión Plan Estratégico de Seguridad y Privacidad de la Información																	
ACTIVIDADES ESPECÍFICAS POR GRUPO																		

ETAPA	ACTIVIDADES	ALCANCE	Año 2020				Año 2021				Año 2022				Año 2023			
			Trimestre				Trimestre				Trimestre				Trimestre			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
(Nota: No se considera la etapa la etapa ya que se contempla en las actividades transversales)																		
HACER	a) Aplicación de la estrategia de uso y apropiación para la verificación de conocimientos internos de Seguridad de la Información b) Implementación plan de tratamiento de riesgos c) Pruebas de efectividad del MSPI propuesto por MinTIC	Grupo 1																
		Grupo 2																
		Grupo 3																
		Grupo 4																
VERIFICAR	a) Verificación de la estrategia de uso y apropiación b) Verificación del resultado de tratamiento de riesgos c) Definición de planes de mejoramiento d) Evaluación de indicadores de medición interna	Grupo 1																
		Grupo 2																
		Grupo 3																
		Grupo 4																
ACTUAR	a) Ejecución y seguimiento de Planes de mejoramiento para la mitigación de los riesgos. b) Retroalimentación con mejores prácticas de la documentación. c) Medición y ajuste de indicadores internos de la implementación de la estrategia.	Grupo 1																
		Grupo 2																
		Grupo 3																
		Grupo 4																

Tabla 2 cronograma plan de trabajo según alcance y vigencia

3. ELEMENTOS ESTRUCTURANTES

3.1 Metas

Para la vigencia 2021 se plantearon las siguientes metas

- Realizar el 100% de la valoración de riesgos de seguridad y privacidad de la información en el nivel central.
- Actualizar 9 políticas relacionadas con la seguridad y privacidad de la información (GESTION DE ACTIVOS, CONTROL DE ACCESO, NO REPUDIO, PRIVACIDAD Y CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN Y/O CONTINUIDAD DEL NEGOCIO, REGISTRO Y AUDITORÍA, GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL).

3.1.2 Indicadores

Indicadores	Variables	Fórmula
% de avance en la valoración de riesgos	1. # de riesgos con valoración 2. # de riesgos identificados	(# de riesgos con valoración / # de riesgos identificados)*100%
Políticas relacionadas con la seguridad y privacidad de la información actualizadas	Cantidad de políticas actualizadas	Cantidad de políticas actualizadas

3.2 Periodo de implementación

El plan se encuentra definido hasta la vigencia 2023 el cual contempla una revisión anual que puede implicar una posible reformulación de acuerdo con las nuevas directrices y normatividades distritales y nacionales. Inicialmente la ejecución del plan y el cumplimiento de las actividades se establecen para el año 2021.

3.3 Metodología de medición

Trimestralmente se hará un seguimiento para determinar el nivel de cumplimiento de plan.

4. DOCUMENTOS RELACIONADOS

4.1 Documentos internos

Código	Documento

GDI-TIC-M006	Manual De Política De Tecnología E Información (TI)
GDI-TIC-M004	Manual de Gestión de Seguridad
GDI-TIC-PL001	Plan Estratégico de Tecnología de Información (PETI)

4.2 Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
Ley 1341	2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnología e Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones	Toda la norma
CONPES 3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.	Toda la norma
Ley 1581	2012	Disposiciones generales para la protección de datos personales	Toda la norma
Decreto 1078	2015	Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)	Toda la norma
Decreto 1081	2015	"Decreto Reglamentario Único del Sector Presidencia de la República" (En especial Libro 2)	Toda la norma
Decreto 415	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.	Toda la norma
Resolución CDS 004	2017	Fortalecimiento Institucional en Materia de TIC, para Plan Estratégico de Tecnología y Sistemas de Información (PETI) y para la Gestión de Proyectos TIC	Toda la norma
CONPES 3854	2017	Política Nacional de Seguridad Digital	Toda la norma
Decreto 1499	2017	Modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.	Capítulo 2
CONPES 3920	2018	Política Nacional de Explotación de datos.	Toda la norma

Norma	Año	Epígrafe	Artículo(s)
Resolución 783	2018	Creación del Comité Institucional de Gestión y Desempeño	Toda la norma
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnología e Información y las Comunicaciones.	Toda la norma
Ley 1978	2019	Moderniza el sector de las Tecnología e Información y las Comunicaciones (TIC), distribuye competencias, crea un regulador único y dicta otras disposiciones.	Articulo 22
Directiva 002	2019	Simplificación de la interacción digital entre los ciudadanos y el estado.	Toda la norma
Decreto 2106	2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.	Toda la norma
Generales		Lineamientos del marco de referencia establecidos por MinTIC y que incluyen Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.	

4.3. Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Lineamientos PETI	2018	MINTIC	https://www.mintic.gov.co/gestionti/615/w3-article-5482.html?_noredirect=1
Ámbitos guardianes de la seguridad	2019	Alta Consejería Distrital de las TICS	http://ticbogota.gov.co/documentos/guardianes-la-informaci%C3%B3n