Tabla de Contenido

ILUSTRACIONES

1. INTRODUCCIÓN

La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** reconoce y declara tanto los datos e información como un activo que tiene valor y el cual es indispensable para la consecución de los objetivos definidos por la estrategia de Gobierno de la Entidad, por esta razón, es necesario establecer un marco basado en los términos legales, mejores prácticas y normativa asociada a la seguridad y privacidad de los datos e información, en el cual se asegure que la información administrada, generada y custodiada es protegida y tratada de una manera adecuada, independientemente de la forma en la que ésta es procesada, transportada y/o almacenada en medio físico, digital y/o electrónico.

Por tanto, este documento describe las políticas internas o de apoyo y los respectivos controles de la Seguridad y Privacidad de la Información definidos por la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**, los cuales se encuentran basados y alineados con la Norma ISO/IEC 27001[1] y las recomendaciones establecidas en el estándar ISO/IEC 27002[2]. Así mismo, estas políticas y estos controles son parte fundamental del Sistema Integrado de Gestión de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** y, por tanto, se convierten en la base para llevar a cabo la implementación de los procedimientos y estándares definidos que contribuyen a la implementación y mejora continua de la seguridad, privacidad y protección de los datos e información que genera, procesa, administra y custodia la Entidad.

Con base en lo anterior, la Seguridad y Privacidad de los Datos e Información es una prioridad para la Entidad y por lo tanto es responsabilidad de todos sus servidores públicos, contratistas y proveedores velar por el cumplimiento de cada una de las políticas y controles establecidos en el presente Manual.

2. OBJETIVO

Establecer y dar a conocer las medidas organizacionales, técnicas, físicas y legales, necesarias para la protección de la Confidencialidad, Integridad y Disponibilidad de los activos de información frente a los posibles riesgos que se encuentran expuestos, disponiendo de los recursos necesarios que garanticen el progreso del Modelo de Seguridad y Privacidad de la

[1] Las normas establecidas en este manual son las necesarias de acuerdo con la Norma ISO 27002 última versión generada por ISO y que se encuentran descritas el numeral 10.2 de este documento. El manual será actualizado de acuerdo con las últimas versiones que genera ISO sobre Seguridad de la Información.

[2] Ítem anterior.

Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

3. ALCANCE

Inicia con la identificación, definición, revisión de la política general, políticas de apoyo o secundarias y los controles establecidos, pasando por la respectiva validación y verificación de lo que actualmente se encuentra desarrollado e implementado y terminando con los respectivos ajustes documentales e implementación de éstos en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.,** para garantizar la confidencialidad, integridad y disponibilidad de los datos e información a través de los accesos lógicos y/o físicos a los sistemas de información, aplicaciones, bases de datos, redes, oficinas, Datacenter, cuartos técnicos, cuartos eléctricos de la Entidad que se gestionan, administran, generan, modifican y son custodiados por los servidores públicos, contratistas y proveedores.

4. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la entidad. (Fuente: http://www.iso27000.es/glosario.html)
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad. (Fuente: http://www.iso27000.es/glosario.html)
Caso: Numero consecutivo asignado al requerimiento o incidente. (Fuente: https://www.mintic.gov.co/portal/inicio/Glosario/)
Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad. (Fuente: ISO/IEC 27032:2012)
Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Fuente: https://www.iso27000.es/glosario.html).
Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Fuente: http://www.iso27000.es/glosario.html)

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. (Fuente: Articulo 3 Definiciones, Ley Estatutaria 1581 del 17 de octubre de 2012)

Declaración de Aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI. (Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150517_Modelo_de_Seguridad_Privacidad.pdf)

Disponibilidad*:* Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Fuente*:* http://www.iso27000.es/glosario.html)

Gestión de incidentes de seguridad de la información: Actividades coordinadas para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (Fuente: http://www.iso27000.es/glosario.html)

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una entidad con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (Fuente: http://www.iso27000.es/glosario.html)

Gestor designado: Es el servidor(es) designado(s) por cada dependencia para llevar a cabo la identificación/actualización de los activos de información en la entidad. (Fuente: Redacción propia)

Hardware: Se refiere a todos los elementos físicos que permiten el correcto funcionamiento de un medio informático. Incluye redes, discos duros o extraíbles, impresoras, servidores, computadoras, dispositivos móviles, entre otros. (Fuente: http://www.iso27000.es/glosario.html)

Impacto: El coste para la entidad de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc. (Fuente: http://www.iso27000.es/glosario.html)

Información: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal. (Fuente: https://www.mintic.gov.co/portal/inicio/Glosario/)

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones entidad y amenazar la seguridad de la información. (Fuente: http://www.iso27000.es/glosario.html)

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de Gestión de Seguridad de la Información - SGSI, que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos. (Fuente: http://www.iso27000.es/glosario.html)

Infraestructura tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios que presta la Secretaría General de la Alcaldía Mayor de Bogotá: equipos de cómputo, equipos de comunicaciones, sistemas de información, equipos de fotocopiado, equipos de digitalización, equipos de telefonía. (Fuente: https://www.mintic.gov.co/portal/inicio/Glosario/)

Integridad: Propiedad de la información relativa a su exactitud y completitud. (Fuente: http://www.iso27000.es/glosario.html)

Inteligencia de Amenazas: La inteligencia de amenazas, también llamada "inteligencia de ciberamenazas" (CTI), es información sobre amenazas detallada y procesable para prevenir y combatir las amenazas a la ciberseguridad dirigidas a una organización. (Fuente: https://www.ibm.com/es-es/topics/threat-intelligence)

MSPI: Modelo de Seguridad y Privacidad de la Información. (Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/)

Requerimiento: Aviso o manifestación de una situación problema a nivel técnico. (Fuente: https://www.mintic.gov.co/portal/inicio/Glosario/)

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (Fuente: http://www.iso27000.es/glosario.html)

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (Fuente: http://www.iso27000.es/glosario.html)

RNBD: Registro Nacional de Bases de Datos. es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos. (Fuente: https://www.sic.gov.co/registro-nacional-de-bases-de-datos)

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. (Fuente: http://www.iso27000.es/glosario.html)

Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet. (Fuente; https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237906_maestro_mspi.pdf). En esta tipología se encuentra la intranet, el internet, el correo electrónico, el servicio de fotocopiado, el servicio de correspondencia, el servicio de ingreso a la entidad, entre otros. Los servicios en la entidad son prestados por diferentes dependencias.

SIC: Superintendencia de Industria y Comercio. (Fuente: https://www.sic.gov.co/)

Sistema de Gestión de Seguridad de la Información - SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. (Fuente: http://www.iso27000.es/glosario.html)

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. El Manual Técnico del MECI 2014 hace referencia a los programas, información y conocimiento (software) como "el conjunto ordenado de instrucciones, información y base de conocimientos dadas al computador y que son requeridas para el trabajo de estos sistemas". (Fuente: https://es.wikipedia.org/wiki/Software)

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento. (Fuente: Articulo 3 Definiciones, Ley Estatutaria 1581 del 17 de octubre de 2012)

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles para evitar una pérdida o daño en un activo de información. (Fuente: http://www.iso27000.es/glosario.html)

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Fuente: http://www.iso27000.es/glosario.html)

Valoración de riesgos: Proceso de análisis y evaluación del riesgo para evitar una pérdida o daño en un activo de información. (Fuente: http://www.iso27000.es/glosario.html)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (Fuente: http://www.iso27000.es/glosario.html)

5. NORMATIVIDAD

Constitución Política de Colombia 1 de 1991 Artículo 15,20. Asamblea Nacional Constitución Política de Colombia de 1991

Conpes 3701 de 2011. Lineamientos de Políticas para ciberseguridad y ciberdefensa

Conpes 3854 de 2016 Política Nacional de Seguridad Digital.

Conpes 3975 de 2019. Política Nacional para la Transformación Digital e Inteligencia Artificial

Conpes 3995 de 2020. Política Nacional de Seguridad y Confianza Digital

Directrices OCDE. Todo el documento OCDE. Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad

Conpes 4144 de 2025. Política Nacional de Inteligencia Artificial.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Ley 1928 de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.
Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2573 del 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
Decreto 1494 de 2015. Por el cual se corrigen yerros en la Ley 1712 de 2014.
Decreto 415 de 2016. Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 1413 de 2017. Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 090 de 2018. Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 255 de 2022. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio,

Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

Decreto 472 de 2024. Por el cual se adopta el Modelo de Gobernanza de Seguridad Digital para el Distrito, se modifica el artículo 5 del Decreto Distrital 025 de 2021 y se dictan otras disposiciones

Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución No 500 de 2021.

Resolución 728 de 2023. Por la cual se unifica y actualiza la reglamentación de las instancias internas de coordinación en la Secretaría General de la Alcaldía Mayor de Bogotá.

Resolución 485 de 2024. Por la cual se actualiza la reglamentación del Comité Institucional de Gestión y Desempeño en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C. y se sustituyen unos Capítulos del Título II de la Resolución 728 de 2023 “Por la cual se unifica y actualiza la reglamentación de las instancias internas de coordinación en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C."

Resolución 373 de 2025 Por la cual se adopta la Política de Seguridad de la Información y Seguridad Digital y la Estrategia de Seguridad Digital de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C

Resolución 2277 de 2025. Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

Directiva 02 de 2002. Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).

Directiva 017 de 2018. Registro Nacional de Bases de Datos – RNBD

Directiva 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

6. ALCANCE DEL MSPI

La implementación del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** cubre todos los procesos y todas las dependencias y se encuentra alineada con la Norma ISO/IEC 27001:2022. Para tal fin, incluye el desarrollo y/o ajuste de políticas, procesos, procedimientos e instructivos, garantizando el cumplimiento de las prácticas descritas en este manual, así como la estrategia de capacitación y sensibilización en Seguridad y Privacidad de la Información para toda la Entidad.

7. OBJETIVOS DEL MSPI

- Establecer y mantener el compromiso del Comité Institucional de Gestión y Desempeño para apalancar el cumplimiento de la **Política de Seguridad Digital** y del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI), al interior de la entidad.

- Establecer y proponer desde la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información los controles para la gestión de la seguridad y privacidad de la información - protección de los datos personales, de manera clara y estructurada, alineado con las buenas prácticas, la Norma ISO/IEC 27001:2022 y demás disposiciones relacionadas[3].

- Revisar, modificar y aprobar desde el Comité Institucional de Gestión y Desempeño los controles para la gestión de la seguridad, privacidad de la información - protección de los datos personales propuestos por la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información.

- Contribuir al cumplimiento de la legislación vigente sobre la Seguridad, Privacidad y Protección de información Pública, Información Pública Clasificada, Información Pública Reservada, propiedad intelectual, transparencia, protección de los datos personales, protección y salvaguarda de los activos de información físicos y digitales para brindar

[3] Norma ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información; ISO/IEC 27002:2013 Códigos de práctica para los controles de Seguridad de la Información; ISO/IEC 27005:2009 Gestión del Riesgo en la Seguridad de la Información.

tranquilidad a los servidores públicos, contratistas, proveedores y ciudadanía en general sobre el cuidado de los datos e información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

- Generar la alineación con los demás sistemas de gestión de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**, en particular con el Sistema de Gestión de Calidad y el Sistema de Gestión de Riesgos, garantizando el cumplimiento de los planes y acciones (preventivas o correctivas) generadas en el seguimiento interno, la revisión por la dirección y/o las auditorías internas y/o externas.

- Gestionar los riesgos de Seguridad Digital, Seguridad de la Información y Privacidad de la Información que se identifiquen en la entidad.

- Sensibilizar y apropiar la gestión adecuada del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) en los servidores públicos, contratistas, proveedores y demás partes interesadas de la entidad.

8. FACTORES DE ÉXITO DEL MSPI

- Generar conciencia en todos los servidores públicos, contratistas y proveedores de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** sobre la importancia de conocer, aplicar y seguir las políticas y controles establecidos en el presente manual, los cuales ayudan a garantizar que la información que la entidad administra, genera, almacena, controla, modifica y custodia, conserven los atributos de confidencialidad, integridad y disponibilidad.

- Contar con instancias de gestión, revisión y decisión a distintos niveles de la Entidad (táctico, operativo, estratégico y de evaluación) en los cuales se realice la presentación de los resultados de los procesos y actividades asociadas al Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI).

- Implementar un esquema de gestión de eventos e incidentes de seguridad de la información que recoja notificaciones continuas por parte de los servidores públicos, contratistas y proveedores, donde se analice cada uno de los eventos, se generen monitoreos y mejoras en los controles establecidos y se reporte a las instancias de revisión y decisión los resultados de la gestión llevada a cabo.

- Incluir en todos los procesos de la entidad, así como en los proyectos prioritarios los criterios de administración y gestión del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI).

9. CONSIDERACIONES GENERALES.

9.1 Línea base

- **Responsabilidad**

Es responsabilidad de las Direcciones, Subdirecciones y jefes de Oficina de la **Secretaría General de la Alcaldía Mayor de Bogotá, D.C**. hacer uso de las políticas, controles, procedimientos, guías e instructivos de seguridad y privacidad de la información como parte de sus herramientas de gobierno y gestión, que garanticen el cumplimiento y mejora del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI).

- **Cumplimiento**

El cumplimiento de las políticas, controles, procedimientos, guías e instructivos de seguridad de la información aplicará para todos los servidores públicos, contratistas y proveedores que interactúen con los activos de información de propiedad de la Entidad, si los parámetros aquí descritos se infringen, la **Secretaría General de la Alcaldía Mayor de Bogotá, D.C.** se reservará el derecho de tomar las medidas correspondientes.

- **Excepciones**

Las excepciones a cualquier incumplimiento de lo descrito en el presente manual deberán ser definidas por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC y preaprobadas por la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información y aprobadas por el Comité Institucional de Gestión y Desempeño. Todas las excepciones a lo descrito en el presente documento deben ser formalmente documentadas, registradas, revisadas y aprobadas.

- **Administración de políticas y controles**

Se debe garantizar una efectiva administración de las políticas de seguridad y de los controles implementados al interior de la entidad. Será potestad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, la implementación de controles tecnológicos. En el caso que se requiera los controles se deberán presentar para aprobación de la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información para a su vez y ser presentados ante el Comité Institucional de Gestión y Desempeño de la **Secretaría General de la Alcaldía Mayor de Bogotá, D.C.** Dichas políticas y/o controles serán revisados como mínimo una vez al año y/o cada vez que sea requerido.

- **Exclusiones**

- No se excluye ningún numeral de la norma ISO/IEC 27001:2022
- Los controles se encuentran definidos en la Declaración de Aplicabilidad (SOA por sus siglas en inglés).

- **Vigencia y actualización del manual.**

La actualización y mantenimiento del Manual de Seguridad de la Información es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC con apoyo de las dependencias de la entidad.

En las revisiones periódicas se deben tener en cuenta factores como:

- Requerimientos normativos y de Ley.
- Requerimientos emitidos por Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Estándares aplicables para la seguridad de la información.
- Mapa de riesgos de la Entidad.
- Eventos/Incidentes de seguridad de la Información.
- Nuevas vulnerabilidades detectadas.
- Cambios en la infraestructura organizacional y/o tecnológica de la Entidad.
- Cambios en la cadena de valor, estrategia, objetivos y/o procesos de la Entidad.

La versión oficial de este documento será la que se encuentre publicada, aprobada y

divulgada en el Sistema de Gestión de Calidad.

10. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ENTIDAD4.

10.1 Roles y responsabilidades para la seguridad de la información.

La Entidad cuenta con un grupo interdisciplinario denominado Comité Institucional de Gestión y Desempeño, que es el órgano encargado de orientar la implementación, seguimiento del Sistema de Gestión y la operación del Modelo Integrado de Planeación y Gestión - MIPG - en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., como instrumento articulador y ejecutor a nivel institucional, de las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento de éste. (…)" - **Artículo 2.1.1. Comité Institucional de Gestión y Desempeño** de la Resolución 728 de 2023**.**

Este comité tiene dentro de sus funciones, asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital, conforme lo descrito en el literal 15 del Artículo 2.2.2. **Funciones del Comité Institucional de Gestión y Desempeño** de la Resolución 728 de 2023, y se apoyará en la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información acorde con las funciones generales definidas en el **Articulo 2.5.3 – Funciones específicas de la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información** contenidas en la misma resolución**.**

Con lo descrito anteriormente, se busca gestionar, fortalecer, revisar y mejorar de manera continua el Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) en la entidad.

Las partes interesadas internas de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**, como lo son: los servidores públicos, contratistas, proveedores y los usuarios de los servicios de la entidad deben tener conocimiento de sus responsabilidades y obligaciones relacionadas con la seguridad digital, seguridad y privacidad de la información, y ésta responsabilidad se debe ver reflejada en los instrumentos jurídicos que regulen las relaciones de éstas partes con la entidad y debe ser verificada por el Comité Institucional de Gestión y Desempeño de manera continua.

[4] Hace referencia al numeral 5.3 de la Norma ISO/IEC 27001:2013: "5.3. Roles, Responsabilidades y Autoridades en la Organización."

La definición de los respectivos roles y responsabilidades se encuentra definida y puede ser consultada en la **Matriz RACI – SGAMB Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI):**

Versión 001	**Modelo de Seguridad y Privacidad de la Información**

BOGOTÁ Secretaría General Alcaldía Mayor de Bogotá

Prácticas Clave de Gestión	Funciones/Dependencias	Comité Institucional de Gestión y Desempeño	Jefe Oficina de Tecnologías de la Información y las	Mesa técnica de Apoyo en Archivo y Seguridad de la Información	Oficial de Seguridad de la Información	Oficial de Protección de Datos Personales	Jefe Oficina de Control Interno	Dueños Procesos de Negocio (Entidad)
Gestión de Seguridad de la Información								
Definir las políticas, planes y programas generales de la Entidad, expedir acuerdos con carácter normativo y hacerle seguimiento a la gestión de la Entidad	C/I	C/I	R/C/I	C/I	C/I	C/I	C/I	
Aprobar y apoyar la implementación del Modelo de Seguridad y Privacidad de la Información de la Entidad.	R/C/I	C/I	C/I	C/I	C/I	C/I	C/I	
Aprobar la política general de seguridad y privacidad de la información de la Entidad	R	C/I	C/I	C/I	C/I	C/I	C/I	
Aprobar las políticas para el fortalecimiento continuo en seguridad de la información y la protección y tratamiento de datos personales.	R	C/I	C/I	C/I	C/I	C/I	C/I	
Planear, Implementar y Mejorar del Modelo de Seguridad y Privacidad de la Información de la Entidad	C/I	C/I	C/I	C/I	C/I	C/I	C/I	

Evaluar las nuevas tecnologías de seguridad y privacidad de la información para la incorporación dentro de la Entidad.	C/I	R	C/I	C/I	C/I	C/I	C/I
Asesorar a las dependencias de la Entidad en la aplicación de las políticas, estrategias y directrices del modelo de seguridad y privacidad de la información	C/I	R	C/I	C/I	C/I	C/I	C/I
Garantizar la disponibilidad, integridad y confidencialidad de la información, para que sea consistente, actualizada y confiable, la cual es necesaria para el cumplimiento de la misión institucional	C/I	R	C/I	C/I	C/I	C/I	C/I
Coordinar las directrices y orientaciones para la elaboración de los planes de capacitación, formación y sensibilización del Sistema de Gestión de Seguridad de la Información para los funcionarios, contratistas y proveedores de la Entidad	C/I	R	C/I	C/I	C/I	C/I	C/I
Evaluar y definir las necesidades y lineamientos para la adquisición y actualización de las plataformas de seguridad y privacidad de la información de la Entidad	C/I	R	C/I	C/I	C/I	C/I	C/I
Responsable de la definición y diseño de las estrategias, políticas, planes, programas y proyectos de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. promoviendo y apoyando la implementación del Sistema de Gestión de Seguridad de la Información a través de la generación de la cultura en la Entidad.	C/I	C/I	C/I	C/I	C/I	C/I	C/I
Definir y liderar las políticas, procesos y procedimientos definidos para el almacenamiento, custodia, seguridad, confidencialidad, integridad y disponibilidad de la información en medios electrónicos al interior de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**	C/I	C/I	C/I	C/I	C/I	C/I	C/I

Orientar y propender porque las acciones del Sistema de Gestión de Seguridad de la Información se encuentren alineadas con la Entidad, se ajusten a la normatividad vigente, y se trabajen en coordinación con la Oficina de Control Interno	C/I	C/I	C/I	C/I	C/I	C/I	C/I
Establecer y/o planear un Sistema de Gestión de Seguridad de la Información							
Generar, desarrollar y gestionar el cronograma de la implementación del Sistema de Gestión de Seguridad de la Información	C/I	C/I	C/I	C/I	C/I	C/I	C/I
Definir los respectivos roles, responsabilidades, entregables y tiempos al interior del equipo para la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.	C/I	C/I	C/I	C/I	C/I	I	I
Realizar el respectivo seguimiento de manera permanente a la ejecución del cronograma establecido, monitoreando los riesgos para darle solución oportuna y escalar a la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información cuando sea necesario	C/I	C/I	C/I	C/I	C/I	C/I	C/I
Gestionar la implementación de políticas, normas, directrices y procedimientos del Sistema de Gestión de Seguridad de la Información							
Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información actuales, a desarrollar, o pendientes por adquirir por la Entidad	I/C	A	C/I	R	R	C/I	C/I
Liderar el proceso de gestión de incidentes de seguridad y su respectiva investigación para determinar causas, posibles responsables y recomendaciones de mejora para los activos de información afectados.	I/A	A	C/I	R	R	C/I	C/I

Verificar el cumplimiento de las obligaciones legales y regulatorias emitidas por el Gobierno Central y Territorial y las cuales se encuentran relacionadas con la seguridad y privacidad de la información.	I/A	A	C/I	R	R	C/I	C/I
Proponer y desarrollar el plan de formación y sensibilización en la Entidad con temas relacionados a seguridad de la información y protección de datos en la Entidad.	I/A	A	C/I	R	R	C/I	C/I
Trabajar con el Comité Institucional de Gestión y Desempeño y los dueños de los procesos misionales al interior de la Entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.	I/A	A	C/I	R	R	C/I	C/I
Verificar y/o revisar el estado de implementación del Sistema de Gestión de Seguridad de la Información							
Dirigir a la Entidad hacia el cumplimiento de la implementación del Sistema de Gestión de Seguridad de la Información	I/A	A	C/I	R	R	I	I
Garantizar y/o supervisar la realización de las pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información en la Entidad	I/A	A	C/I	R	R	I	I
Mantener el Sistema de Gestión de Seguridad de la Información							
Definir los respectivos mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento sobre la implementación de las medidas de seguridad de la información.	I/A	C/I	C/I	R	R	I	I
Supervisar la atención y la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales que se consideren necesarias	I/A	A/I	C/I	R	R	I	I

Mesa Técnica de Apoyo en Archivo y Seguridad de la Información							
Coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**	I/A	A/C/I	R	A/C/I	A/C/I	I	C
Revisar los diagnósticos del estado de la seguridad de la información de la Entidad y proponer acciones de mejora a éste	I/A	A/C/I	R	A/C/I	A/C/I	I	C
Acompañar e impulsar el desarrollo de proyectos de seguridad y privacidad de la información y de protección de datos personales en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**	I/A	A/C/I	R	A/C/I	A/C/I	I	C
Promover la difusión y sensibilización de la seguridad de la información al interior de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**	I/A	A/C/I	R	A/C/I	A/C/I	I	I
Poner en conocimiento de la Entidad, a través del Comité Institucional de Gestión y Desempeño los documentos generados al interior de la Mesa Técnica que impacten de manera transversal a la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**	I/A	A/C/I	R	A/C/I	A/C/I	I	I
Gestión de Riesgos del Sistema de Gestión de Seguridad de la Información							
Liderar la gestión de riesgos de seguridad y privacidad de la Información.	I/A	A/C/I	R/C/I	A/C/I	C/I	I	C
Realizar la identificación y definición de riesgos de seguridad y privacidad de la información para los procesos de la Entidad.	I/A	A/C/I	R	A/C/I	C/I	I	C
Gestionar los riesgos identificados (Seguimiento de implementación de medidas de control).	I/A	A/C/I	R	A/C/I	C/I	R/I	I
Evaluar la eficacia de las acciones tomadas para mitigar los riesgos identificados de la Entidad.	I/A	A/C/I	R	A/C/I	C/I	C/I	C/I

Nota: La Mesa Técnica de Apoyo en Archivo y Seguridad de la Información se encuentra conformada por representantes de las dependencias:
1. Oficina Asesora de Planeación.
2. Oficina Asesora de Jurídica
3. Dirección Administrativa y Financiera
4. Subdirección de Servicios Administrativos
5. Secretaría General

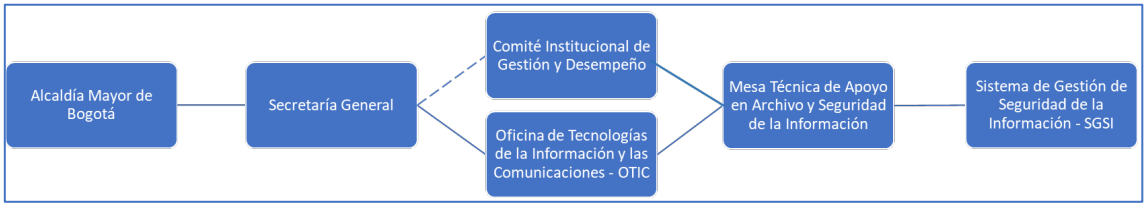
R	Responsable
A	Aprobador (Quien rinde cuentas)
C	Consultado
I	Informado

	Acompañantes
	Responsable del proceso.

10.2 Estructura Organizacional – Seguridad de la Información.

La estructura organizacional para el funcionamiento del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) al interior de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** es el siguiente:

Ilustración 1 Estructura Organizacional Seguridad de la Información – Secretaría General de la Alcaldía Mayor de Bogotá



Fuente: Elaboración propia

La conformación del **Comité Institucional de Gestión y Desempeño** se encuentra detallada en el **artículo 2.2.1. Integración del Comité Institucional de Gestión y Desempeño** de la Resolución No 728 de 2023 publicada en la página de la Secretaría General de la Alcaldía Mayor de Bogotá y se apoya en la **Mesa Técnica de Apoyo en Archivo y Seguridad de la Información,** en la cual se deben abordar los temas asociados y relacionados con el Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI).

10.3 Monitoreo al MSPI (Sistema de Gestión de Seguridad de la Información – SGSI)

El monitoreo al Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** se realizará de manera interna y bajo la responsabilidad directa de la Oficina de Tecnología de la Información y Comunicaciones – OTIC a través del Oficial de Seguridad de la Información, el mismo tendrá una periodicidad de ejecución de al menos una (1) vez al año, en

donde se revisarán las políticas y controles conforme como se establezca en el plan de seguridad privacidad de la información de la vigencia, en donde se validará su implementación, y se realizarán los cambios, modificaciones, actualizaciones y/o eliminaciones de políticas y/o controles allí definidos. Así mismo, será el responsable de mantener actualizado el Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) en su totalidad.

11. POLÍTICA GENERAL DE SEGURIDAD DIGITAL / DE LA INFORMACIÓN

La Política de Seguridad Digital y la Estrategia de Seguridad Digital de la Secretaría General fue aprobada por el Comité Institucional de Gestión y Desempeño de la Entidad en sesión del 31 de julio de 2025, y adoptada mediante resolución Nro. 373 del 2025 y se encuentra publicada en la página web de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C**.

La Secretaría General de la Alcaldía Mayor de Bogotá D.C., para asegurar la dirección estratégica de la Entidad, y evitar la materialización de riesgos relacionados con la pérdida de confidencialidad, integridad y disponibilidad de los activos de información (servidores públicos, contratistas, terceros, información, bases de datos, tecnologías de información incluido el hardware y el software, servicios, redes de comunicaciones, infraestructura física), que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI), implementa controles y responsabilidades generales y específicas que son de estricto cumplimiento para todos los servidores públicos, contratistas y terceros de **LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C.** y la ciudadanía en general.

12. DOMINIOS

En el marco de la actualización de la Norma ISO/IEC 27001:2022, **LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C.** define

los lineamientos controles de seguridad de la información y seguridad digital los cuales se reorganizan en los siguientes dominios:

- Organizacionales
- De personas
- Físicos
- Tecnológicos.

A continuación, se presentan los lineamientos y controles de seguridad y privacidad de la información conforme con lo descrito en la Norma ISO 27001 versión 2022, a los cuales se les debe dar estricto cumplimiento de manera transversal al interior de la entidad.

12.1 CONTROLES ORGANIZACIONALES

Los controles organizacionales establecen el marco de gobierno, las políticas y los procedimientos necesarios para gestionar la seguridad de la información en la Secretaría General. Incluyen la definición de roles y responsabilidades, la gestión de riesgos, la planificación de la continuidad del negocio, la relación con proveedores y terceros, así como la integración de la seguridad en los procesos institucionales. Su propósito es asegurar que la seguridad digital sea un eje transversal en la gestión de la Entidad, garantizando coherencia, cumplimiento normativo y una cultura de mejora continua.

12.1.1 Control 5.1 - Políticas de seguridad de la información

La entidad define una política de seguridad digital mediante acto administrativo y unas políticas específicas, las cuales son de estricto cumplimiento para todos los servidores públicos, contratistas y terceros que acceden a los activos de información de la entidad.

– La Secretaría General establece, mantiene y actualiza las políticas de seguridad de la información y seguridad digital, garantizando su alineación con la normativa vigente, los lineamientos de Gobierno Digital y los estándares internacionales adoptados. Las políticas deberán ser comunicadas, divulgadas y aplicadas en todos los niveles de la Entidad, y contar con procedimientos operacionales documentados que faciliten su implementación y cumplimiento.

12.1.2 Control 5.2 - Roles y responsabilidades de SI

La Entidad define y asigna roles y responsabilidades claras en materia de seguridad de la información, asegurando que los servidores públicos, contratistas y terceros conozcan y cumplan sus deberes. La alta dirección deberá garantizar el liderazgo, la supervisión y el apoyo institucional necesarios para la implementación efectiva del sistema de gestión.

– Todos los servidores públicos, contratistas y proveedores de la **Secretaría General de la Alcaldía Mayor de Bogotá. D.C.** deben conocer y dar cumplimiento al Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) establecido en la entidad.

– Los servidores públicos que en ejercicio de sus labores tengan acceso a: datos e información, infraestructura tecnológica, aplicaciones y sistemas de información, deben contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y privilegios establecidos sobre los activos de información que almacenan los datos e información, con el objetivo de minimizar el uso o modificación no autorizada sobre los activos de información de la entidad.

– Todos los servidores públicos, contratistas y proveedores son responsables de proteger la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido.

– Es responsabilidad de todos los servidores públicos, contratistas y proveedores de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** reportar al correo oticsoporte@alcaldiabogota.gov.co los incidentes de seguridad, eventos sospechosos y el uso inadecuado de los activos de información que se presente en la entidad.

12.1.3 Control 5.3 - Segregación de funciones

La Secretaría General aplica el principio de segregación de tareas para reducir riesgos de error, fraude o uso indebido de la información, evitando la concentración de funciones críticas en una sola persona y asegurando controles cruzados adecuados.

- Los sistemas de información clasificados como críticos deben incluir reglas de acceso que aseguren una adecuada segregación de funciones entre quien autorice, administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información.

- Los cambios o pasos a ambientes productivos solo podrán realizarse una vez sean aprobados por el área/líder funcional o solicitante del requerimiento a través de una gestión de cambios.

- Las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible deben estar deshabilitadas.

- No se debe permitir conexiones concurrentes a los sistemas de información con el mismo usuario.

- Todo cambio en los sistemas de información que vaya a ser desplegado en el ambiente de producción debe dar cumplimiento a la guía **4204000-GS-111 Gestión de Cambios de TI.**

- Se debe garantizar el control de cambios a los sistemas, sitios web y aplicativos: este control se debe asegurar mediante una herramienta de control de código fuente para todos los sistemas, sitios web y aplicativos de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.;** De igual manera, cuando se presenten actualizaciones, mejoras o funcionalidades nuevas a los que están en ambiente productivo, se debe documentar el control de ese cambio mediante el formato que la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC tiene definido para el efecto, el cual debe contar con la aprobación tanto de la dependencia funcional como de la mencionada Oficina.

- El nivel de súper usuario de los sistemas de información debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema. Para el efecto, la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC a través de la delegación de los temas de Seguridad de la Información realizará verificaciones periódicas y aleatorias.

- Las funciones de soporte técnico, planificación, desarrollo y operación deben

estar claramente segregadas, así como distribuidos los ambientes de desarrollo, de pruebas y de producción, según corresponda.

12.1.4 Control 5.4 - Responsabilidades de la dirección

Los responsables de los procesos integran la seguridad de la información en la planeación, ejecución y evaluación de sus actividades, velando por el cumplimiento de las políticas, la protección de los activos de información y la gestión de los riesgos asociados.

– El Comité Institucional de Gestión y Desempeño aprueba este Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI, como muestra de su compromiso con la política de seguridad digital definida y con el diseño e implementación de controles, propendiendo por la seguridad de la información de la entidad.

– Adicionalmente, el Comité Institucional de Gestión y Desempeño de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. demostrará su compromiso a través de:

- La revisión de la **Política de Seguridad Digital** dispuesta para aprobación, publicación y divulgación ante la Entidad.
- La revisión y aprobación de las políticas específicas.
- La promoción activa de una cultura de seguridad y privacidad de la Información.
- La divulgación de este manual a todos los servidores públicos, contratistas y proveedores de la Entidad.
- La solicitud para asegurar la asignación de los recursos adecuados para implementar y mantener las políticas de seguridad descritas,
- La verificación del cumplimiento de las políticas de seguridad y controles de seguridad implementados.
- La promoción de los canales adecuados para que los servidores públicos, contratistas y proveedores reporten sucesos, eventos y/o incidentes que afecten, vulneren o representen un incumplimiento de las políticas de seguridad y/o controles de seguridad de la información.

12.1.5 Control 5.5 - Contacto con autoridades

La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece y mantiene canales formales de contacto y coordinación con las autoridades competentes en materia de seguridad de la información, seguridad digital, protección de datos personales, ciberseguridad y demás instancias regulatorias o de control que resulten aplicables, de conformidad con la normativa vigente.

12.1.6 Control 5.6 - Contacto con grupos de interés

La Entidad mantiene mecanismos de contacto y coordinación con autoridades competentes, organismos de control y grupos de interés especializados en seguridad de la información y seguridad digital, con el fin de atender requerimientos, reportar incidentes relevantes y adoptar buenas prácticas sectoriales.

– La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** establece y mantiene una relación cercana con Entidades del Sistema Distrital de Prevención y Atención de Emergencias (SDPAE), así como, con grupos de interés y/o foros de especialistas en seguridad digital, seguridad y privacidad de la información, para que puedan ser contactados de manera oportuna en caso de que se presente un evento/incidente de seguridad y privacidad de la información.

– Los grupos de interés son los siguientes:

- **ColCert:** Grupo de Respuesta a Emergencia Cibernéticas de Colombia. www.colcert.gov.co – CCOC: Comando Conjunto Cibernético.
- **CSIRT:** Centro de Coordinación Seguridad Informática Colombia. www.csirt-ccit.org.co
- **Centro Cibernético Policial (CAI Virtual):** Ciberseguridad en Colombia comandado por la Policía Nacional. www.policia.gov.co
- **MINTIC:** Ministerio de las Tecnologías y las Comunicaciones www.mintic.gov.co

- **Comando Conjunto Cibernético – CCOC:** Grupo que dirige las mesas de trabajo para garantizar la seguridad de las infraestructuras críticas del país ante cualquier eventualidad informar al correo atencionalciudadano@cgfm.mil.co

En la eventualidad que se llegasen a presentar eventos/incidentes relacionados con la seguridad digital, seguridad y privacidad de la información al interior de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**, deben ser reportados a la mesa de servicios de la entidad y el oficial de seguridad de la información o quien haga sus veces. Dependiendo de la severidad del incidente se debe reportar a las siguientes entidades.

Ilustración 2 Cuadro de reportes de eventos de Seguridad de la Información – Secretaría General de la Alcaldía Mayor de Bogotá

Descripción	Entidad	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	http://www.ccp.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Respuesta a Emergencias Cibernéticas de Colombia	COLCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano Phishing Ingeniería Social	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia o al CSIRT DC o CSIRT Gobierno	https://cc-csirt.policia.gov.co
Emergencia por Incendio	Bomberos	119

Descripción	Entidad	Contacto
Robo	Policía Nacional / Dijin	112 / 157
Antisecuestro y Antiextorsión	Gaula	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja / Centro Toxicológico	132 / 136

Fuente: Elaboración propia

12.1.7 Control 5.7 - Inteligencia de Amenazas

La Secretaría General establece mecanismos de vigilancia continua para identificar amenazas emergentes (malware, phishing, vulnerabilidades críticas, ataques dirigidos) que puedan afectar los activos de información de la Entidad.

– La inteligencia de amenazas se obtendrá de fuentes internas (registros, incidentes previos, auditorías) y externas (CERT Colombia, MinTIC, ANE, proveedores de seguridad, foros especializados), asegurando la validez y actualidad de la información recopilada.

– Los hallazgos de inteligencia de amenazas deberán ser analizados y registrados en el proceso institucional de gestión de riesgos de seguridad digital, con el fin de priorizar acciones preventivas y correctivas.

– Con base en la inteligencia recibida, se adoptarán medidas como actualización de configuraciones, parches de seguridad, fortalecimiento de controles de acceso, alertas tempranas y campañas de sensibilización dirigidas al personal.

– El Oficial de Seguridad de la Información y equipo técnico de apoyo serán responsables de coordinar la recepción, análisis y difusión de la inteligencia de amenazas.

– La información relevante sobre amenazas deberá ser comunicada a los servidores públicos y contratistas, mediante boletines de seguridad, capacitaciones y alertas oportunas, en lenguaje claro y orientado a la acción.

– El control será revisado periódicamente para evaluar la efectividad de las fuentes de información utilizadas, el tiempo de respuesta de las acciones

preventivas y la reducción del impacto de incidentes en la Entidad.

12.1.8 Control 5.8 - Seguridad de la información en la gestión de proyectos

Los proyectos institucionales que se consideren estratégicos (tecnológico, documental, administrativo o de infraestructura) deberán incluir desde la fase de planeación inicial criterios de seguridad de la información, un análisis de riesgos de seguridad de la información, definiendo controles que mitiguen amenazas sobre los activos de información, antes de su entrada en operación.

- Los proyectos deberán verificar y cumplir con la normativa aplicable en materia de protección de datos personales (Ley 1581 de 2012), transparencia (Ley 1712 de 2014), Gobierno Digital, Decreto 472 de 2024 y las políticas internas de seguridad digital de la Entidad.
- El responsable del proyecto deberá designar un enlace, para garantizar que la seguridad se supervise durante todo el ciclo de vida del proyecto.
- Se identificarán los activos de información involucrados en el proyecto (bases de datos, aplicaciones, documentos, plataformas) y se definirán controles de confidencialidad, integridad y disponibilidad para cada uno de ellos.
- Cuando el proyecto involucre contratistas o proveedores, se deberá firmar acuerdos de confidencialidad
- Todo proyecto tecnológico deberá incluir revisiones de seguridad (pruebas de vulnerabilidad, revisiones de configuración segura, gestión de accesos) antes de su puesta en producción.
- Los proyectos deberán mantener evidencia documentada de los análisis de riesgo, decisiones de seguridad adoptadas, incidentes ocurridos y lecciones aprendidas
- Durante la ejecución y cierre del proyecto, se deberá evaluar la eficacia de los controles aplicados y se incorporarán las lecciones aprendidas al portafolio institucional de proyectos, con el fin de fortalecer futuros desarrollo

12.1.9 Control 5.9 - Inventario de información y otros activos asociados

La Secretaría General de la Alcaldía Mayor de Bogotá cuenta y aplica el documento 4204000-IN-086 Instructivo Gestión de Activos de información para identificar y clasificar los activos de información de todos los procesos al interior de la entidad.

- La Secretaría General mantiene un inventario actualizado de la información y de los activos asociados, definiendo reglas para su uso aceptable y

asegurando su devolución o retiro cuando finalicen las responsabilidades de los usuarios o terceros.

– La Secretaría General de la Alcaldía Mayor de Bogotá cuenta y aplica el documento 4204000-IN-086 **Instructivo Gestión de Activos de información** para identificar y clasificar los activos de información de todos los procesos al interior de la entidad.

– **La Secretaría General de la Alcaldía Mayor de Bogotá** dispone de un inventario de activos de información clasificado bajo los criterios de Confidencialidad, Integridad y Disponibilidad de la información, así como, la clasificación respectiva sobre información pública, información pública clasificada e información pública reservada, el cual es actualizado mínimo una vez al año.

– Todos los servidores públicos, contratistas y proveedores deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su vínculo con la entidad y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de la entidad.

– Es responsabilidad de cada una de las dependencias llevar a cabo la implementación de los controles establecidos con la finalidad de mitigar la materialización de los riesgos identificados y asociados los activos de información.

– Los activos de información que sean asignados a los servidores públicos y contratistas para la ejecución de las funciones u obligaciones durante la relación laboral y/o contractual serán utilizados única y exclusivamente para el desarrollo de lo mencionado.

– Cuando el servidor público o contratista se retire de la Entidad, deberá hacer la respectiva devolución de los activos de información a su cargo donde repose los datos e información que durante su vinculación laboral generó, administró, modificó y custodio para el desarrollo de las funciones u obligaciones asignadas.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC debe implementar el escaneo de medios removibles que son conectados a los equipos de la entidad, para la búsqueda de virus o malware en éstos de manera automática.

– Cuando se solicita el reintegro de un equipo sea de escritorio o portátil al almacén, la Subdirección de Servicios Administrativos notificará a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC a través de una solicitud registrada en el sistema de gestión de servicios GLPI para que se realice el borrado seguro de la información.

– Para los medios electromagnéticos y/o digitales donde haya reposado información considerada como información pública clasificada o pública reservada, y así mismo, la información que el servidor público, contratista o proveedor haya producido en el marco de sus funciones y obligaciones, deben ser borrados, eliminados y/o destruidos de forma segura cuando cambien de propósito o sean devueltos por garantía o cuando termine su vida útil.

12.1.10 Control 5.10 - Uso aceptable de la información y otros activos asociados

Es responsabilidad de cada una de las dependencias llevar a cabo la implementación de los controles establecidos con la finalidad de mitigar la materialización de los riesgos identificados y asociados los activos de información.

– Los activos de información que sean asignados a los servidores públicos y contratistas para la ejecución de las funciones u obligaciones durante la relación laboral y/o contractual serán utilizados única y exclusivamente para el desarrollo de lo mencionado.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC debe implementar el escaneo de medios removibles que son conectados a los equipos de la entidad, para la búsqueda de virus o malware en éstos de manera automática.

– Para los medios electromagnéticos y/o digitales donde haya reposado información considerada como información pública clasificada o pública

reservada, y así mismo, la información que el servidor público, contratista o proveedor haya producido en el marco de sus funciones y obligaciones, deben ser borrados, eliminados y/o destruidos de forma segura cuando cambien de propósito o sean devueltos por garantía o cuando termine su vida útil.

12.1.11 Control 5.11 - Devolución de activos

Todos los servidores públicos, contratistas y proveedores deben hacer devolución de los activos de información que se encuentran bajo su custodia al terminar su vínculo con la entidad y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de la entidad.

– Cuando se solicita el reintegro de un equipo sea de escritorio o portátil al almacén, la Subdirección de Servicios Administrativos notificará a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC a través de una solicitud registrada en el sistema de gestión de servicios GLPI para que se realice el borrado seguro de la información.

12.1.12 Control 5.12 - Clasificación de la información

La Secretaría General de la Alcaldía Mayor de Bogotá dispone de un inventario de activos de información clasificado bajo los criterios de Confidencialidad, Integridad y Disponibilidad de la información, así como, la clasificación respectiva sobre información pública, información pública clasificada e información pública reservada, el cual es actualizado mínimo una vez al año.

12.1.13 Control 5.13 - Etiquetado de la información

La información institucional deberá clasificarse y etiquetarse de acuerdo con su nivel de sensibilidad, criticidad y requisitos legales.

12.1.14 Control 5.14 - Transferencia de la información

La Entidad establece controles para la transferencia de información, tanto interna como externa, garantizando que se realice mediante mecanismos autorizados y seguros que preserven su confidencialidad, integridad y disponibilidad.

– Los servidores públicos, contratistas, proveedores deberán firmar compromisos de confidencialidad cuando requieran conocer o intercambiar

información definida como pública clasificada o pública reservada de la Entidad.

– Todo servidor público, contratista y tercero será responsable por proteger la confidencialidad e integridad de la información. Se debe tener especial cuidado con el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

– Los propietarios de la información que se requiera intercambiar son responsables de definir los niveles y perfiles de autorización para el acceso, modificación y eliminación de ésta, garantizando siempre la privacidad de los datos e información, y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de Confidencialidad, Integridad y Disponibilidad requeridos.

– En caso de realizar transferencia de información donde se incluyan datos personales, se debe dar cumplimiento a lo establecido en la Ley N° 1581 de 2012 y normativa reglamentaria vigente.

– Se deberán establecer controles de seguridad en las transferencias de información definida como pública clasificada o pública reservada.

– La información definida como pública clasificada o pública reservada que deba ser transferida deberá contar con autorización por parte del propietario de la información o jefe de dependencia responsable del activo de información.

– La información transferida a entidades externas debe regirse bajo lo establecido por el Decreto 235 de 2010 “Intercambio de información entre Entidades” y/o normatividad vigente.

12.1.15 Control 5.15 - Control de acceso

La Secretaría General define reglas y criterios para el control de acceso a la información y a los sistemas, garantizando que solo las personas autorizadas accedan a los activos de información, de acuerdo con sus funciones y responsabilidades.

- La Oficina de Tecnologías de la información y las Comunicaciones deberá realizar la revisión de las novedades relacionadas con usuarios que sean informadas por la Dirección de Talento Humano y/o la Dirección de Contratación, acorde con la vinculación o desvinculación del personal a la Entidad.

- La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** deberá implementar perímetros de seguridad física y lógica para la protección de las instalaciones, especialmente aquellas clasificadas como áreas seguras; tales como los centros de procesamiento de información, áreas de almacenamiento de información física y lógica, cuartos técnicos, Despacho del alcalde, entre otras.

Responsabilidades de la Administración

- La información de naturaleza pública de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** estará disponible para los servidores públicos, contratistas y/o proveedores, siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.

- La Oficina de Tecnologías de la información y las Comunicaciones establecerá controles para que sólo los servidores públicos, contratistas y/o proveedores responsables de la actualización de los datos e información puedan acceder a su modificación, incorporando los nuevos datos que se produzcan.

- El acceso tanto a los datos e información como a las aplicaciones y sistemas de información será restringido conforme a los roles y responsabilidades asignados a cada uno de los servidores públicos, contratistas y proveedores de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

- Como responsables de los datos e información las partes interesadas deberán administrar y hacer cumplir los controles de seguridad digital, seguridad y privacidad de la información establecidos en el presente documento, con el fin de evitar accesos no autorizados, pérdidas y/o utilización indebida de los datos e información almacenados en los activos de información.

- Es responsabilidad de cada una de las dependencias la solicitud sobre la creación del recurso compartido (carpeta de almacenamiento en la nube) y así mismo, la solicitud a nivel de seguridad y privacidad de la información que requiere sobre el recurso compartido solicitado.

- Es responsabilidad de los propietarios de los activos realizar revisiones periódicas y depuraciones de los accesos asignados a las cuentas de usuarios a intervalos regulares.

- Es responsabilidad de los jefes de dependencias u oficinas brindar la autorización para el acceso en horarios no labores de personal externo a la entidad.

- La responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC se basa en el establecimiento y aplicación de controles de seguridad y privacidad de la información para los recursos de red compartidos, sistemas de información y servicios de la Entidad.

- Las cuentas de correos electrónicos que se creen para funcionarios y/o contratistas deben tener habilitado el doble factor de autenticación, con el fin de evitar la materialización de riesgos asociados a la suplantación de identidad.

- En caso de requerirse accesos privilegiados a los recursos tecnológicos para servidores públicos o contratistas, estos deben ser autorizados por los jefes de las dependencias u oficinas de la entidad.

- Las dependencias responsables de las áreas seguras; Datacenter, cuartos técnicos, Despacho del Alcalde, entre otras, deberán asignar los controles de seguridad necesarios para limitar el acceso a personal no autorizado. Se podrá tener en cuenta la siguiente información:

    - Datos de identificación servidor público, contratista o proveedor que accede al área restringida
    - El motivo del ingreso
    - El tiempo empleado para el desarrollo de la actividad

- La información consultada (si aplica)

– Para el acceso a las áreas identificadas como seguras, siempre las personas deberán estar acompañadas de personal autorizado.

– En caso de que existan servicios de la entidad identificados con usuarios genéricos, (ej. Correo electrónico), debe asignarse un responsable al mismo.

Responsabilidades de los usuarios

– Los servidores públicos, contratistas y proveedores de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** son responsables de velar por la Confidencialidad, Integridad y Disponibilidad de los activos de información de la entidad, asegurándose que éstos sólo sean utilizados para el desarrollo de las labores encomendadas.

– Todos los servidores públicos, contratistas y proveedores cuentan con un usuario y contraseña único, personal e intransferible y asumen la responsabilidad de los eventos e incidentes que puedan ocurrir bajo su autenticación sobre los activos de información asignados. A continuación, se detallan los siguientes lineamientos a tener en cuenta:

- No divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la contraseña de acceso asignada para el acceso a la plataforma tecnológica, correo electrónico, dispositivos, bases de datos, equipos de cómputo, servidores, aplicaciones, sistemas de información y similares.
- Cambiar la contraseña en intervalos de tiempo regulares.
- Construir contraseñas seguras que incluyan como mínimo:
- 1 carácter especial.
- 1 carácter en Mayúscula.
- 1 carácter numérico.
- Debe contener una longitud mínima de 8 Caracteres.
- No utilizar contraseñas de fácil identificación, ejemplo años de nacimiento, nombres de hijos.

- La contraseña no pude ser el mismo usuario.
- No escribir la contraseña en medios físicos, digitales y/o electrónicos.

– Es responsabilidad de todos los servidores públicos y contratistas portar el carnet en un lugar visible dentro de las instalaciones de la entidad.

– Todos los servidores públicos y contratistas que soliciten acceso a los servicios internos de la entidad por VPN deben remitir el formato 4204000-FT-1000 Solicitud de Servicios TIC, el cual debe estar debidamente justificado y aprobado por el jefe de la dependencia. Así como, firmar el documento de compromiso de confidencialidad.

Controles para la gestión de accesos

Respecto al acceso a redes y servicios de red

– Los equipos de terceros que requieran acceder a la red de la Entidad deben cumplir con lo descrito en el documento **2213200-PR-101 Gestión de Incidentes, Requerimientos y Problemas Tecnológicos**.

– Los contratistas o terceros deben garantizar que su equipo se encuentra libre de posibles amenazas que atenten contra la confidencialidad, integridad y disponibilidad de los datos e información que administren, procesen, generen, modifican y utilizan en la Entidad.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC es la dependencia encargada de verificar el uso y funcionamiento de la red, y de conceder los accesos a la red inalámbrica, estableciendo mecanismos de control para proteger la infraestructura y los datos e información de la Entidad.

– Sólo personal autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC realizará actividades de administración remota a dispositivos móviles, equipos de escritorio o portátiles, equipos de infraestructura y de procesamiento de información de la **Secretaría General de la Alcaldía General de Bogotá D.C.**

- No está permitido el uso de aplicaciones y servicios interactivos como: Team Viewer, TightVNC, RemoteVNC, Chrome Remote Desktop, Join.me, Ammy Admin, Putty, WinSCP, Screen Leap, Vyew, Croos Loop, Skype y similares.

- La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC cuenta con la facultad para bloquear todos aquellos sitios de Internet que no son compatibles con las labores de los servidores públicos, contratistas y proveedores y puedan generar un riego para la entidad.

- No está permitido el uso e ingreso a paginas relacionas con pornografía, drogas, terrorismo, segregación racial, hacking, juegos y similares que promuevan y atenten contra los principios de Confidencialidad, Integridad, Disponibilidad y Privacidad de los datos e información institucional.

- El acceso a servicios de música, videos, chat y redes sociales deberá ser controlado por la Oficina de Tecnologías de la Información y las Comunicaciones, y su utilizacióndebe ser solicitado, autorizado y justificado por el jefe de la dependencia.

- No está permitido el uso y conexión de dispositivos alternos que provean servicio a internet y/o configurar los dispositivos de la Entidad para el acceso a estos medios alternos, con excepción de los autorizados para la red **CADE y SUPERCADE**.

- No está permitido el uso de cuentas de usuario de otros servidores públicos para el ingreso a páginas de internet a las cuales no tiene permisos con el usuario asignado.

- El uso de Internet está permitido exclusivamente para actividades institucionales. El uso de internet se medirá de manera mensual para conocer los sitios con mayor visita y tomar acciones preventivas para minimizar la llegada de correos maliciosos a la Entidad

Respecto al Registro y Cancelación de Usuarios

– Para las novedades relacionadas con registro y cancelación de usuarios se debe solicitar autorización al jefe inmediato o supervisor del contrato realizando el diligenciamiento del formato **4204000-FT-1000 Solicitud de Servicios TIC.**

– La entrega de las credenciales del usuario (cuenta y contraseña de red), se entrega a través de la mesa de servicio, donde se entrega al usuario y una contraseña genérica, la cual debe ser cambiada por el usuario.

– Todos los servidores públicos, contratistas y/o terceros tendrán un identificador único (ID del usuario) para su uso personal e intransferible que les permita acceder y hacer buen uso de los datos e información, sistemas de información e instalaciones.

Respecto al acceso a sistemas y aplicaciones

– La creación de usuarios en los sistemas de información se encuentra a cargo de los líderes funcionales o la dependencia que administre o tenga el control correspondiente de estos.

– Se debe mantener el acceso limitado y controlado a los datos e información que se encuentran en los sistemas de información y aplicaciones ubicados en los ambientes de desarrollo y producción.

– Se debe controlar el acceso al código fuente de los programas, sistemas de información y el software desarrollado por la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** y también llevar el respectivo control de los cambios autorizados y realizados a los códigos fuente, lo cual se debe realizar y controlar a través de la herramienta GitLab.

12.1.16 Control 5.16 - Gestión de la identidad

La Entidad deberá establecer procedimientos para el registro, modificación y baja de usuarios, así como para la asignación, revisión y revocación de derechos de acceso, asegurando que estos se mantengan actualizados y controlados.

12.1.17 Control 5.17 - Información de autenticación

La Secretaría General implementa mecanismos de autenticación adecuados que permiten verificar la identidad de los usuarios y la integridad de la información, conforme a los riesgos identificados.

12.1.18 Control 5.18 - Derechos de acceso

Los derechos de acceso se asignan, revisan y ajustan periódicamente de acuerdo con las novedades reportadas, asegurando que los usuarios cuenten únicamente con los permisos necesarios para el desempeño de sus funciones.

12.1.19 Control 5.19 - Seguridad de la información en la relación con proveedores

La Secretaría General establece políticas y lineamientos de seguridad de la información aplicables a las relaciones con proveedores y terceros que accedan o gestionen información institucional.

– La **Secretaría General de la Alcaldía Mayor de Bogotá D.C**. deberá establecer dentro de los estudios previos que los proveedores deben contar con los controles mínimos de seguridad cuando en la contratación se establezca acceso por parte de estos a los activos de información de la entidad.

– La Dirección de Contratación debe solicitar el Visto Bueno (Aval) de la Oficina de Tecnologías de la Información y las Comunicaciones en los procesos de contratación relacionados con la adquisición de bienes y servicios de tecnología, así como, el desarrollo, implementación y mantenimiento de software y/o hardware y todo aquello que corresponde a la inversión en tecnologías de la información para la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

– Se deben identificar los riesgos de seguridad de la información en la contratación con proveedores especialmente si estos tienen acceso o

gestionan activos de información de la entidad.

– Se deben establecer los respectivos acuerdos de niveles de servicios con los proveedores especialmente cuando se vea afectada la disponibilidad de los activos de información gestionados por este como objeto del contrato suscrito con la entidad.

– Se debe incluir dentro de los estudios previos el cumplimiento de las políticas de seguridad y privacidad de la información de la entidad.

– El supervisor del contrato deberá realizar el respectivo seguimiento y verificación del cumplimiento de los requisitos de seguridad de la información contemplados en el contrato suscrito por el proveedor con la entidad.

– Se deberá firmar un acuerdo o compromiso de confidencialidad con los proveedores sin importar la modalidad de contratación, especialmente con los proveedores que tengan acceso a los activos de información de la entidad.

– Los proveedores que cuenten con personal externo laborando en las instalaciones de la Secretaría General de la Alcaldía Mayor de Bogotá deberá suscribir acuerdos o compromisos de confidencialidad con el personal a cargo conforme al objeto del contrato suscrito con la entidad.

– Las partes interesadas de la Entidad deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos que ejecute la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

12.1.20 Control 5.20 - Abordar la seguridad de la información en los acuerdos con los proveedores

Los contratos con terceros deberán incluir cláusulas específicas sobre seguridad de la información, protección de datos personales, confidencialidad y responsabilidades frente a incidentes de seguridad.

– Dentro de los acuerdos de servicios con terceras partes se debe incluir una

cláusula, la cual autorice a la **Secretaría General de la Alcaldía Mayor de Bogotá D.C**. a realizar auditoria para validar los controles utilizados por los terceros para el manejo de la información.

– La Entidad debe contar con la respectiva identificación y documentación del proveedor con el cual la Entidad va a tener o tiene una relación contractual.

– Realizar acuerdos de Confidencialidad con relación a transferencias de la información cuando sea requerido.

– Se debe mantener un proceso y un ciclo de vida para la gestión de las relaciones con el proveedor que contemple:

– La definición de los tipos de acceso a la información que se permitirá al proveedor, el seguimiento, y el control del acceso.

– Los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso.

12.1.21 Control 5.21 - Gestión de la seguridad de la información en la cadena de suministro

La Entidad deberá gestionar los riesgos asociados a la cadena de suministro de tecnologías de la información y a los servicios en la nube, estableciendo mecanismos de monitoreo, revisión y gestión de cambios con proveedores de servicios.

– Cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la Entidad, debe haber cumplido con las autorizaciones respectivas y además contar los acuerdos o compromisos de confidencialidad respectivos debidamente firmados.

– Se debe gestionar el manejo de incidentes y contingencias asociadas con el acceso del proveedor, la resiliencia, y si son necesarias, las disposiciones sobre recuperación y contingencias, para asegurar la disponibilidad de la información o el procesamiento de la información suministrada por cualquiera de las partes.

12.1.22 Control 5.22 - Seguimiento, revisión y gestión de cambios de servicios de proveedores

La Entidad deberá monitorear, revisar y gestionar los cambios en los servicios prestados por proveedores, asegurando que no se afecte la seguridad de la información.

– Se debe permitir la auditabilidad sobre el cumplimiento de los procesos y procedimientos para hacer seguimiento del cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso.
– Al momento de terminar las relaciones contractuales con un tercero el cual maneje información de la Entidad, el tercero debe destruir de una manera adecuada la información o en su debido defecto devolver la información, proceso que deberá estar incluido en el contrato con el tercero.

12.1.22 Control 5.22 - Seguridad de la información para el uso de servicios en la nube

La Secretaría General deberá establecer lineamientos específicos para el uso seguro de servicios en la nube, garantizando el cumplimiento de los controles de seguridad, privacidad y continuidad definidos por la Entidad.

12.1.24 Control 5.24 - Planificación y preparación de la gestión de incidentes de SI.

La Secretaría General cuenta con responsabilidades y procedimientos para la evaluación, decisión y respuesta frente a eventos e incidentes de seguridad de la información, garantizando una actuación oportuna y coordinada.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC debe gestionar los eventos e incidentes de seguridad conforme lo descrito en el documento **424000-GS-042 Guía de gestión de incidentes de seguridad y privacidad de la información y gestión de vulnerabilidades.**

12.1.25 Control 5.25 - Evaluación y decisión sobre los eventos de SI.

La Secretaría General a través del oficial de seguridad de la información evalúa los eventos de seguridad y decide oportunamente si constituyen incidentes, definiendo las acciones de respuesta correspondientes.

– Se deben establecer las categorías de los incidentes de seguridad y conforme a la criticidad, y los mecanismos de atención adecuados para su solución.

12.1.26 Control 5.26 - Respuesta a incidentes de SI.

La Entidad implementa mecanismos para responder a incidentes de seguridad de la información de manera oportuna y coordinada, minimizando su impacto.

12.1.27 Control 5.27 - Aprendiendo de los incidentes de SI

La Secretaría General analiza los incidentes ocurridos y documenta en la herramienta de mesa de servicios las lecciones aprendidas, con el fin de fortalecer los controles y prevenir la recurrencia.

– Se deben tomar acciones correctivas oportunas ante los eventos e incidentes de seguridad reportados, con base en el aprendizaje obtenido en la gestión de incidentes de seguridad de la información en la Entidad.

12.1.28 Control 5.28 - Recopilación de pruebas

La Entidad deberá garantizar la recopilación, preservación y custodia de evidencias relacionadas con incidentes de seguridad de la información, conforme a criterios técnicos y legales.

– Cuando se requiera, se deben mantener las evidencias necesarias para establecer el reporte del incidente de seguridad para toda acción de seguimiento contra una persona y/o Entidad. Así mismo se deben contar con los soportes que sean exigidos por una acción legal (sea civil o criminal).

12.1.29 Control 5.29 - Sistemas de información durante la interrupción

La Secretaría General gestiona adecuadamente las interrupciones ocasionadas por incidentes de seguridad, garantizando la continuidad de los servicios críticos.

12.1.30 Control 5.30 - Preparación de las TIC para continuidad del negocio

La Entidad deberá implementar medidas para gestionar interrupciones que afecten la seguridad de la información, articulando la preparación de las TIC con los planes de continuidad del negocio y recuperación ante desastres.

– La Secretaría General de la Alcaldía Mayor de Bogotá D.C. deberá planificar, implementar, verificar, revisar y evaluar el plan de continuidad del negocio y los planes de contingencia basados en el análisis y la valoración de los riegos a los cuales se encuentra expuesta la Entidad.

– Se deberá realizar una identificación de los procesos críticos de la Entidad, llevando a cabo un análisis de impacto para determinar los aspectos más importantes que afectan en la prestación de servicio y continuidad del negocio.

– El Comité Institucional de Gestión y Desempeño deberá asignar el recurso necesario para la ejecución de las pruebas de continuidad del negocio.

– Se deberán establecer responsabilidades para la ejecución y puesta en marcha de los planes de continuidad del negocio

12.1.31 Control 5.31 - Requisitos legales, estatutarios, reglamentarios y contractuales

La Secretaría General identifica, documenta y cumple los requerimientos legales, estatutarios, regulatorios y contractuales aplicables a la seguridad de la información.

– La Entidad debe contar con un normograma en donde se encuentre el detalle de la legislación actual y requisitos contractuales que se aplican al Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI).

12.1.32 Control 5.32 - Derechos de la propiedad intelectual

La Secretaría General protege los derechos de propiedad intelectual asociados a la información, el software y los contenidos institucionales, conforme a la normativa vigente.

– La Secretaría General de la Alcaldía Mayor de Bogotá D.C. debe identificar y garantizar el cumplimiento adecuado a la legislación vigente y/o requisitos legales aplicables (derechos de propiedad intelectual, protección de registros, privacidad y protección de la información de datos personales, reglamentación de controles criptográficos) relacionados con seguridad de la información.

– Se deben definir, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la Entidad que son relevantes para cada sistema de información al menos una vez al año y/o cada vez que estos sean requeridos.

– Se debe asegurar que el software que se instala y se utiliza en la Entidad cumple con los requisitos de derechos de autor, licenciamiento de uso y es original.

– La Oficina Jurídica, Dirección de Contratación y/o la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC deben establecer en los contratos cláusulas donde se obligue a no divulgar la información restringida o confidencial de la Entidad, a su vez a utilizar la información únicamente para el desarrollo el objeto del contrato

12.1.33 Control 5.33 - Protección de registros

La Secretaría General protege los registros institucionales contra pérdida, alteración o acceso no autorizado, garantizando su integridad y disponibilidad.

– Las aplicaciones y sistemas de información de la Entidad deben contar con la implementación de registros de auditoría que permiten establecer la trazabilidad de una operación y/o transacción y sirven como mecanismo para la detección de fallas, posibles eventos de fraude o violaciones a la seguridad.

– Los registros de auditoría de los sistemas y aplicaciones se deben proteger y almacenar por el tiempo definido por los entes de control y vigilancia.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC debe documentar las acciones que realiza en la revisión periódica de logs de auditoría en las aplicaciones y sistemas críticos de la Entidad.

12.1.34 Control 5.34 - Privacidad y protección de PII

La Secretaría General garantiza la protección y privacidad de los datos personales, en cumplimiento de la normativa vigente sobre protección de datos y privacidad.

– La Entidad se rige por la Resolución que se encuentre activa sobre Protección de Datos Personales y la cual se encuentra desarrollada para la aplicabilidad de la Ley de Protección de Datos Personales en Colombia en la ruta: https://secretariageneral.gov.co/sites/default/files/documentos_normativa/2023-12/Politica_General_Tratamiento_Datos_Personales_v3.pdf

12.1.35 Control 5.35 - Revisión independiente

La Secretaría General deberá realizar revisiones independientes periódicas del sistema de seguridad de la información, con el fin de evaluar su eficacia y cumplimiento.

– Los sistemas de información deben ser auditados de manera regular para validar el cumplimiento con los estándares de implementación de la seguridad. Así mismo, con relación a los procedimientos de análisis, desarrollo y mantenimiento de las aplicaciones, se deben realizar revisiones técnicas con lo cual se determina el incumplimiento de los controles establecidos para tomar acciones de mejora sobre éstos.

12.1.36 Control 5.36 - Cumplimiento de políticas, normas y estándares de seguridad

La Entidad verifica periódicamente el cumplimiento de las políticas, normas y estándares de seguridad de la información establecidos.

– La Secretaría General de la Alcaldía Mayor de Bogotá D.C. debe contar con revisiones periódicas para garantizar el cumplimiento de los controles de seguridad frente al marco regulatorio y los objetivos de la Entidad, a través de la programación de auditorías internas y externas en los intervalos planificados.

– El Comité Institucional de Gestión y Desempeño de Secretaría General de la Alcaldía Mayor de Bogotá D.C. debe apoyar y promover las revisiones del cumplimiento de las políticas de seguridad de la información definidas en el presente documento y/o cualquier otro requerimiento de seguridad.

– La Oficina de Control Interno debe realizar revisiones periódicas al cumplimiento de las políticas de revisión y retención de registros de auditoría y elaborar los informes que permiten la toma de acciones oportunas o corregir situaciones no deseables para la seguridad.

12.1.37 Control 5.37 - Procedimientos operativos documentados

La Secretaría General documenta los procedimientos operacionales necesarios para la implementación y control efectivo de la seguridad de la información.

12.2 CONTROLES DE PERSONAS

Este dominio aborda el factor humano como componente crítico de la seguridad de la información, reconociendo que los riesgos pueden materializarse por desconocimiento, error, negligencia o uso indebido de la información.

12.2.1 Control 6.1 Verificación de antecedentes

La Secretaría General aplica, conforme a la normativa vigente, mecanismos de verificación de antecedentes aplicables a servidores públicos, contratistas y terceros que accedan a información o activos críticos, garantizando que dicha verificación sea proporcional al nivel de riesgo asociado a sus funciones.

– Todos los servidores públicos, contratistas y proveedores de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** aceptan las cláusulas de confidencialidad definidas por la entidad antes de asumir su contratación, dicha cláusula hará parte integral en cada uno de los contratos y/o documentos de vinculación a la entidad.

– La Dirección de Talento Humano y la Dirección de Contratación llevan a cabo las respectivas validaciones para la verificación de antecedentes de todos los posibles candidatos a servidor público, contratista y proveedor en concordancia con las leyes, regulaciones y ética relevante.

– Los contratistas y proveedores deben aceptar y firmar los términos y condiciones de su contrato de prestación de servicios, en el cual se establecen las

condiciones contractuales y las de la entidad relacionadas con el cumplimiento del sistema de gestión de seguridad de la información.

– Para los servidores públicos se deberá dar cumplimiento a la obligación que se establece en la posesión de cargo y de acuerdo con lo establecido por la Dirección de Talento Humano en el documento 2211300-PR-221 Gestión Organizacional.

12.2.2 Control 6.2 - Términos y condiciones de empleo

La Entidad asegura que los términos y condiciones de vinculación laboral o contractual incluyan las responsabilidades en materia de seguridad de la información, confidencialidad, uso adecuado de los activos y cumplimiento de las políticas institucionales.

Antes de asumir el empleo

– Todos los servidores públicos, contratistas y proveedores de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. aceptan las cláusulas de confidencialidad definidas por la entidad antes de asumir su contratación, dicha cláusula hará parte integral en cada uno de los contratos y/o documentos de vinculación a la entidad.

– La Dirección de Talento Humano y la Dirección de Contratación llevan a cabo las respectivas validaciones para la verificación de antecedentes de todos los posibles candidatos a servidor público, contratista y proveedor en concordancia con las leyes, regulaciones y ética relevante.

– Los contratistas y proveedores deben aceptar y firmar los términos y condiciones de su contrato de prestación de servicios, en el cual se establecen las condiciones contractuales y las de la entidad relacionadas con el cumplimiento del sistema de gestión de seguridad de la información.

– Para los servidores públicos se deberá dar cumplimiento a la obligación que se establece en la posesión de cargo y de acuerdo con lo establecido por la

Dirección de Talento Humano en el documento 2211300-PR-221 Gestión Organizacional.

Durante la ejecución del empleo

– Todos los servidores públicos, contratistas y proveedores ya sean nuevos o antiguos deben recibir el apropiado conocimiento y capacitación en temas de Seguridad y Privacidad de la Información, Protección de Datos Personales, mínimo una vez al año y/o cuando se considere necesario y deberá ser definido en conjunto entre la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC y la Dirección de Talento Humano.

– **La Secretaría General de la Alcaldía Mayor de Bogotá**, a través de la Dirección de Talento Humano y la Dirección de Contratación, debe contar con un proceso formal y deberá ser comunicado a todos los servidores públicos y contratistas con el fin de emprender las acciones en caso de no dar cumplimiento a las políticas y directrices de seguridad de la información.

12.2.3 Control 6.3 - Concienciación, educación y capacitación en seguridad de la información

La Secretaría General implementa procesos permanentes de concienciación, educación y capacitación en seguridad de la información y seguridad digital, orientados a fortalecer las competencias del personal y a reducir riesgos derivados del factor humano.

12.2.4 Control 6.4 - Proceso disciplinario

La Entidad cuenta con mecanismos disciplinarios que permitan aplicar medidas correctivas frente al incumplimiento de las políticas y lineamientos de seguridad de la información, de conformidad con el régimen disciplinario aplicable.

12.2.5 Control 6.5 - Responsabilidades después de la terminación o cambio de empleo

La Secretaría General asegura que, al finalizar o modificar una relación laboral o

contractual, se mantengan las obligaciones de confidencialidad y protección de la información, y se adopten las medidas necesarias para prevenir accesos no autorizados.

– La Dirección de Talento Humano, la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, la Subdirección de Servicios Administrativos y el Jefe Inmediato del servidor público y/o supervisor tanto del proveedor o contratista, serán los encargados en el proceso de terminación de la vinculación laboral y/o terminación de contratos de asegurar que todos los activos físicos y de información propios de la Entidad sean devueltos, los accesos físicos y lógicos sean eliminados, y los datos e información pertinente sea transferida, de acuerdo con los procedimientos que se encuentran establecidos en la entidad.

– En caso de que un servidor público, contratista y proveedor tenga un cambio de funciones u obligaciones, se deben seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de éstos, acorde con su nuevo rol o contrato de prestación de servicios, asegurando la Seguridad y Privacidad de los Datos e Información.

– Los retiros de los permisos del personal vinculado de manera directa por la entidad o los contratistas o proveedores son informados a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC a través del documento de Paz y Salvo emitido en el momento de la finalización de la relación contractual con la Entidad.

12.2.6 Control 6.6 - Acuerdos de confidencialidad o no divulgación

La Entidad suscribe acuerdos de confidencialidad o no divulgación con servidores públicos, contratistas y terceros, cuando el acceso a información reservada, clasificada o sensible así lo requiera, asegurando su cumplimiento durante y después de la relación contractual.

– Los respectivos acuerdos o compromisos de confidencialidad para el manejo y

no divulgación de los datos e información que se conocen en el desarrollo de las funciones y obligaciones, se establece con la firma y aceptación de conocimiento del presente documento y la respectiva política de seguridad digital de la entidad.

12.2.7 Control 6.7 - Trabajo remoto

La Secretaría General establece lineamientos para el trabajo remoto que garanticen la protección de la información institucional, considerando el uso seguro de dispositivos, redes, accesos remotos y herramientas colaborativas, conforme a los riesgos identificados.

Sobre el teletrabajo

– Las actividades de teletrabajo que se autoricen en la Secretaría General de la Alcaldía Mayor de Bogotá D.C. se podrán llevar a cabo siempre y cuando éstas cumplan con los controles de seguridad que se encuentran definidos y alineados con las políticas de seguridad de la información y los cuales están alineados con lo establecido en el documento **2211300-PR-221 Gestión Organizacional**.

– El teletrabajador debe realizar la conexión a través del canal VPN autorizado por medio del documento **4204000-FT-1000 Solicitud de Servicios TIC** para acceder a los datos e información de la Entidad de una manera segura, con conexión privada y a través del equipo asignado por ésta.

– El teletrabajador debe cumplir a cabalidad con lo establecido en el acuerdo de confidencialidad para el uso de la VPN y el acceso a los datos e información de la Entidad.

– El teletrabajador debe reportar cualquier incidente de seguridad y seguir el documento 4204000-GS-042 Guía de gestión de incidentes de seguridad y privacidad de la información y gestión de vulnerabilidades de los datos e Información establecido en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

– En caso de que ocurra pérdida o hurto de un equipo asignado por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, en el cual se lleven actividades de teletrabajo, será responsabilidad del teletrabajador reportar este evento, de forma inmediata a través de la mesa de servicios o cuenta de correo oticsoporte@alcaldiabogota.gov.co.

– Todos los teletrabajadores, contratistas y terceros deben hacer uso de las herramientas colaborativas designadas por la entidad para la gestión y almacenamiento de la información relacionada con las funciones u obligaciones, con el fin de evitar riesgos de pérdida de disponibilidad de la información. Por otra parte, no deben almacenar definida como información pública clasificada o pública reservada en sus equipos de cómputo personal.

– Toda información gestionada por la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

– Los equipos asignados desde la Entidad a los servidores públicos, contratistas o proveedores deben permanecer sin alteración en las configuraciones para actualización de sistema operativo, aplicativos y antivirus.

– Los contratistas o proveedores que utilicen equipos de su propiedad para el desarrollo de las obligaciones y responsabilidades asignadas por la Entidad, deben comprometerse a mantener los controles de seguridad necesarios (antivirus actualizado, herramientas adicionales de seguridad (cuando aplique)) para garantizar la protección de la información de la entidad. Por otra parte, deben comprometerse a realizar conexiones seguras a través de wifi conocidas y no de acceso gratuito,

– Se deberán establecer por parte de la Oficina de Tecnologías de la Información y las Comunicaciones los mecanismos de seguridad física y lógica a los equipos y documentos que maneje el teletrabajador.

– Es responsabilidad de la Dirección de Talento Humano informar a la

Subdirección de Servicios Administrativos las personas autorizadas en teletrabajo para que se asignen los recursos necesarios para ello. Si el teletrabajador utiliza equipos personales, el manejo de los datos e información será responsabilidad directa del servidor público ante la pérdida de confidencialidad, integridad y disponibilidad de los datos e información a su cargo.

– Antes de llevar a cabo cualquier actividad de teletrabajo se definirán entre la Entidad y el servidor público, los alcances de las actividades a desarrollar y la información a acceder, así como los sistemas y servicios de la Entidad que se utilizarán.

– Los permisos para el acceso a los servicios y sistemas de información serán establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC definiendo los accesos solicitados a partir del documento **4204000-FT-1000 Solicitud de Servicios TIC** y los cuales deben ser autorizados por el jefe directo o quien haga sus veces.

– Para los temas de trabajo remoto relacionados con contratistas o proveedores de la Entidad, las actividades a desarrollar, los datos e información a consultar, aplicaciones y sistemas de información a acceder y los servicios a utilizar, se definirán entre los respectivos supervisores del contrato y los contratistas y proveedores a través de lo descrito en el documento **4204000-FT-1000 Solicitud de Servicios TIC.**

12.2.8 Control 6.8 - Reporte de eventos de seguridad de la información

La Entidad promueve y facilita el reporte oportuno de eventos de seguridad de la información por parte de servidores públicos, contratistas y terceros, garantizando que estos conozcan los canales y procedimientos establecidos para tal fin.

– La mesa de servicios debe estar disponible para el reporte formal de eventos o incidentes de seguridad y privacidad de la información que sean posiblemente sospechosos, los cuales son reportados por los servidores públicos, contratistas y proveedores de la entidad a través del correo de

soporte para ser registrados en la herramienta de gestión y escalados al Oficial de Seguridad de la Información o quien haga sus veces.

– Todos los servidores públicos, contratistas y proveedores de la Entidad deben realizar el reporte de eventos posiblemente sospechosos como incidentes de seguridad y privacidad de la información a través de la mesa de servicios directamente por la herramienta de gestión o por medio de la cuenta de correo: oticsoporte@alcaldiabogota.gov.co.

– Es deber de todos los servidores públicos, contratistas y proveedores usuarios de los sistemas y servicios de información, reportar cualquier evento o incidente que atente contra la seguridad de los activos de información.

12.3 CONTROLES FÍSICOS

Este dominio establece los lineamientos para proteger las instalaciones, equipos y entornos físicos que soportan los activos de información de la Secretaría General, con el fin de prevenir accesos no autorizados, daños, pérdidas o interrupciones que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

12.3.1 Control 7.1 - Perímetros de seguridad física

La Secretaría General define y mantiene perímetros de seguridad física en las instalaciones donde se encuentren activos de información críticos, estableciendo controles que prevengan accesos no autorizados y protejan las áreas sensibles frente a amenazas internas y externas.

– Las puertas de acceso a cada una de las dependencias, oficinas, salas de capacitación y similares deben permanecer cerradas bajo ausencias temporales. El acceso a estas áreas debe ser únicamente a personal debidamente autorizado.

– Los respectivos centros de cableado, data center y cuartos técnicos en general deben permanecer cerrados y con acceso restringido para personal no autorizado.

- No se debe consumir alimentos ni bebidas en las áreas seguras; Datacenter y centros de cableado de la entidad.

- Se deberán controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas.

- Los equipos deberán estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades de acceso no autorizado.

- Se deberán proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

- Para el retiro de equipos, información o software de la entidad, se debe contar con una autorización previa del propietario de los activos de información.

12.3.2 Control 7.2 - Controles de acceso físico

La Entidad implementa controles de acceso físico a edificios, oficinas, centros de datos y áreas restringidas, asegurando que solo el personal autorizado pueda ingresar, de acuerdo con sus funciones y niveles de responsabilidad.

Respecto al acceso físico

- Todos los servidores públicos, contratistas y proveedores de la Secretaría General deben portar el carnet en un lugar visible y hacer uso de la tarjeta de proximidad durante su permanencia en las instalaciones de la Entidad.

- Para el control de ingreso de terceros (visitantes) se debe entregar un sticker, para su identificación dentro de las instalaciones de la entidad, el cual es devuelto por el tercero al retirarse de la Entidad.

- Todas las áreas destinadas al procesamiento y/o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas seguras y en consecuencia deben

contar con controles adecuados para el control de acceso.

– El ingreso a los datacenter de la Entidad se debe realizar a través de la tarjeta de proximidad y con bitácora de ingreso de visitantes. Los visitantes deben ingresar solamente en compañía de una persona del grupo de infraestructura tecnológica de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

12.3.3 Control 7.3 - Seguridad de oficinas, salas e instalaciones

La Secretaría General adopta medidas de seguridad física en oficinas, salas técnicas e instalaciones, orientadas a proteger los activos de información frente a riesgos como intrusión, vandalismo, robo o daños accidentales.

12.3.4 Control 7.4 - Monitoreo de la seguridad física

La Entidad cuenta con mecanismos de monitoreo de la seguridad física, tales como sistemas de vigilancia, alarmas u otros controles, que permitan detectar oportunamente eventos que puedan comprometer la seguridad de las instalaciones y activos.

12.3.5 Control 7.5 - Protección contra amenazas físicas y ambientales

La Secretaría General implementa medidas de protección frente a amenazas físicas y ambientales, incluyendo incendios, inundaciones, fallas eléctricas y otras condiciones que puedan afectar la infraestructura y los activos de información.

– Los centros de cómputo, cableado y cuartos técnicos de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. deben contar con mecanismos adecuados contra las amenazas ambientales: temperatura, humedad, fuego, entre otras especificados por los fabricantes de los equipos que se custodian.

– No se permite custodiar, mantener y/o guardar elementos inflamables dentro de las áreas destinadas al procesamiento o almacenamiento de información, así como, aquellas en las que se encuentren los equipos y demás

infraestructura de soporte a los sistemas de información y comunicaciones.

12.3.6 Control 7.6 - Trabajo en áreas seguras

El acceso y trabajo en áreas seguras es restringido al personal autorizado, y las actividades realizadas en estas áreas deberán ser supervisadas y registradas cuando sea necesario, garantizando el cumplimiento de los lineamientos de seguridad establecidos.

12.3.7 Control 7.7 - Escritorio limpio y pantalla limpia

La Entidad promueve prácticas de escritorio limpio y pantalla limpia, asegurando que la información sensible no quede expuesta en áreas de trabajo, especialmente en espacios compartidos o de acceso público.

– Los servidores públicos, contratistas y proveedores que tengan un vínculo laboral con la Secretaría General de la Alcaldía Mayor de Bogotá deben mantener la información pública clasificada o pública reservada bajo llave en sus escritorios y/o sitios de trabajo, sea cuando se retiren temporalmente de sus puestos de trabajo o en horas no laborales. Estos documentos incluyen: documentos impresos, dispositivos de almacenamiento, medios removibles en general y similares.

- Se deberá eliminar cualquier información que sea gestionada en equipos que han sido prestados en la entidad, una vez estos sean devueltos.
- Los gabinetes o archivos de gestión donde se almacena información pública clasificada o pública reservada deben estar debidamente asegurados.
- Las salas y áreas de reuniones deben quedar libres una vez se termine de usarlas.
- No se debe hacer uso de documentos que contengan información pública clasificada o pública reservada como papel reciclable.

– En las estaciones de trabajo propias de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** se debe usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente una vez se bloquee la

estación o después de cinco (5) minutos de inactividad, la cual se podrá desbloquear únicamente con la contraseña del usuario.

12.3.8 Control 7.8 - Ubicación y protección del equipo

La Secretaría General garantiza que los equipos que procesan o almacenan información institucional están ubicados y protegidos adecuadamente, minimizando riesgos de acceso no autorizado, daño físico o pérdida.

Respecto a la ubicación y protección de los equipos

– Se debe contar con la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.

– Las identificaciones del equipo de escritorio o equipo portátil en la red indican la red a la cual está autorizado a conectarse y debe estar conectado a una única red. En caso de ser necesario, es importante considerar la protección física del equipo.

– Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

– A través de la consola antivirus se debe garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el Administrador de Red y/o el personal de soporte de hardware y/o software que requiere el acceso.

12.3.9 Control 7.9 - Seguridad de los activos fuera de las instalaciones

La Entidad establece controles para proteger los activos de información que se encuentren fuera de las instalaciones institucionales, tales como dispositivos móviles o equipos portátiles, asegurando su uso seguro y autorizado.

– Los servidores públicos, contratistas y proveedores que utilizan los equipos institucionales, se comprometen a no divulgar los datos e información de la

Entidad al firmar el documento **4204000-FT-1000 Solicitud de Servicios TIC**.

– Al momento de realizar el retiro de los equipos portátiles de la Entidad se debe diligenciar el formato **42331000-FT-311 Autorización de salida de elementos de la Subdirección de Servicios Administrativos.**

– No se permite retirar y/o sacar entre dependencias o fuera de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. los activos de información, sin previa autorización del propietario de estos.

12.3.10 Control 7.10 - Medios de almacenamiento

La Secretaría General define lineamientos para la protección, uso, transporte y eliminación segura de medios de almacenamiento que contienen información institucional, evitando accesos no autorizados o fugas de información.

12.3.11 Control 7.11 - Servicios de apoyo

La Entidad deberá garantizar que los servicios de apoyo (energía, climatización, comunicaciones, entre otros) que soportan los activos de información cuenten con medidas de seguridad y continuidad adecuadas para evitar interrupciones del servicio.

12.3.12 Control 7.12 - Seguridad del cableado

La Secretaría General protege el cableado de energía y comunicaciones contra interceptación, daño o interferencia, especialmente en áreas críticas o de acceso restringido.

– El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información deben permanecer protegidos a través de canaleta para evitar el deterioro y disponibilidad del servicio.

– Los equipos y componentes de los centros de cómputo, cableado y cuartos técnicos deben estar debidamente marcados para reducir riesgos por

manipulación.

12.3.13 Control 7.13 - Mantenimiento del equipo

La Entidad asegura que el mantenimiento de los equipos se realice de forma controlada y segura, por personal autorizado, garantizando que no se comprometa la seguridad de la información durante dichas actividades.

– La infraestructura tecnológica debe contar con estándares de seguridad (hardening), para su respectivo funcionamiento.

– Durante las actividades de mantenimiento correctivo se debe mantener la concordancia con los intervalos y especificaciones del proveedor, así mismo, se deben generar los registros a que haya lugar en donde se realiza la trazabilidad de las fallas, personas involucradas y actividades desarrolladas.

12.3.14 Control 7.14 - Eliminación o reutilización segura del equipo

La Secretaría General implementa procedimientos para la eliminación o reutilización segura de equipos que hayan contenido información institucional, asegurando la destrucción o borrado seguro de los datos antes de su disposición final.

– Todos los equipos que contengan información definida como pública clasificada o pública reservada en sus medios de almacenamiento deben pasar por un procedimiento de borrado seguro, antes de su reutilización o finalización de su vida útil, el cual es validado de manera aleatoria por el oficial de seguridad o quien haga sus veces.

– La información definida como pública clasificada o pública reservada de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. se debe recoger de las impresoras de manera inmediata una vez es impresa.

– Los servidores públicos, contratistas y proveedores no deben realizar cambios

en los equipos de escritorio o portátiles que les sean asignados. Estos cambios son realizados únicamente por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

12.4 CONTROLES TECNOLÓGICOS

Este dominio establece los lineamientos para proteger los sistemas de información, plataformas tecnológicas, redes, aplicaciones y servicios digitales que soportan la gestión institucional de la Secretaría General, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de la información durante todo su ciclo de vida.

12.4.1 Control 8.1 - Dispositivos de usuario final

La Secretaría General establece lineamientos para el uso seguro de dispositivos de usuario final, garantizando que estos cuenten con configuraciones adecuadas de seguridad, control de accesos y protección contra software malicioso, conforme a los riesgos identificados.

12.4.2 Control 8.2 - Derechos de acceso privilegiado

La Entidad gestiona de forma controlada los accesos privilegiados a sistemas y plataformas tecnológicas, asegurando su asignación, uso y revisión periódica, con el fin de prevenir accesos indebidos o abusos de privilegios.

12.4.3 Control 8.3 - Restricción de acceso a la información

La Secretaría General implementa mecanismos tecnológicos que restrinjan el acceso a la información y a los sistemas, conforme a los perfiles de usuario, roles y niveles de autorización definidos a nivel organizacional.

12.4.4 Control 8.4 - Acceso al código fuente

La Entidad protege el acceso al código fuente de aplicaciones y sistemas, garantizando que solo el personal autorizado pueda acceder, modificar o desplegar cambios, y que dichas actividades sean registradas y controladas.

12.4.5 Control 8.5 - Autenticación segura

La Secretaría General implementar mecanismos de autenticación segura para el acceso a sistemas y servicios, considerando el uso de contraseñas robustas, autenticación multifactor u otros mecanismos acordes al nivel de riesgo.

12.4.6 Control 8.6 - Gestión de la capacidad

La Entidad gestiona la capacidad de los sistemas y servicios tecnológicos, asegurando que estos cuenten con los recursos necesarios para operar de manera segura y continua, evitando degradaciones que puedan afectar la disponibilidad.

– Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC monitorear, revisar, proyectar y dar soporte oportuno para el uso y desempeño aceptable de capacidad sobre la infraestructura tecnológica.

12.4.7 Control 8.7 - Protección contra malware

La Secretaría General implementa controles tecnológicos para prevenir, detectar y mitigar software malicioso, incluyendo el uso de herramientas de protección, actualizaciones periódicas y monitoreo continuo.

– Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC que todos los activos de información tipo Hardware cuenten con un sistema de antivirus y antispyware instalado y actualizado activamente para la protección contra códigos maliciosos.

– Los equipos de terceros que son autorizados para conectarse a la red de datos de la Entidad deben contar con las medidas de seguridad apropiadas para la gestión, administración, modificación y custodia de los datos e información de la Entidad.

- Únicamente el administrador de la plataforma de antivirus debe contar con los permisos necesarios para deshabilitar, remover, eliminar y/o desinstalar el software de antivirus.

- Se deben realizar escaneos a intervalos regulares como control del estado de la infraestructura tecnológica

- Los servidores públicos, contratistas y proveedores que cuenten con equipos de escritorio y/o portátiles asignados por la Entidad no realizarán cambios en la configuración del software de antivirus instalado.

- Ante cualquier sospecha o detección de alguna infección por software malicioso se debe notificar a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC a través de la mesa de servicios para que se tomen las medidas de control correspondientes.

- Para las carpetas compartidas en red se deberán asignar los respectivos permisos de acceso al servidor público, contratista o proveedor únicamente a la información que este se encuentre autorizado por medio del documento **4204000-FT-1000 Solicitud de Servicios TIC.**

- Los permisos deberán ser asignados a través de los grupos que están creados en el Directorio Activo para el funcionamiento en Secretaría General de la Alcaldía Mayor de Bogotá D.C.

12.4.8 Control 8.8 - Gestión de vulnerabilidades técnicas

La Entidad identifica, evalúa y trata las vulnerabilidades técnicas de los sistemas de información, priorizando su atención según el nivel de riesgo y manteniendo evidencia de las acciones realizadas.

- Se deben realizar análisis de vulnerabilidades en intervalos programados sobre los servicios críticos de la infraestructura tecnológica para evaluar los riesgos a los cuales se encuentran expuestos.

- A todos los sistemas de información y/o servicios o servidores que se vayan a implementar en el entorno de producción, se les debe realizar el respectivo análisis de vulnerabilidades.

12.4.9 Control 8.9 - Gestión de configuraciones

La Secretaría General define y mantiene configuraciones seguras para los sistemas, redes y dispositivos, controlando los cambios y evitando configuraciones no autorizadas que puedan comprometer la seguridad.

12.4.10 Control 8.10 - Eliminación de información

La Entidad garantiza la eliminación segura de la información cuando ya no sea requerida, utilizando mecanismos tecnológicos que impidan su recuperación no autorizada.

12.4.11 Control 8.11 - Enmascaramiento de datos

La Secretaría General deberá aplicar técnicas de enmascaramiento de datos cuando sea necesario proteger información sensible, especialmente en entornos de prueba, desarrollo o análisis.

12.4.12 Control 8.12 - Prevención de fuga de información

La Entidad implementa controles tecnológicos para prevenir la fuga de información, incluyendo restricciones de copia, transferencia y uso de canales no autorizados.

12.4.13 Control 8.13 - Copias de seguridad

La Secretaría General realiza copias de seguridad de la información y de los sistemas críticos, asegurando su integridad, disponibilidad y recuperación oportuna ante incidentes o fallas.

- La Secretaría General de la Alcaldía Mayor de Bogotá D.C debe documentar el proceso de copias de respaldo y recuperación de la información de valor de la entidad.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe realizar el respaldo de los activos de información de acuerdo con lo definido en el proceso documentado de copias de respaldo y recuperación.

- Se deberá realizar respaldo a todos los sistemas de información y/o servicios identificados como críticos en la entidad.

- Es responsabilidad del servidor público, contratista o tercero realizar el respaldo de la información que se encuentre almacenada en equipos de cómputo, portátiles o dispositivos móviles de la entidad o personales.

- En caso de que se requiera realizar respaldo de la información digital o electrónica por parte de los funcionarios o contratista de las dependencias, estás deben ser solicitadas en la mesa de servicios de TI. Si la información a respaldar corresponde a información de la dependencia, debe ser autorizado por el jefe de la dependencia.

- Los servidores públicos y contratistas deben hace uso de las herramientas colaborativas dispuestas por la entidad para realizar el respaldo de la información de los procesos.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe llevar una bitácora de las copias de respaldo realizadas.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe garantizar el respaldo de las configuraciones de los equipos de la infraestructura tecnológica.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe garantizar el respaldo de los logs o registro de eventos de los equipos de la infraestructura tecnológica.

- Se deberán realizar las respectivas pruebas a las copias de respaldo de manera aleatoria conforme como se indique en el proceso documentado al interior de la entidad.

- Se deberá garantizar el almacenamiento y transporte seguro de las copias de respaldo.

- Cuando se soliciten copias de respaldo de los activos de información que contienen información pública clasificada o publica reservada de acuerdo con lo definido en la Ley 1712 de 2014, se debe firmar un compromiso de confidencialidad para realizar el proceso correspondiente.

- Los propietarios de los activos de información deben establecer el tiempo de retención de las copias de respaldo de la información de acuerdo con los requisitos de ley, una vez cumplido estos tiempos se debe realizar el borrado seguro de la información.

- Toda la información de los procesos de la entidad debe ser almacenados en los repositorios autorizados por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., con el fin de garantizar su respaldo, preservación y disponibilidad en caso de evento no esperado.

- La Oficina de Tecnologías de la Información y Comunicaciones – OTIC debe generar las respectivas copias de respaldo de los sistemas de información y/o servicios identificados como críticos, realizar la restauración y almacenamiento de estas, de acuerdo con lo definido en el documento **4204000-GS-036 Guía de Gestión y Administración de Copias de Respaldo.**

- La Oficina de Tecnologías de la Información y Comunicaciones – OTIC deberá almacenar los medios magnéticos que contienen información de la Entidad en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

12.4.14 Control 8.14 - Redundancia de instalaciones de procesamiento de información

La Entidad deberá implementar mecanismos de redundancia en las instalaciones de procesamiento de información, garantizando la continuidad de los servicios críticos ante fallas o eventos disruptivos.

12.4.15 Control 8.15 - Registro de actividades (logs)

La Secretaría General genera, protege y revisa los registros de actividades de los sistemas de información, con el fin de detectar eventos de seguridad, apoyar investigaciones y garantizar la trazabilidad de las acciones realizadas.

– Para los nuevos sistemas desarrollados in-house o por un proveedor, se deben generar los registros de las actividades de auditoría, excepciones, eventos, fallas y conservar bajo el periodo establecido por el área funcional y la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

– Se debe utilizar una herramienta para realizar monitoreo de los servicios más críticos de la entidad.

– Todos los accesos de usuarios a los sistemas, aplicaciones y redes de datos se deben registrar y/o conservar con el fin de facilitar las labores de auditoría, en las aplicaciones que ameriten este control de auditoría.

– Se deben hacer copias de respaldo de información a los sistemas de información que tienen implementado eventos de auditoría, con el fin de que estén disponibles en el caso que se presente un incidente de seguridad de la información
– Los sistemas de información de la Entidad deberán contar con una protección por default, para que en los procesos de auditoría y el usuario administrador sea el único que genera cambios ya que se encuentra autorizado para realizarlos.

– Todos los accesos de usuarios a los sistemas, aplicaciones y redes de datos se registran y/o conservan con el fin de facilitar las labores de auditoría, en las aplicaciones que ameriten este control de auditoría.

12.4.16 Control 8.16 - Monitoreo de actividades

La Entidad monitorea de manera continua las actividades de los sistemas y redes, utilizando herramientas que permitan identificar comportamientos anómalos o incidentes de seguridad de forma oportuna.

12.4.17 Control 8.17 - Sincronización de relojes

La Secretaría General asegura la sincronización de los relojes de los sistemas de información, garantizando la coherencia temporal de los registros y eventos de seguridad.

– Todos los relojes de los sistemas de procesamiento de información de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. deben estar sincronizados con la fuente de hora legal colombiana del Instituto de Nacional de Metrología.

– La configuración se encuentra descrita en el documento 4204000-GS-091 **Guía para la Administración para la gestión de red LAN, WAN, Wireless y Dispositivos de Seguridad** de Seguridad de la Secretaría General.

12.4.18 Control 8.18 - Uso de programas con privilegios elevados

La Entidad controla el uso de programas que operen con privilegios elevados, limitando su ejecución a casos estrictamente necesarios y asegurando su monitoreo.

– La OTIC a través de la mesa de servicios son los encargados de realizar instalación del software operacional en los equipos de la Entidad, previa autorización del jefe de dependencia remitida por medio del formato FT-1000.

– La OTIC debe definir cuál es el software operacional base con el que deben contar los equipos de cómputo asignados a los servidores públicos y contratistas de la entidad, y la mesa de servicios debe garantizar su instalación durante el proceso de alistamiento para entrega.

– El control de la gestión del software operacional instalado en los equipos de cómputo de la entidad es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones.

– La OTIC debe probar y evaluar la aplicación de actualizaciones antes de su instalación y valorar los riesgos asociados, para asegurar que son eficaces y no producen efectos secundarios.

– La mesa de servicios debe realizar revisiones periódicas con el fin de garantizar que el software operacional instalado en los equipos de cómputo de la entidad cuenta con las últimas versiones estables y no exista software no autorizado, y en caso de encontrarlo realizar la desinstalación respectiva.

– La OTIC debe contar con un inventario actualizado del software autorizado a instalar en los equipos de la entidad.

– La OTIC debe implementar controles con el objetivo de proteger el licenciamiento del software operacional, que permitan que la entidad cumpla con los acuerdos de propiedad intelectual y no haga uso de software no autorizado.

– Los servidores públicos y contratistas deben dar cumplimiento a los requisitos legales y regulatorios relacionados con la protección de los derechos de propiedad intelectual y derechos de autor en Colombia.

– Cualquier requerimiento de instalación de software operacional debe ser solicitado por la herramienta de la mesa de servicios de TI para su respectiva verificación, evaluación y autorización.

– La OTIC debe implementar controles de seguridad para la detección y respuesta temprana de incidentes de seguridad relacionados con el software operacional instalado en los equipos de cómputo de la entidad. Estos incidentes deberán ser registrados y documentados en la herramienta de mesa de servicios.

– La OTIC debe realizar revisiones y/o auditorías periódicas para garantizar el cumplimiento de los derechos de propiedad intelectual y derechos de autor, en relación con las licencias de software operacional utilizadas en la entidad.

12.4.19 Control 8.19 - Instalación de software en sistemas operativos

La Secretaría General regula la instalación de software en los sistemas operativos, permitiendo únicamente aplicaciones autorizadas y verificadas.

– El software instalado en la Entidad debe contar con su respectiva licencia de validez y legalidad en el mercado.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC debe verificar el normal funcionamiento de los aplicativos que se entregan a producción o están en producción, con el objetivo de no afectar la integridad, disponibilidad y desempeño de estos.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC se debe asegurar que para las aplicaciones desarrolladas internamente o por

terceros se realicen las respectivas pruebas antes de salir a producción, lo cual se apoya en lo descrito en el documento **4204000-GS-006 Guía de Arquitectura de Software para Soluciones Tecnológicas.**

– Se debe dar cumplimiento al proceso de gestión de cambios para todos los cambios que se realicen en sistemas de información o servicios que se encuentren en producción o para los desarrollados internamente o por terceros en su salida a producción.

– La instalación de cualquier tipo de hardware y/o software en los equipos de escritorio o equipos portátiles de la Entidad es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC y por tanto son los únicos autorizados para llevar a cabo esta labor.

– Para las dependencias que solicitan la instalación de software libre, la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC deberá realizar el análisis, verificación y la aprobación para la correspondiente instalación.

– Los medios de instalación de software son los proporcionados por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. a través de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

– En caso de encontrarse software instalado en los equipos que no esté debidamente licenciado, este debe ser desinstalado.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC deberá definir y actualizar de manera periódica la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los equipos de la Entidad.

12.4.20 Control 8.20 - Seguridad de redes

La Entidad implementa controles de seguridad en redes de comunicaciones, protegiendo la información transmitida y previniendo accesos no autorizados.

– Únicamente los servidores públicos, contratistas y proveedores autorizados por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, previa solicitud a través de la mesa de servicio por parte de la dependencia que lo requiera se podrá conectar a la red inalámbrica de la

Secretaría General de la Alcaldía Mayor de Bogotá D.C.

– La conexión autorizada para acceder a los servicios de la entidad es por VPN y esta solicitud se debe realizar a través del documento **4204000-FT-1000 Solicitud de Servicios TIC, con autorización del jefe de la dependencia,**

12.4.21 Control 8.21 - Seguridad de los servicios de red

La Secretaría General asegura que los servicios de red utilizados cuenten con mecanismos de seguridad adecuados, conforme a los riesgos identificados.

– Se debe realizar el monitoreo de los canales de comunicación, con el fin de establecer el desempeño mensual de los mismos y generar los mecanismos de control a que haya lugar.

– Se deben aplicar los respectivos controles para la detección de intrusos con el fin de detectar cualquier tipo de actividad contra los sistemas presentes.

– Las redes se deben manejar de una manera adecuada y debidamente controladas para protegerlas de amenazas, y para mantener la seguridad de los sistemas y aplicaciones.

– Se deben contar con controles “routing" para las redes que aseguran las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso.

Sobre el correo electrónico

– El único servicio de correo electrónico autorizado por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. es el dispuesto por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

– Todos los servidores públicos y contratistas de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. tienen derecho a una cuenta de correo electrónico institucional para el desarrollo de sus funciones. Este principio también aplica para las dependencias, proyectos y eventos oficiales de la Entidad.

– Todas las cuentas de correo que sean creadas para las dependencias,

proyectos y eventos oficiales de la Entidad, deben tener un responsable.

– La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) será la dependencia encargada de proporcionar, administrar y supervisar el servicio de correo electrónico institucional, así como de velar por su correcto funcionamiento y uso conforme a las políticas de seguridad de la información. Para tal fin, la OTIC asignará a cada usuario una cuenta de correo asociada a un buzón electrónico en el cual se almacenarán los mensajes enviados y recibidos.

– Cada buzón de correo institucional contará con un espacio máximo definido por la OTIC y podrá enviar o recibir archivos adjuntos hasta el tamaño máximo establecido. Dicho espacio comprenderá la totalidad de los mensajes enviados, recibidos y almacenados en las carpetas creadas por el usuario. Para las cuentas de dependencias, proyectos o eventos oficiales, se podrá asignar un espacio adicional de acuerdo con la necesidad, previa solicitud debidamente justificada del jefe del área o dependencia correspondiente ante la Oficina de Tecnologías de la Información y las Comunicaciones.

– Cada usuario es responsable de realizar periódicamente la depuración de su buzón de correo, con el fin de mantener disponibilidad de espacio y asegurar la continuidad del servicio.

– La información contenida en el correo electrónico institucional se considera información privada y deberá ser tratada como una comunicación directa entre el remitente y el destinatario, sin perjuicio de las facultades legales y administrativas de la Entidad para su gestión, custodia o verificación, conforme a la normativa vigente.

– Los mensajes y la información contenida en los buzones de correo son propiedad de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. y de cada responsable, por lo tanto, solo se debe manejar información institucional para el desarrollo de sus actividades.

– Las cuentas de correo institucional son personales e intransferibles. En consecuencia, los usuarios deberán utilizar claves seguras y no compartir sus credenciales de acceso con terceros. Cada usuario será responsable de la información enviada, recibida o reenviada desde su cuenta de correo

institucional.

– Aunque la Entidad cuenta con mecanismos automáticos de detección y control de software malicioso en los mensajes de correo electrónico entrantes, los usuarios deberán actuar con precaución cuando la información sea proveniente de remitentes desconocidos (archivos adjuntos o enlaces). En caso de recibir mensajes con estas características del cual se sospeche, se deberá informar oportunamente a la Oficina de Tecnologías de la Información y las Comunicaciones, a través de los canales de soporte definidos.

– Las cuentas de correo electrónico institucional y los accesos a la red serán desactivados dentro del plazo definido por la Entidad, contado a partir de la fecha en que el servidor público o contratista finalice su vinculación, o cuando una dependencia, proyecto o evento oficial deje de existir, o por solicitud expresa del jefe del área o dependencia correspondiente.

– La **Oficina de Tecnologías de la Información y las Comunicaciones** podrá cancelar las cuentas de correo que no evidencien uso durante un periodo prolongado definido por la Entidad, exceptuando aquellos casos en que los usuarios se encuentren en vacaciones, licencias o situaciones administrativas debidamente justificadas. Así mismo, el uso indebido del correo electrónico institucional podrá dar lugar a la cancelación de la cuenta y a las acciones administrativas a que haya lugar.

– Los servidores públicos y contratistas de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. no deberán emplear direcciones de correo electrónico diferentes a las cuentas institucionales para atender asuntos oficiales de la Entidad.

Sobre otras herramientas colaborativas

– Todos los servidores públicos y contratistas deberán hacer uso de la herramienta autorizada de mensajería instantánea (remoto, chats, llamadas y video conferencias) definida en la Entidad, la cual es administrada por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, dependencia que vela por su actualización y correcto funcionamiento.

– La configuración de seguridad de los chats y reuniones debe ser parametrizada en la herramienta, para salvaguardar la confidencialidad e integridad de la

información gestionada por los usuarios de la Secretaría General.

– Toda la información gestionada por los servidores públicos y contratistas que este relacionada con el cumplimiento de su cargo o contrato, deberá estar alojada en los repositorios designados por la entidad.

Prohibiciones sobre el del correo electrónico institucional y herramientas colaborativas

Se encuentran prohibidas las siguientes actividades en el uso del correo electrónico institucional:

- **Envíos masivos internos no institucionales**

  Enviar correos electrónicos dirigidos a “Todas las dependencias” cuyo contenido no sea de carácter estrictamente institucional. Cuando se trate de comunicaciones institucionales, la información incluida en dichos mensajes no deberá superar el tamaño máximo definido por la Entidad. En caso de requerirse la difusión de archivos de mayor tamaño, estos deberán ser publicados a través de la Intranet institucional, previa solicitud a la **Oficina de Tecnologías de la Información y las Comunicaciones (OTIC)**.
  El personal diferente al nivel directivo solo podrá enviar mensajes a “Todas las dependencias” con autorización previa del jefe de la dependencia respectiva.

- **Envío de correos externos masivos y cadenas de mensajes**

  Enviar correos electrónicos externos masivos, así como enviar o responder cadenas de mensajes dirigidas a una o varias personas, por representar riesgos para la seguridad de la información y afectar el uso adecuado de los recursos institucionales.

- **Vulneración de derechos de autor**

  Enviar correos electrónicos que contengan material o información que transgreda las normas nacionales o internacionales relacionadas con los derechos de autor y la propiedad intelectual.

- **Propaganda político-partidista**

  Enviar o reenviar correos electrónicos que contengan propaganda, proselitismo

o cualquier tipo de información de carácter político-partidista, tanto en comunicaciones internas como externas.

- **Contenido contrario a la ley, la moral o las buenas costumbres** Enviar correos electrónicos internos o externos con material o información que vaya en contra de la moral, las buenas costumbres o que constituya o fomente comportamientos que puedan dar lugar a responsabilidades civiles, administrativas o penales.

- **Promoción de intereses particulares**

  Promocionar, a través del correo electrónico institucional, bienes o servicios de carácter particular que no tengan relación directa con los objetivos, funciones o actividades institucionales de la Entidad.

- **Uso del correo para fines no institucionales**

  Utilizar el correo electrónico institucional para fines distintos a los objetivos, funciones y actividades propias de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

- **Conexiones a servicios de inteligencia artificial no autorizados**

  Integrar servicios de inteligencia artificial de terceros no autoriados por la entidad con herramientas colaborativas Ej. Servicio para la trascripción de reuniones.

Sobre el uso de internet

- La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) será la dependencia encargada de proporcionar, administrar y supervisar el servicio de acceso institucional a Internet, así como de vigilar su correcto uso, disponibilidad y funcionamiento. Para tal fin, la OTIC asignará a cada usuario una cuenta institucional con privilegios de acceso específicos, asociados a una clave de acceso personal.

- Todos los usuarios deberán estar identificados de manera individual y contar con permisos de acceso expresamente autorizados, de acuerdo con las necesidades propias de sus funciones y los principios de necesidad y privilegio mínimo.

- Las cuentas de acceso son personales e intransferibles; en consecuencia,

cualquier uso indebido de una cuenta y de los privilegios asociados a la misma será atribuido inicialmente al servidor público o contratista responsable de dicha cuenta. Por lo anterior, los usuarios deberán adoptar prácticas responsables en el manejo y custodia de sus credenciales, evitando su uso por personas no autorizadas.

– El uso de Internet estará permitido exclusivamente para el desarrollo de actividades institucionales. Los usuarios deberán utilizar únicamente los servicios y recursos para los cuales han sido autorizados. La OTIC podrá implementar herramientas de monitoreo y análisis de tráfico de red con el fin de detectar usos indebidos, no autorizados o contrarios a las políticas institucionales de seguridad de la información.

– El uso de servicios de comunicación interactiva temporal, tales como chats, mensajería instantánea u otros servicios similares, solo podrá realizarse cuando exista autorización expresa del jefe del área o dependencia correspondiente. Dicha autorización deberá ser solicitada de manera formal y debidamente justificada ante la **Oficina de Tecnologías de la Información y las Comunicaciones**, la cual evaluará la solicitud y decidirá sobre su viabilidad, atendiendo criterios de seguridad de la información y necesidad institucional.

– La **Oficina de Tecnologías de la Información y las Comunicaciones** estará facultada para bloquear el acceso a sitios de Internet que no sean compatibles con las labores institucionales o que representen riesgos para la seguridad de la información. En los casos en que se requiera una excepción debidamente justificada, el jefe del área o dependencia correspondiente deberá presentar la solicitud formal ante la OTIC, exponiendo las razones que sustenten la necesidad del acceso excepcional, para su análisis y aprobación.

Prohibiciones sobre el uso de Internet y de los recursos tecnológicos

– Se encuentra **prohibido** para todos los servidores públicos y contratistas que tengan asignados puestos de trabajo con computadores y acceso a Internet institucional:

- **Acceder a contenidos no permitidos**
  Ingresar a páginas de contenido pornográfico, así como a sitios de personas u organizaciones al margen de la ley, o que contengan contenidos ilegales, inapropiados o contrarios a la normatividad vigente y a los principios

institucionales.

- **Descargar o utilizar software no autorizado**
  Descargar, instalar o utilizar programas que permitan realizar conexiones automáticas o no autorizadas, así como emplear los recursos tecnológicos de la Entidad para la distribución o reproducción de este tipo de programas, ya sea a través de la web o mediante medios de almacenamiento externos.

- **Descargar contenido multimedia y realizar actividades de entretenimiento**
  Descargar música, videos u otros contenidos multimedia, especialmente mediante servicios o plataformas especializadas para tal fin, así como utilizar o participar en juegos de entretenimiento en línea, cuando dichas actividades no estén directamente relacionadas con el ejercicio de las funciones institucionales.

- **Uso de servicios de radio y televisión por Internet**
  Utilizar servicios de radio y televisión a través de Internet, salvo que dicha información sea requerida de manera justificada para el ejercicio de las funciones a cargo. En estos casos, el jefe del área o dependencia correspondiente deberá presentar la solicitud debidamente motivada ante la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) para su análisis y aprobación.

- **Instalación o modificación no autorizada de software y configuraciones**
  Descargar o instalar programas, así como modificar los paquetes de software o las configuraciones existentes en los computadores de la Entidad, con el fin de prevenir riesgos de seguridad, infecciones por malware o reconfiguraciones no autorizadas de los equipos. En caso de requerir la instalación de nuevo software o la modificación de alguno ya existente, el jefe del área o dependencia correspondiente deberá solicitarlo formalmente a la **Oficina de Tecnologías de la Información y las Comunicaciones**, a través de los canales de soporte definidos por la Entidad.

12.4.22 Control 8.22 - Filtrado web

La Secretaría General implementa mecanismos de filtrado web para prevenir el acceso a sitios maliciosos o no autorizados que puedan comprometer la seguridad de la información.

12.4.23 Control 8.23 - Segmentación de redes

La Entidad segmenta las redes de comunicaciones para limitar la propagación de incidentes de seguridad y proteger los activos críticos.

– Se debe contar con reglas específicas en el Firewall, teniendo en cuenta únicamente los servicios, puertos de origen y destino necesarios y expresamente autorizados, acorde a lo establecido en el documento **4204000-GS-091 Guía de la Administración para la gestión de red LAN, WAN, Wireless y dispositivos de seguridad** de la Secretaría General.

– Se debe contar con una red segmentada, conforme a los roles y responsabilidades de los servidores públicos, contratistas y proveedores de la Entidad haciendo uso de VLANs, y controlar el acceso remoto a las plataformas por medio del uso de VPN previamente autorizadas y de acuerdo con lo establecido en el presente documento.

– Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.

12.4.24 Control 8.24 - Uso de criptografía

Con el fin de proteger la confidencialidad, integridad, autenticidad y no repudio de la información, la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** establece el uso de protocolos y controles criptográficos para transmitir o transferir información, enlaces de comunicaciones, acceso remoto (VPN), firmas electrónicas y digitales con entidades externas. Estos accesos se conceden a través del establecimiento de VPN site-to-site y se establecen convenios interadministrativos para llevar a cabo la respectiva configuración del mencionado canal.

– La Oficina de Tecnologías de la Información y las Comunicaciones - OTIC debe establecer mecanismos de cifrado de información apropiados de acuerdo con las necesidades de la Entidad y proveer los mismos a los propietarios de la información.

– El uso de herramientas de cifrado es autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de la Entidad.

– Es responsabilidad tanto de los servidores públicos o contratistas de la Entidad:

  - Hacer uso correcto de los certificados digitales, los respectivos tokens para firma digital con que cuentan los accesos a los servicios y páginas web en la Entidad.

  - Utilizar exclusivamente las herramientas de cifrado autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones, especialmente para la gestión de información pública clasificada y pública reservada.

  - En caso de requerir cifrar archivos, carpetas, unidades externas deben realizar una solicitud a la mesa de servicios, la cual debe venir debidamente autorizada por el jefe inmediato.

– La Mesa de servicios deberá realizar la instalación únicamente de las herramientas de cifrado autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones.

– Todas las credenciales de acceso que se generen del proceso de cifrado de información en una dependencia deben ser debidamente protegidas y almacenadas en un sitio seguro y conocidas por el jefe de la dependencia.

– En los procesos de cifrado definidos se debe tener en cuenta el estándar de generación de contraseñas definido por la Oficina de Tecnologías de la Información y las Comunicaciones.

Gestión de claves criptográficas

La Secretaría General gestiona de manera segura las claves criptográficas, asegurando su generación, almacenamiento, distribución, uso y eliminación conforme a buenas prácticas.

– La Oficina de Tecnología será la dependencia responsable de brindar los lineamientos en el manejo y gestión de las llaves criptográficas.

– Se debe garantizar que el proceso del ciclo de vida de las llaves criptográficas

se encuentre documentado.

– Se debe establecer un proceso de generación segura de las llaves criptográficas.

– Se debe hacer uso de algoritmos fuertes para la generación de las llaves criptográficas.

– Se debe establecer un proceso de respaldo y almacenamiento seguro para las llaves criptográficas.

– En caso de que una llave criptográfica se encuentre comprometida, se deberá seguir lo definido en el proceso de incidentes de seguridad de la entidad.

– Se debe establecer el proceso de auditoría y monitoreo de las llaves criptográficas con el fin de rastrear su uso.

12.4.26 Control 8.26 - Seguridad del ciclo de vida del desarrollo

La Entidad integra la seguridad de la información en el ciclo de vida del desarrollo de sistemas y aplicaciones, considerando controles desde el diseño hasta la operación.

12.4.27 Control 8.27 – Principios de ingeniería de sistemas seguros

La Secretaría General deberá aplicar principios de ingeniería de sistemas seguros en el diseño, adquisición, desarrollo, implementación, operación y mantenimiento de los sistemas de información y servicios digitales, con el fin de garantizar que la seguridad de la información sea integrada de manera sistemática y consistente durante todo el ciclo de vida de los sistemas.

12.4.28 Control 8.28 - Codificación Segura

– Las nuevas aplicaciones, desarrollos, y/o sistemas operativos o modificaciones a estos y que soporten los sistemas de información, solamente deben ser

implementados en el ambiente de producción después de un protocolo de pruebas adecuado que involucre aspectos funcionales, de seguridad, de compatibilidad con otros sistemas de información y facilidad de uso.

- Los administradores de las plataformas de producción son los responsables de controlar el acceso y uso de los programas fuente de los sistemas y/o de las aplicaciones que operan en ellas, así como de coordinar y/o ejecutar las actualizaciones programadas.

- La administración del código fuente de las aplicaciones debe mantenerse en un sistema de versionamiento, el cual debe ser accedido únicamente por personal autorizado.

- Es responsabilidad del administrador de la plataforma, el acceso a los sistemas de producción, en caso de requerirse actividades de soporte o mantenimiento, esta actividad e deberá llevarse a cabo con el respectivo monitoreo.

- Se deberán implementar controles de seguridad bajo metodologías de desarrollo seguro para los sistemas de información de la entidad, para protegerlos contra:

    - La pérdida de control de acceso
    - Fallas criptográficas
    - Inyección de código
    - Diseño inseguro
    - Fallas en la configuración de seguridad
    - Fallas de identificación y autenticación
    - Fallas en el software y en la integridad de los datos
    - Fallas en el registro y monitoreo
    - Falsificación de solicitudes del lado del servidor

- Se deben suministrar opciones de desconexión o cierre de sesión en los aplicativos (logout), que permiten terminar completamente con la sesión o conexión asociada, las cuales deben estar disponibles en todas las páginas, sitios o aplicaciones protegidas por autenticación.

– Se debe monitorear el desarrollo de software donde se tenga en cuenta los acuerdos de licenciamiento, los cuales especifican las condiciones de uso del software y los derechos de propiedad intelectual.

– Los desarrolladores deben garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, que se implementen mensajes de error genéricos.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC debe velar por mantener la separación de los ambientes: para desarrollo, para pruebas y para producción, acorde con lo establecido e identificado a través del direccionamiento IP a nivel de sistema operativo Windows y sistema operativo Linux.

12.4.29 Control 8.29 - Pruebas de seguridad

La Entidad deberá realizar pruebas de seguridad a los sistemas y aplicaciones, con el fin de identificar vulnerabilidades antes de su puesta en operación o tras cambios significativos.

– Se deberán realizar pruebas de seguridad a los sistemas de información nuevos y/o funcionalidades de sistemas existentes de la entidad.

– La solicitud de los requerimientos para los sistemas nuevos y/o mejoras en los sistemas existentes deben especificar los requerimientos de los controles de seguridad cuando los hubiere.

– Se debe aplicar lo establecido en el documento **4204000-GS-108 Guía Metodológica para el desarrollo y mantenimiento de soluciones de software.**

– Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

– Se deben realizar revisiones entre el funcional y desarrollador, efectuando pruebas de calidad antes de desplegar aplicaciones o correcciones en

producción.

- Se deben gestionar las autorizaciones de despliegue por parte de los funcionales y guardar las evidencias de dicho proceso.

- Se deben implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y pruebas hacia ambiente de producción hayan sido aprobadas tanto por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC como por el área usuaria del sistema o aplicativo en cuestión.

- La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC en conjunto con los propietarios de los aplicativos deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.

- La respectiva aceptación de los sistemas se debe realizar a través de una lista de chequeo que aprueba el dueño funcional del sistema de información, aplicación nueva o cambio que se presente en ella.

- La información entregada a los desarrolladores para realizar las pruebas no puede ser información confidencial de los ambientes de producción.

12.4.30 Control 8.30 - Seguridad en servicios tercerizados de desarrollo

La Secretaría General deberá asegurar que los servicios de desarrollo de software tercerizados cumplan con los lineamientos de seguridad de la información establecidos.

- Se deben tener en cuenta los acuerdos sobre: las licencias, propiedad de los códigos y derechos de propiedad intelectual y convenios a que haya lugar en caso de falla de la tercera parte, derechos de acceso para auditar la calidad y exactitud del trabajo realizado, requisitos contractuales para la calidad y la funcionalidad de la seguridad del código, ejecución de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

- El seguimiento respectivo se debe apoyar en lo descrito en el documento

4204000-PR-106 Gestión para la adquisición de infraestructura tecnológica, el desarrollo o adquisición de nuevas soluciones tecnológicas.

12.4.31 Control 8.31 – Separación de ambientes de desarrollo, prueba y producción

La Secretaría General separa adecuadamente los entornos de desarrollo, prueba y producción, evitando accesos indebidos y riesgos de seguridad.

– La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC cuenta con direccionamiento IP a nivel de sistemas operativos Windows y Linux de manera separados para los ambientes de desarrollo, pruebas y producción al interior de la Entidad.

12.4.32 Control 8.32 – Gestión del cambio

– La Secretaría General deberá establecer y aplicar un proceso formal de gestión del cambio para todos los cambios que puedan afectar la seguridad de la información, los sistemas de información, la infraestructura tecnológica y los servicios digitales institucionales. Dicho proceso deberá garantizar que los cambios sean evaluados, autorizados, implementados, documentados y revisados de manera controlada, con el fin de prevenir impactos negativos sobre la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información.

– Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC las revisiones periódicas, aprobaciones y evaluación de errores de los cambios programados a nivel de las aplicaciones antes, durante y después de su ejecución y debe existir una aprobación previa de las dependencias interesadas para la ejecución del cambio.

– El mantenimiento y el copiado de las librerías fuente de programas deben estar sujetos a un procedimiento estricto de control de cambios.

12.4.33 Control 8.33 – Protección de los datos de prueba

– La Secretaría General deberá garantizar que los datos utilizados en entornos

de prueba, desarrollo, capacitación o soporte no comprometan la confidencialidad, integridad, disponibilidad ni la privacidad de la información institucional. En ningún caso se deberán utilizar datos reales o datos personales en dichos entornos, salvo que exista una justificación debidamente autorizada y se apliquen controles de seguridad equivalentes a los de los entornos productivos.

– No se permite el uso y copia de información operacional como datos de pruebas, salvo autorización previa del Oficial de Seguridad de la Información o quien haga sus veces y el responsable del activo, o previa ejecución de procesos de anonimización de ésta. Esta autorización se debe solicitar cada vez que se requiera realizar la copia de información operacional en un sistema de aplicación de prueba; de igual forma, la información operacional se borra de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba; se registra el copiado y uso de la información operacional para proporcionar un rastro de auditoría.

12.4.34 Control 8.34 – Controles de auditoría de sistemas de información

– Se deberán realizar revisiones internas programadas a los sistemas de información nuevos, desarrollados in-house o por intermedio de terceros, según lo establecido en el programa de auditorías definido por la Entidad.

13. POLITICAS

13.1 Política para Dispositivos móviles.

Descripción General: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices necesarias para la gestión de los dispositivos móviles con el fin de evitar la pérdida de confidencialidad, integridad y disponibilidad de la información institucional.

13.2 Política para teletrabajo

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C establece las directrices necesarias para dar cumplimiento a la normativa

relacionada con el teletrabajo respecto a la gestión de la seguridad y privacidad de la información manejada por los servidores públicos bajo esta modalidad.

13.3 Política para control de acceso

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices y controles necesarios para permitir el acceso a las oficinas, áreas seguras, e instalaciones de procesamiento de la entidad, con la finalidad de preservar la Confidencialidad, Integridad, Disponibilidad, Privacidad y Autenticidad los activos de información.

13.4 Política para controles criptográficos

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece lineamientos y controles criptográficos para transmitir o transferir la información definida como pública clasificada y pública reservada.

13.5 Política para Política la gestión de llaves criptográficas

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C establece las directrices y controles necesarios para la gestión del ciclo de vida de las llaves criptográficas.

13.6 Política para la seguridad física y del entorno.

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices y controles necesarios para controlar el acceso a las instalaciones físicas de la entidad, con la finalidad de preservar la Confidencialidad, Integridad, Disponibilidad de los activos de información.

13.7 Política de escritorio y pantalla limpia

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C establece las directrices necesarias para el manejo responsable de la información definida como pública clasificada y pública reservada gestionada en el cumplimiento de sus funciones.

13.8 Política de Copias de Respaldo y Recuperación

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C establece las directrices y controles de seguridad relacionados con el respaldo y restauración de la información.

13.9 Política de Control de Software Operacional

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C establece las directrices y controles de seguridad que permitan controlar el uso del software operacional en la entidad, dando cumplimiento a la normativa de propiedad intelectual y derechos de autor.

13.10 Política para transferencia de información

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices y controles para asegurar la transferencia de información institucional definida como pública clasificada y pública reservada.

13.11 Política de Desarrollo Seguro

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices y controles para implementar la seguridad en la etapa de desarrollo de los sistemas de información, aplicaciones y servicios para una adecuada prestación de servicio a la ciudadanía.

13.12 Política para relaciones con proveedores.

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices y controles en la relación con los proveedores que acceden a los activos de información con el fin de evitar la pérdida de confidencialidad, integridad y disponibilidad de estos

13.13 Política para privacidad y protección de información de datos personales.

Descripción: La Secretaría General de la Alcaldía Mayor de Bogotá D.C. establece las directrices y controles para dar cumplimiento a la normativa relacionada con la protección de datos personales y garantizar la privacidad de estos.

	NOMBRE	CARGO	FECHA
ELABORÓ	Lourdes María Acuña	Contratista-Oficina TIC	Diciembre 2025
REVISÓ	Erika Tatiana Quintero Quintero	Contratista-Oficina TIC	Diciembre 2025
APROBÓ	Arleth Patricia Saurith Contreras	Jefe de Oficina - Oficina TIC	Diciembre 2025

CONTROL DE CAMBIOS			
SECCIÓN DEL DOCUMENTO MODIFICADA	**CAMBIO REALIZADO**	**FECHA**	**VERSIÓN**
Creación del Documento	Se crea el documento	27/07/2018	01
Documento Inicial	Modificación del nombre del Comité Técnico de Seguridad de la Información por Comité Institucional de Gestión y Desempeño, ajustes matrices RACI y estructura organizacional. Se ajustó la Política para transferencia de información, en cuanto a la Política de uso aceptable de los activos asignados, de igual manera se ajustó el texto en relación con la resolución de la Política de Privacidad y Tratamiento de Datos Personales y el "Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales", y su finalidad. Se incluyó en la Política para desarrollo seguro, el tema de control de cambios.	21/07/2020	02
Actualización Documento	Modificación de nombres e información de las políticas y controles de acuerdo con la Norma ISO/IEC 27001:2013. Se incluyó y ajusto algunos controles que se encuentran establecidos en los Lineamientos para la implementación y Sostenibilidad del Sistema de Gestión de Seguridad de la Información.	15/12/2021	03
Actualización Documento	Modificación del alcance del documento. Modificación acorde a los controles establecidos en el Anexo A de la norma ISO/IEC 27001 y lo descrito en ISO/IEC 27002:2015.	12/10/2022	04
Actualización Documento	Modificación del alcance del documento. Modificación acorde a los controles establecidos en el Anexo A de la norma ISO/IEC 27001 y lo descrito en ISO/IEC 27002:2015.-	21/02/2023	05
Encabezado Actualización Documento	Se ajusta procedimiento al que pertenece el documento. Reorganización general del documento Inclusión de lineamientos de seguridad	21/12/2023	06

Actualización del documento	Inclusión de política de software operacional y política de copias de respaldo y recuperación. Ajuste e inclusión de lineamientos generales de seguridad.	28/08/2024	07
Actualización del documento	Se reorganiza el documento conforme con la actualización de la norma ISO 27001:2022	Diciembre 2025	08