SECRETARÍA GENERAL
ALCALDÍA MAYOR DE BOGOTÁ.

	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	Ana María Bocanegra Stephanie Villarreal Ramirez	Contratista Contratista	15/12/2021	
REVISÓ	Rafael Londoño Carantón	Jefe Oficina TIC	22/12/2021	
APROBÓ	Rafael Londoño Carantón	Jefe Oficina TIC	22/12/2021	

Contenido

Ilustraciones

1. INTRODUCCIÓN

La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** reconoce y declara la 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 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.

Este documento describe las políticas 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 en 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 del dato e información que genera, procesa, administra y custodia la Entidad ya sea en cualquier medio físico o electrónico que alberga el dato y/o la información.

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

[1] Las normas establecidas en este manual son las necesarias de acuerdo con la Norma ISO27002 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] Ídem anterior.

2. OBJETIVO DEL MANUAL DE POLÍTICAS Y CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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 Sistema de Gestión de Seguridad de la Información en la **Secretaría General de la Alcaldía Mayor de Bogotá, D.C.**

3. ALCANCE DEL MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los establecido en el presente documento son de obligatorio cumplimiento y aplica a todos los funcionarios, contratistas, proveedores y aliados sin excepción, que posean algún tipo de acceso físico a oficinas de las dependencias que conforman la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.,** acceso lógico a la información de la Entidad y/o, sean responsables y/o encargados de los activos de información[3], activos físicos, infraestructura física y recurso humano de la Secretaría General, y la cual se encuentre disponible en cualquier formato ya sea de manera digital, impresa, en medio audiovisual o documentos archivados de la Entidad en el desarrollo de la misión institucional y el cumplimiento de los objetivos estratégicos de ésta.

4. NORMATIVIDAD

- **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 454 del 21 de marzo de 2020.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la

[3]Este tipo de activo representa los datos de la Entidad, información que tiene valor para los procesos de la Secretaría General de la Alcaldía Mayor de Bogotá, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil; Activos Físicos: Muebles y Enseres, equipos para el desarrollo de las funciones; Infraestructura física el sitio en el cual se desarrollan las actividades asignadas; Recurso Humano todo funcionario, proveedor y/o aliados de dicha Secretaría.

política de gestión de la información estadística a las políticas de gestión y desempeño institucional.

- **Decreto 1287 del 24 de septiembre de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Directiva Presidencia 03 de 15 de marzo de 2021:** Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.
- **Documento CONPES 3701 de 2011** - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.
- **Documento CONPES 3854 de 2016** - Política Nacional de Seguridad Digital.
- **Documento CONPES 3995 de 2020** - Política Nacional De Confianza y Seguridad Digital.
- **Ley Estatutaria 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **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 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 1955 de 2019.** por la cual se expide el Plan Nacional de Desarrollo 2018-2022, establece en su artículo 147 como uno de los principios de los proyectos estratégicos de transformación digital en la permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las que la Política de Gobierno Digital como política de gestión y desempeño institucional, debe contemplar como acción prioritaria el aprovechamiento de tecnologías emergentes en el sector público, incremento de la confianza y seguridad digital y el fomento a la participación y la democracia por medios digitales.
- **NTC/ISO 27001:2013**. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- **Resolución Distrital 305 de 2008**, Por la cual se expiden políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La implementación del Sistema de Gestión de Seguridad de la Información 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 en su última versión disponible[4]. 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.

6. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

- Establecer y mantener el compromiso del Comité Institucional de Gestión y Desempeño para apalancar el cumplimiento de la **Política de Seguridad y Privacidad de la Información y Gobierno Digital** del Sistema de Gestión de Seguridad de la Información, así como el Manual de la Información al interior de la Entidad.
- Establecer desde el Comité Institucional de Gestión de Desempeño los controles para la gestión de la seguridad, privacidad de la información y la protección de los datos personales, de manera clara y estructurada, de acuerdo con las buenas prácticas, la Norma ISO/IEC 27001 y demás disposiciones relacionadas[5].
- Contribuir al cumplimiento de la legislación vigente sobre la Seguridad y protección de información pública y personal, propiedad intelectual, transparencia, protección de los datos personales, protección y salvaguarda de los activos de información físicos y digitales, entre otras, para brindar tranquilidad a los funcionarios, contratistas, proveedores y aliados sobre el cuidado de la 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

[4] Ídem pie de nota Nro. 1
[5] 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.

(preventivas o correctivas) generadas en el seguimiento interno, la revisión por la dirección y/o las auditorías internas o externas.
- Gestionar los riesgos de Seguridad y Privacidad de la Información que se identifiquen en la Entidad.
- Sensibilizar y apropiar la gestión adecuada de Seguridad y Privacidad de la Información en los funcionarios, contratistas, proveedores, aliados y demás partes interesadas de la Entidad.

7. FACTORES DE ÉXITO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

- Generar conciencia en todos los funcionarios, contratistas, proveedores y aliados 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 ayuden a garantizar que la Información que la Entidad administra, genera, controla y maneja conserve los atributos de Confidencialidad, Integridad y Disponibilidad .
- Contar con instancias de gestión, revisión y decisión a distintos niveles de la Entidad (táctico, operativo y estratégico) en los cuales se realice la presentación de los resultados de los procesos y actividades asociadas al Sistema de Gestión de Seguridad de la Información.
- Implementar un esquema de gestión de incidentes de seguridad de la información que recoja notificaciones continuas por parte de los funcionarios, contratistas, proveedores y aliados , analice cada uno de los eventos, genere mejoras en los controles y 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 gestión del Sistema de Seguridad de la información.

8. CONSIDERACIONES GENERALES.

8.1. Línea base

8.1.1. 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 procesos, procedimientos, guías e instructivos de seguridad de la información como parte de sus herramientas de gobierno y gestión, que garanticen el cumplimiento y mejora del Sistema de Gestión de Seguridad de la Información.

8.1.2. Cumplimiento

El cumplimiento de las políticas, controles, procesos, procedimientos, guías e instructivos de Seguridad de la Información aplicara para todos los funcionarios, contratistas, proveedores y aliados 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 reservara el derecho de tomar las medidas correspondientes.

8.1.3. Excepciones

Las excepciones a cualquier cumplimiento de lo descrito en el presente Manual deberán ser pre aprobadas por la Oficina de Tecnologías de la Información y las Comunicaciones 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 y revisadas.

8.1.4. Administración de políticas y controles

Toda política y/o control(es) de seguridad de la información nuevo, modificado y/o eliminado, serán propuestos por la Oficina de Tecnologías de la Información y las Comunicaciones y serán aprobadas por el Comité Institucional de Gestión de 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.

8.2. Exclusiones.

- No se excluye ningún numeral de la norma ISO/IEC 27001 versión actual[6].

[6] Ídem pie de nota Número. 1

- Las exclusiones a los controles se encuentran definidos en la Declaración de Aplicabilidad (SOA por sus siglas en inglés).

8.3. Referencias informativas.

- Ver documento Normograma **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

8.4. Vigencia y actualización del manual.

La actualización y mantenimiento del Manual de Seguridad de la Información son responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones, conforme a lo aprobado en la **Política de Seguridad y Privacidad de la Información y Gobierno Digital.**

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

- Requerimientos de ley.
- Requerimientos emitidos por Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Requerimientos emitidos por la Coordinación Nacional de Seguridad Digital[7].
- Mapa de riesgos de la Entidad.
- Incidentes de seguridad de la Información.
- Nuevas vulnerabilidades detectadas.
- Cambios en la infraestructura organizacional y/o tecnológica de la Entidad.
- Cambios en la estrategia, objetivos y/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.

9. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ENTIDAD[8].

[7] Documento Modelo Integrado de Planeación y Gestión – MIPG, Pág. 46 Numeral "3.2.1.4 Política de Seguridad Digital".
[8] Hace referencia al numeral 5.3 de la Norma ISO/IEC 27001:2013: "5.3. Roles, Responsabilidades y Autoridades en la Organización."

9.1. Roles y responsabilidades para la seguridad de la información.

La Entidad cuenta con un grupo interdisciplinario denominado Comité Institucional de Gestión de Desempeño, el cual vela por el gobierno y cumplimiento de la seguridad de la información en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** Mencionado comité se apoya en la *Mesa técnica de Archivo y Seguridad de la Información*, la cual tiene como objetivo *Definir, establecer y asegurar que exista soporte técnico y administrativo para la gestión, administración y desarrollo de iniciativas sobre Seguridad y Privacidad de la Información, protección de datos personales y ciberseguridad, a través de compromisos apropiados y uso de recursos adecuados en la Entidad, así como la implementación, el mantenimiento y seguimiento para el cumplimiento de la política de seguridad de la información de la Secretaría General, atendiendo las directrices establecidas desde el Archivo Distrital, así como las dadas por la Dirección de Desarrollo institucional y las que rijan para la administración, manejo y control documental a través de las funciones de Gestión Documental. De igual manera este organismo será un apoyo en la coordinación de la formulación, implementación y continuidad del Sistema de Gestión de Seguridad de la Información.* Con este apoyo, se busca gestionar, fortalecer, revisar y mejorar de manera continua el proceder del Sistema de Gestión de Seguridad de la Información en la Entidad.

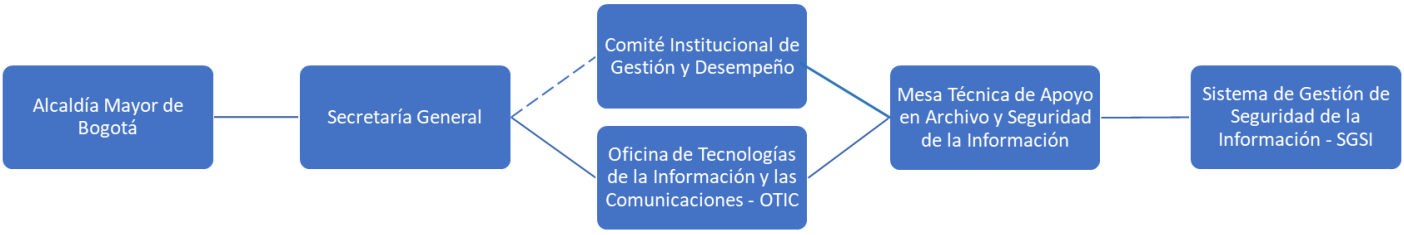
Las partes interesadas internas de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**, los funcionarios, contratistas, proveedores, aliados y los usuarios de los servicios de la Entidad deben tener conocimiento de sus responsabilidades y sus obligaciones relacionadas con la seguridad de la 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.

Esta matriz puede ser consultada en el documento **Matriz RACI Sistema de Gestión de Seguridad de la Información.**

9.2. Estructura Organizacional – Seguridad de la Información.

La estructura organizacional para el funcionamiento del Sistema de Seguridad de la Información al interior de la Secretaría General de la Alcaldía Mayor de Bogotá 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 la **Resolución No 494 de 2019** publicada en la página de la Secretaría General de la Alcaldía Mayor de Bogotá y la cual indica la creación de la ***Mesa Técnica de Apoyo en Archivo y Seguridad de la Información*** la cual debe abordar los temas asociados y relacionados con el Sistema de Gestión de Seguridad de la Información.

9.3. Segregación de Funciones.

Los funcionarios, contratistas, proveedores y aliados que en ejercicio de sus labores tengan acceso a la información, infraestructura tecnológica y a los 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 y/o la información misma, con el fin de reducir y evitar el uso o modificación no autorizada sobre los activos de información de la Entidad.

Específicamente la segregación de funciones cubre:

- Los sistemas de información clasificados como críticos, con alta o media disponibilidad, 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 usuaria o solicitante del requerimiento a través de una gestión de cambios.
- 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 a través de la delegación sobre 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.

9.4. Contacto con las autoridades y grupos de interés especial.

La Secretaría General de la Alcaldía Mayor de Bogotá deberá establecer y mantener una relación cercana con Entidades del Sistema Distrital de Prevención y Atención de Emergencias (SDPAE[9]), así como con grupos de interés o foros de especialistas en seguridad de la información, para que puedan ser contactados de manera oportuna en caso de que se presente un incidente de seguridad 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 al correo atencionalciudadano@cgfm.mil.co

En la eventualidad que se llegasen a presentar incidentes relacionados con la seguridad de la información al interior de la Secretaría General de la Alcaldía Mayor de Bogotá, deben ser reportados de la siguiente manera:

- Seguridad de la Información: segsecretaria@alcaldiabogota.gov.co
- El oficial o encargado de la seguridad de la información debe reportar acorde a lo que se encuentra a continuación:

[9] Tener en cuenta lo definido por la Alcaldía Mayor de Bogotá con relación al manejo de Atención de Desastres en el Distrito Capital.

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		
Phishing		
Ingeniería Social		
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	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co
Emergencia por Incendio	Bomberos	119
Robo	Policía Nacional	112
Antisecuestro y Antiextorsión	Gaula	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja	132
Incidentes laborales	Centro Toxicológico	136
Robo	Dijin	157
Cuadrante de la Policía Plaza de Bolívar		

Fuente: Elaboración propia

9.5. Monitoreo al Sistema de Gestión de Seguridad de la Información de la Secretaría General de la Alcaldía Mayor de Bogotá

El monitoreo al Sistema de Gestión de Seguridad de la Información de la Secretaría General de la Alcaldía Mayor de Bogotá se realizará de manera interna y bajo la responsabilidad directa de la Oficina de Tecnología de la Información y Comunicaciones 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 revisará la aplicabilidad de las políticas y controles definidos en el presente documento, en donde se validará su implementación, resultados, 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 Sistema de Seguridad de la Información de Seguridad de la Información en su totalidad.

10. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN.

10.1. Política de Seguridad de la Información.

Política de Seguridad y Privacidad de la Información y Gobierno Digital aprobada por el Comité Institucional de Gestión y Desempeño de la Entidad y el cual se encuentra publicado como componente en el Sistema Integrado de Gestión de la Secretaría General de la Alcaldía Mayor de Bogotá.

10.1.1. Responsabilidades de la Dirección.

El Comité Institucional de Gestión y Desempeño aprueba este Manual de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de acciones eficientes que garanticen 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 demostrará su compromiso a través de:

- La revisión de la **Política de Seguridad y Privacidad de la Información y Gobierno Digital** y puesta a disposición para su revisión y su respectiva aprobación, publicación y divulgación ante la Entidad.
- La revisión y aprobación de las Políticas específicas y controles asociados contenidos en este documento.
- La promoción activa de una cultura de seguridad.
- La divulgación de este manual a todos los funcionarios, contratistas, proveedores y aliados de la Entidad.
- La solicitud para asegurar la asignación de los recursos adecuados para implementar y mantener las políticas y controles mencionadas en este manual.
- La verificación del cumplimiento de las políticas y controles mencionadas en este

manual.

- La promoción de los canales adecuados para que los funcionarios, contratistas, proveedores y aliados reporten sucesos, eventos o incidentes que afecten, vulneren o representen un incumplimiento de las políticas o controles de seguridad de la información.

10.2. Seguridad de la información en la gestión de proyectos.

Los proyectos que se denominen estratégicos y/o sean prioritarios, impacten los procesos de la Entidad y/o la actualización o implementación de un nuevo sistema de información, deben asegurar que los riesgos de Seguridad de la Información asociados a éstos sean gestionados, usando una combinación de controles automáticos y manuales. Se deben especificar de manera clara los requerimientos de Seguridad de la Información en los proyectos, garantizando el balance entre seguridad, funcionalidad y los demás objetivos establecidos.

10.3. Políticas internas de Seguridad de la Información.

Por el presente Manual de Seguridad de la Información se adoptan políticas internas alineadas a lo descrito en la Norma ISO/IEC 27002[10], así:

1. Política para dispositivos móviles.
2. Política para teletrabajo.
3. Política para control de acceso.
4. Política para controles criptográficos.
5. Política para la gestión de llaves.
6. Política para seguridad física y del entorno
7. Política de escritorio y pantalla limpia.
8. Política para transferencia de información.
9. Política para desarrollo seguro.
10. Política para relaciones con los proveedores.
11. Política General de Tratamiento de Datos Personales de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

[10] Ídem pie de nota No. 1

Estas políticas se deberán comunicar a los funcionarios, contratistas, proveedores y aliados y a las demás partes interesadas a través de los canales y mecanismos institucionales dispuestos para estos fines. Además, deberán ser incluidas en las iniciativas de generación de cultura en seguridad de la información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

10.3.1. Política para dispositivos móviles

El uso de medios de dispositivos móviles (ejemplo: teléfonos inteligentes o smartphones, tabletas, relojes inteligentes, reproductores digitales, discos duros externos), sobre la infraestructura para el procesamiento de la información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** se encontrará autorizado a todos los funcionarios, contratistas, proveedores y aliados por la Oficina de Tecnologías de la Información y las Comunicaciones de la mencionada Entidad y será responsabilidad directa de cada autorizado su buen uso y la fuga de datos y/o información que se llegase a presentar.

La Oficina de Tecnologías de la Información y las Comunicaciones tiene la responsabilidad de diseñar, validar, verificar y monitorear los respectivos controles que deben aplicarse en la Entidad para el uso correcto de los dispositivos móviles autorizados y así mismo, será la responsable de implementar estos controles para asegurar que el ingreso a los sistemas de información y el uso de los medios de almacenamiento removibles definidos en la Entidad sea realizado únicamente por los funcionarios, contratistas, proveedores y aliados autorizados o que cuenten con una vinculación laboral vigente con la Entidad.

Así mismo, los funcionarios, contratistas, proveedores y aliados quienes hagan uso de alguno de los dispositivos, enunciados en este numeral, se comprometen a proteger y asegurar física y lógicamente el dispositivo físico autorizado, con el de objeto de no poner en riesgo la información de la Entidad que éste contenga.

10.3.2. Política para 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 descritos en el numeral *10.4. Controles definidos y que apoyan tanto a las Políticas Internas como a la Política de Seguridad y Privacidad de la Información y Gobierno Digital de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.* del presente documento y también se encuentran alineados con lo establecido en el procedimiento 2211300-PR-221 Gestión Organizacional donde se define el proceso que se debe llevar a cabo para el reconocimiento de la calidad de teletrabajador, sin dejar de lado el respectivo análisis del riesgo.

10.3.2.1. Condiciones Obligatorias

Con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información en el desarrollo de las actividades de teletrabajo se establecerán e implementarán, de manera obligatoria, las siguientes condiciones:

- Mecanismos de seguridad física y lógica a los equipos y documentos que maneje el teletrabajador durante el periodo establecido por Talento Humano.
- Previo análisis de riesgos, se adoptarán mecanismos de control para la protección de los datos e información, aplicaciones y sistemas de información de la Entidad.
- Antes de llevar a cabo cualquier actividad de teletrabajo se definirán entre la Entidad y el funcionario, los alcances de las actividades a desarrollar y la información a acceder, así como los sistemas y servicios de la Entidad que se utilizarán.
- Para los temas de teletrabajo relacionados con contratistas o proveedores de la Entidad, también se definirán los respectivos alcances de las actividades a desarrollar, los datos e información a consultar, aplicaciones y sistemas de información a acceder y los servicios a utilizar entre los respectivos supervisores de contrato y los contratista y proveedores

10.3.3. Política para control de acceso

Con la finalidad de preservar la Confidencialidad, Integridad, Disponibilidad, Privacidad y Autenticidad de los activos de información que son accedidos o se encuentran a cargo de los funcionarios, contratistas, proveedores y aliados debido a su cargo y/o responsabilidades, se han establecido controles que permitan regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad 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 de suministro de energía eléctrica, aire acondicionado, entre otras.

La Secretaría General llevará a cabo un control de acceso a la información que tendrá en cuenta tanto los aspectos lógicos como físicos que permitan garantizar la trazabilidad de las acciones realizadas, identificando, entre otros, datos relevantes tales como: quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados, entre otros.

Una vez se apruebe el acceso a la información, los funcionarios, contratistas, proveedores y aliados deben abstenerse de realizar modificaciones sobre la información sin la debida autorización, o acciones que vulneren los controles de seguridad establecidos por la Entidad; así mismo, deben guardar confidencialidad de la información a la cual tienen acceso e informar a la Oficina de Tecnologías de la Información y las Comunicaciones acerca de las debilidades o eventos de seguridad que se identifiquen.

10.3.3.1. 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 funcionarios, contratistas y proveedores, siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.
- Se establecerán controles para que sólo los funcionarios, contratistas o proveedores responsables de su actualización puedan acceder a su modificación, incorporando los nuevos datos que se produzcan.
- El acceso tanto a los datos o información como a las aplicaciones y sistemas de información será restringido conforme a los roles y responsabilidades de los funcionarios, contratistas y proveedores de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C**.
- Como responsables de la información las partes interesadas deberán administrar y hacer cumplir los controles de seguridad de la información establecidos en el presente documento, con el fin de evitar accesos no autorizados, pérdidas y/o utilización indebida de los activos de información.
- Los funcionarios, 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 datos e información, los activos y los sistemas informáticos para los cuales han sido designados y/o autorizados, asegurándose que éstos sólo sean utilizados para el desarrollo de las labores encomendadas.

- Tanto el responsable del área restringida como el Encargado del manejo del activo de información tienen la responsabilidad de realizar al menos una revisión anual (o cuando sea requerido) de los derechos de acceso de los usuarios en intervalos regulares, con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información.
- Es responsabilidad de cada una de las dependencias la solicitud sobre la creación del recurso compartido y así mismo, la solicitud a nivel de seguridad y privacidad de la información que requiere sobre el recurso compartido solicitado.
- La responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones se basa en el establecimiento y aplicación de parámetros de seguridad y privacidad de la información para los recurso de red compartidos en la Entidad.
- Para las dependencias que cuentan con sistemas de información y su administración, es su responsabilidad de cada una de ellas mantener y garantizar el control de acceso de usuarios sobre estos sistemas.

10.3.3.2. Responsabilidades de los usuarios

- Todos los funcionarios, contratistas, proveedores y aliados 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 a los cuales acceden y procesan dentro del desarrollo de sus funciones y responsabilidades.
- Se debe dar uso adecuado a los activos de información y deben ser usados únicamente bajo las condiciones netamente laborales.
- No está permitido 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, funcionarios, aplicaciones, sistemas de información y similares.
- Todos los funcionarios, contratistas, proveedores y aliados, que requieran tener acceso a los sistemas de información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C**. deben estar debidamente autorizados por el Jefe, Director, y/o Subdirector directo y debe acceder a dichos sistemas haciendo uso de un usuario y contraseña y cumplir los

siguientes lineamientos:

- No divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la(s) contraseña(s) de usuario(s) por los que accede a la plataforma tecnológica en ninguna circunstancia.
- 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.

10.3.4. Política para controles criptográficos

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, protección de medios fijos y/o removibles, acceso remoto, firmas electrónicas y digitales con Entidades externas.

Estas herramientas están incluidas en el listado de software autorizado, y no se permite el uso de herramientas o mecanismos de cifrado de información diferentes a los autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones.

Así mismo, es responsabilidad directa tanto de los funcionarios o contratistas de la Entidad de hacer uso correcto de los certificados digitales con que cuentan los servicios y páginas web en la Entidad.

10.3.5. Política para gestión de llaves.

La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** como responsable tanto de garantizar el control sobre los Activos de Información como preservar la confidencialidad,

integridad y disponibilidad de los datos e información, cuando ésta es generada, administrada, consultada, revisada, modificada y/o eliminada, por tanto debe definir los mecanismos de cifrado de información que se encuentren acorde con las necesidades de la Entidad y se basen en el respectivo análisis de riesgos de seguridad de la información asociados a la pérdida de las claves de criptografía de los sistemas de información, por lo tanto, el uso de las herramientas de cifrado para la gestión de claves serán autorizados y alineados a los roles y/o responsabilidades de los funcionarios, contratistas y proveedores de la Entidad.

Para lograr lo anterior, la Entidad debe contar y tener en cuenta la respectiva normatividad colombiana vigente alineada a la protección de datos, estándares del mercado aplicables y la tecnología existente, por lo cual, la Oficina de Tecnologías de la Información y las Comunicaciones de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** realizara la revisión para adquirir o crear, activar y distribuir los mecanismos de control para la gestión de claves criptográficas.

10.3.6. Política para seguridad física y Ambiental.

Con el objetivo de garantizar la respectiva seguridad física de las instalaciones de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** las puertas de acceso a cada una de las dependencias, oficinas, centros de cableado, data center, salas de capacitación y similares deben permanecer cerradas bajo ausencias temporales.

Por tanto, la Entidad cuenta con el establecimiento y asignación de permisos de acceso a las dependencias, oficinas, centros de cableado, data center, salas de capacitación y similares únicamente a los funcionarios, contratistas, proveedores y aliados autorizados para su acceso.

Así mismo, todas las áreas destinadas al procesamiento 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, son áreas de acceso restringido y en consecuencia cuentan con controles adecuados para su acceso. Los centros de cómputo, cableado y cuartos técnicos de la Secretaría General cuentan con mecanismos adecuados contra las amenazas ambientales (temperatura, humedad, fuego, etc.), especificados por los fabricantes de los equipos que albergan.

También es responsabilidad de los funcionarios, contratistas, proveedores y aliados no afectar la disponibilidad de los equipos que componen la infraestructura tecnológica en el momento de beber y/o consumir cualquier tipo de alimento cerca de ellos.

10.3.7. Política de escritorio y pantalla limpia

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios, contratistas, proveedores y aliados que tengan un vínculo laboral con la Secretaría General de la Alcaldía Mayor de Bogotá deben mantener la información clasificada con acceso restringido o confidencial 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.

Así mismo, todas las estaciones de trabajo propias de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** deberán 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.

10.3.8. Política para transferencia de información

La Secretaría General de la Alcaldía Mayor de Bogotá firmará acuerdos de confidencialidad con los funcionarios, contratistas, proveedores, aliados y ciudadanos que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario, 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 la 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.

10.3.9. Política para desarrollo seguro

Con el fin de minimizar el riesgo de corrupción de los sistemas de información que se encuentran en producción, no se permite la instalación de herramientas de desarrollo ni programas fuente en los sistemas mencionados.

Las nuevas aplicaciones, desarrollos, y/o sistemas operativos o modificaciones a éstos, que soporten 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. El acceso de los funcionarios, contratistas, proveedores y aliados a los sistemas de producción sólo es permitido para realizar labores de soporte o mantenimiento, previa autorización del administrador de la plataforma y con el respectivo monitoreo.

10.3.10. Política para relaciones con proveedores.

La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** deberá identificar y exigir controles de seguridad de la información específicamente con el acceso de los proveedores a la información de la Entidad.

Así mismo, 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.**

10.3.11. Política General de Tratamiento de Datos Personales de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

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: Política General de Tratamiento de Datos Personales de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

10.4. Controles definidos y que apoyan tanto a las Políticas Internas como a la Política de Seguridad y Privacidad de la Información y Gobierno Digital de la Secretaría General de la Alcaldía Mayor de Bogotá D.C.

A continuación, se detallan los controles asociados al cumplimiento no solamente de las políticas definidas en el presente documento, sino también a dar cumplimiento a lo establecido en la Norma ISO/IEC 27001:2013 en su Anexo A, para garantizar la Confidencialidad, Integridad y Disponibilidad de los datos e información que se almacenan en los activos de información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** que administra, custodia, controla, produce, procesa y modifica en pro del cumplimiento de las funciones y objetivos para lo cual fue creada la Entidad.

10.4.1. Política de Seguridad y Privacidad de la Información y Gobierno Digital.

- Gestionar de manera los riesgos de Seguridad y Privacidad de la Información identificados en la Entidad.
- Cumplir con los niveles de Confidencialidad, Integridad y Disponibilidad establecidos por la Entidad.
- Sensibilizar y apropiar la gestión de Seguridad y Privacidad de la Información en los funcionarios, contratistas, proveedores y aliados de la Entidad.
- Verificar por el cumplimiento de las políticas, procesos, procedimientos, instructivos y guías de Seguridad de la Información en la Entidad.

10.4.2. Organización de Seguridad de la Información.

10.4.2.1. Organización Interna.

- Todos los funcionarios, contratistas, proveedores y aliados de la **Secretaría General de la Alcaldía Mayor de Bogotá. D.C.** deben conocer y dar cumplimiento al Sistema de Gestión de Seguridad de la Información establecido en la Entidad.
- Los funcionarios 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 objeto de minimizar el uso o modificación no autorizada sobre los activos de información de la Entidad.
- Todos los sistemas de disponibilidad crítica o media de la Entidad cuentan con reglas de acceso en las cuales hay segregación de funciones entre quien las administra, opera, realiza mantenimiento y audita.
- Todos los funcionarios, contratistas, proveedores y aliados 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 funcionarios, contratistas, proveedores y aliados de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los activos de información que se presente en la Entidad.
- No está permitido el uso de los recursos tecnológicos para difundir o participar en actividades de partidos y movimientos políticos.

10.4.2.2. Dispositivos móviles.

- Los dispositivos móviles que hagan uso de información de la Entidad o que se conecten a la red se deben acogerse a las políticas y controles establecidos de seguridad de la información definidas en el presente manual.
- Se restringe la conexión de dispositivos móviles tales como smartphones y/o tablets a las redes principales de la Entidad, a excepción de los dispositivos que sean propiedad de la Entidad o cuenten con autorización expresa del jefe de cada dependencia.
- Cualquier funcionario, contratista, proveedor y aliados tendrá acceso a la información desde las redes externas mediante un proceso de autenticación sobre el uso de conexión segura y cumpliendo los respectivos requisitos de seguridad de los equipos desde donde se accede por medio de conexión VPN autorizada por la Oficina de Tecnologías de la

Información y las Comunicaciones – OTIC de la Entidad.

- La asignación de dispositivos móviles institucionales está a cargo de la Subdirección de Servicios Administrativos.
- Se permite el uso y conexión de dispositivos móviles que adquiera la Entidad y el cual se encuentre identificado dentro de los inventarios de ésta sobre la infraestructura tecnológica de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** siempre y cuando éstos sean utilizados para cumplir con las actividades y funciones de la Entidad y sean revisados por el funcionario o contratista asignado por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC y utilizando la herramienta de revisión para software malicioso.

10.4.2.3. Teletrabajo.

- El teletrabajador debe realizar la conexión a través del canal VPN autorizado para acceder a los datos e información de la Entidad de una manera segura y 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 establecido en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** para el desarrollo de las actividades a que haya lugar por parte de la Oficina de Tecnologías de la Información y las Comunicaciones de la Entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones, con la información remitida por la Dirección de Talento Humano o Supervisor del contratista, habilitará o denegará el acceso a los datos e información, aplicaciones y/o sistemas de información a través de los equipos usados para las actividades de teletrabajo según las autorizaciones concedidas al respectivo teletrabajador y firmando el acuerdo respectivo para la activación y uso del canal VPN.
- En caso de que ocurra pérdida o hurto de un equipo asignado por la Oficina de Tecnologías de la Información y las Comunicaciones, en el cual se lleven actividades de teletrabajo, será de cargo del teletrabajador responsable de este evento, informarlo de forma inmediata a través del correo electrónico oticsoporte@alcaldiabogota.gov.co con el objeto de aplicar las medidas de seguridad adecuadas para la protección de la información contenida.

- 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.

10.4.3. Seguridad en los Recursos Humanos.

10.4.3.1. Antes de asumir el empleo

- Todos los funcionarios, contratistas proveedores y aliados de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** aceptan las cláusulas de confidencialidad definidos por la Entidad antes de asumir su contratación y/o cualquier prestación de servicios, dicha cláusula hará parte integral en cada uno de los contratos.
- Se llevan a cabo chequeos periódicos definidos por la Dirección de Talento Humano y la Dirección de Contratación para la verificación de antecedentes de todos los posibles candidatos a funcionarios, contratistas, proveedores y aliados en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos en la pertinente verificación realizada.
- Como parte de su obligación contractual los contratistas, proveedores y aliados deben aceptar y firmar los términos y condiciones de su contrato de prestación de servicios, en el cual se establecen sus responsabilidades y las acciones a tomar si no se cumple con los términos y condiciones contractuales y las de la Entidad cumpliendo con los establecido en el Sistema de Gestión de Seguridad de la Información.
- Para los funcionarios, la obligación se encuentra de acuerdo con la posesión de cargo y de acuerdo con lo establecido por la Dirección de Talento Humano.

10.4.3.2. Durante la ejecución del empleo

- Todos los funcionarios, contratistas, proveedores y aliados nuevos deben asistir y aprobar las inducciones corporativas luego de firmar su contrato sobre Seguridad y Privacidad de la Información y Protección de Datos Personales.
- Todos los funcionarios, contratistas, proveedores y aliados antiguos deben recibir el apropiado conocimiento y capacitación en temas de Seguridad y Privacidad de la Información, Protección de Datos Personales, una vez al año y/o cuando se considere necesario.

10.4.3.3. Terminación y/o cambio de empleo

- La Dirección de Talento Humano, la Oficina de Tecnologías de la Información y las Comunicaciones, la Subdirección de Servicios Administrativos y el Jefe Inmediato del funcionario y/o supervisor tanto del proveedor, contratista o funcionario, serán los encargados del proceso de terminación de la vinculación laboral y/o terminación de contratos y asegurarán que todos los activos 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 el Sistema Integrado de Gestión.
- En caso de que un funcionario, contratista y proveedor tenga un cambio de funciones, 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.

10.4.4. Gestión de Activos.

- La Secretaría General de la Alcaldía Mayor de Bogotá cuenta y aplica el documento 2213200-PR-187 Activos de Información para identificar y clasificar los activos de información de todos los procesos al interior de la Entidad.

10.4.4.1. Responsabilidad por los activos de 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, actualizado una vez al año.
- Todos los funcionarios, contratistas y proveedores deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de la Secretaría General.

- 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.

10.4.4.2. Manejo de medios

- La Oficina de Tecnologías de la Información y las Comunicaciones tiene implementado a través de la consola antivirus el escaneo de medios removibles que son conectados para la búsqueda de virus o malware en éstos de manera automática.
- Los funcionarios, contratistas y proveedores se comprometen a asegurar física y lógicamente el dispositivo a fin de no poner bajo ningún riesgo, la información de la Secretaría General y los demás activos de información bajo su custodia.
- Cuando se crea una 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 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 confidencial y/o sensible, y así mismo, la información que el funcionario, contratista o proveedor haya producido en el marco de sus funciones y/o responsabilidades, 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.

10.4.5. Control de Accesos.

- En caso de observar incidentes de seguridad sobre los activos de información o los datos o información, éstos deben ser reportados a través del correo electrónico oticsoporte@alcaldiabogota.gov.co .
- Todos los funcionarios, contratistas y 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.
- Los accesos tanto físicos como lógicos asignados a los funcionarios, contratistas y proveedores deberán ser desactivados y/o modificados una vez terminados los vínculos contractuales con la **Secretaría General de la Alcaldía Mayor de Bogotá D.C**., teniendo

en cuenta los comunicados emitidos de la Dirección de Talento Humano y la Dirección de Contratación.

- El responsable del área restringida establecerá los controles necesarios para limitar el acceso a éstos, determinará los mecanismos de registro, datos de identificación funcionario, contratista, proveedor o aliado que accede al área restringida, el motivo del ingreso, el tiempo empleado para el desarrollo de la actividad, la información consultada si es del caso, y cuidará que un responsable del área acompañe a la persona durante su estancia en ella.
- En caso de que existan identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente individualizados los responsables, validados y gestionados los respectivos riesgos de seguridad de la información y de esta manera, encontrarse aprobados los controles respectivos por la Oficina de Tecnologías de la Información y las Comunicaciones.

10.4.5.1. Requisitos del negocio para control de acceso Internet

- La Oficina de Tecnologías de la Información y las Comunicaciones es la única dependencia encargada de proveer el servicio de acceso a internet, así como de vigilar su correcto uso y funcionamiento.
- La Oficina de Tecnologías de la Información y las Comunicaciones asignará los permisos de acceso conforme a la necesidad que requiera para la ejecución de las labores de los funcionarios, contratistas, proveedores y aliados a través de las políticas definidas y establecidas en el firewall perimetral de la Entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones, cuenta con la facultad para bloquear todos aquellos sitios de Internet que considere que no son compatibles con las labores de los funcionarios, contratistas, proveedores y aliados.
- No está permitido el uso e ingreso a paginas relacionas con pornografía, drogas, terrorismo, segregación racial, hacking, chat, redes sociales, correos electrónicos personales, WhatsApp Web, YouTube, música, videos, TV, juegos y similares que promuevan y atenten contra los principios de Confidencialidad, Integridad, Disponibilidad y Privacidad de los datos e información, salvo que dicha información se requiera para el ejercicio de las funciones al cargo y no exista otro medio para consultarla.
- 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 funcionarios 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, los usuarios utilizarán únicamente los servicios para los cuales están autorizados.

10.4.5.2. Mensajería instantánea

- Microsoft Teams, es la herramienta autorizada de mensajería instantánea (remoto, chats, llamadas y video conferencias) en la Entidad.
- Para iniciar sesión se debe ingresar con las credenciales autorizadas y entregadas por la Oficina de Tecnologías de la Información y las Comunicaciones al ingreso en la Entidad y que se encuentran creadas en el directorio activo.
- La configuración y seguridad de los chats y reuniones se encuentran incluidos en la confidencialidad e integridad de la herramienta, las cuales pueden ser visualizadas por los usuarios de la Secretaría General.

10.4.5.3. Acceso a redes y servicios de red

- Los equipos de terceros que requieran acceder a la red de la Entidad deben cumplir con el procedimiento de sanitización informática antes de conceder dicho acceso.
- Los equipos de terceros que hayan sido autorizados para acceder a las redes de datos de la Entidad solo podrán hacerlo una vez haya cumplido con el escaneo para determinar si cuenta con software defectuoso, malicioso o que pueda afectar la operación de la Entidad al realizar la conexión a la red, y así mismo, cuando se termine la vinculación laboral, debe pasar por la revisión respectiva para proceder a la eliminación de información de la Entidad.
- Los equipos que se conecten a la red y sean de contratistas o terceros deben contar con software debidamente licenciado y legal.
- Ningún funcionario, contratista, proveedor o aliado está autorizado para conectar computadores de escritorio, computadores portátiles y demás recursos tecnológicos que no sean propiedad o bajo el dominio de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**, de manera cableada o inalámbrica.
- El personal de la Oficina de las Tecnologías de la Información y de las Comunicaciones es

el único autorizado para conectar equipos de escritorio, equipos portátiles y demás recursos tecnológicos a la red de la Entidad, siempre y cuando se cumplan los requisitos para hacerlo.

- Los accesos a la red inalámbrica deberán ser autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones, previa verificación de que cuente con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.
- Sólo personal autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones 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.,** así mismo, las conexiones establecidas para este fin utilizan esquemas y herramientas de seguridad los cuales son definidos y administrados por la mencionada oficina.
- 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, los cuales permiten realizar conexiones con cualquier dispositivo y estos atentan contra la seguridad y privacidad de los datos e información que se almacenan en los activos de información de la **Secretaría General de la Alcaldía General de Bogotá D.C.**

10.4.5.4. Recursos compartidos

10.4.5.4.1. <u>Carpetas compartidas</u>

- Para las carpetas compartidas en red, se asignan los respectivos permisos de acceso al funcionario, 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 son 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.**

10.4.5.4.2. <u>Sistemas de Información</u>

- Se tiene 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 para mantener la seguridad del identificador del equipo.

- Se controla el acceso físico y lógico a los puertos de diagnóstico y configuración.
- A través de la consola antivirus se garantiza 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.
- A través de la consola antivirus se validan los puertos, servicios y prestaciones similares instaladas en los equipos de escritorio, portátiles o equipos de red que no se requieran específicamente para la funcionalidad de la Entidad y se deshabilitan o en otros casos, se retiran.

10.4.5.5. Control de acceso a sistemas y aplicaciones

- La creación de usuarios de ciertos aplicativos se encuentra a cargo de los líderes funcionales o la dependencia que administre o tenga el control correspondiente del aplicativo.
- Se cuenta con el control de acceso limitado y controlado a los datos e información que se encuentran en los ambientes de desarrollo y productivos por parte de los desarrolladores internos o externos que se encuentren laborando para la Entidad.
- Se cuenta con el control hacia 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.** solo al personal autorizado y así mismo, se lleva el respectivo control de los cambios autorizados y realizados al código fuente de éstos.

10.4.5.6. Gestión de acceso de usuarios

- El acceso a las plataformas, aplicaciones, servicios y en general a cualquier recurso de información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** cuenta con las autorizaciones de los dueños de procesos propietarios de éstos para su acceso.
- Los privilegios de acceso se asignan a los usuarios de acuerdo con las necesidades y eventos, sólo y durante el tiempo requerido y aprobado para ello.
- Toda asignación de permisos de acceso cuenta con previa autorización del Jefe, Director y/o Subdirector de área responsable, y se soporta a través de la herramienta de mesa de

servicio por medio del formato 4204000-FT-1000.

- La entrega de las credenciales del usuario (cuenta y contraseña de red), se entrega a través de la mesa de servicio, quien indica una contraseña genérica y de esta última, el usuario realiza el cambio inmediatamente de la contraseña.
- Así mismo, recibirá por medio de correo electrónico la bienvenida e indicaciones sobre el uso de los accesos y su comportamiento durante la ejecución de sus funciones y/u obligaciones contractuales.
- Cuando el usuario solicita el cambio de la contraseña y se encuentre fuera del dominio o la red, lo realiza a través de solicitud a la mesa de servicios para una nueva asignación de contraseña y esta se envía por medio de la herramienta establecida, la cual cuenta con la opción ***privado,*** y es sólo visualizada por el usuario solicitante.
- Los derechos de acceso de todos los funcionarios, contratistas, proveedores y aliados para acceder a los datos e información y a los servicios de procesamiento de información se retiran al terminar el vínculo laboral y/o se deben ajustar cuando existan cambios de dependencias y/o responsabilidades.

10.4.6. Criptografía.

- La administración de claves criptográficas y certificados digitales estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.
- El software que se desarrolla en la Entidad o por un tercero y que amerite alto nivel de confidencialidad utiliza un algoritmo de cifrado de datos solo cuando dentro de los requerimientos funcionales del sistema de información lo especifica o cuando un requisito de ley así lo exige.

10.4.7. Gestión de llaves.

- Todas las claves criptográficas de la Entidad están resguardadas en sistemas de cifrado que garantizan la confidencialidad integridad y disponibilidad, en caso de desastres y/o incidentes que se presenten en la Entidad.
- La solicitud de generación de claves de criptografía sobre los sistemas de información y/o comunicación de la Entidad se realiza de manera formal a través de una solicitud por medio del correo electrónico oticsoporte@alcaldiabogota.gov.co .
- Las llaves criptográficas cuentan con un tiempo de vida establecido, las cuales son

revisadas y/o actualizadas de manera periódica, con el propósito de mitigar riesgos asociados a claves no usadas, claves comprometidas, claves no deshabilitadas de usuarios y/o sistemas no vigentes de la Entidad.

- Los funcionarios, contratistas y proveedores autorizados para el acceso/uso de claves las de criptografía son responsables por preservar la confidencialidad, la integridad y la disponibilidad.

10.4.8. Seguridad Física y Ambiental.

- Todos los funcionarios, contratistas, proveedores y aliados portan el carné vigente de la Secretaría General en un lugar visible y durante su permanencia en la Entidad.
- Todos los terceros se registran al ingreso y portan el desprendible que lo acredita como visitante y el carné de la Entidad de la cual proviene en un lugar visible y durante su permanencia en la Entidad, y así mismo ingresan y están en acompañamiento en todo momento por un funcionario o contratista responsable de sus labores al interior de la Entidad.
- No se permite albergar, mantener y/o guardar elementos inflamables dentro de las áreas destinadas al procesamiento 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.

10.4.8.1. Áreas seguras

- Se establecieron y asignaron permisos de acceso a las dependencias, oficinas, centros de cableado, data center, salas de capacitación y similares únicamente a los funcionarios, contratistas, proveedores y aliados autorizados para su ingreso.
- Las puertas de acceso a cada una de las dependencias, oficinas, centros de cableado, data center, salas de capacitación y similares permanecen cerradas y en lo posible bajo llave en ausencias temporales y/o totales.
- Todas las personas portan el carnet que los acredita como funcionarios, contratistas, proveedores y aliados de la Secretaría General en un lugar visible y durante su permanencia en la Entidad.
- Los funcionarios, contratistas, proveedores y aliados cuentan con la respectiva tarjeta de proximidad para el ingreso a las instalaciones de la **Secretaría General de la Alcaldía**

Mayor de Bogotá D.C.

- Todos los terceros se registran al ingreso de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** en donde reciben un sticker que lo acredita como visitante y una tarjeta de acceso si se requiere. Este sticker lo portan en un lugar visible durante su permanencia en la Entidad y lo devuelven junto con la tarjeta de acceso en momento de retirarse de la Entidad.
- Todas las áreas destinadas al procesamiento 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 de acceso restringido y en consecuencia cuentan con controles adecuados para el control de acceso.
- Los centros de cómputo, cableado y cuartos técnicos de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** cuentan con mecanismos adecuados contra las amenazas ambientales: temperatura, humedad, fuego, etc.), especificados por los fabricantes de los equipos que albergan,
- por otro lado, se debe registrar el ingreso de los visitantes, funcionarios y contratistas en una bitácora ubicada a la entrada de estas áreas de forma visible y se realiza en el Formato 4204000-FT-267.
- Todos los terceros ingresan y están acompañados durante la ejecución de las actividades por un por un funcionario, contratista y/o tercero de la Entidad a los centros de cómputo, cableado y cuartos técnicos de la Entidad.
- Se modifica de manera inmediata los privilegios de acceso físico al centro de cómputo, cableado y cuartos técnicos, en los eventos de desvinculación o cambio en las labores de un funcionario o contratista autorizado.

10.4.8.2. Equipos

- Los funcionarios, contratistas y proveedores que utilizan los equipos institucionales en préstamo deberán comprometerse a no divulgar dicha información firmando Formato *4204000-FT-1186 Acuerdo de confidencialidad y reserva de manejo de información* y el formato *42331000-FT-311 Autorización de salida de elementos de la Subdirección de Servicios Administrativos.*
- Los funcionarios, contratistas y proveedores no deben realizar cambios en los equipos de escritorio o portátiles que les sean asignados en la configuración que ya le son

entregados a nivel de: conexiones de red, usuarios locales, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por la Oficina de Tecnologías de la Información y las Comunicaciones.

- Toda la infraestructura tecnológica cuenta con estándares de seguridad (hardening), para su respectivo funcionamiento.
- El Oficial de Seguridad de la Información establece los controles e identifica, clasifica, valora y analiza los riesgos que garantizan los principios de Confidencialidad, Disponibilidad e Integridad de la información.
- El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información permanecen protegidos a través de canaleta para evitar el deterioro y disponibilidad del servicio.
- Los centros de cómputo, cableado y cuartos técnicos permanecen debidamente marcados para reducir riesgos por manipulación.
- Durante las actividades de mantenimiento preventivo y/o correctivo se mantiene la concordancia con los intervalos y especificaciones del proveedor, así mismo, se generan los registros a que haya lugar en donde se realiza la trazabilidad de las fallas, personas involucradas y actividades desarrolladas.
- 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 responsable y sus registros de ingresos y salidas pertinentes.
- Todos los equipos que contengan información sensible y/o confidencial en sus medios de almacenamiento pasan por un procedimiento de borrado seguro y es aprobado por el Jefe de Tecnologías de la Información y las Comunicaciones antes de su reutilización o finalización de su vida útil.
- La información sensible o confidencial de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** se recoge de las impresoras de manera inmediata una vez impresa.

10.4.8.3. Política de escritorio y pantalla limpia

- La información sensible o confidencial de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** se recoge de las impresoras de manera inmediata una vez impresa.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas

las aplicaciones y dejar los equipos apagados.

- Los funcionarios, contratistas y proveedores son responsables de mantener el escritorio del equipo de cómputo libre de información sensible, confidencial y de uso diario (Carpetas, archivos, accesos directos y similares), para evitar el fácil acceso a la información.
- Todos los funcionarios, contratistas y proveedores bloquean la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario.
- Al finalizar las actividades laborales, los funcionarios, contratistas y proveedores cierran todas las aplicaciones y dejan los equipos apagados.

10.4.9. Seguridad en las Operaciones.

10.4.9.1. Procedimientos operacionales y responsabilidades

- Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones 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.
- Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones monitorear, revisar, proyectar y dar soporte oportuno para el uso y desempeño aceptable de capacidad sobre la infraestructura tecnológica.
- El mantenimiento y el copiado de las librerías fuente de programas deben estar sujetos a un procedimiento estricto de control de cambios.
- Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones separar los ambientes de desarrollo, pruebas y producción de los desarrollos internos y externos.
- La Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, deberá mantener actualizados los manuales y guías de los Sistemas de Información, aplicativos y sitios web con los que cuenta la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

10.4.9.2. Controles contra códigos maliciosos

- Es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones

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 licenciamiento de antivirus licenciado y contar con las medidas de seguridad apropiadas.
- Únicamente el administrador de la plataforma de antivirus cuenta con los permisos necesarios para deshabilitar, remover, eliminar y/o desinstalar el software de antivirus, estas actividades se llevan a cabo bajo autorización previa del jefe de la Oficina de Tecnologías de la Información y las Comunicaciones.
- Se realizan escaneos a intervalos regulares como control del estado de la infraestructura tecnológica
- Los funcionarios, contratistas, proveedores y aliados no realizan cambios en la configuración del software de antivirus.
- Se garantiza que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos de la Entidad.
- Ante cualquier sospecha o detección de alguna infección por software malicioso se notifica a la Oficina de Tecnologías de la Información y las Comunicaciones para que se tomen las medidas de control correspondientes.

10.4.9.3. Copias de respaldo

- La Oficina de Tecnologías de la Información y Comunicaciones, tiene el compromiso de la generación de copias de respaldo y almacenamiento de su información confidencial, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades, de igual manera definirá la estrategia a seguir y los periodos de retención una vez realizada la copia a cinta.
- La Oficina de Tecnologías de la Información y Comunicaciones, vela porque los medios magnéticos que contienen información de la Secretaría General se almacenen en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguarden las copias de respaldo cuenta con los controles de seguridad física y medioambiental apropiados.

- Para la restauración de las cintas los administradores funcionales de las dependencias que tengan su backup dentro del software DataProtector solicitan una restauración trimestral, con el fin de que el administrador de copias de respaldo seleccione la cinta aleatoria del trimestre y la información sea entregada al administrador funcional, para que verifique la autenticidad la restauración de la información.
- Se cuenta con la guía para la ejecución los procedimientos para de la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- Ningún funcionario, contratista o proveedor está autorizado para realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto es fuga de información.

10.4.9.4. Registro y seguimiento

- Para los nuevos sistemas desarrollados in-house o por un proveedor, se producen registros de las actividades de auditoría, excepciones, eventos, fallas y se conservan bajo el periodo establecido por el área funcional y de acuerdo con la Oficina de Tecnologías de la Información y las Comunicaciones.
- 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.
- Todos los relojes de los sistemas de procesamiento de información de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** están sincronizados con la fuente de hora exacta definida por el Gobierno Nacional, a través de la Superintendencia de Industria y Comercio.
- Se hacen 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.

10.4.9.5. Control de software operacional

- La Oficina de Tecnologías de la Información y las Comunicaciones establece una guía para la instalación del software en la Entidad.
- El software instalado en la Entidad cuenta con su respectiva licencia de validez y legalidad

en el mercado.

- Para las dependencias que solicitan la instalación de software libre, la Oficina de Tecnologías de la Información y las Comunicaciones realiza el análisis, verificación y la aprobación para la correspondiente instalación.
- La Oficina de Tecnologías de la Información y las Comunicaciones, verifica el normal funcionamiento de los aplicativos que se entregan a o están en producción de la Entidad, con el objetivo de no afectar la integridad, disponibilidad y desempeño de estos.
- 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, y por tanto son los únicos autorizados para llevar a cabo esta labor.
- 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, y es de aclarar que cuando se encuentre software instalado en los equipos que no esté debidamente licenciado, el funcionario, contratista o proveedor del equipo es responsable de las consecuencias que se presenten ante la materialización eventos o incidentes de Seguridad.
- La Oficina de Tecnologías de la Información y las Comunicaciones define y actualiza de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los equipos de la Entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones se asegura que para las aplicaciones desarrolladas internamente o por la Entidad y las de terceros se realicen las respectivas pruebas antes de salir a producción.
- La Oficina de Tecnologías de la Información y las Comunicaciones autoriza los accesos temporales y controlados a los terceros para realizar las actualizaciones sobre el software, así como monitorea las actualizaciones, en caso de ser necesario.
- La Oficina de Tecnologías de la Información y las Comunicaciones valida los riesgos que genera la migración hacia nuevas versiones de software.

10.4.9.6. Gestión de las vulnerabilidades técnicas

- Se realizan análisis de vulnerabilidades sobre toda la infraestructura tecnológica para evaluar los riesgos a los cuales se encuentran expuestos y generar los planes de tratamiento apropiados para mitigar dichos riesgos.

- No está permitido que los funcionarios, contratistas, proveedores y aliados realicen pruebas y/o aprovechen las debilidades de seguridad en la infraestructura tecnológica.
- Se debe restringir la práctica de instalación de software no autorizado a través de políticas de dominio y se otorgan los permisos únicamente a los funcionarios, contratistas o proveedores autorizados.

10.4.9.7. Consideraciones sobre auditorías de sistemas de información

- Se realizan revisiones internas programadas a los sistemas de información nuevos, desarrollados in-house o por intermedio de terceros, con el fin de determinar si las políticas, procesos, procedimientos y controles establecidos dentro del Sistema de Gestión de Seguridad de la Información se encuentran conforme con los requerimientos institucionales, requerimientos de seguridad, regulaciones aplicables, y si éstos se encuentran implementados y mantenidos eficazmente.

- Estas auditorías se ejecutan según lo establecido en el programa de auditorías definido por la Entidad y en caso de ser necesario se pueden programar revisiones parciales o totales sobre una o varias líneas de acción o trabajo, dependencia, etc., con el fin de verificar la eficacia de las acciones correctivas.

10.4.10. Seguridad en Comunicaciones.

10.4.10.1. Gestión de la seguridad de las redes

- Únicamente los funcionarios, contratistas, proveedores y aliados autorizados por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, previa solicitud a través de correo electrónico por parte de la dependencia que lo requiera se conecta a la red inalámbrica de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** siempre y cuando el equipo de cómputo sea propiedad de la Entidad. En algunos casos excepcionales por solicitud del despacho de la Alcaldía Mayor de Bogotá se suministra una contraseña temporal a eventos especiales como reuniones de alto nivel que involucran personas de otras Entidades.
- La conexión a redes inalámbricas externas para funcionarios, contratistas y proveedores con equipos portátiles de propiedad de la **Secretaría General de la Alcaldía Mayor de**

Bogotá D.C. que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la Entidad deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones.

- Los servicios de información, usuarios y sistemas de información se segregan en las redes.
- Se implementaron controles "routing" para las redes que aseguran las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso.
- Las redes manejan de una manera adecuada y debidamente controladas para protegerlas de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito a través del documento 4204000-GS-091 Guía de la Administración para la gestión de red LAN, WAN, Wireless y dispositivos de seguridad de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**
- Se tiene distribuida la red conforme a los roles y responsabilidades de los funcionarios, contratistas, proveedores y aliados de la Entidad haciendo uso de VLANs, y se restringe el acceso remoto de las plataformas por medio del uso de VPN previamente autorizadas y de acuerdo con lo establecido en el presente documento.
- Se realiza 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.
- La comunicación entre Entidades internas y externas a través de accesos dedicados, conmutados y/o públicos, se monitorea en todo momento.
- Se aplican los respectivos controles para la detección de intrusos con el fin de detectar cualquier tipo de actividad contra los sistemas presentes.
- Se configuraron las reglas específicas en el Firewall, teniendo en cuenta únicamente los servicios, puertos, 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 de la Alcaldía Mayor de Bogotá D.C.**

10.4.10.2. Transferencia de información

- Se deben establecer y hacer firmar acuerdos para la transferencia de información, confidencialidad o no divulgación para la transferencia de información con las partes

interesadas.

- El único servicio de correo electrónico controlado por la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** es el asignado directamente por la Oficina de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
- 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, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.

10.4.11. Adquisición, Desarrollo y Mantenimiento de Software.

10.4.11.1. Requisitos de seguridad de los sistemas de información

- La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** cuentan con la respectiva identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información.
- La solicitud de los requerimientos para los sistemas nuevos y/o mejoras en los sistemas existentes especifican los requerimientos de los controles de seguridad cuando los hubiere.
- El suministro de la información para prueba de aplicaciones es validado por el área usuaria de la aplicación para asegurar que la data es correcta y apropiada. Se validan los acuerdos de confidencialidad para asegurar la respetiva eliminación de dicha información.
- Los desarrolladores deshabilitan las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores aseguran que no se permitan conexiones concurrentes a los sistemas de información con el mismo usuario.

10.4.11.2. Seguridad en los procesos de desarrollo y de soporte

- Se incorporan chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
- Se cumplen con las revisiones entre funcional y desarrollador, realizando pruebas de

calidad antes de desplegar aplicaciones o correcciones en producción

- adicionalmente se gestionan las autorizaciones de despliegue por parte de los funcionales y se guardan las evidencias de dicho proceso.
- Se aclaran 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.
- Se monitorea el desarrollo de software donde se cuenta con el acuerdo de licenciamiento el cual especifica las condiciones de uso del software y los derechos de propiedad intelectual.
- La Oficina de Tecnologías de la Información y las Comunicaciones en conjunto con los propietarios de los aplicativos realizan las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.
- Se implementan 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 como por el área usuaria del sistema o aplicativo en cuestión.
- Los desarrolladores garantizan 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, se implementan mensajes de error genéricos.
- Los desarrolladores suministran opciones de desconexión o cierre de sesión de los aplicativos (logout) que permiten terminar completamente con la sesión o conexión asociada, las cuales se encuentran disponibles en todas las páginas protegidas por autenticación.

10.4.11.3. Política de desarrollo seguro

- Todo software construido por la Entidad o construido por un tercero utiliza un ambiente de cifrado de datos sólo cuando dentro de los requerimientos funcionales del sistema de información se haya especificado, o cuando un requisito de ley así lo exija.
- Se garantiza el control de cambios a los sistemas, sitios web y aplicativos: este control está asegurado 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 hay actualizaciones, mejoras o funcionalidades nuevas a los que están en ambiente productivo, se documenta el control de ese cambio mediante el formato que la Oficina de Tecnologías de la Información y las Comunicaciones tiene definido para el efecto, el cual debe contar con la aprobación tanto de la dependencia funcional como de la mencionada Oficina.

10.4.11.4. Datos de prueba

- Se selecciona cuidadosamente, se protege, se genera y se controla la data para prueba.
- No se permite el uso y copia de información operacional como datos de pruebas, salvo autorización previa del Oficial de Seguridad de la Información y el responsable del activo, o previa ejecución de procesos de anonimización de ésta. Esta autorización se solicite cada vez que se requiere realizar la copia 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.
- Se certifica que la información entregada a los desarrolladores para realizar las pruebas no revela información confidencial de los ambientes de producción.

10.4.12. Relaciones con proveedores.

10.4.12.1. Seguridad de la información en las relaciones con los proveedores

- En los casos a los que diera lugar la Entidad podrá exigir controles adicionales a los proveedores con quienes tiene relaciones comerciales tales como:
    - La identificación y documentación del proveedor.
    - Realizar acuerdos de Confidencialidad con relación a transferencias de la información.
    - Mantener un proceso y un ciclo de vida para la gestión de las relaciones con el proveedor.
    - 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.

- 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.
- 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.
- La formación, para toma de conciencia del personal de la Entidad involucrado en contratación, relativa a políticas, procesos y procedimientos aplicables.

10.4.12.2. Gestión de la prestación de servicios de proveedores

- 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 de confidencialidad respectivos debidamente firmados.
- 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.
- 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.

10.4.13. Gestión de Incidentes de Seguridad de la Información.

10.4.13.1. Gestión de incidentes y mejoras en la seguridad de la información

- La mesa de servicios se encuentra disponible para el reporte formal de eventos que son reportados por los funcionarios, contratistas y proveedores que sean posiblemente sospechosos de incidentes de seguridad de la información para ser registrado en la respectiva herramienta de gestión y escalado al Oficial de Seguridad de la Información.
- Todos los funcionarios, contratistas, proveedores y aliados de la Entidad conocen que deben realizar el reporte de eventos posiblemente sospechosos como incidentes de seguridad a la cuenta de correo: oticsoporte@alcaldiabogota.gov.co .

- Se toman acciones correctivas oportunas ante los eventos e incidentes de seguridad reportados, con base en el aprendizaje obtenido en la gestión de incidentes de seguridad en la Entidad.
- Es deber de todos los funcionarios, contratistas, proveedores y aliados usuarios de los sistemas y servicios de información, reportar cualquier evento o incidente que atente contra la seguridad de los activos de información.
- Se mantienen 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 cuenta con los soportes que sean exigidos por una acción legal (sea civil o criminal).
- Se cuenta con las categorías de los incidentes de seguridad y conforme a la criticidad, se establecen los mecanismos de atención adecuados para su solución.

10.4.14. Aspectos de Seguridad de la Información en la Continuidad de Negocio.

10.4.14.1. Continuidad de seguridad de la información

- La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** planifica, implementa, verifica, revisa y evalúa 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 realiza 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.
- Todos los funcionarios, contratistas, proveedores y aliados de la **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** participan en las actividades que son designadas por el Comité Institucional de Gestión y Desempeño, para las pruebas de continuidad del negocio y cumple con los controles establecidos por el Sistema de Gestión de Seguridad de la Información para la satisfacción de las pruebas.
- El Comité Institucional de Gestión y Desempeño asigna el recurso necesario para la ejecución de las pruebas de continuidad del negocio.
- Se establecen responsabilidades para la ejecución y puesta en marcha de los planes de continuidad del negocio.
- Los planes de continuidad se planean, prueban y actualizan de manera regular para asegurar que son fiables y efectivos.

10.4.14.2. Redundancias

- Se analizan y se establecen los requerimientos de redundancia para los sistemas de información que son utilizados en los procesos críticos y la plataforma tecnológica.
- La Oficina de Tecnologías de la Información y las Comunicaciones implementa las redundancias suficientes y garantiza la Confidencialidad, Integridad y Disponibilidad de la infraestructura tecnológica.
- La dependencia funcional y la Oficina de Tecnologías de la Información y las Comunicaciones establecen la prioridad de las aplicaciones para ser incluidas en los ambientes redundantes de la Entidad.

10.4.15. Cumplimiento.

10.4.15.1. Cumplimiento de requisitos legales y contractuales

- Las aplicaciones y sistemas de la Entidad cuentan con la implementación de registros de auditoría que permiten establecer la trazabilidad de una operación 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 protegen y almacenan por el tiempo definido por los entes de control y vigilancia.
- La Oficina de Tecnologías de la Información y las Comunicaciones documenta las acciones que realiza en la revisión periódica de logs de auditoría en las aplicaciones y sistemas críticos de la Entidad.
- La Oficina de Control Interno Interna realiza 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.
- La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** identifica y garantiza 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 definen, documentan y actualizan 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 asegura que el software que se utiliza se instala y se usa en la Entidad cumple con los requisitos de derechos de auto, licenciamiento de uso y es original.
- Los funcionarios, contratistas, proveedores y aliados cumplen con las leyes de derechos de autor y acuerdos de licenciamiento de software.
- La Oficina Asesora Jurídica, Dirección de Contratación y/o la Oficina de Tecnologías de la Información y las Comunicaciones establecen 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

10.4.15.2. Revisiones de seguridad de la información

- La **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** cuenta con revisiones periódicas para revisar y 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.
- Los responsables de activos de información garantizan que los roles y responsabilidades, controles, procedimientos y estándares de seguridad cumplen dentro de su área de responsabilidad.
- Los sistemas de información se chequean de manera regular para 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 realizan revisiones técnicas con lo cual se determina el incumplimiento de los controles establecidos para tomar acciones de mejora sobre éstos.
- El Comité Institucional de Gestión y Desempeño de **Secretaría General de la Alcaldía Mayor de Bogotá D.C.** apoya y promueve las revisiones del cumplimiento de las políticas de seguridad de la información definidas en el presente documento y/o cualquier otro requerimiento de seguridad.

11. GLOSARIO.

Activo de información: Este tipo de activo hace relación a los datos o información que tiene para la Entidad valor en los procesos del modelo de negocio, independientemente de su ubicación. Puede ser un documento físico, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad.

Amenaza informática: Es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS), de la Secretaría General de la Alcaldía Mayor de Bogotá.

Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos de los activos o bienes de información e identificar sus fuentes.

Autenticación: Garantía de que un el funcionario es quien realmente se autentica en el sistema al cual está intentando ingresar, se realiza a través de la validación de directorio activo de la Secretaría General de la Alcaldía Mayor de Bogotá.

Ciberdefensa: Es el empleo de las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.[11]

Ciberespacio: Es el ambiente, tanto físico como virtual, compuesto por sistemas computacionales, programas y aplicaciones (software), redes de telecomunicaciones incluido el internet, datos e información y la infraestructura física asociada que es utilizada para la interacción entre usuarios, entre máquinas y entre máquinas y usuarios.[12]

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la Entidad en el ciberespacio.[13]

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, Entidades o procesos no autorizados.

Continuidad del negocio: Plan orientado a permitir la continuidad de las principales

[11] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[12] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Resolución CRC.**

[13] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Resolución ITU.**

funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, ya sean de carácter administrativo, técnico o legal.

Copia de seguridad: Copia de respaldo de la información.

Criticidad: Medida del impacto que tendría la Entidad debido a un incidente de seguridad de un sistema y que éste no funcione como es requerido.

Custodio: Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.

Encargado de Activo de Información: Individuo, cargo, grupo de trabajo o proceso designado por la Entidad para administrar y hacer efectivos los controles que el responsable del activo haya definido, con base en los controles de seguridad disponibles en la Entidad.

Equipo de Cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Gestión de claves: Actividad dirigida a establecer y aplicar los controles que se realizan mediante la implementación de claves criptográficas.

Gestión de incidentes de seguridad de la información: Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo. Se compone de la identificación, evaluación y el tratamiento de riesgos.

Habeas data: Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Incidente de Seguridad de la Información: Cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Impacto: El costo para la empresa a causa de un incidente -de la escala que sea-, que

puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Infraestructura: Conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una Entidad cualquiera.[14]

Infraestructura Cibernética (Ic): Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO).[15]

Infraestructura Crítica (IC): Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.[16]

Infraestructura Crítica Cibernética (ICC): Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.[17]

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Infraestructura Estratégica (IE): Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales.[18]

Infraestructura Estratégica Cibernética (IEC): Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales.[19]

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

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, que tengan valor para la Entidad y necesiten por tanto ser protegidos de potenciales riesgos.

---

[14] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[15] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[16] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Ley 8/2011-Gobierno de España.**

[17] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

[18] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Adaptación Ley 8/2011-Gobierno de España.**

[19] Sectores Estratégicos de la República de Colombia desde la óptica Cibernética - Un acercamiento a la Identificación de la Infraestructura Crítica Cibernética Nacional - **Comando Conjunto Cibernético – CCOC Fuente: Ministerio de Defensa.**

Medio removible: Medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB, o similares que a futuro llegaren a utilizarse para este fin.

Parte interesada externa: Ente de control definido dentro del contexto Gubernamental y que se encuentre autorizado para realizar revisiones a través de auditorías o, actúe como asesor para el monitoreo, revisión y actualizaciones del Sistema de Gestión de Seguridad de la Información de la Secretaría General de la Alcaldía Mayor de Bogotá.

Parte interesada interna: funcionario que pertenezca a cualquier dependencia de la Secretaría General de la Alcaldía Mayor de Bogotá, así como sus proveedores y usuarios finales de los servicios de la Entidad.

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.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario/responsable: Individuo, cargo, grupo de trabajo o proceso, designado por la Entidad, que tiene la responsabilidad de identificar, definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información a su cargo.

Responsable de activo de información: Es el funcionario de velar porque la información a su cargo sea protegida de manera adecuada.

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 consideraciones.

Segregación de tareas: Reparto de tareas sensibles entre distintos funcionarios para reducir el riesgo del mal uso, deliberado o por negligencia, de los sistemas o información.

Seguridad de la información: Preservación de la Confidencialidad, Integridad y Disponibilidad de la información.

Sensibilidad: Nivel de impacto que una divulgación no autorizada podría generar.

Servicio: Es cualquier acto o desempeño que la Entidad o sus funcionarios pueden ofrecer a otras personas, en desarrollo de su objeto y funciones.

Sistema de Gestión de Seguridad de la Información: 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, basando en un enfoque de gestión y de mejora a un individuo o Entidad.

Soportes físicos: Datos en soporte papel (cartas, informes, normas, contratos) o en medios de almacenamiento físico.

Terceros: Toda persona jurídica o natural, que se relacionan con la Secretaría General de la Alcaldía Mayor de Bogotá como proveedores, proveedores o consultores, que proveen servicios o productos a la Entidad.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

CONTROL DE CAMBIOS			
ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	**DETALLE DE LOS CAMBIOS EFECTUADOS**	**FECHA DEL CAMBIO**	**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 a la resolución de la Política de Privacidad y Tratamiento de Datos Personales y el “Manual de Políticas y Procedimientos para el	21/07/2020	02

CONTROL DE CAMBIOS			
ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	**DETALLE DE LOS CAMBIOS EFECTUADOS**	**FECHA DEL CAMBIO**	**VERSIÓN**
	Tratamiento de Datos Personales", y su finalidad. Se incluyó en la Política para desarrollo seguro, el tema de control de cambios.		
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