

Control de cambios

Versión	Fecha	Descripción de la modificación
1	28 de diciembre de 2015	Primera versión del Manual
01	28 de noviembre de 2017	Se realiza ajuste de normalización como consecuencia de la entrada en vigor de la resolución 162 de 2017, que crea el proceso Gerencia de TIC como parte del mapa de procesos de la Entidad, y en cumplimiento de lo establecido en la circular 16 del 1 de noviembre de 2017. Los lineamientos operativos descritos en este documento corresponden íntegramente a los aprobados en la versión 1 de fecha 28 de diciembre de 2015, la cual fue aprobada por Juan Carlos Garzón Barreto como líder del proceso Planeación y Gerencia Estratégica, vigente en ese momento.
02	30 de julio de 2018	Segunda versión del Manual. Compilación del GDI-TIC-M004 Manual de Gestión de Seguridad de la Información y GDI-TIC-M001 Manual de Políticas de Uso y Seguridad de la Infraestructura Tecnológica, con su correspondiente actualización a la nueva estructura de la secretaria de Gobierno Derogación Resolución 177/2007 “Políticas para la Administración, Manejo y Uso del Recursos Tecnológico de la Secretaría Distrital de Gobierno de Bogotá”. Derogación Circular 15/2006 “Indicaciones para la asignación de los equipos de cómputo” Cambio de nombre a “Manual de Gestión de Seguridad”
03	21 de agosto de 2018	Tercera versión del Manual. Se revisa y corrige la redacción del enunciado de la política en el Numeral 6. Y se revisan en el numeral 10 las funciones para el rol Responsable de orientar la implementación de la Política de Seguridad
04	18 de noviembre de 2021	Se actualiza el objetivo general, los objetivos específicos de la política de seguridad de la información. Se actualiza el enunciado de la política general de seguridad de la información. Se incluyen los 13 dominios de políticas a implementar de acuerdo con el anexo A de la ISO 27001:2013.
05	08 de junio de 2022	Se actualiza el capítulo 7.1 en el cual se adicionan los lineamientos relacionados con la política de seguridad de la información del recurso humano, la política de cumplimiento de requisitos legales y contractuales en seguridad de la información, política de seguridad en las operaciones y la política de organización de la seguridad de la información. Se actualiza la tabla de roles y responsabilidades en el cual se adicionan actividades al grupo de seguridad de la información. Se actualiza el glosario, se incluyen términos y definiciones.
06	16 de septiembre de 2022	Se actualizan los capítulos 7.1.8, 7.1.9 y 7.1.11 en los cuales se completan los lineamientos en relación con las comunicaciones, los sistemas de información y a los incidentes de seguridad de la

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera “Copia no Controlada”. La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno”

		información; Se actualiza la tabla de roles y responsabilidades; Se actualiza el glosario. Se realizó presentación del manual al Comité de Gestión y Desempeño Institucional el día 16 de septiembre de 2022.
07	20 de diciembre de 2022	Se actualizan los capítulos 7.1.3, 7.1.4, 7.1.5, 7.1.10 y 7.1.11 en relación con las políticas específicas de gestión de activos, de control de acceso, de criptografía, en la relación con los Proveedores y en la gestión de incidentes de seguridad de la información.
08	28 de marzo de 2023	Se actualizan los capítulos 7.1.4.5, 7.1.8.3, 7.1.8.6, 7.1.10.1 en los que se complementan los lineamientos con relación a la responsabilidad de usuarios, acuerdo de transferencia de información, acuerdo de confidencialidad y seguridad de la información en relación con los proveedores; e inclusión en el Ítem 12 documentos relacionados del formato de transferencia de información aprobado por la OAP.
09	13 de septiembre de 2023	Se incluyen lineamientos de la política de seguridad física y del entorno, y se realizan modificaciones en los ítems 7.1.1.1, 7.1.1.2, 7.1.1.4, 7.1.1.6.2, 7.1.4.2, 7.1.7.5, 7.1.7.9, 7.1.8.4, 7.1.10.1, 7.1.12.1 para modificar grupo de seguridad de la información por Dirección de Tecnologías e Información o cambiar la sigla DTI por el nombre.
10	14 de agosto de 2024	Se incorpora el procedimiento de GDI-TIC-P012 de Borrado seguro y el instructivo GDI-TIC-IN021 para el transporte de medios físicos y se retiran otros documentos que ya no son de uso en la Entidad.
11	04 de diciembre de 2024	Se incorporan puntos de la Circular 004 de 2024 de la Oficina Consejería de Comunicaciones y Oficina Consejería TIC en el ítem 7.1.8.5. Uso de redes sociales.
12	19 de mayo de 2026	Se actualiza el Manual de Seguridad de la Información para incorporar los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC para el Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando su alineación con los requisitos de la norma ISO/IEC 27001:2022.

Método de Elaboración	Revisa	Aprueba
El documento se elabora de acuerdo con la normatividad que regula la materia, los profesionales de DTI realizan los ajustes correspondientes, a las mesas de trabajo realizadas con las diferentes dependencias y con el apoyo metodológico de la Oficina Asesora de Planeación	<p>Mario Alexander Ortiz Salgado Director de Tecnologías e Información</p> <p>Olga Milena Arias Aguirre Promotora de Mejora</p> <p>Nelson Enrique Arroyo Fontalvo Profesional OAP – Analista del proceso</p>	<p>Carine Pening Gaviria Subsecretaría de Gestión Institucional Líder de macroproceso</p>

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera “Copia no Controlada”. La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno”

TABLA DE CONTENIDO

1	PROPÓSITO	6
2	INTRODUCCIÓN	6
3	OBJETIVO	8
3.1	OBJETIVO GENERAL.....	8
3.2	OBJETIVOS ESPECIFICOS	8
4	ALCANCE	8
5	RESPONSABLES Y FUNCIONES	8
6	TÉRMINOS Y DEFINICIONES	12
7	SANCIONES POR INCUMPLIMIENTO	20
8	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	20
8.1	DIRECTRICES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	21
8.2	POLÍTICAS DE CONTROLES ORGANIZACIONALES (A.5).....	21
8.2.1	<i>Roles y Responsabilidades en la seguridad de la información (A.5.2)</i>	21
8.2.2	<i>Segregación de Deberes (A.5.3)</i>	22
8.2.3	<i>Contacto con las Autoridades (A.5.5)</i>	22
8.2.4	<i>Contacto con Grupos de Interés Especial (A.5.6)</i>	22
8.2.5	<i>Inteligencia de Amenazas (A.5.7)</i>	22
8.2.6	<i>Seguridad de la Información en la Gestión de Proyectos (A.5.8)</i>	22
8.2.7	<i>Inventario de Información y Otros Activos Asociados (A.5.9)</i>	23
8.2.8	<i>Uso Aceptable de la Información y Otros Activos Asociados (A.5.10)</i>	23
8.2.9	<i>Devolución de Activos (A.5.11)</i>	23
8.2.10	<i>Clasificación de la información (A.5.12)</i>	24
8.2.11	<i>Transferencia de Información (A.5.14)</i>	24
8.2.12	<i>Control de acceso (A.5.15)</i>	25
8.2.13	<i>Información de Autenticación (A.5.17)</i>	26
8.2.14	<i>Derechos de Acceso (A5.18)</i>	27
8.2.15	<i>Seguridad de la información en las relaciones con proveedores (A.5.19)</i>	28
8.2.16	<i>Abordar la Seguridad de la Información en los Acuerdos con los Proveedores (A.5.20)</i>	28
8.2.17	<i>Gestión de la Seguridad de la Información en la Cadena de Suministro de la Tecnología de la Información y las Telecomunicaciones (TIC) (A.5.21)</i>	29
8.2.18	<i>Seguimiento, Revisión y Gestión del Cambio de los Servicios de los Proveedores (A.5.22)</i>	29
8.2.19	<i>Planificación y Preparación de la Gestión de Incidentes de la Seguridad de la Información (A.5.24)</i> ...	29
8.2.20	<i>Evaluación y Decisión sobre Eventos de Seguridad de la Información (A.5.25)</i>	29
8.2.21	<i>Respuestas a Incidentes de Seguridad de la Información (A.5.26)</i>	30
8.2.22	<i>Aprender de los incidentes de seguridad de la información (A.5.27)</i>	30
8.2.23	<i>Recopilación de Evidencias (A.5.28)</i>	30

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera “Copia no Controlada”. La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno”



8.2.24	Preparación de las TIC para la continuidad de negocio (A.5.30)	30
8.2.25	Requisitos Legales, Reglamentarios y Contractuales (A.5.31)	31
8.2.26	Derechos de Propiedad Intelectual (A.5.32)	31
8.2.27	Procedimientos Operativos Documentados (A.5.37)	31
8.3	POLITICA CONTROLES A PERSONAS (A.6)	31
8.3.1	Selección, Términos y Condiciones de Empleo (A.6.1, A.6.2)	31
8.3.2	Conciencia de Seguridad de la Información, Educación y Formación (A.6.3)	32
8.3.3	Responsabilidades Después de la Terminación o el Cambio de Empleo (A.6.5)	32
8.3.4	Acuerdos de Confidencialidad o no Divulgación (A.6.6)	33
8.3.5	Trabajo inteligente (A.6.7)	33
8.3.6	Informes de Eventos de Seguridad de la Información (A.6.8)	34
8.4	POLÍTICA DE CONTROLES FÍSICOS (A.7)	35
8.4.1	Perímetros de Seguridad Física (A.7.1)	35
8.4.2	Entrada Física (A.7.2)	35
8.4.3	Asegurar Oficinas, Habitaciones e Instalaciones (A.7.3)	36
8.4.4	Monitoreo de la Seguridad Física (A.7.4)	36
8.4.5	Protección Contra Amenazas Físicas y Ambientales (A.7.5)	36
8.4.6	Trabajar en Áreas Seguras (A.7.6)	36
8.4.7	Escritorio y Pantalla Limpios (A.7.7)	37
8.4.8	Seguridad del Cableado (A.7.12)	37
8.4.9	Mantenimiento de Equipos (A.7.13)	37
8.5	POLÍTICAS DE CONTROLES TECNOLÓGICOS (A.8)	37
8.5.1	Dispositivos de Punto Final de Usuario (A.8.1)	37
8.5.2	Restricción de Acceso a la Información (A.8.3)	38
8.5.3	Acceso al Código Fuente (A.8.4)	39
8.5.4	Autenticación Segura (A.8.5)	39
8.5.5	Gestión de la Capacidad (A.8.6)	40
8.5.6	Protección Contra Malware (A.8.7)	40
8.5.7	Gestión de Vulnerabilidades Técnicas (A.8.8)	40
8.5.8	Gestión de la Configuración (A.8.9)	41
8.5.9	Eliminación de información (A.8.10)	41
8.5.10	Prevención de fugas de datos (A.8.12)	42
8.5.11	Copias de Seguridad de la Información (A.8.13)	42
8.5.12	Registro (A.8.15)	42
8.5.13	Sincronización de Reloj (A.8.17)	42
8.5.14	Uso de programas de utilidad privilegiados (A.8.18)	42
8.5.15	Instalación de Software en los Sistemas Operativos (A.8.19)	42
8.5.16	Seguridad de Redes (A.8.20)	43
8.5.17	Seguridad de los servicios de red (A.8.21)	43
8.5.18	Segregación de Redes (A.8.22)	43
8.5.19	Filtrado Web (A.8.23)	44
8.5.20	Uso de la Criptografía (A.8.24)	44
8.5.21	Ciclo de Vida de Desarrollo Seguro (A.8.25)	44
8.5.22	Requisitos de Seguridad de las Aplicaciones (A.8.26)	44
8.5.23	Arquitectura de Sistemas Seguros y Principios de Ingeniería (A.8.27)	45
8.5.24	Codificación Segura (A.8.28)	45
8.5.25	Pruebas de Seguridad en el Desarrollo y la Aceptación (A.8.29)	45

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno"



8.5.26	Desarrollo Externalizado (A.8.30)	45
8.5.27	Separación de Entornos de Desarrollo, Evidencia y Producción (A.8.31).....	45
8.5.28	Gestión del Cambio (A.8.32)	46
8.5.29	Información de las Pruebas (A.8.33).....	46
9	PERIODICIDAD.....	46
10	DOCUMENTOS RELACIONADOS.....	46
10.1	DOCUMENTOS INTERNOS	46
10.2	NORMATIVIDAD VIGENTE	48
10.3	DOCUMENTOS EXTERNOS.....	49

ÍNDICE DE ILUSTRACIONES

Ilustración 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información y de riesgo de seguridad digital	7
Ilustración 2 Ciclo de vida de las políticas TI. Creación Propia	9

ÍNDICE DE TABLAS

Tabla 2 Roles y Responsabilidades	12
Tabla 1 Política de Seguridad y Privacidad de la Información y Seguridad Digital.....	21

1 PROPÓSITO

La Secretaría Distrital de Gobierno, a través de la Dirección de Tecnologías e Información, establece el presente Manual de Seguridad y Privacidad de la Información con el fin de orientar la implementación, gestión y mejora continua de las prácticas de protección de la información y de gestión del riesgo de seguridad digital (ciberseguridad) en la Entidad apoyados con el Plan de Seguridad de la Información y el Plan de Tratamiento de Riesgos de Seguridad.

Este manual se formula en cumplimiento de los lineamientos definidos en el componente de Seguridad y Privacidad de la Información y Seguridad Digital de la Estrategia de Gobierno Digital, así como del Modelo Integrado de Planeación y Gestión – MIPG, conforme a lo dispuesto en:

- J Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC.
- J Decreto 1499 de 2017 – Implementación y actualización del MIPG.
- J Decreto 1008 de 2018 – Lineamientos de la política de Gobierno Digital.

En concordancia con estas disposiciones, la Entidad busca garantizar la confidencialidad, integridad y disponibilidad de la información, así como gestionar adecuadamente el riesgo asociado a los activos de información que soportan sus procesos misionales, administrativos y estratégicos. Con ello, se promueve un Estado más eficiente, transparente y participativo, fortaleciendo la confianza ciudadana y la continuidad de los servicios institucionales.

2 INTRODUCCIÓN

Hoy día, la información es el activo más valioso para las organizaciones sin importar su tamaño o su naturaleza y por ende existe la necesidad de brindar protección a la información ante los diferentes riesgos de seguridad de la información a los cuales está expuesta.

La información, en sus múltiples códigos y formas, así como los trámites y servicios que las Entidades del Estado proveen a los ciudadanos se consideran un bien público. La Secretaría Distrital de Gobierno en sus funciones de articular las autoridades distritales, garantizar la convivencia pacífica y el cumplimiento de la ley en el Distrito Capital, proteger los derechos y promover los deberes de los ciudadanos y buscar una ciudadanía activa y responsable, entre otras; registra, organiza y transforma datos personales y misionales en información que facilita la toma de decisiones para el cumplimiento de los objetivos de la Entidad y permite la publicación de datos abiertos e información que genere transparencia y valor público en entornos físicos y digitales. Esta información en conjunto con las tecnologías utilizadas para su gestión constituye los Activos de Información de la Entidad. En ese sentido, los activos de información que conforman los bienes y servicios que provee la Entidad son activos públicos y, por lo tanto, deben protegerse adecuadamente.

La protección y seguridad de los activos de información, parte del concepto fundante de seguridad de la información la cual se desarrolla mediante el principio rector de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos para el correcto manejo, gestión y control de la información, en todo su ciclo de vida, así como para garantizar sus propiedades fundamentales; la preservación de la confidencialidad, integridad y disponibilidad de la información que se complementan con otras propiedades como accesibilidad,

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera “Copia no Controlada”. La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno”

autenticidad, no repudio, entre otros, mediante el resguardo de datos y la protección frente a accesos no autorizados. Conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte tecnológico y legal de la Alta Dirección, y con el objetivo que estas sean una herramienta para la definición de los estándares y procesos internos de la Entidad, la Secretaría Distrital de Gobierno, a través de este documento define la política de seguridad y privacidad de la información y seguridad digital y reglamenta los lineamientos para la implementación, medición y seguimiento, los roles y responsables de su implementación y mejora continua, y la estrategia para su adopción mediante las pautas para su uso y apropiación.

La Secretaría Distrital de Gobierno, se compromete a implementar un modelo de gestión sistemático y cíclico de Seguridad y Privacidad de la Información y de riesgo de seguridad digital, en el cual la gestión del riesgo constituye un componente integral y transversal del Sistema de Gestión de Seguridad de la Información (SGSI). Este modelo, en concordancia con los lineamientos establecidos en la presente política, debe evidenciar de manera clara y documentada las siguientes fases:



Ilustración 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información y de riesgo de seguridad digital

3 OBJETIVO

3.1 OBJETIVO GENERAL

Establecer las políticas que regulen la seguridad de la información en la Secretaría Distrital de Gobierno y presentar en forma clara y coherente los elementos que conforman los lineamientos de seguridad de la información que deben conocer, acatar y cumplir todos los servidores públicos, contratistas, proveedores y partes interesadas que presten sus servicios o tengan algún tipo de relación con la Entidad, bajo el liderazgo de la Dirección de Tecnología e Información y el responsable de la seguridad de la información.

3.2 OBJETIVOS ESPECIFICOS

- J Implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros conforme a las necesidades de la Entidad, y a los requerimientos regulatorios.
- J Establecer lineamientos para sensibilizar a servidores públicos, contratistas, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información, en cuanto a la necesidad de salvaguardar los activos de información.
- J Establecer lineamientos para monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.
- J Establecer lineamientos para actualizar y proteger los activos de información identificados en la Secretaría Distrital de Gobierno.
- J Establecer lineamientos para permitir la continuidad de su operación frente a incidentes de seguridad.

4 ALCANCE

Los lineamientos contenidos en este Manual de Gestión de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Secretaría Distrital de Gobierno, a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos; para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el Comité de Gestión y desempeño Institucional.

Así mismo las alcaldías locales acogerán estas buenas prácticas de seguridad de la información, dentro de su entorno y gobierno tecnológico y de seguridad de la información.

5 RESPONSABLES Y FUNCIONES

La Alta Dirección de la Secretaría Distrital de Gobierno tiene como función aprobar esta política y propender su implementación y sus modificaciones, por esta razón deben crearse dentro de la organización, los siguientes roles

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno"

que garanticen su cumplimiento, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión.

La Ilustración 2 muestra la estructura requerida para el establecimiento de la política de seguridad y privacidad de la información y seguridad digital, y en la Tabla 2 se encuentran descritos los principales roles y funciones en lo referente al desarrollo de esta política:

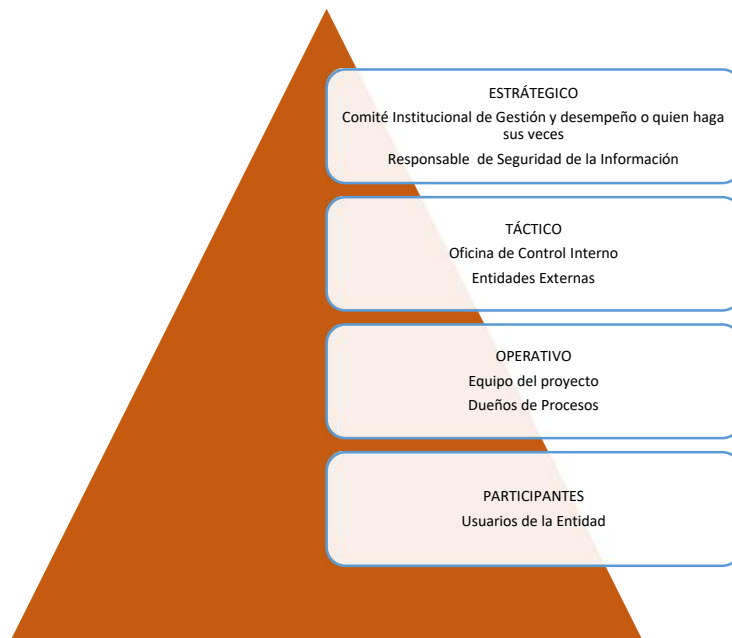


Ilustración 2 Ciclo de vida de las políticas TI. Creación Propia

ROL	PARTICIPANTES	FUNCIONES
Comité Institucional de Gestión y desempeño	Subsecretario(a) de Gestión Institucional, quien lo preside. Asesor del Despacho del Secretario de Gobierno. Director Jurídico Jefe de la Oficina Asesora de Planeación, quien actúa como secretario técnico del Comité Jefe de la Oficina Asesora de Comunicaciones Director de Tecnologías e Información Director de Contratación	<ul style="list-style-type: none"> *Fijar las acciones y estrategias orientadas al buen uso y aprovechamiento de las Tecnologías de Información y las Comunicaciones, así como la gestión y la protección de los activos de información de la Entidad. Uso y aprovechamiento de Tecnologías de Información y las Comunicaciones. Gestión y Protección de Activos de Información. *Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del modelo de privacidad y seguridad de la información. *Adelantar y promover acciones periódicas de autodiagnóstico para facilitar la valoración interna de la gestión.

ROL	PARTICIPANTES	FUNCIONES
	<p>Director de Gestión del Talento Humano Director Financiero Director Administrativo</p>	<p>*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. *Fijar acciones y estrategias orientadas al buen uso y aprovechamiento de las Tecnologías de Información y las Comunicaciones, así como a la protección de los activos de información de la Entidad.</p>
Oficial de seguridad de la información	Cercano a la Alta dirección (profesional especializado o contratista)	<p>*Establecer el gobierno de seguridad de la información de la Entidad. *Establecer la estrategia para la gestión de riesgos de seguridad de la información. *Seguir y controlar la estrategia TI que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información. *Desarrollar y gestionar el plan de seguridad de la información. *Establecer, desarrollar y gestionar la estrategia de incidentes de seguridad de la información. *Verificar el cumplimiento de las obligaciones legales y regulatorias relacionadas con la seguridad de la información. *Generar y monitorear el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.</p>
Profesionales de la DTI	Profesionales de la Dirección de Tecnología e Información y especialistas de la Mesa de servicios.	<p>*Ejecutar las acciones de Seguridad digital. *Realizar el acompañamiento en el levantamiento y actualización del inventario de activos de información de nivel central y de alcaldías locales. *Liderar y acompañar el proceso de gestión de incidentes de seguridad digital, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados, ayudando con las cuestiones disciplinarias y legales necesarias. *Coordinar y/o supervisar pruebas de vulnerabilidad sobre los diferentes recursos tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. *Velar por el mantenimiento y actualización de la documentación del proyecto, su custodia y protección.</p>

ROL	PARTICIPANTES	FUNCIONES
Oficina de Control Interno	Profesionales delegados del área	*Llevar las auditorías periódicas (mínimo anualmente) al Modelo de Seguridad y Privacidad de la Información de acuerdo con la normatividad vigente.
Entidades Externas	Consejería Distrital de TIC MINTIC, entre otros.	*Brindar asesoría técnica especializada a la Entidad .
Equipo del Proyecto	*Profesionales delegados de las áreas. *Equipo responsable del tratamiento de los datos personales y Profesionales de la Dirección de Tecnología e Información.	*Apoyar a la Dirección de Tecnologías e Información, de acuerdo con el cronograma establecido. *Coordinar la interacción con consultores externos. *Analizar el riesgo de los activos de información de la Secretaría Distrital de Gobierno y verificar la aplicación de las medidas de seguridad necesarias para la protección de esta. *Tomar las decisiones sobre las bases de datos personales a que hubiere lugar y direccionar las actividades de los encargados de los datos personales. *Generación, revisión, aprobación, seguimiento, apoyo y/o plan de mejora para el cambio de protocolo IPV4 a IPV6 *Autodiagnóstico del MSPI y seguridad digital *Apoyar con el desarrollo de la documentación de seguridad de la información. *Apoyar en las diversas actividades del MINTIC relacionadas.
Dueños del proceso	Persona nombrada que ejerce como responsable de un proceso de la organización y/o aplicación especializada relacionada	*Actúa como el "administrador del activo de información" para todos los aspectos de seguridad de la información relacionados con el procesamiento de datos dentro de este proceso particular de la organización. *Clasificar los activos de información de su proceso, de acuerdo con el grado de sensibilidad y criticidad de la misma, documentar y mantener actualizada la clasificación efectuada, y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.
Usuarios de la Entidad	*Toda persona con vínculo contractual con la Entidad *Personal outsourcing de terceros con contrato con la Entidad *Ciudadanos que requieren de los servicios de la Entidad	*Conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

Tabla 1 Roles y Responsabilidades

6 TÉRMINOS Y DEFINICIONES

- J **ACCESO REMOTO:** Es la posibilidad de acceder desde una ubicación lejana a una red o a un ecosistema digital de una organización; el acceso remoto seguro es una combinación de procesos o soluciones de seguridad que se han diseñado para evitar el acceso no autorizado a los activos digitales de una organización y la pérdida de datos confidenciales.
- J **ACTIVO DE INFORMACIÓN:** Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la Secretaría Distrital de Gobierno. En su sentido más amplio, estos hacen referencia a la información que se recibe, transforma y produce en la Secretaría Distrital de Gobierno en el cumplimiento de sus funciones.
- J **ACUERDO DE CONFIDENCIALIDAD:** Es el documento que suscriben los servidores públicos, contratistas, subcontratistas y pasantes-practicantes de la Secretaría Distrital de Gobierno, con el fin de afianzar su compromiso con la Entidad respecto del uso pertinente de los recursos informáticos y de la información que la Entidad dispone y que les entrega, o a la cual tiene acceso con ocasión al cumplimiento de sus funciones u obligaciones.
- J **ACUERDO DE INTERCAMBIO DE INFORMACIÓN:** Es un contrato por medio del cual las partes se comprometen a intercambiar información y a no revelar la información de carácter confidencial que les es suministrada, en el cual se comprometen a custodiar, asegurar y a eliminar cuando se concluyan los términos del acuerdo de intercambio de información.
- J **ACUERDO DE NIVELES DE SERVICIO (ANS):** Es un acuerdo documentado entre un proveedor de servicios de TI y un usuario. El Acuerdo de Nivel de Servicio - ANS describe un servicio de TI, documenta los objetivos de nivel de servicio y especifica las responsabilidades del proveedor de servicios de TI y del usuario. En este acuerdo, se establecen las métricas por las que se mide el servicio, así como las soluciones o penalizaciones en caso de que no se alcancen los niveles de servicio acordados.
- J **ALTA DISPONIBILIDAD:** Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente; es decir, el tiempo en el que no estará accesible. Este nivel de funcionamiento (o el tiempo máximo de caída) ha de ser acordado entre el proveedor y el cliente en el caso de un servicio, en el marco de un Acuerdo de Nivel de Servicio. Es una funcionalidad necesaria para garantizar los servicios esenciales o imprescindibles de una empresa, cuando esta se enfrenta a incidentes que puedan afectar a su funcionamiento normal o disponibilidad.
- J **AMBIENTE DE PRUEBA:** Es un sitio (servidores, URLs, computadores, etc.) donde se alojan las aplicaciones o servicios para que sean probadas (la mayoría de los usuarios aún no tiene acceso), previo a que sean publicados en ambiente de producción (donde todos los usuarios si tienen acceso).
- J **AMBIENTE DE DESARROLLO:** Es un sitio (servidores, URLs, computadores, etc.) que se usa para desarrollar o construir el software de un programa, aplicación o servicio tecnológico (generalmente se usan lenguajes de programación, librerías, frameworks, base de datos, entre otros).

- J **AMBIENTE DE PRODUCCIÓN:** El ambiente de producción se utiliza para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la Entidad.
- J **AUTENTICACIÓN:** Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico, etc.
- J **BACKUP:** Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. Los dispositivos más empleados para llevar a cabo la técnica de backup pueden ser discos duros, discos ópticos, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube. Es de suma importancia mantener actualizada la copia de seguridad, así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal. Además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.
- J **CADENA DE CUSTODIA:** Es un conjunto de medidas que deben tomarse para proteger la identidad e integridad de un elemento o muestra que puede ser fuente de prueba de un posible hecho delictivo para asegurar su adecuada validez procesal. La cadena de custodia incluye la ubicación y el movimiento de la evidencia física o digital desde que se descubrió o se movió de la escena del incidente hasta que se presentó ante el juez.¹
- J **CADENA DE SUMINISTRO O ABASTECIMIENTO:** Un sistema de gestión de la seguridad de la cadena de suministro combina prácticas tradicionales en la gestión de la cadena de suministro con medidas de seguridad, lo que le permite proteger su negocio de amenazas como la piratería, el terrorismo o el robo. Entre los aspectos importantes de la gestión de la seguridad se incluyen validar las credenciales de los proveedores, proteger la carga y asegurar el transporte de esta.
- J **CENTRO DE RESPALDO:** Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia. Las características de un centro de respaldo deben ser las siguientes:
- o Su localización debe ser totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal.
 - o El equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal.
 - o El equipamiento software debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

¹ <https://revistaseguridad360.com/destacados/la-cadena-de-custodia/>

- J **CMDB:** Es un repositorio centralizado que almacena y gestiona información sobre los elementos de configuración de una organización de TI y las relaciones entre ellos.
- J **CONFIDENCIALIDAD:** Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información; Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.
- J **CONTROL DE ACCESO:** Es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios de los sistemas, recursos o información.
- J **CRIPTOGRAFIA:** Es el proceso de convertir texto sin formato ordinario en texto ininteligible y viceversa. Es un método para almacenar y transmitir datos en una forma particular para que solo aquellos a quienes está destinado puedan leerlos y procesarlos.²
- J **CUSTODIO DE LA INFORMACIÓN:** Es el funcionario o contratista encargado de administrar el activo de información, aplicar las políticas, procedimientos y protocolos definidos por la Entidad y por el dueño del Activo de Información.
- J **DERECHO DE AUTOR:** “Son los derechos de los creadores sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos”. (OMPI, s.f.)
- J **DENEGACIÓN DE SERVICIO:** Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones. También llamado DoS.
- J **DESARROLLO SEGURO:** Es el uso de principios y/o buenas prácticas de seguridad de la información durante el ciclo de vida del software (SDLC), pudiendo ser adquirido o construido al interior de la Entidad.
- J **DISPONIBILIDAD:** Se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.
- J **DISPOSITIVOS MÓVILES:** También conocidos como computadora de bolsillo o computadora de mano, con capacidades de procesamiento, con conexión a Internet, con memoria y pantalla. Se dividen en: Portátiles, Teléfonos inteligentes y Tabletas.
- J **DOBLE FACTOR DE AUTENTICACIÓN (2FA):** método de seguridad de administración de identidad y acceso, que requiere dos formas de identificación para acceder a los recursos y los datos.³

² <https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/>

³ [https://www.microsoft.com/es-co/security/business/security-101/what-is-two-factor-authentication-2fa#:~:text=La%20autenticaci%C3%B3n%20en%20dos%20fases%20\(2FA\)%20es%20un%20m%C3%A9todo%20de,y%20sus%20redes%20m%C3%A1s%20vulnerables.](https://www.microsoft.com/es-co/security/business/security-101/what-is-two-factor-authentication-2fa#:~:text=La%20autenticaci%C3%B3n%20en%20dos%20fases%20(2FA)%20es%20un%20m%C3%A9todo%20de,y%20sus%20redes%20m%C3%A1s%20vulnerables.)

- J **DUEÑO DE LA INFORMACIÓN:** Es el Directivo de una dependencia específica, designado por la SDG, que tiene la responsabilidad de garantizar que el activo de información se clasifique adecuadamente, debe definir, revisar periódicamente las restricciones y niveles de acceso.
- J **ESCANEO DE VULNERABILIDADES:** Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.
- J **FIRMA DIGITAL:** es un proceso automatizado para la validación de la firma de un suscriptor basado en algoritmos y criptografía
- J **FIRMA ELECTRÓNICA:** se refiere a todos los métodos para firmar (o validar) un documento electrónico o identificar a una persona.
- J **FRAMEWORK:** es un marco de trabajo, librerías o estructura previa que se puede aprovechar para desarrollar un proyecto, que simplifica la elaboración de una tarea, ya que solo es necesario complementarlo de acuerdo con lo que se quiere realizar.
- J **GESTION DE CAMBIOS:** Es el proceso que reúne un conjunto de prácticas y procesos que ayudan al equipo a enfrentar las transformaciones que puedan ocurrir en la Entidad. Esto permite que la oficina o dependencia de TI sustituya tecnologías desactualizadas por soluciones más eficaces o actualizadas.
- J **GESTIÓN DE PROYECTOS:** Es administrar, planificar, coordinar, seguir y controlar todas las actividades y los recursos asignados para un proyecto de una forma que se pueda cumplir con el alcance en el tiempo establecido y con los costos presupuestados.
- J **GESTIÓN DE INCIDENTES:** Listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la Entidad. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.
- J **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL:** Actividades coordinadas para dirigir y controlar dentro de una organización el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- J **HARDWARE:** Son aquellos elementos físicos que hacen parte de los sistemas computacionales como los son CPU (procesador), memoria, monitor, teclados, impresoras, parlantes, etc.
- J **IMPACTO:** Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.
- J **IDS:** Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es una aplicación usada para detectar accesos no autorizados a un computador, sistema de información o a una

red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.

- J **INCIDENTE:** Cualquier evento que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la Entidad, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información. (ISO 27000)
- J **INFORMACIÓN PÚBLICA:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. 4
- J **INFORMACIÓN PÚBLICA RESERVADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley. 5
- J **INFORMACIÓN PÚBLICA CLASIFICADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias o los derechos particulares o privados consagrados en el artículo 18 de esta ley. 6
- J **INFRAESTRUCTURA CRÍTICA CIBERNÉTICA NACIONAL:** aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.
- J **INTEGRIDAD:** Se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios.
- J **IPS:** Del inglés Intrusion Prevention System; Es un software que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.
- J **ISO:** Del inglés *International Organization for Standardization; Organización Internacional de Estandarización.*
- J **LAN:** También llamada Red de Área Local, es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos de todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. Las Redes de Área Local pueden ser cableadas o no cableadas (también conocidas como

⁴ <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

⁵ <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

⁶ <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>

redes inalámbricas). Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivos.

- J **LINEAMIENTOS TI:** Son reglas que especifican una acción o respuesta que se debe seguir en una situación determinada. En sí, son especificaciones técnicas que tienen una función instrumental que responden a cómo se implementa una política. Pueden cambiar con frecuencia debido a que los procedimientos manuales, estructura organizacional, procesos del negocio y las tecnologías de la información que se mencionan cambian rápidamente.
- J **LOG:** Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio o salida de sesión, tiempo de actividad o conexiones, entre otros. Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización.
- J **MATRIZ RACI:** Es una herramienta de gestión de proyectos y procesos que se usa para definir claramente roles y responsabilidades en una actividad, proceso o proyecto.
- J **MEDIOS DE ALMACENAMIENTO:** Los medios de almacenamiento son dispositivos o soportes físicos o digitales utilizados para guardar, conservar y recuperar información de manera temporal o permanente. Su función principal es permitir que los datos —documentos, imágenes, videos, programas o registros— permanezcan disponibles incluso después de apagar un equipo o transferirlos entre sistemas. Entre ellos tenemos RAM, memoria caché, discos duros, unidades de estado sólido, memoria USB, Tarjetas SD, Discos ópticos (CD, DVD, Blu-Ray), Cintas magnéticas.
- J **MEJORES PRÁCTICAS:** Es una técnica o metodología que, a través de la experiencia y la investigación, ha demostrado llevar de forma fiable a un resultado deseado. Es un compromiso de utilizar todos los conocimientos y la tecnología a disposición de uno para asegurar el éxito.
- J **PERFIL:** Es la definición de un conjunto de funcionalidades o propiedades que se le pueden asignar a un usuario; la asociación de un usuario a un perfil le permite iniciar una sesión en un sistema, o acceder a ciertas funciones específicas de dicho perfil.
- J **PERIFÉRICOS:** Los periféricos son dispositivos externos o auxiliares que se conectan a un computador para ampliar sus funciones, permitir la interacción con el usuario o complementar el procesamiento de datos. Facilitan la entrada, salida y almacenamiento de información. Los periféricos pueden conectarse mediante puertos (USB, HDMI, VGA, etc.) o de forma inalámbrica (Bluetooth, Wi-Fi). Entre ellos tenemos periféricos de entrada, periféricos de salida, periféricos mixtos y periféricos de almacenamiento.
- J **PERIMETRO DE SEGURIDAD:** Es el conjunto de mecanismos y sistemas relativos al control del acceso físico de personas a las instalaciones, así como la detección y la prevención de intrusiones en la Entidad.⁷
- J **PHISHING:** Técnica o tipo de ataque en el que alguien suplanta a una Entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o por ejemplo información de la

⁷ <https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/>

tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

- J) **POLÍTICAS TI:** Son directrices u orientaciones que debe generar la DTI y que reflejan la intención de la alta dirección, con el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Son establecidas para que perduren a largo plazo y aplican a grupos grandes de áreas o personas dentro y, muchas veces, fuera de la organización (deben ser cumplidas por los contratistas y terceros que trabajan con la organización y que por sus funciones deben tener acceso a su información y a su infraestructura). Para efecto de este manual, solo serán llamadas políticas.
- J) **PLAN DE SEGURIDAD DE LA INFORMACION (PSI):** Es un documento que tiene por objetivo trazar y planificar la manera como la Entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
- J) **PRIVACIDAD:** Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de los actores.
- J) **PROPIEDAD INTELECTUAL:** “La propiedad intelectual (P.I.) se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. La legislación protege la P.I., por ejemplo, mediante las patentes, el derecho de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de P.I. procura fomentar un entorno propicio para que prosperen la creatividad y la innovación”. (OMPI, s.f.).
- J) **PROTECCIÓN DE DATOS PERSONALES:** Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por Entidades de naturaleza pública o privada.
- J) **PROVEEDOR:** Es la persona natural o jurídica que provee o suministra profesionalmente de un determinado bien o servicio a la Entidad por medio de un acuerdo contractual.
- J) **RECURSO TECNOLÓGICO:** Son todos los bienes tangibles e intangibles que posee la Entidad, que constituyen herramientas informáticas para el desarrollo de las labores diarias. Los recursos tecnológicos y la Información son de propiedad de la Secretaría Distrital de Gobierno y deben ser utilizados únicamente para propósitos legítimos de la Entidad. Se permite que los Usuarios utilicen estos Recursos para facilitarles el desempeño de sus tareas. El uso de estos Recursos es un privilegio que puede ser revocado en cualquier momento.
- J) **RIESGO:** Es el efecto de la incertidumbre sobre los objetivos de seguridad de la información.
- J) **RIESGO DE SEGURIDAD DIGITAL:** Está asociado con la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
- J) **SEGURIDAD DE LA INFORMACIÓN:** Es el conjunto de políticas, medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.

- J **SEGURIDAD DIGITAL:** Es la situación de normalidad y de tranquilidad en el entorno digital (cibespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- J **SERVIDOR PÚBLICO:** Se refiere a todos los empleados, contratistas, consultores o trabajadores temporales de la Secretaría Distrital de Gobierno.
- J **SENSIBILIZACIÓN:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- J **SGSI:** Un Sistema de Gestión de la seguridad de la Información -SGSI es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
- J **SOFTWARE:** Son aquellos elementos informáticos que permiten que las labores de procesamiento de Información sirvan como herramienta de productividad y gestión. Están conformados entre otros por: A) Sistemas operativos. B) Software de ofimática, c) Software de desarrollo, D) Software comercial, E) Software de comunicaciones.
- J **SPYWARE:** Es un programa maligno que recopila información de un ordenador y después la envía a una Entidad remota sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.
- J **TELETRABAJO:** Es la modalidad de trabajo inteligente que consiste en el desempeño de las actividades remuneradas o prestación de servicios a terceros, utilizando como soporte las tecnologías de la información y comunicación – TIC – para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- J **TERCERO O PROVEEDOR:** Es la persona natural o jurídica que provee o suministra profesionalmente de un determinado bien o servicio a la Entidad por medio de un acuerdo contractual.
- J **TRABAJO EN CASA:** Es la modalidad de trabajo inteligente la cual se aplica por razones apremiantes, urgentes y temporales. En efecto, los recientes hechos de salud pública han evidenciado la necesidad en el sector público de plantear, organizar y desarrollar las actividades laborales a través del trabajo a distancia, cuando se presenten diferentes circunstancias ocasionales, excepcionales, especiales o transitorias, privilegiando el uso de las tecnologías de la información y las comunicaciones.
- J **TRABAJO INTELIGENTE:** Es un proceso de innovación pública basado en un enfoque organizacional del ámbito laboral que busca mejorar la eficiencia y la eficacia en la producción de resultados a través de la combinación de flexibilidad, autonomía y colaboración, en paralelo con el mejoramiento de las

herramientas tecnológicas, el equilibrio entre la vida personal y laboral y los ambientes de trabajo de los colaboradores y una gestión basada en resultados (Circular 13 de 2021).

- J **TRANSMISIÓN DE INFORMACIÓN:** La transmisión de datos hace referencia al flujo constante de información inmediata, y es el elemento principal del modelo de software de la arquitectura basada en eventos. Las aplicaciones modernas pueden utilizarla para procesar, almacenar y analizar los datos.⁸
- J **USUARIO:** Se refiere a todos los servidores públicos y cualquier otra persona o Entidad que utilice los Recursos Tecnológicos de la Secretaría Distrital de Gobierno.
- J **VIRUS:** Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.
- J **VPN:** Es una tecnología de red que sirve para conectar una o más computadoras a una red privada utilizando como medio una red pública como internet.
- J **VLAN (Virtual Local Area Network):** Es una red local virtual que permite dividir una red física en varias redes lógicas independientes, aunque todos los dispositivos estén conectados al mismo switch o infraestructura.
- J **VULNERABILIDAD:** Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre, el fabricante del software o hardware lo solucionará publicando una actualización de seguridad del producto.

7 SANCIONES POR INCUMPLIMIENTO

La inobservancia e incumplimiento de los lineamientos de este documento podrá dar lugar según corresponda, a la iniciación de investigaciones y aplicación de sanciones de conformidad a la normativa de la Entidad, incluyendo las disposiciones legales que compete al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

8 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

NOMBRE DE LA POLÍTICA
Seguridad, Privacidad de la Información y Seguridad digital
ENUNCIADO
La Secretaria Distrital de Gobierno y su Alta Dirección se comprometen en el establecimiento, implementación, mantenimiento y mejora de la seguridad y privacidad de la información, mediante la definición de un modelo de gestión sistemático, adecuado a la gestión de activos, riesgos e incidentes en seguridad de la información, fomentando una cultura en seguridad y privacidad de la información en todos los niveles de la organización, con el fin de apoyar en el cumplimiento de los objetivos estratégicos y al propósito de la Entidad.

⁸ <https://www.redhat.com/es/topics/integration/what-is-streaming-data>

Tabla 2 Política de Seguridad y Privacidad de la Información y Seguridad Digital

8.1 DIRECTRICES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Para la implementación de la Política de Seguridad y privacidad de la Información y Seguridad digital a manera de lineamientos, directrices y prohibiciones se definen cuatro (04) categorías de políticas para la adopción de los controles relacionados con seguridad de la información y la seguridad digital, los cuales se construyen con base en los principios y servicios de seguridad de la información (integridad, confidencialidad, disponibilidad, autenticidad, no repudio, autorización y auditabilidad) y con las características particulares de la Secretaría Distrital de Gobierno, sus activos de información, sus procesos, los servicios de información que presta, los cuales deberán ser actualizados mínimo una vez al año. A continuación, se presentan los 04 dominios de control tanto técnicos como administrativos, establecidos en la norma ISO 27001:2022, que harán parte de la política general de seguridad de la información con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

8.2 POLÍTICAS DE CONTROLES ORGANIZACIONALES (A.5)

Establecer lineamientos que regulen la seguridad de la información en la Secretaría Distrital de Gobierno, con el fin de conservarla, salvaguardarla y protegerla, por esta razón todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad, deben conocer y dar cumplimiento a la Política organizacional de seguridad de la información.

8.2.1 Roles y Responsabilidades en la seguridad de la información (A.5.2)

- J La Entidad es la responsable de aprobar y designar al responsable de la Seguridad de la Información, el cual estará bajo la supervisión del funcionario a quien ellos deleguen. El responsable de la Seguridad de la información tendrá dentro de sus responsabilidades velar por el establecimiento del gobierno de seguridad de la información, gestión de riesgos de seguridad de la información, desarrollar y gestionar el plan de seguridad de la información y plan de tratamiento de riesgos de seguridad de la información y realizar la gestión sobre los incidentes de seguridad de la información de la Entidad.
- J La Dirección de Tecnologías e Información debe velar porque los dueños y custodios de los activos de información de las diferentes dependencias y Alcaldías Locales identifiquen y/o actualicen, se valoren y se clasifiquen los activos de información de acuerdo con el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de Información y el Formato GDI-TIC-F032 de Identificación, Valoración y Clasificación de Activos de Información.
- J La Dirección de Tecnologías e Información debe velar porque cada dependencia y Alcaldías Locales cuenten con un dueño y custodio del activo de información y que se encargue de garantizar la integridad, confidencialidad y disponibilidad según se requiera. Igualmente, esto debe ser debidamente documentado en el Formato GDI-TIC-F032 de Identificación, Valoración y Clasificación de Activos de Información.
- J La Dirección de Tecnologías e Información debe velar porque el dueño y el custodio de la información defina y documente los niveles de acceso a la información de la Entidad.
- J El director de la Dirección de Tecnologías e Información debe velar porque el personal encargado de la Seguridad informática cuente con las competencias técnicas necesarias para el manejo tecnológico de la ciberseguridad.
- J La Dirección de Tecnologías e Información con el apoyo de las demás dependencias de la Entidad debe velar porque se identifiquen y documenten los requisitos que se puedan ver afectados en materia de seguridad de la información, en las relaciones con los terceros que tengan acceso a la información de la Entidad.

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno"

8.2.2 Segregación de Deberes (A.5.3)

- J La Dirección de Tecnologías e Información debe velar porque las áreas diferencien los roles y perfiles para reducir las posibilidades de modificación no autorizada o no intencional o que se presente uso indebido de los activos de información de la Entidad.
- J Los dueños y custodios de la información con el apoyo de la Dirección de Tecnologías e Información deben validar periódicamente que ninguna persona pueda acceder o modificar activos de información sin autorización.

8.2.3 Contacto con las Autoridades (A.5.5)

- J La Dirección de Tecnologías e Información debe garantizar que se mantenga una comunicación permanente con las autoridades pertinentes para estar informados sobre las tendencias de amenazas en temas de seguridad de la información y ciberseguridad.
- J La Dirección de Tecnologías e Información de acuerdo con el procedimiento GDI-TIC-P009 Gestión de incidentes de seguridad de la información notificará a las autoridades competentes la materialización de un incidente de seguridad de la información.

8.2.4 Contacto con Grupos de Interés Especial (A.5.6)

- J La Dirección de Tecnologías e Información debe mantener contacto con grupos o foros profesionales especializados en temas de seguridad de la información.
- J La Dirección de Tecnologías e Información debe velar por mantener capacitación continua y estar actualizado en todo lo referente a temas de seguridad de la información.
- J La Dirección de Tecnologías e Información debe velar por generar una cultura institucional en seguridad de la información, mediante sensibilizaciones y capacitaciones periódicas.
- J La Dirección de Tecnologías e Información debe contar con alertas de ataques masivos a nivel mundial, avisos de emergencia y parches, que remedien vulnerabilidades que puedan ser explotadas por grupos criminales.
- J La Dirección de Tecnologías e Información debe contar con enlaces adecuados que permitan adquirir conocimiento sobre el tratamiento de un incidente de seguridad de la información.

8.2.5 Inteligencia de Amenazas (A.5.7)

- J El administrador de redes sociales o a quien delegue tendrá la obligación de validar las cuentas Oficiales en redes sociales de la Entidad, en caso de encontrar una suplantación reportará el incidente de seguridad de la información a través de la Mesa de Servicios.

8.2.6 Seguridad de la Información en la Gestión de Proyectos (A.5.8)

- J Todos los proyectos asociados a gestión de tecnología deben estar estructurados acorde al Procedimiento formulación, programación y seguimiento a los proyectos de inversión (PLE-PIN-P008).
- J Todos los terceros vinculados a la ejecución de proyectos de la Secretaría Distrital de Gobierno deben firmar el acuerdo de confidencialidad establecido para tal fin.
- J La Dirección de Tecnologías e Información es el responsable de identificar y evaluar los riesgos asociados a seguridad de la información. Estas actividades están involucradas en el GDI-TIC-PL003 Plan de Tratamiento de Riesgos de Seguridad de la Información.
- J La Dirección de Tecnologías e Información es el responsable de identificar, evaluar, gestionar (si aplica) y realizar seguimiento a los riesgos asociados a los proyectos que involucren tecnología teniendo en cuenta los requisitos de seguridad de la información.

8.2.7 Inventario de Información y Otros Activos Asociados (A.5.9)

- J La Secretaría Distrital de Gobierno, como propietaria de la información que se genera, procesa, almacena y transmite en su plataforma tecnológica o medios físicos, otorga la responsabilidad a los jefes de área y estos a los servidores públicos que considere sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma, por lo que se encuentran sujetos a auditorías por parte de las áreas competentes.
- J Las diferentes dependencias y alcaldías locales participarán de forma articulada en el proceso de identificación y clasificación de los activos de información acorde al GDI-TIC-PL002 Plan de Seguridad y Privacidad de la Información.
- J La creación de cuentas de redes sociales institucionales deberá ser aprobada previamente por parte de la Oficina Consejería Distrital de Comunicaciones y la Oficina Consejería Distrital de Tecnologías de la Información y las Comunicaciones -TIC, quienes evaluarán atributos estratégicos.
- J La Oficina Asesora de Comunicaciones deberá contar con un inventario actualizado de las cuentas de redes sociales institucionales y reportarlo periódicamente al grupo de seguridad de la información de la Dirección de Tecnologías e Información o quienes hagan sus veces. Dicho inventario deberá contemplar mínimo: nombre de la red social, nombre/usuario de la cuenta de la red social, URL de perfil, correo institucional asociado, objetivo de la cuenta, responsable de la gestión y datos de contacto.

8.2.8 Uso Aceptable de la Información y Otros Activos Asociados (A.5.10)

- J Los funcionarios, colaboradores y terceros deben utilizar los recursos tecnológicos de la Secretaría Distrital de Gobierno de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Entidad.
- J Los funcionarios, colaboradores y terceros no deben utilizar software no autorizado, ni copiar software licenciado de la Entidad para utilizarlo en computadores personales, y/o entregarlos a terceros.
- J Los funcionarios, colaboradores o terceros son responsables por la custodia de los medios de almacenamiento que le son asignados.
- J Los usuarios entienden y aceptan que la Secretaría Distrital de Gobierno puede utilizar procedimientos y recursos manuales o automáticos para monitorear la utilización de sus Recursos Tecnológicos.
- J La información que se publique por servidores públicos, contratistas y terceros por cualquier medio de internet, redes sociales como Twitter®, Facebook®, YouTube®, LinkedIn®, etc., se considera fuera del alcance del SGSI y, por lo tanto, su confiabilidad, integridad, disponibilidad, daños y perjuicios que puedan llegar a causar serán de completa responsabilidad de la persona que las haya generado.

8.2.9 Devolución de Activos (A.5.11)

- J Es responsabilidad de los funcionarios, colaboradores y terceros hacer entrega de los recursos tecnológicos que le fueron asignados al iniciar sus actividades con la Entidad, una vez sus labores con la Secretaría Distrital de Gobierno hayan finalizado, sin perjuicio de la responsabilidad administrativa, fiscal disciplinaria o penal, en que se pueda incurrir por cualquier daño o pérdida, bajo las mismas características técnicas que le fueron entregadas.
- J La Dirección de Tecnologías e Información y la Dirección Administrativa deben aplicar lineamientos para la disposición segura de dispositivos que almacenen información de la Secretaría Distrital de Gobierno, ya sea cuando son dados de baja o asignados a un nuevo usuario.

8.2.10 Clasificación de la información (A.5.12)

- J) Toda la información de la Secretaría Distrital de Gobierno se identifica, clasifica y se documenta de acuerdo con el procedimiento GDI-TIC-P004 Identificación y Valoración de Activos de información y aplicando el documento GDI-TIC-F032 Formato identificación, valoración y clasificación de activos de información, establecidos por la Dirección de Tecnologías e Información y/o TRD- GDI-GPD-F024 Formato Tabla de Retención Documental – TRD del grupo de Gestión Documental. Los custodios de los activos de información tipo información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario su reclasificación de acuerdo con el procedimiento. Estas actividades están involucradas en el GDI-TIC-PL002 Plan de Seguridad y Privacidad de la Información.
- J) La información física y digital de la Secretaría Distrital de Gobierno debe tener un periodo de almacenamiento de acuerdo Resolución 0228 del 31 de Mayo de 2018 - Por la cual se adopta la Tabla de Retención Documental de la Secretaría Distrital de Gobierno, Resolución 0269 del 25 de Junio de 2018 - Por la cual se adopta la Política de Gestión Documental de la Secretaría Distrital de Gobierno, Acuerdo 07 de 2018 - Por el cual se convalida la tabla de Retención Documental de la Secretaría Distrital de Gobierno.
- J) Los funcionarios, colaboradores y terceros deberán verificar que, en las impresoras, escáneres, fotocopiadoras u otros elementos y en las áreas adyacentes a éstas, no queden documentos clasificados como confidenciales o sensibles, para lo cual se recomienda que de manera inmediata sean recogidos con objeto de evitar su divulgación no autorizada.

8.2.11 Transferencia de Información (A.5.14)

- J) Los usuarios de la Entidad tienen prohibido la transferencia de información catalogada como restringida o confidencial a Entidades externas, sin previa autorización del jefe directo. Igualmente, deben realizar transferencia de información únicamente por los medios permitidos dispuestos por la Dirección de Tecnologías e Información - DTI.
- J) La Dirección de Tecnologías e Información debe establecer los lineamientos y los mecanismos de cifrado de información para la protección de esta en el momento de ser transferida o intercambiada con otras Entidades y establecerá los procedimientos y controles necesarios para el intercambio de información con el fin de proteger la confidencialidad e integridad.
- J) Los dueños de los activos de la información deben solicitar formalmente a la DTI asesoría sobre los mecanismos que se podrían utilizar para cada caso particular en el intercambio de información con otras Entidades. Adicionalmente, el área interesada en el intercambio de información deberá asesorarse jurídicamente para suscribir los acuerdos que sean necesarios para formalizar dicho intercambio de información Digital.
- J) Todo intercambio de información con otros usuarios y otras organizaciones a través del correo electrónico institucional y/o SharePoint queda en los registros de auditoría de la plataforma colaborativa Office 365, de manera que cada usuario asume la responsabilidad por la información que distribuya a través de este medio.
- J) La Dirección de Tecnologías e Información o quien haga sus veces, debe velar porque el intercambio de información de la Secretaría Distrital de Gobierno con Entidades externas se realice en cumplimiento de las Políticas de Seguridad de la Información y dentro del marco de interoperabilidad para Gobierno Digital, el acuerdo transferencia de información GDI-TIC-F041, donde los dueños o a quienes ellos deleguen dejen registro del tipo de información intercambiada, el emisor y receptor de esta y la fecha de entrega y recepción, previa autorización y entrega de la misma. Es de aclarar que este acuerdo de transferencia de información GDI-TIC-F041 aplica para los proveedores cuyo objeto contractual esté relacionado con transferencia de información y la socialización será responsabilidad del supervisor del contrato.

- J El único servicio de correo electrónico controlado y autorizado por la Secretaría Distrital de Gobierno es el asignado directamente por la Dirección de Tecnologías e Información (Suite de office 365), el cual cumple con todos los requerimientos técnicos, imagen corporativa y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso, el cual es personal e intransferible y debe dar cumplimiento de acuerdo con los lineamientos de uso aceptable de activos de información.
- J Los mensajes y la información contenida en los buzones de correo electrónico son propiedad de la Entidad y cada usuario, como responsable de su buzón, debe mantener únicamente los mensajes relacionados con el desarrollo de sus funciones.
- J Los usuarios de correo electrónico tienen prohibido el envío de correos o cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana o que atente contra la integridad de las personas o instituciones y resulten ofensivas para los servidores públicos de la Entidad y el personal provisto por terceras partes.
- J Es responsabilidad de cada usuario asegurar los destinatarios a los cuales va dirigida una comunicación. Si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.
- J El servicio de correo electrónico debe ser usado de manera ética, prudente, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen de la Entidad.
- J Es obligación del usuario realizar la activación de las repuestas automáticas en el servicio de correo de la Entidad, cuando su ausencia sea mayor a tres (3) días, igualmente, está deberá indicar quién es la persona asignada para cubrir su ausencia. Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato.
- J La Dirección de Tecnologías e Información genera y divulga boletines para el manejo de cuentas y grupos de correo electrónico.
- J La Dirección de Tecnologías e Información se reserva el derecho de filtrar los tipos de archivo que vengán anexos al correo electrónico, con el fin de evitar la propagación de software malicioso.
- J La Dirección de Tecnologías e Información debe generar campañas para concientizar a todos los colaboradores de la Entidad sobre el correcto uso del manejo de la Información a través del correo electrónico.
- J Está prohibida la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor.
- J Para todos los usuarios de la Entidad les está prohibido dar declaraciones a medios de comunicación sin el apoyo de la Oficina Asesora de Comunicaciones.
- J La Oficina Asesora de Comunicaciones implementará los controles para asegurar una adecuada protección de la información en el uso de mensajería instantánea y de redes sociales de la Entidad, por parte de los usuarios autorizados, de preferencia, empleados de carrera administrativa.

8.2.12 Control de acceso (A.5.15)

- J La Dirección de Tecnologías e Información, debe velar porque las redes de datos y los servicios de red se encuentren debidamente protegidos contra accesos no autorizados implementando controles de acceso lógico.
- J La conexión remota a la red de área local de la Secretaría Distrital de Gobierno se establece a través de una conexión VPN segura, para lo cual toda solicitud de creación, modificación, bloqueo o eliminación de usuarios de acceso a los servicios de red a través de VPN, se debe realizar mediante caso en la herramienta de gestión de servicios vigente en la Entidad y es responsabilidad de dichos usuarios autorizados, seguir los lineamientos de las políticas de seguridad de contraseña segura.

- J Todos los equipos (de escritorio y portátiles de propiedad de la Entidad) que se conecten a la red de la Secretaría Distrital de Gobierno de forma local, lo realizarán a través de la integración del equipo al dominio de la Entidad, de acuerdo con solicitud a la Mesa de Servicios.
- J La Dirección de Tecnologías e Información asegura que las redes inalámbricas de la Secretaría Distrital de Gobierno cuenten con métodos de autenticación que eviten accesos no autorizados y realizará el cambio de dicha contraseña con una frecuencia de mínimo dos (2) veces al año.
- J La Dirección de Tecnologías e Información garantiza que los equipos ajenos a la Secretaría Distrital de Gobierno no accedan a la red local de la Entidad, excepto cuando sean propiedad de:
 - o Los contratistas: para lo cual deben contar con el permiso debidamente justificado y autorizado por la Dirección de Tecnologías e Información.
 - o Otras Entidades que estén contemplados dentro del respectivo acto administrativo para el cumplimiento de su objetivo.
- J La Dirección de Tecnologías e Información debe velar por el correcto nombramiento de los equipos en el dominio, de acuerdo con el documento interno para dicho fin.

8.2.13 Información de Autenticación (A.5.17)

- J La Secretaría Distrital de Gobierno con el apoyo de la Dirección de Tecnologías e Información, hace entrega de los usuarios y contraseñas para el uso de los servicios tecnológicos a los cuales el usuario esté autorizado a ingresar, teniendo en cuenta su perfil y área para el desempeño de las funciones y actividades a su cargo. Una vez entregados no habrá opción de cambio, excepto por cuestiones jurídicas.
- J La asignación de un usuario tipo administrador local del equipo, debe ser asignado únicamente para los usuarios que lo requieran con previa autorización del líder del área y validación de la Dirección de Tecnologías e Información. En ningún caso el usuario podrá trabajar con el usuario general administrador local del equipo y en caso de encontrarse sin la respectiva autorización, el equipo será eliminado del dominio de la Entidad.
- J El personal provisto por terceras partes que posean acceso a la plataforma tecnológica y/o servicios tecnológicos de la Entidad debe acogerse a las políticas de seguridad de la información de la Entidad.
- J La Dirección de Tecnologías e Información con el apoyo de la Mesa de Servicios, garantiza que los usuarios, realicen el cambio de contraseña de acceso a los servicios de la Entidad, por lo menos cada 45 días calendario. Aplica para los sistemas de información que sincronizan con Directorio Activo.
- J Los contratistas cuando no tengan vínculo laboral vigente NO pueden acceder a los recursos de red en ninguna circunstancia, excepto cuando el jefe de la dependencia realice la solicitud expresa en la herramienta de gestión vigente.
- J La Dirección de Tecnologías e Información implementa políticas de seguridad que garantice de forma periódica el cambio de las contraseñas por parte de los usuarios para el ingreso a los servicios de red y que no sean visibles en texto claro.
- J Las contraseñas de acceso a servicios tecnológicos, sincronizados con Directorio Activo, deben cumplir con las siguientes características mínimas de complejidad:
 - o Tener mínimo diez (10) caracteres.
 - o Usar una combinación entre mayúsculas, minúsculas, números y caracteres especiales [!@#\$%^&*()@*_+?<>.,]
- J No se pueden repetir las últimas seis contraseñas utilizadas.
- J Es de obligatorio cumplimiento el uso del doble factor de autenticación (2FA).
- J Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicadas.

- J La dirección o dependencia receptora es responsable por toda contraseña entregada por un externo para el ingreso a un sistema de información por parte de usuarios de la Secretaría Distrital de Gobierno, y por tanto asume la responsabilidad de la custodia y administración de esta.
- J La contraseña es de uso personal e intransferible y, por lo tanto, los usuarios de la red de la Secretaría Distrital de Gobierno son responsables de las acciones que otros puedan hacer con ella, en las situaciones que la den a conocer a terceras personas.
- J En el caso de bloqueo de contraseña o expiración de la contraseña, el usuario no tendrá acceso a los servicios de red y tendrá que restablecerla a través de la aplicación dispuesta en la intranet Aranda Passrecovery y en caso de no poder reestablecer la contraseña contactarse con la Mesa de Servicios por los canales establecidos para ello y publicados en la Intranet.
- J En caso de que el usuario considere que su contraseña ha sido comprometida por terceros, debe comunicar el incidente a la Mesa de Servicios de la Secretaría Distrital de Gobierno y realizar el cambio de esta.
- J La Dirección de Tecnologías e Información es la responsable de realizar el seguimiento y control a los accesos de todos los sistemas de información (misional, de apoyo y estratégico) que actualmente lo soporten.
- J La Dirección de Tecnologías e Información de forma periódica realizará revisión a los usuarios de Directorio Activo para validar que se estén llevando a cabo los respectivos procesos de creación y depuración.

8.2.14 Derechos de Acceso (A5.18)

- J La Dirección de Tecnologías e Información; Mesa de Servicios apoya a los dueños de los activos de información para el debido control de acceso a la información.
- J Los directivos y/o alcaldes locales deberán solicitar los activos de información de software e información para su personal, por medio de la herramienta de gestión de servicios (HOLA) vigente en la Entidad. Si la persona está ingresando a la Entidad en la modalidad de contrato de prestación de servicios, se debe adjuntar la impresión de pantalla respectiva del SECOP o acta de inicio. Si la persona está ingresando en la modalidad de planta a la Entidad, se debe adjuntar la copia de resolución de nombramiento y/o memorando de ubicación en la Entidad.
- J La Dirección de Tecnologías e Información puede otorgar el acceso a los recursos de red mediante el uso de usuario y contraseña personal, de acuerdo con la autenticación que se administra con el directorio activo.
- J Con una periodicidad anual, la Dirección de Tecnologías e Información debe realizar depuración de los privilegios de acceso a las redes como medida de control de seguridad de la información.
- J La DTI debe asegurar que los derechos de acceso de todos los participantes del proyecto de construcción de software se deshabiliten de todos los aplicativos e infraestructura una vez concluyan todas las actividades programadas.
- J La Dirección de Tecnologías e Información debe establecer lineamientos para la revisión periódica de los accesos otorgados a los servidores públicos, contratistas y terceros, con el fin de validar que no se realicen acceso no permitidos dentro de las diferentes redes de la organización.
- J El acceso a Internet de los equipos de cómputo propiedad de contratistas o proveedores que estén dentro de la red de la Entidad, depende de su vínculo activo con la Entidad. Quienes no cuenten con usuario y contraseña solo pueden conectarse a la Wifi pública disponible.
- J La Oficina Asesora de Comunicaciones debe informar a la Dirección de Tecnologías e Información de la Secretaría Distrital de Gobierno, cuando haya cambio de administrador de las redes sociales, con el fin de realizar el debido acompañamiento y renovación de contraseñas de acceso.

8.2.15 Seguridad de la información en las relaciones con proveedores (A.5.19)

- J La Dirección de Tecnologías e Información debe generar un directorio actualizado de fabricantes y proveedores que puedan servir de apoyo en caso de materializarse vulnerabilidades que puedan ser mitigadas con la ayuda de estos.

8.2.16 Abordar la Seguridad de la Información en los Acuerdos con los Proveedores (A.5.20)

- J Los supervisores de contrato deberán cumplir lo señalado en el numeral “Acuerdos de Confidencialidad o no Divulgación” del presente manual.
- J Los supervisores de contrato, con el apoyo de la Dirección de Tecnologías e Información, deben garantizar el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) y de los requisitos de seguridad de la información por parte de las terceras partes o proveedores de servicios. Estos lineamientos serán divulgados a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos. En caso de presentarse incumplimientos, se aplicarán las sanciones establecidas en el contrato celebrado entre las partes.
- J Los supervisores de contratos establecen mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tenga acceso o servicios que sean provistos a colaboradores o terceros, cumplan con las políticas de seguridad de la información en cuanto a las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios, para lo cual en la Dirección de Tecnologías e Información, previa solicitud Caso HOLA se evalúan y aprueban los accesos a la información de la Entidad requeridos por terceras partes.
- J La Dirección de Tecnologías e Información apoya a los supervisores de contrato, en identificar, monitorear y mitigar los riesgos, mediante el plan de tratamiento de riesgos relacionados con el manejo de la información de la Secretaría Distrital e Gobierno a la cual tienen acceso los proveedores, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología de la Entidad.
- J Cuando el proveedor sea persona jurídica o cualesquiera formas asociativas derivadas de contratos de colaboración se debe contar con políticas, normas y estándares de seguridad de la información al interior de su organización, así mismo deberán dar cumplimiento a la legislación colombiana vigente, en cuanto a protección de datos personales (Ley 1581 de 2012), propiedad intelectual (Ley 23 de 1982) y las demás políticas de seguridad de la información de la Secretaría Distrital de Gobierno.
- J El proveedor debe dar a conocer las políticas de seguridad de la información, manuales, formatos y acuerdos de confidencialidad GDI-TIC-F020, establecidos por la Entidad, a sus trabajadores y en general a todo tercero con el cual genere vínculos con la entrega de información de la Secretaría Distrital de Gobierno.
- J Los proveedores deben adoptar los procedimientos para el acceso y divulgación, almacenamiento, generación de copias, transmisión, etiquetado y destrucción de la información electrónica y física a su cargo.
- J El uso de los activos de información de la Entidad por parte de los proveedores será exclusivo para el desarrollo de sus obligaciones contractuales; estos recursos no deben ser utilizados para actividades personales y cualquier uso inadecuado de estos recursos son asumidos bajo su responsabilidad y riesgo.
- J Los proveedores implantan los mecanismos de control necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información alojada en los recursos tecnológicos y los sistemas de información que se encuentran bajo su custodia.
- J Los proveedores no deben ejecutar programas o software, cuya instalación no esté autorizada, con el fin de evitar el ingreso de software malicioso o factores que eleven los niveles de riesgo frente a una eventual pérdida, alteración o divulgación de la información.
- J Los supervisores y/o apoyo a la supervisión deben verificar que todas las personas que ingresen a la Entidad por parte del proveedor tengan una autorización previa, de acuerdo con los procedimientos de control definidos para ese propósito.

8.2.17 Gestión de la Seguridad de la Información en la Cadena de Suministro de la Tecnología de la Información y las Telecomunicaciones (TIC) (A.5.21)

-) Los supervisores de contratos con terceros deben monitorear periódicamente los requisitos de seguridad de la información, administrar los cambios en el suministro de servicios por parte de los proveedores y monitorear la aparición de nuevos riesgos. Adicional a estos lineamientos, los proveedores deben cumplir con las siguientes normas de seguridad:
- Reportar los incidentes de seguridad que se puedan presentar a la Dirección de Tecnologías e Información.
 - Cifrar la información catalogada como Pública Confidencial y Pública Reservada que sea suministrada por la Secretaría Distrital de Gobierno.

8.2.18 Seguimiento, Revisión y Gestión del Cambio de los Servicios de los Proveedores (A.5.22)

-) Al finalizar la relación laboral o contractual, los servidores públicos o colaboradores administradores de las redes sociales institucionales deben entregar todas las credenciales de acceso que hayan gestionado. La entrega de credenciales de acceso debe ser efectuada de manera formal al jefe inmediato o supervisor de contrato y se deberá hacer el cambio de las claves de acceso.

8.2.19 Planificación y Preparación de la Gestión de Incidentes de la Seguridad de la Información (A.5.24)

-) La Secretaría Distrital de Gobierno establece como encargados de la Gestión de Incidentes de seguridad de la información a la Dirección de Tecnologías e Información, quien debe aplicar el procedimiento GDI-TIC-P009 Gestión de incidentes de seguridad de la información, teniendo en cuenta que la alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante las Entidades externas.
-) La Dirección de Tecnologías e Información cuenta con:
- Un directorio que contiene la información de contacto de cada una de las personas que conforman la Mesa de Servicios o quienes realicen sus funciones; los formatos necesarios para el reporte de un evento y la lista de chequeo de acciones que debe verificar ante un incidente de seguridad (esta última en el GDI-TIC-P009).
 - Un listado de puertos conocidos y de puertos utilizados que puedan ser usados para un ataque, el cual debe clasificarse como reservado, y solo podrán acceder a él las personas autorizadas.
 - Un diagrama de red para tener la ubicación rápida de los recursos existentes.
 - Una línea base de información de servidores (Nombre, IP, Aplicaciones, parches, usuarios configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada del incidente cuando este ocurra.

8.2.20 Evaluación y Decisión sobre Eventos de Seguridad de la Información (A.5.25)

-) La Mesa de Servicios debe validar si el evento reportado es o no un incidente de seguridad de la información, antes de escalarlo para su investigación al equipo de seguridad de la información, de acuerdo con la matriz de escalamiento vigente y antes de iniciar el procedimiento de incidentes de seguridad.
-) La Secretaría Distrital de Gobierno debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia.

- J La Secretaría Distrital de Gobierno debe propender por adquirir las herramientas apropiadas para atender y/o evitar los incidentes de seguridad de la información que pudieran presentarse.

8.2.21 Respuestas a Incidentes de Seguridad de la Información (A.5.26)

- J La Dirección de Tecnologías e Información, debe analizar los incidentes de seguridad de la información que le son reportados y activar el procedimiento GDI-TIC-P009 Gestión de incidentes cuando sea necesario, para dar respuesta a los incidentes de seguridad de la información en conjunto con la Mesa de Servicios. Así mismo, debe cerrar el incidente una vez sea tratado de manera exitosa. Para ello debe registrarse adecuadamente en el formato GDI-TIC-F036 Informe de incidentes de seguridad de la información.
- J La Dirección de Tecnologías e Información debe informar la existencia del incidente de seguridad de la información al personal interno que necesite saberlo.
- J Es responsabilidad de los servidores públicos, informar sobre posibles anomalías en su equipo de cómputo, ataques informáticos de los que sean víctimas, correos electrónicos sospechosos y/o cualquier incidente relacionado con seguridad digital. Estos casos deben ser registrados a través de la herramienta de gestión de Mesa de Servicios TI vigente en la Entidad, con el objeto de tomar las medidas de seguridad adecuadas.

8.2.22 Aprender de los incidentes de seguridad de la información (A.5.27)

- J La Dirección de Tecnologías e Información debe planificar, socializar y ejecutar periódicamente pruebas de ingeniería social, con el fin de poner a prueba los conocimientos sobre seguridad de la información y ciberseguridad de los servidores públicos, contratistas y terceros.

8.2.23 Recopilación de Evidencias (A.5.28)

- J La Dirección de Tecnologías e Información debe identificar, recolectar, adquirir y preservar las evidencias del incidente de seguridad de la información, de acuerdo con los diferentes tipos de medios y dispositivos utilizados en la Entidad.
- J La Dirección de Tecnologías e Información debe velar porque la recolección de evidencia tenga en cuenta la cadena de custodia, la seguridad del personal, los roles y responsabilidades del personal involucrado, la competencia del personal, y la documentación.

8.2.24 Preparación de las TIC para la continuidad de negocio (A.5.30)

- J La Dirección de Tecnologías e Información establecerá los requisitos necesarios de seguridad de la información para la continuidad de la operación y el plan de recuperación en caso de situaciones adversas.
- J Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan de recuperación, deberán estar incorporados y definidos en los Planes de contingencias.
- J La Dirección de Tecnologías e Información define el plan de contingencia tecnológico para mitigar los riesgos de disponibilidad en los recursos tecnológicos de la Secretaría Distrital de Gobierno.
- J La Dirección de Tecnologías e Información establecerá y ejecutará el plan de pruebas de forma periódica de acuerdo con el plan de Continuidad Tecnológica de la Secretaría Distrital de Gobierno.
- J La Dirección de Tecnologías e Información con el apoyo de las diferentes dependencias establecerá y ejecutará los análisis de impacto al negocio (BIA por sus siglas en inglés), por medio de los cuales se mitigará la indisponibilidad de los servicios tecnológicos críticos de la Secretaría Distrital de Gobierno

- J La Dirección de Tecnologías e Información y las Áreas interesadas diseñan las estrategias y tiempos de recuperación de la operación de los servicios tecnológicos críticos de la Secretaría Distrital de Gobierno.

8.2.25 Requisitos Legales, Reglamentarios y Contractuales (A.5.31)

- J La Secretaría Distrital de Gobierno respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación y documentación de acuerdo con el cumplimiento del Procedimiento para la identificación, actualización, monitoreo y evaluación de requisitos legales GJR-P002 aplicables para la Entidad, relacionada con la seguridad de la información.
- J La Secretaría Distrital de Gobierno con el apoyo del responsable de la protección de datos personales y de la Dirección Jurídica, establecerán los lineamientos para la protección de derechos de autor y propiedad intelectual de acuerdo con la Ley 23 de 1982, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.
- J La Dirección de Tecnologías e Información deberá garantizar que todo el software que se ejecute en los activos de información de la Secretaría Distrital de Gobierno debe estar protegido por la Ley 23 de 1982 - Derechos de autor y la Ley 603 de 2000 cumplimiento de licencias de software.
- J Los servidores públicos y contratistas deberán cumplir con las leyes de derechos de autor ley 23 de 1982 y acuerdos de licenciamiento de software Ley 603 de 2000; se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y la reproducción no autorizada es una violación a la ley.

8.2.26 Derechos de Propiedad Intelectual (A.5.32)

- J La DTI debe asegurar que los sistemas de información adquiridos y/o desarrollados por proveedores cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y/o los derechos de propiedad intelectual. En los casos de realizarse contratación de personal para desarrollo, se deberá incluir cláusulas de propiedad intelectual.

8.2.27 Procedimientos Operativos Documentados (A.5.37)

- J La Dirección de Tecnologías e Información mantendrá documentado un plan anual de mantenimiento de los activos de TI que garantice su normal operación contemplando mantenimientos preventivos y correctivos.
- J Todo proceso operativo que se realice por personal de la Dirección de Tecnologías e Información deberá ser documentado en alguno de los tipos documentales que para tal fin dispone la Entidad: Manuales, Procedimientos, Instructivos y Planes.
- J La Dirección de Tecnologías e Información mantendrá actualizada y a disposición de todos los usuarios que requieran las guías y/o procedimientos relacionados con la operación de los servicios de TI, publicados en la intranet.

8.3 POLÍTICA CONTROLES A PERSONAS (A.6)

8.3.1 Selección, Términos y Condiciones de Empleo (A.6.1, A.6.2)

- J La Secretaría Distrital de Gobierno con el apoyo de la Dirección de la Gestión del Talento Humano cuenta con el procedimiento de Vinculación a la Planta de Personal GCO-GTH-P001, la aplicación de los formatos Verificación y Certificación cumplimiento de requisitos mínimos GCO-GTH-F045 y la firma del formato del Acuerdo de Confidencialidad GDI-TIC-F020.

- J La Dirección de Contratación o el área encargada de adelantar el proceso de contratación de prestación de servicios, debe dar cumplimiento al Manual de Contratación GCO-GCI-M003, y las Instrucciones para la modalidad contratación directa GCO-GCI-IN007, de acuerdo con el perfil establecido en los estudios previos, mediante el Formato Estudios previos para contratación directa prestación de servicios profesionales / de apoyo a la gestión GCO-GCI-F011, Formato de idoneidad para contratos de prestación de servicios profesionales o de apoyo a la gestión GCO-GCI-F028, el Formato Lista de chequeo - Expediente contractual de contratos de prestación de servicios profesionales y de apoyo a la gestión GCO GCI F090 y el Formato del Acuerdo de Confidencialidad GDI-TIC-F020.
- J Todos los funcionarios, contratistas y colaboradores de la Secretaría Distrital de Gobierno deberán firmar como responsable de los activos de información el Formato traslado, de cambio responsable GCO-GCI-F142.
- J La Dirección de Contratación o el área encargada de adelantar el proceso de contratación de prestación de servicios y apoyo a la Gestión, debe dar cumplimiento al Manual de Contratación GCO-GCI-M003 conforme a las modificaciones, supervisión, certificaciones de cumplimiento y demás situaciones que se presenten en la ejecución del contrato.
- J La Dirección de Gestión del Talento Humano encargada de adelantar el proceso de contratación de los servidores públicos de planta, debe dar cumplimiento conforme al proceso de desvinculación, licencias, vacaciones o cambio de labores de los empleados de la Entidad llevando a cabo los procedimientos e instrucciones como son:
 - o Procedimiento para incapacidades y/o licencias médicas GCO-GTH-P002.
 - o Procedimiento para la reubicación de servidores públicos GCO-GTH-P006.
 - o Instrucciones para la provisión transitoria de empleos mediante el derecho preferencial a encargo GCO-GTH-IN001.
 - o Procedimiento identificación de peligros, evaluación y valoración de los riesgos en el SGSST - GCO-GTH-P003.
 - o Procedimiento para reporte e investigación de incidentes y accidentes de trabajo GCO-GTH-P005.
 - o Procedimiento del Desempeño Laboral de Servidores de Carrera Administrativa y en Periodo de Prueba GCO-GTH-P007.
 - o Procedimiento para el desarrollo de exámenes médicos ocupacionales GCO-GTH-P009.
 - o Procedimiento teletrabajo SDG GCO-GTH-P011.

8.3.2 Conciencia de Seguridad de la Información, Educación y Formación (A.6.3)

- J Los funcionarios y contratistas de la Secretaría Distrital de Gobierno deben realizar el curso de Seguridad de la Información y Ciberseguridad de la SDG alojado en <https://moodle.gobiernobogota.gov.co/>, mediante el cual se busca concientizar a los funcionarios y servidores de la Entidad.
- J El responsable de seguridad de la información o quien haga sus veces, debe realizar sensibilizaciones o capacitaciones a los funcionarios, colaboradores y terceros de la Entidad, de acuerdo con las políticas e instructivos existentes relacionados con el uso apropiado de redes y sistemas de información, en concordancia con los estándares de seguridad de la Entidad.

8.3.3 Responsabilidades Después de la Terminación o el Cambio de Empleo (A.6.5)

- J La Dirección de Contratación cuando aplique debe realizar el proceso de liquidación de los contratos previa solicitud del supervisor, dando cumplimiento al Manual de Contratación GCO-GCI-M003.

- J La Dirección de Talento Humano reportará por lo menos una vez al mes a la Dirección de Tecnologías e Información, la desvinculación o cambio de labores del personal de planta a través de memorando por medio del aplicativo Orfeo o correo electrónico institucional de la Secretaría Distrital de Gobierno.
- J El supervisor de contrato debe reportar de manera inmediata la desvinculación o cambio de labores de los contratistas o colaboradores, reportándolo a través de caso en la herramienta de la Mesa de Servicios de la Entidad.
- J Es responsabilidad del funcionario o colaborador realizar la entrega del cargo aplicando las Instrucciones para la Entrega de Puesto de Trabajo Servidor de Planta GCO-GTH-IN011 de la información a su cargo al respectivo jefe inmediato y dejarla en el SharePoint correspondiente a su dependencia, de ser necesario.

8.3.4 Acuerdos de Confidencialidad o no Divulgación (A.6.6)

- J La Dirección de Tecnologías e Información en acompañamiento del oficial de seguridad de la información, o quien haga sus veces, asesorados por la Dirección Jurídica y la Dirección de contratación definirán los formatos de Acuerdos de Confidencialidad GDI-TIC-F020 y/o Transferencia de Información GDI-TIC-F041 entre la Entidad y terceras partes incluyendo los compromisos adquiridos y las sanciones civiles o penales por el incumplimiento de dichos acuerdos. En estos documentos se incluye la prohibición de divulgar la información entregada por la Entidad a los terceros con quienes se establecen acuerdos y la destrucción de dicha información una vez cumpla su propósito, donde estos acuerdos deberán ser firmados al momento de iniciar el vínculo con la Entidad y reposará en el respectivo expediente contractual. Es de aclarar que el acuerdo de confidencialidad aplica para todos los servidores públicos (funcionarios y contratistas) y proveedores.
- J La Secretaría Distrital de Gobierno, con el apoyo del responsable de Seguridad de la Información, o quien haga sus veces, debe velar por el cumplimiento del acuerdo de confidencialidad GDI-TIC-F020 con las terceras partes con quienes se realice dicho intercambio.

8.3.5 Trabajo inteligente (A.6.7)

- J En las modalidades de trabajo inteligente con que cuenta Entidad; se pondrá a disposición los recursos tecnológicos que sean necesarios y que estén disponibles en pro de preservar la seguridad de la información, para llevar a cabo la realización de las funciones fuera de las instalaciones de la Entidad. Estas políticas deben ser conocidas y aplicadas por todos los funcionarios y contratistas que realicen las actividades laborales en las modalidades de trabajo inteligente y su objetivo es garantizar los lineamientos y medidas de soporte para proteger la información, accedida, procesada o almacenada.
- J Para el desarrollo de las actividades en las modalidades de trabajo inteligente se requiere de una conexión remota a la red de datos de la Secretaría Distrital de Gobierno, a través de una VPN (Red Privada Virtual) como requisito indispensable para garantizar la integridad, confidencialidad y disponibilidad en la transferencia de información.
- J Para los usuarios que requieran el uso del software VPN deberán realizar la solicitud de instalación a través de la mesa de servicio con un caso HOLA.
- J Para el establecimiento de la conexión remota el usuario debe tener en cuenta los siguientes aspectos:
 - o Evitar establecer conexiones desde redes inalámbricas desconocidas o que estén habilitadas sin seguridad, es decir, que no solicite claves de ingreso. El riesgo aparece cuando el punto de acceso está abierto intencionalmente con un propósito malicioso, para obtener información de forma indebida por parte de una persona no autorizada.
 - o Cambiar periódicamente las credenciales institucionales.
 - o Las credenciales asignadas para el establecimiento de la VPN son de uso personal e intransferible, por tanto, no se comparten o divulgan. Su uso inadecuado es responsabilidad exclusiva de cada usuario.

- J La Dirección de Gestión del Talento Humano y la Dirección de Tecnologías e Información identificará y autorizará a los servidores públicos que contarán con el esquema de las modalidades de trabajo inteligente en la Entidad.
- J Las modalidades de trabajo inteligente de la Entidad estarán autorizadas por el jefe inmediato ante la Dirección de Gestión de Talento Humano, mediante el formato GCO-GTH-F053 Aprobación del jefe para ingreso o renovación de teletrabajo. Luego se remite el formato GCO-GTH-F057 Validación condiciones tecnológicas para el teletrabajo, a cargo de la Dirección de Tecnologías e Información para validación de los recursos tecnológicos necesarios para el desarrollo de su labor.
- J La Dirección de Tecnologías e Información con el apoyo del jefe inmediato del servidor público que se encuentre en alguna de las modalidades de trabajo inteligente y según las funciones asignadas en el cargo, autorizaran los permisos de acceso, instalación de la VPN, sistemas de información y/o servicios de la Entidad que utilizará para la ejecución de sus labores.
- J Se debe garantizar a través de la conexión VPN, que los equipos de la Secretaría Distrital de Gobierno cumplan con los requisitos de seguridad mínimos establecidos de acuerdo con las políticas de seguridad de la información conforme a lo indicado en “protección contra malware” de la Norma ISO/IEC 27001:2022.
- J Se debe garantizar que los equipos de propiedad de la Entidad que se encuentren en algunas de las modalidades de trabajo inteligente estén restringidos del uso y/o instalación de programas utilitarios no autorizados por la Entidad.
- J Es obligación por parte de los funcionarios, contratistas y terceros que toda la información institucional generada deba almacenarse en los repositorios autorizados por la Entidad; con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información almacenada.
- J Los funcionarios, contratistas y terceros deben asegurarse de que los dispositivos que utilicen para conectarse a la red de la Entidad estén libres de vulnerabilidades de seguridad, correos sospechosos o cualquier incidente relacionado con la seguridad de la información. Ante cualquier señal de riesgo, deberán reportarlo de manera inmediata a la Mesa de Servicios mediante un caso en la herramienta de gestión, con el fin de activar las medidas de seguridad correspondientes. Asimismo, deben cumplir y aplicar los lineamientos establecidos para el uso de dispositivos móviles y las directrices relacionadas con la prevención de software malicioso.
- J Controles adicionales para el cumplimiento del presente lineamiento de las modalidades de trabajo inteligente:
 - Infraestructura:
 - o Se debe cambiar cada 45 días las claves de ingreso de acuerdo con lo definido en el lineamiento de gestión de acceso de la Entidad.
 - o Utilizar claves seguras.
 - o El personal de soporte debe utilizar canales de transmisión segura de entrega de claves.
 - Telecomunicaciones:
 - o Hacer uso de la VPN configurada y entregada por la Entidad, para establecer la conexión segura.
 - o La Dirección de Tecnologías e Información debe garantizar el uso de firewalls para supervisar, filtrar y monitorear el tráfico entrante y saliente de la Entidad.

8.3.6 Informes de Eventos de Seguridad de la Información (A.6.8)

- J La Secretaría Distrital de Gobierno debe promover entre los servidores públicos, colaboradores y personal provisto por terceras partes, el reporte de cualquier evento o incidentes de seguridad de la información del que se tenga conocimiento y sus medios de procesamiento, de almacenamiento de información (plataforma tecnológica, sistemas de información, los medios físicos de almacenamiento), y la pérdida o divulgación no

autorizada de información clasificada como de uso interno, reservada o clasificada, con la mayor prontitud posible, a través de la Mesa de Servicios o los canales dispuestos para dicho fin.

- J Los encargados de los activos de información deben reportar a la Dirección de Tecnologías e Información por medio la herramienta de gestión de servicios, los incidentes de seguridad de la información que identifiquen o que reconozcan su posibilidad de materialización.
- J La Dirección de Tecnologías e Información como apoyo a las demás áreas involucradas debe diligenciar el formato GDI-TIC-F036 Informe de incidentes de seguridad de la información, el cual servirá de soporte ante auditorías o revisiones de entes externos.
- J Todos los servidores públicos, colaboradores y terceros deben reportar las debilidades de seguridad de la información de las que tengan conocimiento, por los canales dispuestos por la Entidad (herramienta de gestión TI vigente en la Entidad, teléfonos y correo de la Mesa de Servicios). La Mesa de Servicios debe informar de los incidentes relevantes a la Dirección de Tecnologías e Información.

8.4 POLÍTICA DE CONTROLES FÍSICOS (A.7)

8.4.1 Perímetros de Seguridad Física (A.7.1)

- J La Secretaría Distrital de Gobierno y con el apoyo de las Alcaldías Locales, de la Dirección de Tecnologías e Información y la Dirección Administrativa deberán contar con perímetros de seguridad en las áreas y/o sedes donde se encuentren instalados los centros de procesamiento de la información, suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas de Información, servicios de conectividad y red de la Entidad, los cuales estarán protegidos frente a posibles fallas en el suministro de energía eléctrica, para asegurar la continuidad del servicio.
- J La Dirección de Tecnologías e Información, las Alcaldías Locales y la Dirección Administrativa son los responsables de velar por la protección del acceso a las zonas donde se ubica el cableado de energía eléctrica y de comunicaciones que transporta datos y brinda apoyo a los servicios de información de la Entidad.
- J Es responsabilidad de la Dirección Administrativa y Alcaldías Locales velar por el registro de ingreso o salida de los equipos portátiles, ya sean propios o de la Entidad, ante el personal de vigilancia o quien haga sus veces, de acuerdo con el procedimiento establecido para tal fin.

8.4.2 Entrada Física (A.7.2)

- J La Dirección de Tecnologías e Información y los administradores de red de las Localidades, deberán propender porque las instalaciones de procesamiento de información que manejan datos sensibles cuenten con controles de acceso que eviten el ingreso de personas no autorizadas.
- J La Subsecretaría de Gestión Institucional y los Alcaldes Locales deberán proporcionar los recursos necesarios; previa aprobación del ordenador del gasto, para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implementados en las instalaciones de nivel central y de las diferentes alcaldías locales. de acuerdo con las instalaciones que tengan a su cargo y la Dirección de Tecnología e Información con el apoyo de la Dirección Administrativa deberán identificar mejoras en los mecanismos implantados y, de ser necesario, implementar nuevos mecanismos, con el fin de proveer la seguridad física necesaria en las instalaciones de la Entidad.
- J Los ingresos y egresos de personal a las instalaciones de la Secretaría Distrital de Gobierno deben ser registrados; por consiguiente, los empleados, colaboradores y el personal provisto por terceras partes, deben cumplir completamente con los controles físicos implantados en la Entidad.

- J Los visitantes que requieran ingresar a las instalaciones de la Secretaría Distrital de Gobierno deberán realizar el registro en la recepción de la Entidad.
- J Es responsabilidad del visitante al momento de terminar su visita realizar el registro de salida en la recepción, con la entrega del sticker u otro elemento que se le dio al momento de su ingreso.
- J Los servidores públicos, contratistas y demás colaboradores deberán acreditar su vínculo con la Entidad por medio del carné (virtual o físico) que los identifica como tales mientras se encuentren en las instalaciones de la Entidad. En caso de pérdida del carné o tarjeta de acceso a las instalaciones, deberán reestablecer su contraseña y el carné físico reportarlo a la mayor brevedad a la Dirección de Gestión del Talento Humano.
- J Los servidores públicos, contratistas y demás colaboradores no deberán intentar ingresar a áreas a las cuales no tengan autorización.
- J Los proveedores deberán portar el sticker de identificación institucional en un lugar visible, asignado por la empresa de vigilancia, siempre que esté dentro de las instalaciones de la Entidad.

8.4.3 Asegurar Oficinas, Habitaciones e Instalaciones (A.7.3)

- J El director de Tecnologías e Información, los alcaldes locales, los Profesionales 222-24 (coordinadores) y Administradores de Red Local deberán velar mediante monitoreo por la efectividad de los controles de acceso físico, mecanismos de vigilancia y autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar el registro y supervisión de cada ingreso a las áreas restringidas.
- J La Dirección de Tecnologías e Información, los Profesionales 222-24 (coordinadores) y los administradores de red de las alcaldías locales deberán garantizar que se cuenta con sistemas de alarma y otros mecanismos de seguridad de acceso a su cargo. Estos sistemas deberán ser utilizados por los empleados autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos pueden ser transferidos a otros empleados de la Entidad.

8.4.4 Monitoreo de la Seguridad Física (A.7.4)

- J Las Alcaldías Locales y/o empresas de vigilancia, deberán almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la Entidad y controlarán el ingreso de los visitantes a las instalaciones de la Entidad. En los casos que la administración y custodia de los registros de control de acceso a las instalaciones físicas sea por parte de un tercero, cuando finalice su contrato deberá entregar dichos registros al supervisor del contrato.
- J Todos los usuarios de la Entidad deben seguir los procedimientos y planes de comunicaciones internas y externas.

8.4.5 Protección Contra Amenazas Físicas y Ambientales (A.7.5)

- J La Secretaría Distrital de Gobierno cuenta con el plan de prevención, preparación y respuesta ante emergencias, el cual presenta el análisis de vulnerabilidades y amenazas que podrían ocasionar una situación de emergencia e indica las acciones a seguir antes, durante y después de la misma, enfocado de manera prioritaria a salvar las vidas de los ocupantes de la edificación, mediante la capacitación y entrenamiento, que conduzcan a la adecuada preparación de los servidores y contratistas que laboran en las instalaciones: <http://gaia.gobiernobogota.gov.co/sig/subsistema-gesti%C3%B3n-de-seguridad-y-salud-en-el-trabajo-sgsst>

8.4.6 Trabajar en Áreas Seguras (A.7.6)

- J Los equipos de cómputo serán transportados con las medidas de seguridad apropiadas que garanticen su integridad física, de acuerdo con los contratos que tengan para dicho fin y este transporte deberá ser

coordinado y supervisado por el dueño del activo de información de acuerdo con lo establecido en el GDI-TIC-IN021 Instrucciones para el transporte de medios físicos que contienen información.

8.4.7 Escritorio y Pantalla Limpios (A.7.7)

- J Los funcionarios, colaboradores o terceros se deben asegurar de que, al momento de ausentarse del puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento confidenciales o privados, que son utilizados para el desempeño de sus actividades; los cuales deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación para que no sean accesibles por otras personas.
- J La Dirección de Tecnologías e Información restringe el uso de accesos directos o información sensible en el escritorio de los equipos de cómputo.

8.4.8 Seguridad del Cableado (A.7.12)

- J La Dirección de Tecnologías e Información, las Alcaldías Locales y la Dirección Administrativa son los responsables de velar por la protección del cableado de energía eléctrica y de comunicaciones que transporta datos y brinda apoyo a los servicios de información de la Entidad, y asegurar que las labores de mantenimiento de redes eléctricas y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

8.4.9 Mantenimiento de Equipos (A.7.13)

- J La Dirección de Tecnologías e Información y Alcaldías Locales deberán asegurar el correcto mantenimiento preventivo y correctivo de los recursos de la plataforma tecnológica de la Entidad, de acuerdo con el plan anual de mantenimiento.

8.5 POLÍTICAS DE CONTROLES TECNOLÓGICOS (A.8)

8.5.1 Dispositivos de Punto Final de Usuario (A.8.1)

- J Las siguientes políticas deben ser conocidas y aplicadas por todos los funcionarios, contratistas y terceros que utilicen dispositivos móviles para el desarrollo de las actividades de la Secretaría Distrital de Gobierno y su objetivo es garantizar la seguridad en uso de los dispositivos móviles de la Entidad.
- J La Dirección de Tecnologías e Información en conjunto con la aprobación de las Directivas de la Secretaría Distrital de Gobierno debe garantizar el diseño, validación e implementación de los respectivos controles de seguridad que se deben aplicar para el uso seguro de los dispositivos móviles.
- J Los funcionarios y contratistas que requieran conectar algún dispositivo móvil a la red de datos de la Secretaría Distrital de Gobierno deben realizar la solicitud de instalación de la VPN a la Mesa de Servicios, al igual que el supervisor del contrato de los terceros, con el objeto de no poner en riesgo la información Pública Reservada, información Pública Clasificada, Información Pública No Clasificada y/o Pública que éste contenga.
- J Los funcionarios y contratistas que requieran conectar algún dispositivo móvil a la red de datos en las instalaciones de la Secretaría Distrital de Gobierno podrán utilizar las redes inalámbricas con las que cuenta la Entidad dependiendo de su rol en la Entidad, los cuales son:
 - o Despacho (solo para el Secretario de Gobierno)
 - o Asesores (asesores y Directivos SDG)
 - o Funcionarios (funcionarios que poseen clave del dominio)
 - o Visitantes (personas que pueden conectarse a solo internet con el servicio proporcionado por la Entidad)Esto aplica para portátiles personales, portátiles institucionales, teléfonos y tabletas personales.
- J En caso de pérdida o robo de un dispositivo móvil de propiedad de la Secretaría Distrital de Gobierno que contenga información de la Secretaría Distrital de Gobierno, funcionarios y contratistas, tendrán que realizar la

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno"

respectiva denuncia ante la autoridad competente, luego debe generar un caso HOLA en la Mesa de Servicios y dar aviso al grupo de seguridad de la información o quien haga sus veces. Adicionalmente, deben informar mediante memorando a la Dirección Administrativa, haciendo un breve recuento de cómo sucedieron los hechos adjuntando la respectiva denuncia, con una cotización de un bien de iguales o mejores características del siniestrado.

- J En caso de pérdida o robo de un dispositivo móvil personal que contenga información de la Secretaría Distrital de Gobierno, funcionarios, contratistas y terceros deberán informar a la Dirección de Tecnologías e Información mediante un caso HOLA del incidente del robo y deberá solicitar el cambio de contraseña de los servicios que el usuario maneje.
- J La Dirección Administrativa, Alcaldías Locales y administradores de red local, con apoyo de la empresa de vigilancia tendrán la potestad de recoger y/o alertar sobre los equipos en el caso de que el responsable del equipo se encuentre ausente. El responsable del equipo deberá recogerlo y firmar el acta de compromiso de no volver a cometer la falta.
- J La Dirección Administrativa y Alcaldías Locales con el apoyo de la Dirección de Tecnologías e Información, mantendrán actualizado el inventario total de las estaciones de trabajo asignadas a los usuarios de la Entidad.
- J Sólo el personal autorizado por la Dirección de Tecnologías e Información y administradores de red local podrán realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la Entidad; las conexiones establecidas para este fin que utilizan los esquemas de seguridad establecidos, se podrán habilitar únicamente con una autorización y justificación previa del jefe de área, por medio de caso en la herramienta de gestión de servicios.
- J La Dirección Administrativa y los almacenistas de las localidades, con el apoyo de la Dirección de Tecnologías e Información y los administradores de red local, serán los únicos autorizados para realizar movimientos y asignaciones de equipos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier empleado o colaborador de los equipos tecnológicos de la Entidad.
- J Cuando se presente un incidente de hardware o software en el equipo de cómputo o servicio tecnológico propiedad de la Entidad, es obligación del usuario generar un caso en la Herramienta de gestión de servicios en donde se le atenderá o escalará al interior de la Entidad, con el fin de realizar la asistencia adecuada. El usuario no debe intentar solucionar el problema.
- J La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás servicios tecnológicos de la Entidad, será realizado por el personal de soporte técnico, administradores de red local o personal autorizado por la Dirección de Tecnologías e Información.

8.5.2 Restricción de Acceso a la Información (A.8.3)

- J La Dirección de Tecnologías e Información se reserva el derecho de autorizar o denegar el acceso a la red a aquellos dispositivos móviles externos que se conecten a cualquiera de las redes de la Entidad en caso de identificarse que exista alguna amenaza. Los equipos externos a la Entidad deben tener instalado un software antivirus o en su defecto el cliente VPN institucional, el cual tiene características de software antivirus. Adicionalmente, es responsabilidad de cada usuario que el equipo externo de su propiedad cuente con un sistema de autenticación, como un código de desbloqueo o una clave.
- J Para los equipos institucionales conectados al dominio gobiernobogota.gov.co el acceso de los usuarios a estos equipos se realizará utilizando la contraseña institucional del directorio activo que se entrega a cada usuario y que le permite a funcionarios y contratistas de prestación de servicios de la Entidad iniciar sesión y acceder a los servicios de correo electrónico y plataforma colaborativa.

- J Es responsabilidad de cada usuario de la Entidad velar porque los elementos que requieran protección especial se deben salvaguardar de manera que solo puedan ser accedidos por el personal pertinente en los tiempos necesarios.
- J Los equipos de cómputo de visitantes o terceros que se conecten o deseen conectarse a las redes de datos de la Entidad deberán cumplir con todos los requisitos o controles dispuestos por la Dirección de Tecnologías e Información para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- J Todos los usuarios de la red de la Secretaría Distrital de Gobierno deberán bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo por lo que, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, o en caso de que estén siendo transportados.
- J La Dirección de Tecnologías e Información con el apoyo de los líderes funcionales, debe velar porque los servicios brindados por las aplicaciones y sistemas de información sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles, perfiles y la matriz de control de acceso para cada sistema de información.
- J La Dirección de Tecnologías e Información debe proporcionar los controles que sean necesarios para la protección de la información y los recursos de la plataforma tecnológica, adoptando las medidas necesarias para evitar la divulgación, modificación o daño permanente.

8.5.3 Acceso al Código Fuente (A.8.4)

- J La DTI debe proteger el código fuente de los aplicativos construidos, de tal forma que no pueda ser descargado ni modificado por usuarios no autorizados.

8.5.4 Autenticación Segura (A.8.5)

- J Los equipos institucionales conectados a la red cableada se sincronizan permanentemente con el controlador de dominio, lo que le permite acceder a los recursos de red. Cuando los equipos del dominio estén durante un largo periodo de tiempo sin conexión con el controlador de dominio, se perderá la relación de confianza con el servidor de manera que el equipo cliente quedará fuera del dominio. El usuario deberá solicitar mediante un caso HOLA la inclusión del equipo en el dominio gobiernobogota.gov.co.
- J La Dirección de Tecnologías e Información debe establecer lineamientos para que el personal de seguridad digital emplee controles de acceso de mínimo doble factor de autenticación para la administración de las soluciones asignadas a su rol.
- J La Dirección de Tecnologías e Información establece mecanismos que permitan deshabilitar las funcionalidades de autocompletar en formularios de solicitud que requieran información sensible.
- J La Dirección de Tecnologías e Información asegura que no se permitan conexiones concurrentes con el mismo usuario a los sistemas de información, si así lo requiere el área funcional.
- J La Dirección de Tecnologías e Información establece el tiempo de duración de cada sesión activa de las aplicaciones, y preferiblemente cuando no se registre actividad, las finaliza automáticamente una vez ese tiempo sea superado.
- J Las cuentas de redes sociales de la Entidad estarán asociadas a cuentas de correo institucional únicamente.
- J Los responsables de las comunicaciones de la Entidad deberán velar porque las cuentas de las redes sociales institucionales tengan activado el doble factor de autenticación (2FA), para evitar posibles ataques o su pérdida y garantizar que, a través de este método, sea posible su recuperación.

8.5.5 Gestión de la Capacidad (A.8.6)

- J La Dirección de Tecnologías e Información debe realizar las actividades de seguimiento al uso de los servicios y recursos tecnológicos y en caso de ser necesario se informará a quien compete las alertas sobre la capacidad.
- J La Dirección de Tecnologías e Información debe tratar de que la capacidad de los recursos tecnológicos requerida para la prestación de los servicios tecnológicos y sistemas de información de la Entidad sea la adecuada, efectuando proyecciones de crecimiento sobre la capacidad futura.

8.5.6 Protección Contra Malware (A.8.7)

- J La Dirección de Tecnologías e Información debe promover la generación de una cultura de seguridad entre los servidores públicos, colaboradores y proveedores frente a los ataques de software malicioso, a través de actividades de socialización.
- J La Secretaría Distrital de Gobierno contará con herramientas tales como antivirus, antimalware, antispam y antispyware, las cuales deben estar licenciadas y con acceso a las últimas actualizaciones de bases de datos de firmas de amenazas, las cuales serán de instalación obligatoria en todos los equipos de cómputo, servidores de propiedad de la Entidad.
- J La Dirección de Tecnologías e Información, a través de la Mesa de Servicios y los administradores de red local, debe asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam y antimalware.
- J El acceso a la red de datos de la Secretaría Distrital de Gobierno de los equipos de cómputo propiedad de contratistas o proveedores que estén ubicados en las instalaciones de la Entidad deberían contar con software actualizado de antivirus, antispyware licenciado, y con las debidas actualizaciones de seguridad del sistema operativo e instalación de agente para VPN de acuerdo con su rol dentro de la Entidad.
- J La Dirección de Tecnologías e Información debe generar lineamientos para verificar la información relacionada con el software malicioso y asegurarse de emitir boletines de advertencia informativos a través de los canales oficiales, que ayuden a sensibilizar y concientizar a los funcionarios y contratistas sobre las falsas alarmas que se pueden generar, y las acciones a tomar en caso de que se presenten.
- J La Dirección de Tecnologías e Información debe velar porque ningún usuario pueda instalar o ejecutar programas que perjudiquen los equipos de cómputo, los sistemas operativos, programas internos, redes, servidores y aplicaciones, tales como virus informáticos, troyanos, Ransomware, spam, gusanos informáticos, malware, ataques Distribuidos de denegación de servicio DDoS, Red de equipos zombie, keylogger, entre otros.

8.5.7 Gestión de Vulnerabilidades Técnicas (A.8.8)

- J La Dirección de Tecnologías e Información debe coordinar, planificar, socializar y ejecutar periódicamente pruebas de vulnerabilidad y ethical hacking a los activos de sistemas de información y de infraestructura, con el objetivo de identificar posibles riesgos asociados a la arquitectura de seguridad digital de la Entidad, los cuales deben ser mitigados a través de planes de acción donde se generarán lineamientos y recomendaciones para atenuar dichas vulnerabilidades.
- J La Dirección de Tecnologías e Información debe realizar escaneos periódicos de su infraestructura tecnológica para detectar posibles vulnerabilidades.
- J La Dirección de Tecnologías e Información debe realizar consultas periódicas de fuentes de información que alerten sobre nuevas vulnerabilidades detectadas y ser socializadas por los canales oficiales.
- J La Dirección de Tecnologías e Información realizará las actualizaciones emitidas por los fabricantes de Software y Hardware a todas las estaciones de trabajo propiedad de la Entidad.

- J La Dirección de Tecnologías e Información asegura que la entrega de los ambientes de pruebas y producción estén libres de vulnerabilidades en sus sistemas operativos.

8.5.8 Gestión de la Configuración (A.8.9)

- J Ningún usuario efectuará cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente serán realizados por el personal autorizado por la Dirección de Tecnologías e Información.
- J La Dirección de Tecnologías e Información debe aplicar las configuraciones de seguridad digital para hardware y software, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.
- J La Dirección de Tecnologías e Información deber implementar una Base de datos de gestión de la Configuración CMDB para el control de la configuración de todo elemento tecnológico, para mantener el control de todo el software implementado y sus configuraciones.
- J La Dirección de Tecnologías e Información debe contemplar el análisis y monitoreo de la actualización de sistemas operativos debido a que los antiguos presentan vulnerabilidades de seguridad que son corregidas en nuevas versiones.
- J La Dirección de Tecnologías e Información debe autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Secretaría Distrital de Gobierno.
- J La Dirección de Tecnologías e Información, por medio de la Mesa de Servicios, es responsable de preparar los equipos de cómputo fijos y portátiles, propiedad de la Secretaría Distrital de Gobierno, para hacer entrega de estos a los funcionarios y colaboradores a quienes les sean asignados, ya sea por reasignación o disposición final, con el apoyo del área de Inventarios de la Dirección Administrativa; para el caso de las Alcaldías Locales serán responsables el administrador de red junto con el almacenista.
- J Los administradores de red local y la Mesa de Servicios son responsables de que todos los equipos de cómputo que hacen parte de la Red de la Secretaría Distrital de Gobierno estén en el dominio y de acuerdo con la nomenclatura establecida para tal fin. El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Secretaría Distrital de Gobierno serán reglamentados por la Dirección de Tecnologías e Información considerando las necesidades y condiciones de uso para el cumplimiento de sus obligaciones por parte de los funcionarios, colaboradores y terceros.
- J Toda nueva implementación deber contemplar desde la etapa de su planeación y desarrollo el uso de sistemas operativos en sus últimas versiones. No se deberán desarrollar proyectos tecnológicos en versiones obsoletas de sistemas operativos.

8.5.9 Eliminación de información (A.8.10)

- J La DTI debe aplicar el procedimiento de borrado seguro GDI-TIC-P012 previa solicitud en la herramienta de gestión de servicios (HOLA), para la destrucción de la información suministrada a los terceros, en situaciones como baja de elementos o traslado de elementos.
- J La Dirección Administrativa con el apoyo del grupo de Gestión Documental utilizan los medios necesarios para destruir o desechar correctamente la documentación física que se requiera, con el fin de evitar la reconstrucción de esta, acogiéndose al procedimiento establecido para tal fin en la TRD, una vez se ha cumplido su ciclo de almacenamiento:

https://gaia.gobiernobogota.gov.co/sites/default/files/sig/procedimientos/gdi-gpd-p007_v4.pdf

8.5.10 Prevención de fugas de datos (A.8.12)

- J La Dirección de Tecnologías e Información debe implementar soluciones de seguridad perimetral que permitan mantener la confidencialidad y disponibilidad de la información de la Entidad, como los son firewall o cortafuegos, IPS - software de prevención de intrusos, IDS - software de detección de intrusos, WAF - Firewall de aplicaciones web, entre otros.

8.5.11 Copias de Seguridad de la Información (A.8.13)

- J La Dirección de Tecnologías e Información debe asegurar la generación de copias de respaldo de Bases de Datos de los sistemas de información de uso oficial de la SDG, con la posibilidad de ser restauradas previa solicitud.
- J La Dirección de Tecnologías e Información no realizará copias de respaldo de la información almacenada directamente en los equipos de cómputo de los usuarios finales.
- J La Dirección de Tecnologías e Información solo se responsabiliza de las copias de respaldo en los espacios de almacenamiento de la plataforma colaborativa SharePoint como repositorio digital definido por gestión documental en el cual todos los usuarios deberán almacenar el producto de sus labores.
- J La Dirección de Tecnologías e Información se responsabiliza de la restauración de copias de respaldo del buzón de correo y OneDrive solo cuando estén avaladas por el respectivo jefe de dependencia y no se entregarán copias de respaldo a funcionarios o contratistas que ya no tengan vínculo con la Entidad.
- J Por ningún motivo se permite alojar en ningún recurso tecnológico de la Entidad, información catalogada como personal tal como: música, videos, fotografías, etc., que no sean insumo de sus actividades laborales.

8.5.12 Registro (A.8.15)

- J La Dirección de Tecnologías e Información debe establecer lineamientos para la generación y custodia de los eventos generados a través de dichas soluciones de seguridad digital.

8.5.13 Sincronización de Reloj (A.8.17)

- J La Dirección de Tecnologías e Información, debe garantizar que todos los sistemas de procesamiento de información, los equipos de cómputo y demás servicios tecnológicos que lo ameriten se sincronicen con una única fuente de referencia de tiempo.

8.5.14 Uso de programas de utilidad privilegiados (A.8.18)

- J La Dirección de Tecnologías e Información de establecer lineamientos para las restricciones y limitaciones para la instalación del software en los sistemas operativos de los equipos de cómputo de la Entidad, es decir que se establecerá formalmente una línea base la cual es el software que deberán contener los equipos de cómputo de la Entidad.
- J La Dirección de Tecnologías e Información restringe el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento de este.

8.5.15 Instalación de Software en los Sistemas Operativos (A.8.19)

- J La Dirección de Tecnologías e Información, debe designar responsables y establecer instructivos y guías para controlar la instalación de software en los sistemas operativos. Estas instalaciones deberán ser tenidas en cuenta para que les aplique el procedimiento de gestión cambios existente en la Entidad, cerciorándose de contar con

el soporte de los proveedores de dicho software y verificando que no afectará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el sistema operativo es actualizado.

- J La Dirección de Tecnologías e Información puede conceder accesos temporales y controlados a través de una conexión VPN a los fabricantes y terceros autorizados para realizar actualizaciones sobre los sistemas operativos, aplicaciones, librerías de programas o plataforma tecnológica, así como para realizar tareas de monitoreo de dichas plataformas que sean requeridas por la misma Dirección de Tecnologías e Información.
- J La Dirección de Tecnologías e Información debe evaluar en su interior los riesgos que implica realizar instalaciones de nuevas versiones de sistemas operativos, de acuerdo con el procedimiento de gestión de cambios existente en la Entidad. Se debe asegurar el correcto funcionamiento de los sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

8.5.16 Seguridad de Redes (A.8.20)

- J La Dirección de Tecnologías e Información debe establecer mediante una matriz RACI las responsabilidades y procedimientos para la gestión de equipos de redes.
- J La Dirección de Tecnologías e Información debe gestionar las configuraciones de red que comprenden el direccionamiento y enrutamiento, minimizando los riesgos de seguridad de la información asociados al transporte de información por medio de las redes de datos debidamente segmentadas (topología de red, topología de arquitectura de seguridad).
- J El acceso a equipos de cómputo o servidores de la Entidad desde ubicaciones fuera de la Entidad se realizará utilizando una comunicación VPN (Virtual Private Network), mediante el usuario y contraseña institucional y solamente a los equipos que el usuario tenga autorizados.
- J Los recursos de red de la Entidad son de uso estrictamente laboral, la Dirección de Tecnologías e Información podrá realizar controles o restricciones sobre el contenido que pueden consultar los usuarios, para preservar tanto la seguridad de estos como para optimizar el uso del recurso tecnológico.

8.5.17 Seguridad de los servicios de red (A.8.21)

- J La Dirección de Tecnologías e Información debe realizar de manera periódica el cambio de las claves de acceso a la red inalámbrica de la Entidad.
- J La Dirección de Tecnologías e Información debe solicitar al proveedor de los servicios de telecomunicaciones el cumplimiento de los ANS solicitados contractualmente y reportes del funcionamiento de los diferentes canales de conectividad.
- J La Dirección de Tecnologías e Información debe verificar en el momento de la conexión y cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo de los terceros en la red de datos de la Entidad, bajo las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia terceros.

8.5.18 Segregación de Redes (A.8.22)

- J La Dirección de Tecnologías e Información debe mantener las redes de datos segmentadas por VLAN, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para mejorar la seguridad de los usuarios de la Entidad (topología de red, topología de arquitectura de seguridad digital).
- J El acceso a las redes inalámbricas de la Entidad se da para los usuarios institucionales por medio de un portal cautivo en el cual los usuarios deberán autenticarse para acceder. Para el caso de los visitantes, podrán ingresar

solamente a internet por un tiempo limitado mediante la conexión a un portal de visitantes que no les permita acceso a recursos internos de la Entidad.

8.5.19 Filtrado Web (A.8.23)

- J El acceso a redes sociales está permitido para el personal de comunicaciones y/o prensa o que tengan dentro de sus funciones laborales la consulta de este tipo de contenidos.
- J La Dirección de Tecnologías e Información debe monitorear continuamente los canales que prestan el servicio de internet, en donde se establecen tiempos de navegación y páginas visitadas o sitios catalogados como peligrosos por parte de los usuarios, con el fin de prevenir y atender cualquier incidente de seguridad de la información que se presente tan pronto como sea posible, así como su correcto funcionamiento.
- J La Dirección de Tecnologías e Información debe restringir el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking o cualquier otra página que vaya en contra de la ética moral (Ley 1273 de 2009 – Ley de delitos informáticos), salvo que sean requeridas para investigaciones relacionadas con las funciones de la Entidad, con previa autorización del responsable de seguridad de la información o quien haga sus veces.

8.5.20 Uso de la Criptografía (A.8.24)

- J La Dirección de Tecnologías e Información es la única dependencia autorizada para el uso de herramientas para controles criptográficos.
- J Todo sistema de información web deberá ser publicado a los usuarios utilizando certificados digitales firmados por una Entidad de certificación (CA) confiable.
- J La Dirección de Tecnologías e Información debe propender porque se utilicen algoritmos de cifrado en los servicios de correo electrónico y VPN, utilizados internacionalmente.
- J La administración de certificados digitales estará a cargo de la Dirección de Tecnologías e Información para Nivel Central y por los administradores de red local para las alcaldías locales.

8.5.21 Ciclo de Vida de Desarrollo Seguro (A.8.25)

- J La Dirección de Tecnologías e Información incluye los lineamientos de desarrollo seguro y posteriormente asegura que estos se cumplan durante las pruebas realizadas sobre los desarrollos del software.
- J La Dirección de Tecnologías e Información identifica y mantiene actualizados todos los requerimientos para la infraestructura necesaria o requerida para los procesos de desarrollo de software, con el objetivo de mitigar los riesgos asociados a la seguridad de la información.
- J La Dirección de Tecnologías e Información establece las metodologías para el desarrollo de software seguro, que incluyan la definición de requerimientos de seguridad y las buenas prácticas, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

8.5.22 Requisitos de Seguridad de las Aplicaciones (A.8.26)

- J El líder del proceso o de la administración de los sistemas de información puede definir qué perfiles deben contener los sistemas de información a desarrollar y deberá aprobar la asignación de estos perfiles cuando sea necesario.

- J La Dirección de Tecnologías e Información y las áreas interesadas identifican los activos de información y los riesgos asociados para nuevos desarrollos o proyectos, con el fin de establecer los controles para el aseguramiento de la información.

8.5.23 Arquitectura de Sistemas Seguros y Principios de Ingeniería (A.8.27)

- J La Dirección de Tecnologías e Información asegura que todo sistema de información adquirido o desarrollado utilice un framework de desarrollo reconocido y soportado en el mercado.

8.5.24 Codificación Segura (A.8.28)

- J La DTI deberá asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros, así como opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
- J La DTI propende la no divulgación de información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión, fragmentos de código, directorios de los sistemas de información construidos o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- J La DTI evita incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales deberán estar cifrados.
- J La DTI debe asegurar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.
- J La DTI debe implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

8.5.25 Pruebas de Seguridad en el Desarrollo y la Aceptación (A.8.29)

- J Cuando se pretenda implementar un sistema de información ya sea propio o de terceros, este sea sometido a un análisis de vulnerabilidades, las cuales deberán ser remediadas antes del despliegue en producción por las áreas encargadas.

8.5.26 Desarrollo Externalizado (A.8.30)

- J La DTI debe asegurar que todos los productos de software entregados por un tercero cuenten con una validación de que todos los componentes del sistema y software estén protegidos de vulnerabilidades y código de software malicioso.
- J La DTI debe asegurar que, durante la ejecución del proyecto de desarrollo, el tercero involucrado cumpla con las políticas de seguridad de la información de la Entidad, de acuerdo con la confidencialidad, integridad y disponibilidad.

8.5.27 Separación de Entornos de Desarrollo, Evidencia y Producción (A.8.31)

- J La Dirección de Tecnologías e Información debe proporcionar los recursos necesarios para la implantación de controles que permitan la separación de ambientes de pruebas y producción, teniendo en cuenta

consideraciones como: controles para el intercambio de información entre los ambientes de pruebas y producción, la inexistencia de compiladores editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes. Estos ambientes se manejarán en infraestructuras separadas, sin acceso de la una con la otra.

- J Los ambientes de desarrollo y pruebas se utilizan para propósitos de implementación, modificación, ajuste o revisión de código fuente; además, se deberán utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo.

8.5.28 Gestión del Cambio (A.8.32)

- J La Dirección de Tecnologías e Información dispone de un procedimiento de implementación de cambios GDI-TIC-P011 para los servicios tecnológicos, infraestructura tecnológica y sistemas de información.
- J Los cambios en procesos y documentos de TI deben ser socializados y aprobados por la Dirección de Tecnologías e Información y será articulado por el gestor de mejora de la Dirección de Tecnologías e Información.
- J La Dirección de Tecnologías e Información, con el apoyo del área de comunicaciones, debe informar a la Entidad la fecha, hora y servicios tecnológicos y de sistemas de información que no estarán disponibles.
- J La Dirección de Tecnologías e Información debe definir y documentar las reglas para el paso a producción de software del ambiente de pruebas a producción para lo cual es necesario realizar las pruebas respectivas del software en ambientes separados, de acuerdo con los procedimientos establecidos en el proceso de gerencia TIC.
- J La DTI cuenta con un sistema de control de versiones para administrar los cambios en los sistemas de información, el cual permita almacenar los códigos fuente, archivos ejecutables y archivos de configuración con el principio del privilegio mínimo.
- J La Dirección de Tecnologías e Información debe garantizar que los cambios propuestos a los servicios tecnológicos, infraestructura o sistemas de información de la Entidad cumplan con los requisitos de Seguridad de la información.

8.5.29 Información de las Pruebas (A.8.33)

- J La Dirección de Tecnologías e Información debe proteger los datos de los ambientes de pruebas a los cuales tienen acceso los desarrolladores y terceros, asegurando que no se revele información confidencial, de acuerdo con el Manual de gestión de seguridad de la información (GDI-TIC-M004).

9 PERIODICIDAD

El presente manual de gestión de seguridad de la información y las políticas de seguridad aquí contenidas, serán examinados en las revisiones del Modelo de Seguridad y Privacidad de la Información por la alta Dirección, a través del Comité de Gestión y Desempeño Institucional, siempre que se produzcan cambios significativos o una vez al año, teniendo como referencia los lineamientos de MinTIC, Consejería Distrital de TIC, Función Pública, SIC y demás organismos regulatorios en temas de seguridad de la información.

10 DOCUMENTOS RELACIONADOS

10.1 Documentos Internos

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno"

Código	Documento
GDI-TIC-PL002	Plan de Seguridad y Privacidad de la Información
GDI-TIC-PL003	Plan de Tratamiento de Riesgos de Seguridad de la Información
GDI-TIC-P004	Identificación y Valoración de Activos de información
GDI-TIC-P009	Gestión de Incidentes de Seguridad de la información
GDI-TIC-P011	Implementación de cambios
GDI-TIC-P012	Procedimiento de Borrado Seguro
GDI-TIC_IN021	Instrucciones para el transporte de medios físicos
GDI-TIC-F020	Formato Acuerdo de confidencialidad
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	Formato de acuerdo de transferencia de información
GDI-GPD-F024	Formato Tabla de Retención Documental
GCO-GCI-M003	Manual de contratación
GCO-GCI-F011	Formato estudios previos para contratación directa prestación de servicios profesionales / de apoyo a la gestión
GCO-GCI-F028	Formato de idoneidad para contratos de prestación de servicios profesionales o de apoyo a la gestión
GCO-GCI-F090	Lista de chequeo - expediente único de contratos de prestación de servicios profesionales y de apoyo a la gestión
GCO-GCI-F142	Traslado cambio responsable y/o reintegro de bienes
GCO-GCI-IN007	Instrucciones para la modalidad contratación directa
GCO-GTH-P001	Vinculación a la Planta de Personal
GCO-GTH-P002	Procedimiento para incapacidades y/o licencias médicas
GCO-GTH-P003	Procedimiento identificación de peligros, evaluación y valoración de los riesgos en el SGSST
GCO-GTH-P005	Reporte e investigación de incidentes y accidentes de trabajo
GCO-GTH-P006	Procedimiento para la reubicación de servidores públicos
GCO-GTH-P007	Procedimiento de Evaluación del Desempeño Laboral de Servidores de Carrera Administrativa y en Periodo de Prueba
GCO-GTH-P009	Procedimiento para el desarrollo de exámenes médicos ocupacionales
GCO-GTH-P011	Procedimiento teletrabajo SDG

Código	Documento
GCO-GTH-F045	Verificación y certificación cumplimiento de requisitos mínimos
GCO-GTH-IN001	Instrucciones para la provisión transitoria de empleos mediante el derecho preferencial a encargo.
GCO-GTH-IN011	Instrucciones para la Entrega de Puesto de Trabajo Servidor de Planta
GJR-P002	Procedimiento para la identificación, actualización, monitoreo y evaluación de requisitos legales
PLE-PIN-P008	Procedimiento formulación, programación y seguimiento a los proyectos de inversión
GDI-TIC- F043	Indicadores de Seguridad de la Información

10.2 Normatividad Vigente

Norma	Año	Epígrafe	Artículo(s)
Circular 004	2024	Buenas prácticas para el uso de correos electrónicos institucionales en la creación y gestión de cuentas de redes Sociales	Oficina consejería distrital de tecnologías de la Información y las comunicaciones – TIC y oficina consejería Distrital de comunicaciones
Norma ISO/IEC 27001	2022	Sistema de Gestión de Seguridad de la Información	https://www.iso.org/es/contents/data/standard/08/84/88435.html
Norma ISO/IEC 27032	2023	Ciberseguridad: Directrices para la seguridad en Internet	https://www.iso.org/es/contents/data/standard/07/60/76070.html
Decreto 767	2022	Política Gobierno Digital	https://www.mintic.gov.co/portal/715/articles-210461_recurso_1.pdf
COBIT	2019	Objetivos de Control para la Información y Tecnologías Relacionadas	https://www.isaca.org/resources/cobit
Decreto 1499	2017	MIPG	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433
Conpes 3854	2016	Ciberseguridad Colombia	https://colaboracion.dnp.gov.co/cdt/conpes/econ%C3%B3micos/3854.pdf
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector TIC	https://normograma.mintic.gov.co/mintic/compilacion/decreto_unico_sector_tic.html
Decreto 1081	2015	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República	Decreto 1081 de 2015 Sector Presidencia de la República - Gestor Normativo - Función Pública

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera “Copia no Controlada”. La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno”

Norma	Año	Epígrafe	Artículo(s)
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 Tecnologías de la Información y las Comunicaciones	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902
Decreto 1377	2013	Reglamentar parcialmente la Ley 1581 de 2012	Decreto 1377 de 2013 - Gestor Normativo - Función Pública
Ley 1581	2012	Ley de Protección de Datos Personales	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
Ley 734	2002	Código Disciplinario Único	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4589
Ley 1952	2019	Modifica Ley 734 de 2002	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=90324#0
Ley 80	1993	Estatuto General de la Contratación Pública	32 numeral 3
Ley 23	1982	Sobre derechos de autor	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3431
Ley 603	2000	Por la cual se modifica el artículo 47 de la Ley 222 de 1995	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=13960

10.3 Documentos Externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información	2025	MINTIC	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf
MIPG- FURAG		DNP	https://www1.funcionpublica.gov.co/web/mipg/medicion_desempeno

Nota: Por responsabilidad ambiental no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en el aplicativo MATIZ de la Secretaría Distrital de Gobierno"

Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 7	2025	DAFP	https://www.funcionpublica.gov.co/documents/d/guest/2025-09-11_guia_gestion_integral_riesgo_v7?download=true
Marco de Referencia Arquitectura Empresarial	2023	MINTIC	https://mintic.gov.co/arquitecturaempresarial/630/articles-204807_recurso_2.pdf
Política Gobierno Digital		MINTIC	https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/
Manual Gobierno en Línea	2023	MINTIC	https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/