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
03	25 de mayo del 2021	Se ajusta el plan de seguridad de la información, de acuerdo con los siguientes ítems: ➢ Se actualiza los resultados del instrumento de Mintic vigencia 2021 ➢ Se actualiza cronograma de actividades vigencia 2021 ➢ Se ajusta la introducción ➢ Se adiciona capítulo del plan de trabajo, de acuerdo con la fase de implementación del MSPI
04	31 de enero 2022	Se realiza la actualización del plan de seguridad de para la vigencia 2022
05	30 de noviembre 2022	Se realiza la actualización del plan de seguridad de para la vigencia 2023
06	30 de enero de 2024	Se realiza la actualización del Plan de seguridad y Privacidad de la Información de para la vigencia 2024

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 Tecnologías e Información.	**Mario Alexander Ortiz Salgado** Proceso Gerencia de TIC Director de Tecnologías e Información **Angela Patricia Cabeza** Profesional analista de proceso de la OAP	**Carine Pening Gaviria** Líder del Macroproceso Gerencia de la Información Subsecretaría de Gestión Institucional Aprobado en sesión de comité CIGD del 30 de enero 2024 y publicado mediante caso en HOLA No. **14425**

1. INFORMACIÓN GENERAL

1.1 Propósito

Implementar y gestionar el Modelo de Seguridad y Privacidad de la Información, con el objetivo de garantizar la confiabilidad, disponibilidad e integridad de los activos de información de la Secretaria Distrital de Gobierno de Bogotá, de acuerdo con los lineamientos de MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, el Departamento Administrativo de Función Pública y la Alta Consejería Distrital TIC, en cumplimiento del marco normativo vigente y la Política Nacional de Seguridad Digital (CONPES 3995)

1.2 Responsable

Dirección de Tecnologías e Información.

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.

1.4 Siglas

- **BCP**: Plan de Continuidad del Negocio.
- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **ColCERT:** Grupo de Respuestas a Emergencias Cibernéticas en Colombia.
- **CSIRT:** Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
- **DRP:** Plan de Recuperación de desastres
- **DTI:** Dirección de Tecnologías e Información.
- **ISO**: Organización Internacional de Estandarización.

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

- **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.
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **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 y el responsable de la Seguridad y Privacidad de la información y el equipo asignado, el cual definen la Política de Seguridad, Privacidad de la Información y Seguridad Digital, la cual se encuentra establecida en el Manual de Gestión de Seguridad de la Información.

Igualmente se tienen en cuenta las directrices establecidas en las buenas prácticas de la norma ISO 27001:2013, ISO 27002:2013, así como los lineamientos que emite el Ministerio de Tecnologías de la Información y las Comunicaciones, garantizando la evolución y permanencia de su implementación y el marco normativo de la Política Nacional de Seguridad Digital (CONPES 3995).

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, realizó la actualización del instrumento de autodiagnóstico de MinTic en el año 2022 con corte de mayo, 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	40	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	29	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	51	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	35	100	REPETIBLE
A.9	CONTROL DE ACCESO	44	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	38	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	36	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	45	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	27	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	42,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		36	100	REPETIBLE

Ilustración 1 Autodiagnóstico 2021

De acuerdo con los resultados obtenidos en el resultado del autodiagnóstico se actualizó el plan de seguridad que se tenía aprobado y publicado para la vigencia 2021, en el cual se establecieron unas actividades, se ejecutaron y se reportaron sus avances ante el comité de gestión y desempeño.

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	31	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	51	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	39	100	REPETIBLE
A.9	CONTROL DE ACCESO	49	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	38	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	37	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	45	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	24	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	30	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		37	100	REPETIBLE

Ilustración 2 Autodiagnóstico 2022

Se realiza la actualización del autodiagnóstico a corte de septiembre de 2022, donde se ve reflejado en el aumento de la evaluación algunos controles. Con respecto a la vigencia anterior se ve un leve aumento en la calificación promedio, Sin embargo, llegar al 100% de la calificación objetivo plantea un plan de trabajo a corto y mediano plazo.

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	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	71	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	69	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	58	100	EFECTIVO
A.9	CONTROL DE ACCESO	51	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	38	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	37	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	50	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	26	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	30	100	REPETIBLE
	PROMEDIO EVALUACIÓN DE CONTROLES	**48**	**100**	EFECTIVO

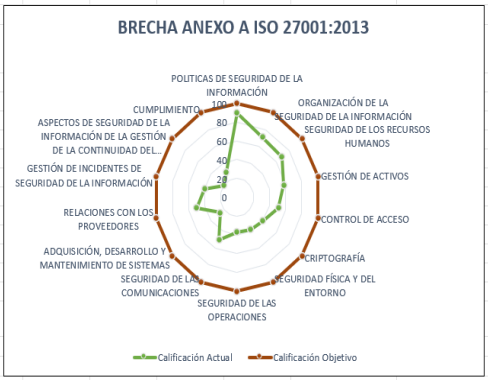

Ilustración 3 Autodiagnóstico 2023

Se realiza la actualización del autodiagnóstico a corte de septiembre de 2023, donde se ve reflejado en el aumento de la evaluación algunos controles. Con respecto a la vigencia anterior se ve un leve aumento en la calificación promedio, Sin embargo, llegar al 100% de la calificación objetivo plantea un plan de trabajo a corto y mediano plazo.

De acuerdo con el reporte FURAG, las recomendaciones en lo relacionado con la seguridad y privacidad de la información para 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.
- Realizar la identificación de riesgos de seguridad de la información de la entidad y aprobarlo mediante el Comité de Gestión y Desempeño Institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
- Realizar seguimiento al Plan 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.

Como una de las actividades principales a desarrollar para la implementación de este plan, se recomienda que la Secretaría Distrital de Gobierno cuente con un perfil idóneo que cumpla las obligaciones de oficial o Responsable 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 • Oficina Asuntos Disciplinarios • Oficina Asesora de Control Interno • Dirección de Contratación • Dirección Jurídica • Subsecretaría de Gestión Institucional • Dirección Financiera • Dirección Administrativa	• 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 • Alcaldías Locales	**CUARTO GRUPO** • 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

Tabla 1 Grupos de implementación del MPSI

2.3 Plan de Trabajo

La Secretaria de Gobierno de Bogotá, ha adoptado la Política de Seguridad de la Información, como parte del sistema integral de gestión, y para lograr su implementación y adopción ha creado un plan de seguridad de la información, con el objetivo de avanzar en la implementación orientado a dar cumplimiento a las directrices de Mintic - Ministerio de Tecnologías de Información y de las Comunicaciones, en cuanto a la adopción e implementación del Modelo de Seguridad y Privacidad de la Información.

Todas las acciones que se proponen en este plan están orientadas al fortalecimiento de la Política de Seguridad Digital como habilitador de dicha política. Así mismo, en atención tanto a lo especificado en el modelo de

seguridad y privacidad, como lo estipulado en el estándar NTC ISO 27001:2013, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad digital, como parte fundamental del modelo y en cumplimiento en lo dispuesto en la Política de Seguridad Digital.

A continuación, se presentan las fases de implementación del Modelo de Seguridad y Privacidad de la información para la Secretaría Distrital de Gobierno de Bogotá,

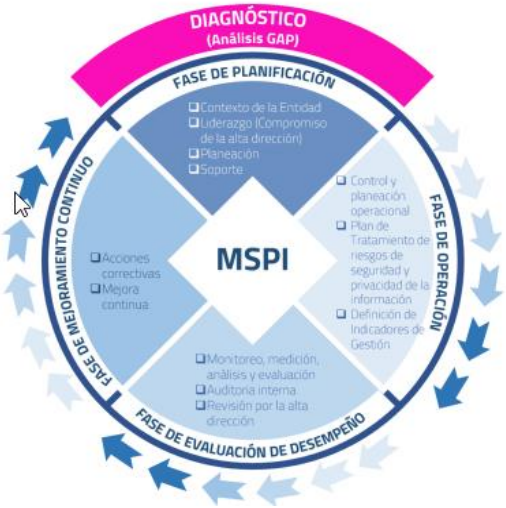

Ilustración 3 Ciclo del Modelo de Seguridad y Privacidad de la Información

Fuente: Anexo 1 Modelo de Seguridad y Privacidad de la información

2.3. Detalle de actividades del plan de trabajo según alcance y vigencia

DESCRIPCIÓN DEL PLAN						
FASE	**ACTIVIDAD**	**TAREA POR DESARROLLAR PARA EL PLAN**	**FECHA INICIO**	**FECHA FINALIZACIÓN**	**RESPONSABLE DEL CUMPLIMIENTO Y SEGUIMIENTO**	**SEGUIMIENTO**
P	Identificación de activos	Realizar la actualización del inventario de activos de información de las localidades	Enero 2024	Diciembre 2024	Responsable de Seguridad de la Información	Trimestral
P	Identificación de activos	Realizar la actualización del inventario de activos de información de nivel central	Julio 2024	Diciembre 2024	Responsable de Seguridad de la Información	Trimestral
V	Políticas específicas de seguridad de la información	Realizar seguimiento a las políticas específicas de acuerdo con el anexo A de la norma ISO 27001, lo cual se refleja en el Autodiagnóstico MSPI	Julio 2024	Diciembre 2024	Responsable de Seguridad de la Información	Trimestral

Tabla 2 cronograma plan de trabajo según alcance y vigencia

3. ELEMENTOS ESTRUCTURANTES

3.1 Metas

Para la vigencia 2024 se plantearon las siguientes metas

- Actualizar en 12 alcaldías la identificación, valoración y clasificación de activos
- Realizar la actualización del inventario de activos de información para 14 dependencias del Nivel Central
- Realizar el seguimiento a los lineamientos establecidos en 2 de las políticas específicas de seguridad de la información, de acuerdo con el anexo A de la ISO 27001:2013

3.1.2 Indicadores

Indicadores	Variables	Fórmula
Número de alcaldías con activos de información identificados, valorados y clasificados	Alcaldías con activos de información identificados, valorados y clasificados	Número de alcaldías con activos de información identificados, valorados y clasificados
Número de dependencias del Nivel Central con activos de información valorados, clasificados y actualizados	Dependencias del Nivel Central con activos de información valorados, clasificados y actualizados	Número de dependencias del Nivel Central con activos de información valorados, clasificados y actualizados
Número de políticas con seguimientos	Políticas específicas de seguridad de la información, de acuerdo con el anexo A de la ISO 27001:2013	Número de políticas con seguimientos

3.2 Periodo de implementación

El plan de seguridad y privacidad de la información se encuentra definido hasta la vigencia 2024, el cual contempla una revisión anual que puede implicar una posible reformulación de acuerdo con las nuevas directrices, normatividades distritales y nacionales y el resultado de seguimientos y auditorías internas. Inicialmente la ejecución del plan y el cumplimiento de las actividades se establecen para el año 2024.

3.3 Metodología de medición

Se hará un seguimiento para determinar el nivel de cumplimiento de plan dentro del reporte que se realiza al comité de gestión y desempeño.

4. DOCUMENTOS RELACIONADOS

4.1 Documentos internos

Código	Documento
GDI-TIC-M004	Manual de Gestión de Seguridad de la información
GDI-TIC-PL001	Plan Estratégico de las Tecnologías de la Información (PETI)
GDI-TIC-M007	Política para el tratamiento y protección de datos personales
GDI-TIC-P004	Identificación y Valoración de Activos de información
GDI-DTI-P006	Procedimiento Apertura de Datos
GDI-DTI-P009	Gestión de incidentes de seguridad de la información
GDI-DTI-P010	Levantamiento del catálogo de componentes de información
GDI-TIC-F020	Formato Acuerdo de confidencialidad
GDI-TIC-F026	Autorización para el tratamiento de datos personales sensibles
GDI-TIC-F027	Autorización y privacidad para el tratamiento de datos personales
GDI-TIC-F028	Reclamación para tratamiento de datos personales
GDI-TIC-F029	Formato de Cronograma de Apertura de datos
GDI-TIC-F032	Formato Identificación, valoración y clasificación de activos de información
GDI-TIC-F036	Informe de incidente de seguridad de la información
GDI-TIC-F041	Acuerdo de transferencia de información

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

Norma	Año	Epígrafe	Artículo(s)
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
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	

Norma	Año	Epígrafe	Artículo(s)
		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