	Responsable del Proceso	**Dirección de Planeación**
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	Wisman Yesid Cotrino García	Michael Andrés Ruiz Falach
Cargo:	Director Técnico	Director Técnico
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	Dirección de Planeación
R.R. Nº 012		**Fecha: Abril 22 de 2021**

COPIA CONTROLADA

Andrés Castro Franco
Contralor de Bogotá, D.C.

Patricia Duque Cruz
Contralora Auxiliar

Michael Andrés Ruiz Falach
Director Técnico de Planeación

Wisman Yesid Cotrino García
Director Técnico de Tecnologías de la Información y las Comunicaciones

Marzo de 2021

COPIA CONTROLADA

TABLA DE CONTENIDO

COPIA CONTROLADA

COPIA CONTROLADA

1. INTRODUCCIÓN

La Contraloría de Bogotá, D.C. como Entidad que vigila la gestión fiscal de la Administración Distrital y de los particulares que manejan fondos o bienes públicos, en el ejercicio de sus deberes constitucionales se encuentra comprometida con la seguridad de la información y la seguridad digital como parte fundamental de la protección y confianza con el Estado y los ciudadanos, todo enmarcado en el cumplimiento de las leyes y en concordancia con una gestión confiable y efectiva en la vigilancia y control del uso adecuado de los recursos públicos.

Es por esto que en la Contraloría de Bogotá, D.C., la información es un activo fundamental para el cumplimento de las funciones misionales y de apoyo, así como para la toma de decisiones, razón por la cual, existe un compromiso expreso en su protección, como parte de una estrategia orientada a la administración de riesgos y consolidación de una cultura de seguridad, toda vez que con el aseguramiento de la información se busca identificar y minimizar los riesgos a los que se expone y disminuir el impacto generado sobre sus activos, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, disponibilidad y privacidad de la información, acorde con las necesidades del estado, la ciudadanía, los funcionarios, terceros, contratistas, proveedores, sujetos de control, en cumplimiento de las normas legales vigentes.

De conformidad con lo anterior, se establece dentro del Subsistema de Gestión de Seguridad de la Información – SGSI de la Contraloría de Bogotá D.C., el documento de políticas de seguridad de la información y seguridad digital, el cual expresa el compromiso de la alta dirección con la seguridad de la información y seguridad digital, así como, la identificación de las reglas y procedimientos que cada usuario que accede o usa los recursos tecnológicos de la Entidad debe conocer para preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información que usan.

2. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL

La Contraloría de Bogotá, D.C. manifiesta su compromiso con el fortalecimiento de capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en los que puedan verse comprometidos los activos de Información que soportan los procesos de la Entidad, mediante la implementación de medidas para asegurar su confidencialidad, integridad, disponibilidad y privacidad, en el marco de confianza en el ejercicio de sus deberes con el Distrito y los Ciudadanos.

3. OBJETIVO

La Política de seguridad de la información y seguridad digital, busca definir las estrategias, mecanismos y lineamientos mediante los cuales se desarrolla e implementa la Política de seguridad de la información y seguridad digital en la Contraloría de Bogotá D.C., la cual está comprometida con los tres (3) pilares fundamentales de la seguridad de la información - confidencialidad, integridad y disponibilidad -, mediante la gestión y control de la

COPIA CONTROLADA

implementación de la seguridad de la información y la seguridad digital al interior de la entidad, por medio de la definición de roles y responsabilidades en seguridad, la separación de deberes, el contacto con las autoridades y grupos de interés, la incorporación de la seguridad en la gestión de los proyectos y la definición de controles para la mitigación de riesgos digitales, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC. Esta política en la entidad, está a cargo de la Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C.

3.1. OBJETIVOS ESPECIFICOS

- Definir, precisar y formalizar los elementos normativos sobre aspectos de protección de la información.
- Definir y aplicar los lineamientos necesarios en seguridad que permitan proteger los activos de información, buscando mantener la confidencialidad, la disponibilidad e integridad de estos.
- Facilitar de manera integral la gestión de los riesgos de seguridad de la información, seguridad digital y continuidad de la operación institucional.
- Garantizar la integridad, confidencialidad y el acceso a la información de acuerdo con los niveles y criterios de seguridad establecidos por la Entidad y los exigidos por la normatividad vigente.
- Mitigar el impacto de los incidentes de seguridad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.
- Minimizar y dar tratamiento integral a los riesgos de seguridad de la información, de seguridad digital y continuidad de la operación institucional, para que sean conocidos y gestionados de forma eficiente.
- Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad de la información y la seguridad digital.
- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de seguridad de la información y seguridad digital.

4. ALCANCE Y APLICABILIDAD

El alcance del Subsistema de Gestión de la Seguridad de la Información – SGSI, aplica a los activos de información de todos los procesos que conforman el mapa de procesos de la Contraloría de Bogotá D.C.

Por lo anterior, estas políticas aplican a toda la entidad, sus funcionarios, contratistas, sujetos de control fiscal, usuarios internos y externos que acceden o hacen uso de cualquier activo de información, así como exfuncionarios y excontratistas que hayan tenido acceso a cualquier activo de información, independientemente de su ubicación, medio o formato de la Contraloría de Bogotá D.C., así como a la ciudadanía en general que se relacione con el ente de control. De igual manera, esta política aplica a toda la información creada, procesada o utilizada por

COPIA CONTROLADA

la Contraloría de Bogotá D.C., sin importar el medio, formato, presentación o lugar en el cual se encuentre.

5. REVISIÓN, ACTUALIZACION Y APROBACION

La Política de seguridad de la información y seguridad digital de la Contraloría de Bogotá D.C., será revisada anualmente o antes, si existiesen modificaciones que así lo requieran para asegurar su conveniencia, oportunidad, adecuación y eficacia continuas.

Este proceso será liderado por la Dirección de Tecnologías de la Información y las Comunicaciones y/o el Oficial de Seguridad de la Información de la entidad, el cual será revisado y aprobado por el Comité PG-DIGITAL o quien haga sus veces.

6. DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización. [Norma ISO 27000:2018].
Análisis de riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Norma ISO 31000:2018].
Bring Your Own Device (BYOD): Su traducción es "trae tu propio dispositivo", hace referencia a una tendencia que se está generalizando cada vez más en el ámbito empresarial, en la cual los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos (ordenadores portátiles, smartphones y tabletas) para acceder a los recursos de su empresa. [https://computerhoy.com/noticias/moviles/que-es-byod-ventajas-e-inconvenientes-7250]
Confidencialidad: Característica que asegura la intimidad y el secreto de la información que se genera en el proceso de atención entre el servidor público y el ciudadano.
Control: Medida que mantiene y/o modifica el riesgo. [Norma ISO 31000:2018].
Disponibilidad: Propiedad de ser accesible y utilizable a pedido por una entidad autorizada. [Norma ISO 27000:2018].
Entornos VUCA: Acrónimo inglés formado por los términos Volatility (V), Uncertatinty (U), Complexity (C) y Ambiguity (A). Término adaptado a ambientes empresariales, se refiere a la resiliencia de las empresas e instituciones cuando se ven obligadas a adaptarse a los continuos cambios que atacan o afectan su programación estratégica y sus rutinas profesionales sobre cada una de las cuatro variables:
Volatilidad: Existe una enorme dinámica de cambio en la actualidad, que además llegan a una velocidad de vértigo.
Incertidumbre: Se da un notable incremento de situaciones imprevistas en las empresas, lo que significa mayor complejidad a la hora de entender, analizar y diagnosticar situaciones.
Complejidad: Aparecen multitud de situaciones y conflictos que resolver, incluso muchas veces sin una relación causa-efecto detectable, que generan en ocasiones escenarios críticos.
Ambigüedad: Hay una gran falta de claridad en situaciones cotidianas, derivadas de todo lo dicho en las variables anteriores. [https://corporateyachting.es/es/los-entornos-vuca-y-el-nuevo-paradigma-empresarial/].

COPIA CONTROLADA

Gestión del riesgo: Actividades coordinadas para dirigir y controlar la organización con relación al riesgo. [Norma NTC-ISO 31000:2018].
Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. [Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4, octubre de 2018].
Integridad: Propiedad de precisión e integridad. [Norma ISO 27000:2018].
Seguridad Digital: La ciberseguridad o la seguridad digital es el área de una empresa u organización enfocada en procesos informáticos y telemáticos para proteger toda la infraestructura física y digital relacionada con la tecnología computacional. [DocuSign].
Seguridad de la Información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos. [obsbusiness. school].
Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas. [Norma ISO 27000:2018].
Wearable: Palabra proviene del inglés, y hace referencia a accesorios tecnológicos que una persona puede llevar puestos, 'wear' es el verbo, y 'wearable' es el adjetivo que en español se traduciría como ponible. [https://designificados.com/wearable/]

7. POLÍTICAS ESPECÍFICAS DE MANEJO DE INFORMACIÓN

La Contraloría de Bogotá D.C., establece las siguientes políticas específicas de la seguridad de la información que soportan el Subsistema de Gestión de Seguridad de la Información - SGSI de la entidad, a fin de:

- Minimizar el riesgo en los procesos de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de la ciudadanía y funcionarios.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos de la entidad.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, pasantes y grupos de interés de la Contraloría de Bogotá D.C.
- Garantizar la continuidad de Operación Institucional frente a incidentes.

7.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En la Contraloría de Bogotá D.C., se definen los roles, responsabilidades y directrices para gestionar y ejecutar actividades de administración, operación y gestión de la seguridad de la información, y de esta forma prevenir que se presenten conflictos de intereses que conlleven

COPIA CONTROLADA

a modificaciones no autorizadas o el uso inadecuado de los activos de la información.Esto es posible organizando una adecuada comunicación para que la entidad pueda aprobar los lineamientos de seguridad de la información así como coordinar la implementación de la seguridad en todos los procesos de la entidad.

Lineamientos:

7.1.1. Los diferentes roles y sus responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI, se encuentran definidos en el numeral “Liderazgo, Compromiso, Autoridades y Responsabilidades” del manual del Sistema Integrado de Gestión – SIG de la Entidad.

7.1.2. El Comité de Política de Gobierno Digital – PG-DIGITAL - o quien haga sus veces, establece las políticas generales para garantizar la seguridad y la integridad de la información, la implementación de la Política de Gobierno Digital, conforme a los lineamientos del orden Nacional y Distrital relativos a la seguridad de la información, la seguridad digital, los sistemas informáticos, el uso adecuado de la información y su integración y coordinación con el proceso de gestión documental de la Entidad.

7.1.3. Se debe asignar al responsable de cada activo o proceso de seguridad de la información, y se deben documentar los detalles de esta responsabilidad.

7.1.4. Se deben definir las responsabilidades para las actividades de gestión del riesgo de la seguridad de la información y seguridad digital.

7.1.5. Para tener la capacidad de cumplir las responsabilidades en seguridad de la información, los funcionarios designados deberán ser competentes y se les deberá brindar oportunidades de mantenerse actualizados con los avances en este tema.

7.1.6. La Contraloría de Bogotá, D.C. establece un documento de Políticas Institucionales para dar cumplimiento al quehacer de la entidad, enmarcadas dentro del Sistema Integrado de Gestión: Calidad, Ambiental, Seguridad y Salud en el Trabajo, Seguridad de la Información, Riesgos Institucionales, Gestión Documental, entre otras, las cuales deben ser interiorizadas y aplicadas por los funcionarios y contratistas. En este sentido, el presente documento es complemento y prolijo de algunas de las políticas mencionadas, razón por la cual las que no se encuentren descritas detalladamente en el presente documento deberán ser consultadas y analizadas en la documentación respectiva para su aplicación integral.

7.1.7. Condiciones de uso del portal web e intranet de la Contraloría de Bogotá D.C. El sitio web y la intranet de la entidad tienen como función principal proveer información y servicios, así como divulgar, promover normas y directrices del ente de Control Distrital. Por medio del sitio Web, la Contraloría de Bogotá, D.C. publica, entre otros, los temas y actividades que tienen que ver con su misión, su visión, objetivos y las funciones que le corresponden. Adicionalmente, por este medio, la entidad da a conocer información sobre políticas, planes, programas y proyectos institucionales, indicadores de gestión, publicaciones, normatividad, y en general, información relacionada con el control fiscal distrital y de la entidad y ofrece herramientas de interacción para los usuarios del sitio. Este lineamiento es complementario a las

COPIA CONTROLADA

condiciones de uso y política de privacidad publicadas en el sitio web e intranet de la entidad.

7.2. TELETRABAJO

La Contraloría de Bogotá D.C., según lo establecido en sus procedimientos debe proteger la información a la que tienen acceso los funcionarios con ocasión del empleo que desempeñan, en consecuencia, y respecto de los teletrabajadores se indica que, el acceso a los diferentes entornos y sistemas informáticos de la Entidad será efectuado siempre y en todo momento bajo el control y responsabilidad del teletrabajador, siguiendo los procedimientos establecidos por la Entidad. El teletrabajador se compromete a respetar la legislación en materia de protección de datos, las políticas de seguridad y privacidad de la información que la Entidad ha implementado, como también con el cumplimiento de:

Lineamientos:

7.2.1. El funcionario autorizado para trabajar en la modalidad de teletrabajo deberá acoger las recomendaciones dadas por el Comité Coordinador de Teletrabajo, frente a posibles riesgos tecnológicos, identificados en la visita de valoración y adoptará los controles necesarios para la mitigación de dichos riesgos.

7.2.2. Los teletrabajadores deben cumplir con el esquema de licenciamiento de software definido, así como, mantener el antivirus activo y actualizado, y respetar los controles que la Contraloría de Bogotá D.C., ha definido y que le apliquen.

7.2.3. El acceso remoto únicamente se podrá realizar desde equipos propiedad de la Contraloría de Bogotá, D.C. o los aprobados por el Comité Coordinador de Teletrabajo, cumpliendo los requisitos y mecanismos de seguridad establecidos por la entidad, para conexión segura.

7.2.4. Los funcionarios que utilicen su equipo de cómputo personal para teletrabajar deben separar el entorno de teletrabajo del entorno personal, utilizando cuentas de usuario diferentes para cada uno de ellos.

7.2.5. Los teletrabajadores deben cumplir con las medidas de seguridad que la entidad haya implementado para asegurar la confidencialidad e integridad de los datos de carácter personal a los que tenga acceso, así como, comprometerse a no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso.

7.2.6. En el esquema de teletrabajo no se permite almacenar información clasificada en servicios en la nube no licenciados por la entidad.

7.2.7. Los teletrabajadores son responsables de la información utilizada y procesada para el desarrollo de sus funciones, por tal razón deberán realizar copias de respaldo de la información regularmente para asegurar la continuidad de las funciones realizadas.

7.2.8. La administración, mantenimiento y soporte de equipos que son propiedad de los teletrabajadores, es responsabilidad de estos, en ningún momento la Contraloría de Bogotá D.C. se hace responsable por estas actividades; la entidad las asume, para los equipos de su propiedad que suministre al teletrabajador.

7.2.9. En caso de pérdida, suplantación o robo de un equipo portátil o cualquier medio de almacenamiento, utilizado para teletrabajar y que contenga información relacionada con la Contraloría de Bogotá D.C., se deberá realizar de forma inmediata, el respectivo reporte de acuerdo con el procedimiento para la Gestión de Incidentes de Seguridad

COPIA CONTROLADA

vigente en la entidad y se deberá poner la denuncia ante la autoridad competente, si aplica.

7.2.10. La información institucional que es almacenada en los equipos de cómputo personales deberá ser transferida a los equipos de la entidad cuando el funcionario o contratista tenga acceso a los equipos de la entidad.

7.3. CONTROLES CRIPTOGRÁFICOS

Esta política define el uso de controles encaminados a la protección de la información de la Entidad con base en análisis de riesgos que se realicen, con el fin de garantizar una adecuada protección de la confidencialidad, integridad y disponibilidad de la información. Esta política aplica a todas las personas que usen mecanismos criptográficos sobre los servicios o información de la Contraloría de Bogotá D.C.

Lineamientos:

7.3.1. La información digital catalogada como, pública reservada y/o pública clasificada, se debe almacenar y/o transmitir bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad, no obstante, en caso de no poderse aplicar un mecanismo criptográfico, se deberá asignar clave de apertura a los archivos digitales que contengan este tipo de información o consultar con la Dirección de Tecnologías de la Información y las Comunicaciones un mecanismo para la protección de la información.

7.3.2. Al utilizar firmas y certificados digitales, se debe considerar la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.

7.3.3. Los usuarios de las llaves criptográficas o mecanismos de cifrado deberán protegerlas contra modificación y destrucción y las llaves privadas deberán ser protegidas contra uso indebido, copia o divulgación no autorizada.

7.3.4. Los usuarios de mecanismos criptográficos adquiridos por la entidad serán responsables de su adecuada custodia, administración y protección.

7.3.5. La solicitud y tiempo de vida de las llaves o mecanismos criptográficos será definido por el responsable de la dependencia usuaria, determinándolo según la finalidad, propósito y cumplimiento a la legislación y reglamentación pertinente a la adquisición y uso de mecanismos criptográficos. La llave deberá tener fecha de inicio y caducidad de vigencia, definida de manera que solo podrá ser utilizada por un lapso de tiempo definido.

7.3.6. Las dependencias que adquieran o gestionen mecanismos criptográficos deberán reportar a la Dirección de Tecnologías de la Información y las Comunicaciones, la solicitud, existencia, revocación de mecanismos de cifrado que son expedidos por entidades certificadoras para poder tener un inventario de éstas y saber qué medidas criptográficas se están aplicando.

7.4. COPIAS DE RESPALDO

La Contraloría de Bogotá D.C., debe realizar copias de respaldo de la información institucional la cual deberá estar centralizada y se deberá asegurar la ejecución de copias de respaldo ante cualquier afectación por pérdida o degradación. De igual manera se especifica que cada

COPIA CONTROLADA

usuario es responsable de la información que maneja en su equipo de cómputo y/o medio de almacenamiento externo, en consecuencia, es el responsable de realizar las copias de respaldo de esta.

Lineamientos:

7.4.1. Los medios de copias de respaldo de la información institucional generada por la Dirección de Tecnologías de la Información y las Comunicaciones se deberán almacenar en custodia externa o en una sede alterna de la Contraloría de Bogotá D.C., asegurando que tenga implementado mecanismos de protección ambiental.
7.4.2. Realizar pruebas de restauración de la información, de acuerdo con un plan de restauración de copias de respaldo establecido, para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.
7.4.3. Para la información considerada relevante o importante por cada dependencia de la Entidad, se cuenta con una unidad de almacenamiento centralizada, en la cual se almacena dicha información por los funcionarios autorizados; unidad que se encuentra incluida dentro de los esquemas de copias de respaldo implementados por la Dirección de Tecnologías de la Información de la Contraloría de Bogotá, D.C.
7.4.4. Definir los tiempos de retención y de protección en instalaciones adecuadas que provean la debida seguridad física y ambiental, permitiendo minimizar el impacto de la operación de la Entidad, en caso de presentarse una falla o desastre y poder contar con la información necesaria en el momento oportuno para responder con los tiempos de restauración de los servicios.
7.4.5. Se debe contar con registros exactos y completos de las copias de respaldo.
7.4.6. Definir la frecuencia y tipo de copias de respaldo a realizar.
7.4.7. Las pruebas de restauración se deberán hacer en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que se cause un daño o pérdida de la información.

7.5. DESARROLLO SEGURO

La Contraloría de Bogotá D.C., debe crear y mantener mecanismos que incluyan los requerimientos de seguridad en todo el ciclo de vida de desarrollo y mantenimiento seguro de las aplicaciones y sistemas de información, los desarrolladores en conjunto con el grupo o funcionarios designados para temas de seguridad de la información, revisarán y determinarán la acción a seguir para el tratamiento de las vulnerabilidades, para evitar que tengan brechas de seguridad, esto aplicará tanto para los desarrollos realizados con terceros, como los realizados al interior de la Entidad.

Lineamientos:

7.5.1. Se deben identificar y acordar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software, y se deben justificar, acordar y documentar.
7.5.2. Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.

COPIA CONTROLADA

7.5.3. El cambio de versión de las aplicaciones implementadas en el ambiente de producción se debe hacer de acuerdo con lo definido en el procedimiento para la adquisición, desarrollo y mantenimiento de sistemas de información, además, debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso que se deba realizar marcha atrás, para mantener la integridad y disponibilidad de los datos y de los sistemas de información.

7.5.4. Se deben realizar pruebas de seguridad en un ambiente controlado con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.

7.5.5. Los ambientes de desarrollo, pruebas y producción deben estar separados.

7.5.6. El paso de software de un ambiente a otro debe ser controlado y gestionado de acuerdo con lo definido en el procedimiento para la adquisición, desarrollo y mantenimiento de sistemas de información.

7.5.7. El ambiente de prueba debe simular el ambiente de producción.

7.5.8. El desarrollo de contratos de mantenimiento deberá contar con la asignación de un supervisor permanente, encargado de controlar que se cumplan los estándares de seguridad tanto en la parte física como lógica de los sistemas. Ningún mantenimiento podrá ser realizado por personal que no cumpla los requisitos definidos por la Dirección de Tecnologías de la Información y las Comunicaciones.

7.5.9. La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., aplicará el procedimiento para el desarrollo de software y sistemas de información, el cual debe ser aplicado a los desarrollos y adaptaciones de los sistemas en la entidad, en el que se debe asegurar que cuando se efectúen cambios en la plataforma de operación no haya impacto adverso en las operaciones y en la seguridad de la información.

7.5.10. La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., aplicará mecanismos de prueba de aceptación de nuevos sistemas de información, actualizaciones y versiones nuevas, así como supervisar, monitorear la actividad del desarrollo de los sistemas tercerizados y realizar pruebas de funcionalidad de la seguridad.

7.5.11. Todo hardware y software que se vaya a adquirir y/o conectar a la infraestructura tecnológica de la Contraloría de Bogotá D.C., por cualquier dependencia o proyecto de la Entidad, deberá ser adquirido por intermedio de la Dirección de Tecnologías de la Información y las Comunicaciones y gestionado por la misma dirección para su correcto funcionamiento.

7.5.12. El software proporcionado por la Contraloría de Bogotá D.C. no puede ser copiado o suministrado a terceros.

7.5.13. En los equipos de la Contraloría de Bogotá D.C. se debe utilizar software licenciado o libre que la Dirección de Tecnologías de la Información y las Comunicaciones, haya adquirido o avalado como resultado de proyectos o programas que se encuentran en la entidad.

7.5.14. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Dirección de Tecnologías de la Información y las Comunicaciones de acuerdo con lo establecido en el procedimiento para la adquisición, desarrollo y mantenimiento de sistemas de información.

7.5.15. El software que se adquiera la Entidad debe quedar licenciado a nombre de la Contraloría de Bogotá D.C.

COPIA CONTROLADA

7.6. RELACIONES CON LOS PROVEEDORES

La Contraloría de Bogotá D.C., debe identificar requisitos de seguridad para proteger la información, e incluirlos dentro de los acuerdos con proveedores, por medio de un análisis que permita identificar riesgos asociados para implementar planes de acción dependiendo de las actividades a realizar, de igual manera se debe establecer, aprobar y divulgar los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos posean.

Lineamientos:

7.6.1. Los proveedores deben aceptar y firmar los acuerdos de confidencialidad establecidos por la Contraloría de Bogotá D.C.

7.6.2. Se debe tener en cuenta la documentación relacionada con los servicios, infraestructura de TI, sistemas de información y activos a los cuales tendrá acceso los proveedores, esto deberá ser controlado teniendo en cuenta los permisos de acuerdo con el trabajo a realizar y los acuerdos firmados, los cuales deben tener requisitos mínimos de seguridad, que se deben hacer cumplir haciendo seguimiento por medio de mecanismos establecidos.

7.6.3. La Entidad debe incluir dentro de los acuerdos a firmar con el proveedor, los controles de seguridad aplicables, conforme a las actividades a desarrollar dentro del marco contractual.

7.6.4. Cuando exista la necesidad de otorgar acceso de terceras partes a los sistemas centrales, deberá realizarse siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:

- El tipo de acceso requerido (físico, lógico y a qué recurso).
- Los motivos para los cuales solicita el acceso.
- Los controles empleados por la tercera parte.

7.6.5. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados, se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

7.6.6. El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo, este junto con los encargados de la infraestructura tecnológica, aprobarán y autorizarán el acceso y uso de la información.

7.6.7. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

- Forma en los que se cumplirán los requisitos legales aplicables.
- Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.

COPIA CONTROLADA

- Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información.
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
- Niveles de seguridad física que se asignará al equipamiento tercerizado.

7.6.8. Todos los funcionarios y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos, utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o Entidades externas.

7.6.9. Se deben formalizar los acuerdos de niveles de servicio y los acuerdos de intercambio de información con cada proveedor dentro del contrato realizado, de acuerdo con los lineamientos establecidos por Contraloría de Bogotá. D.C.

7.6.10. Se deben definir las cláusulas por incumplimiento en los contratos de los proveedores, para establecer las situaciones que puedan generar multas o penalizaciones, dentro de los cuales se contempla los acuerdos de confidencialidad y no divulgación de la información.

7.6.11. Los encargados de la infraestructura tecnológica deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros.

7.7. GESTIÓN DE ACTIVOS

La Contraloría de Bogotá D.C., debe identificar todos los activos de información, y mantener un inventario actualizado, exacto, consistente y documentado con todos los aspectos relevantes de cada uno, clasificándolos de acuerdo con la confidencialidad, integridad y disponibilidad de la información, para identificar su valor y criticidad, además, cada activo debe tener un propietario que garantice los niveles de seguridad que correspondan según sea el caso.

Lineamientos:

7.7.1. La Contraloría de Bogotá D.C. es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

7.7.2. Los funcionarios de la Entidad se deben comprometer a identificar, clasificar, etiquetar, disponer, devolver, y gestionar los activos de información establecidos como tal, de acuerdo con la presente política y el procedimiento establecido para la gestión de activos.

7.7.3. La identificación, clasificación y valoración de los activos de información se debe realizar de acuerdo con el procedimiento establecido.

7.7.4. Toda la información producida, tratada, procesada, almacenada o transmitida en la Contraloría de Bogotá D.C., debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad según metodología y/o procedimiento establecido por la entidad.

COPIA CONTROLADA

7.7.5. Se debe mantener un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, de acuerdo con lo establecido en el procedimiento para la gestión de activos.
7.7.6. Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.
7.7.7. Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información, de acuerdo con lo establecido en el procedimiento para la gestión de activos.
7.7.8. Los documentos de la Contraloría de Bogotá D.C., que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.
7.7.9. El acceso a carpetas compartidas debe delimitarse a los funcionarios que las necesitan y deben ser protegidas con contraseñas y/o acceso por roles y responsabilidades.
7.7.10. Los funcionarios y contratistas deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la Contraloría de Bogotá D.C. en el proceso de desvinculación o finalización de la relación laboral o contractual, de igual manera deberán documentar los conocimientos importantes relacionados con la labor ejecutada.
7.7.11. La Contraloría de Bogotá D.C., de acuerdo con la normatividad y procedimientos vigentes ejecutará las actividades necesarias para garantizar la eliminación, retiro, traslado o reúso de los activos, de forma segura y correcta.
7.7.12. Los medios y equipos donde se almacena, procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

7.8. NO REPUDIO

La política de no repudio comprende la capacidad de definir diferentes mecanismos o estrategias que están encaminadas a que un funcionario o tercero evite negar que ha realizado alguna acción.

Lineamientos:

7.8.1. Para los procesos que se consideren, se deben implementar mecanismos en los que no exista la posibilidad de desafiar la validez de una acción por parte de quien la generó, los cuales deberán contar con la responsabilidad de un tercero en que todos confíen y quien permita avalar la integridad y origen de los datos.
7.8.2. Se deben contar con registros que permita hacer trazabilidad de las acciones de creación, origen, recepción, entrega de información y otros, que servirán de evidencia para poder garantizar el no repudio.
7.8.3. Estos registros se deben proteger contra pérdida o modificación de tal manera que se garantice su disponibilidad e integridad.
7.8.4. Se deben realizar auditorías continuas a los mecanismos de control y a los procesos, para asegurarse que las partes implicadas no nieguen haber realizado una acción.

COPIA CONTROLADA

7.8.5. Los servicios de intercambio electrónico de información, deben incorporar mecanismos que sean garantía de no repudio.

7.9. PRIVACIDAD Y CONFIDENCIALIDAD

La política de Privacidad y Confidencialidad determina los lineamientos de tratamiento y protección sobre los datos personales y sobre la información considerada como sensible y sobre la cual se deberán implementar controles de acuerdo con su nivel de clasificación, los lineamientos descritos a continuación son complementarios a la Política de Tratamiento de Datos Personales establecida por la Contraloría de Bogotá D.C. mediante acto administrativo.

Lineamientos:

7.9.1. En la Contraloría de Bogotá D.C. se tienen implementados acuerdos de confidencialidad los cuales todo funcionario, contratista y/o tercero vinculado a la Entidad debe firmar con el compromiso de no divulgar la información clasificada, reservada o confidencial de la Entidad.

7.9.2. El ciudadano y/o funcionario reconoce que el ingreso de información personal por cualquiera de los mecanismos establecidos por la Entidad, lo realiza de manera voluntaria y lo hará ante la solicitud de requisitos específicos por la Contraloría de Bogotá D.C. para llevar a cabo un trámite, una queja o reclamo o una solicitud o para acceder a los mecanismos interactivos que ofrece la Entidad.

7.9.3. Para la recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el sitio web, se deberá informar al titular de los datos la finalidad de estos.

7.9.4. Todo funcionario, contratista o tercero debe firmar un acuerdo de confidencialidad, el cual debe contener un compromiso del funcionario, contratista y/o tercero vinculado a la Contraloría de Bogotá D.C., de no divulgar la información interna y externa que conozca como parte del desarrollo de las funciones que desempeña o de su vinculación con la Entidad.

7.9.5. Este acuerdo de confidencialidad debe indicar la vigencia de este, el cual debe mantenerse por un tiempo adicional que considere la Contraloría de Bogotá D.C., luego de terminada la vinculación con la Entidad.

7.9.6. El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.

7.9.7. La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

7.9.8. Al presentar la queja ante la entidad frente al manejo de la privacidad y/o confidencialidad de los datos personales, esta se dirigirá al área o funcionario encargado o designado para responder los temas relacionados con la protección de los datos personales a los que refiera la queja conforme a la normatividad vigente.

COPIA CONTROLADA

7.10. INTEGRIDAD

La política de Integridad se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administrada por usuarios internos y externos relacionados con la Contraloría de Bogotá D.C.

Lineamientos:

7.10.1. Toda la información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas autorizadas y a través de los medios correspondientes, sin modificaciones ni alteraciones.
7.10.2. En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa debe hacer parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información.
7.10.3. Para la información que se clasifique como Reservada, Clasificada, Pública, y requiera ser transmitida a través de canales de comunicación, se deben utilizar mecanismos que permitan garantizar que la información mantiene su integridad mientras es transmitida por la red, es decir, que la información es completa y exacta de punto a punto en la transmisión.
7.10.4. Los funcionarios y contratistas adoptarán y aplicarán los mecanismos técnicos y tecnológicos tendientes a la integridad y originalidad de los documentos producto del desarrollo de su función en la entidad y garantizará su aplicación en el proceso de la producción documental física y electrónica.

7.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Contraloría de Bogotá D.C., debe promover en los usuarios internos y externos el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

Lineamientos:

7.11.1. En la Contraloría de Bogotá D.C., se aplicarán procedimientos y se asignarán responsables de gestión que permita evaluar y decidir cuándo un evento de seguridad corresponde a un incidente de seguridad de la información, así como asegurar una atención que brinde respuesta rápida, eficaz y metódica a los incidentes detectados.
7.11.2. Todo evento de seguridad ocurrido en la Contraloría de Bogotá D.C., deberán ser comunicados mediante canales de gestión apropiados.
7.11.3. Los funcionarios, contratistas y terceros que hagan uso de los sistemas de información de la Entidad, que tengan conocimiento de cualquier debilidad en la seguridad de la información, en los sistemas o servicios, deben informarlo a la Dirección de Tecnologías de la Información y las Comunicaciones.

COPIA CONTROLADA

7.11.4. Se debe reportar en la mesa de servicios o haciendo uso de los canales institucionales de comunicación, los incidentes de seguridad de la información, donde se gestionará de acuerdo con su criticidad, con la participación de la Dirección de Tecnologías de la Información y las Comunicaciones, el equipo de respuesta ante incidentes de seguridad de la información – CSIRT y el Oficial de Seguridad de la Información.
7.11.5. Los propietarios de los activos de información, funcionarios y terceros deben informar los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización, de acuerdo con el procedimiento “Gestión de Incidentes de Seguridad de la Información”.
7.11.6. Se deben documentar y clasificar los incidentes de acuerdo con las indicaciones especificadas en el procedimiento de “Gestión de Incidentes de Seguridad de la Información”.
7.11.7. Se deben analizar los incidentes de seguridad para identificar cuáles serán escalados y realizar el contacto con las autoridades, cuando se estime necesario.
7.11.8. Todo evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la Confidencialidad, Integridad, y Disponibilidad de la infraestructura tecnológica, deberá ser reportado de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad de la Información.
7.11.9. En los casos que sea necesario realizar recolección y preservación de la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información, la entidad acudirá a las instancias especializadas para el tratamiento de esta evidencia, a fin de conservar la integralidad de ésta.

7.12. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La política de Capacitación y Sensibilización en Seguridad de la Información se centra en formar y dar a conocer a los funcionarios y contratistas temas relacionados con la seguridad de la información, cuya finalidad es que puedan identificar y reportar de manera oportuna los incidentes de seguridad de la información y disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Lineamientos:

7.12.1. Se debe proveer al personal activo las habilidades requeridas a través de entrenamientos para proteger los sistemas y cumplir con las responsabilidades de administración y uso de manera oportuna, correcta y segura los activos de información.
7.12.2. Se debe crear una cultura que promueva la seguridad, donde todos los individuos apliquen los controles de seguridad y prevengan que la información sensible de la Entidad se vea comprometida.
7.12.3. Determinar los temas y las estrategias de sensibilización para reforzar el nivel de conocimiento en temas de seguridad de la información para todos los funcionarios.
7.12.4. Se debe definir un mecanismo de inducción en seguridad de la información para todos los funcionarios que sean asignados en un nuevo cargo, bien sea por nombramiento, traslado o por disposiciones internas.
7.12.5. Se debe incorporar en el Plan Institucional de Capacitación, un programa de capacitación y sensibilización de tal forma que de manera periódica se refuercen los diferentes conceptos relacionados con la seguridad de la información, para que los

COPIA CONTROLADA

funcionarios cuenten con información actualizada y sepan cómo actuar ante incidentes y como reportarlos.

7.12.6. La asistencia a las sesiones de capacitación y sensibilización en seguridad de la información deben ser de carácter obligatorio.

7.12.7. Los mensajes de sensibilización deben dar a conocer y entender de fácil manera las políticas de seguridad de la información.

7.12.8. Se debe evaluar a todos los funcionarios de manera periódica, los niveles de sensibilización en temas de seguridad de la información, así como utilizar medios institucionales de comunicación masiva para informar o sensibilizar a los funcionarios de la Entidad en temas de seguridad de la información.

7.13. TRANSFERENCIA DE LA INFORMACIÓN

Para la transferencia de información entre la Contraloría de Bogotá D.C., y otra Entidad de cualquier orden y naturaleza, sea pública, privada o mixta, se deberán establecer requisitos de confidencialidad y no divulgación de la información, para lo cual será necesario establecer los respectivos acuerdos de confidencialidad, enmarcados en las leyes vigentes.

La Entidad debe implementar mecanismos y controles que permitan establecer una comunicación segura en la transferencia de la información, evitando la interceptación por parte de terceros, que puedan copiar, modificar, o eliminar la información.

Lineamientos:

7.13.1. Utilizar mecanismos de autenticación o contraseña para garantizar la confidencialidad e integridad de la información durante la transferencia de la información.

7.13.2. Los propietarios de la información a transferir deben asegurar que la clasificación de ésta se encuentre actualizada teniendo en cuenta las propiedades de seguridad: confidencialidad, integridad y disponibilidad, con el fin de permitir el acceso únicamente a los autorizados.

7.13.3. Únicamente se entregará información a receptores autorizados quienes garanticen por escrito la reserva legal y protección de la información que se les vaya a suministrar.

7.13.4. Cuando proceda, la dependencia responsable de dar respuesta legal a un requerimiento de información clasificada, deberá asegurarse que:

- La solicitud se ajuste a la normatividad aplicable vigente.
- La respuesta identifique el nivel de clasificación, correspondiente a la naturaleza del documento o la información que se ponga en conocimiento de la autoridad competente.
- La respuesta cumpla con los protocolos de seguridad, acceso y reserva.
- La respuesta con la información suministrada no debe poner en peligro o riesgo la seguridad de la Entidad o sus funcionarios.
- La respuesta no debe dar a conocer capacidades, procedimientos, medios, elementos técnicos, operaciones o actividades que comprometan la seguridad de la Entidad.

7.13.5. Se debe dar cumplimiento a lo establecido en el procedimiento de Gestión de Activos de la Entidad.

COPIA CONTROLADA

7.14. POLÍTICA DE LA CONTINUIDAD DE OPERACIÓN INSTITUCIONAL

La Contraloría de Bogotá D.C., dispondrá los planes necesarios para la continuidad de Operación Institucional, asimismo proporcionará los recursos suficientes y desarrollará esfuerzos tendientes a garantizar la continuidad de las operaciones para sus procesos con el fin brindar la disponibilidad de los servicios; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante eventos adversos, de igual manera se mantendrán canales de comunicación adecuados hacia los funcionarios y demás partes interesadas.

Lineamientos:

7.14.1. La Contraloría de Bogotá D.C., conforme a su misionalidad, establece que debe contar con un Plan de Continuidad de Operación Institucional que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
7.14.2. El Plan de Continuidad de Operación Institucional contendrá el Plan de Respuesta a Emergencia, la Metodología de Riesgos adoptada por la entidad, el Análisis de Impacto al Negocio, el Plan de Recuperación de Desastres, las estrategias de manejo y comunicación de crisis, así como cualquier estrategia orientada a la continuidad del desarrollo de la misionalidad de la entidad.
7.14.3. Todo cambio que se realice a la infraestructura física y de comunicaciones de la entidad deberá ser documentada y gestionada conforme a lo descrito en el Procedimiento de Gestión de Cambios Tecnológicos del Proceso de Gestión de Tecnologías de la Información.
7.14.4. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionadas con el plan, deben estar incorporados y definidos.
7.14.5. Los Acuerdos de Niveles de Servicio (ANS) establecidos por la Dirección de Tecnologías de la Información y las Comunicaciones, estará definido en el catálogo de servicios y será revisado periódicamente para conocimiento de los usuarios. Para los Acuerdos de Niveles de Servicios (ANS) establecidos con terceros, estos deberán ser definidos en los contratos y serán gestionados y monitoreados por los funcionarios responsables de la gestión de los servicios ofrecidos.
7.14.6. Los responsables de los procesos de la recuperación, serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio a todos los interesados.
7.14.7. Los análisis de riesgos, impacto al negocio y estrategias de recuperación realizados sobre los planes que estén operando, deben ser evaluados por lo menos cada año, para asegurar que continúan reflejando las estrategias y necesidades de la operación.
7.14.8. Todos los sistemas de información que soportan las funciones críticas de la entidad deben tener un plan de recuperación de TI que le permita garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupciones mayores, el cual estará a cargo de la Dirección de Tecnologías de la Información y las Comunicaciones.
7.14.9. Los procesos críticos deben soportarse en aplicaciones e infraestructura técnica robusta, software y hardware confiable y en instalaciones alternas o duplicadas.
7.14.10. Se requiere proveer al personal activo, la documentación de las acciones a llevar a cabo en el evento de un desastre o una emergencia que puede afectar las aplicaciones

COPIA CONTROLADA

de la operación y la infraestructura técnica, habilitando los procesos críticos de la Entidad, para ser restaurados en escalas de tiempo aceptables.

7.14.11. Los planes de recuperación deben ser probados periódicamente y como resultado de estas pruebas realizar los ajustes correspondientes.

7.14.12. Se debe identificar, acordar y documentar todas las responsabilidades y los procedimientos para la recuperación de los servicios identificados como críticos.

7.15. REGISTRO Y AUDITORÍA

Esta política de Registro y Auditoría define lo pertinente a las auditorías que se realizan a los procesos que incluyen activos del Subsistema de Gestión de Seguridad de la Información e indica temas del registro y conservación de las evidencias de las actividades y acciones que afectan los activos de información.

Lineamientos:

7.15.1. La oficina de Control Interno de la Entidad debe definir un plan de auditoria y un equipo auditor que lo ejecute, el cual debe cumplir con las capacidades, habilidades y conocimientos para su ejecución.

7.15.2. La oficina de Control Interno de la Entidad, debe asegurar que los resultados de las auditorías se informan al Oficial de Seguridad de la Información y al Director de Tecnologías de la Información y las Comunicaciones y se conserve información documentada como evidencia de la implementación del programa de auditoria.

7.15.3. Como parte del programa de auditoria, se deben incluir auditorias periódicas al Subsistema de Gestión de Seguridad de la Información.

7.15.4. Los registros de auditoría deben incluir toda la información de registro y monitoreo de eventos de seguridad, estos registros se deben almacenar por lo menos por un periodo de dos años.

7.15.5. Las auditorias se deben realizar acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.

7.15.6. Se debe definir a qué es necesario hacer seguimiento y medición dentro del Subsistema de Gestión de Seguridad de la Información.

7.15.7. Se deben desarrollar planes de auditoría interna para evaluar los niveles de aplicabilidad de la seguridad de la información en todos sus ámbitos, tanto digitales como físicos.

7.15.8. Se debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar lo pertinente sobre las deficiencias detectadas.

7.15.9. El almacenamiento de los registros de las auditorías internas realizadas al Subsistema de Gestión de Seguridad de la Información se debe realizar de acuerdo con lo establecido en el procedimiento de Auditorías Internas.

COPIA CONTROLADA

8. POLÍTICAS DE SEGURIDAD DIGITAL - USO ACEPTABLE DE LOS SERVICIOS TECNOLÓGICOS

Todos los servidores públicos o contratistas que hagan uso de los recursos tecnológicos de la Contraloría de Bogotá D.C. tienen la responsabilidad de cumplir completamente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación institucional y, por ende, el cumplimento de su misionalidad. Para ello, deben acatar las siguientes disposiciones:

8.1. CONTROL DE ACCESO LÓGICO Y FÍSICO

En la Contraloría de Bogotá D.C., se establecerán medidas de control de acceso a la información y demás servicios de TI, estos controles deben limitar el acceso a la información de acuerdo con la clasificación de la información, las funciones y cargos que desempeñen los funcionarios, contratistas y terceros. Siempre se brindarán accesos de acuerdo con el principio de privilegio más bajo, con los cuales todos los funcionarios, contratistas y terceros puedan desempeñar correctamente sus funciones sin brindar accesos de mayor alcance a los que se requiere.

Lineamientos:

8.1.1. La Contraloría de Bogotá D.C, aplicará un procedimiento mediante el cual se brinden las pautas para una correcta gestión del control de acceso a usuarios en todos sus niveles; en este procedimiento se debe contemplar la restricción y control de los accesos privilegiados a la información y los sistemas de información, así como establecer las definiciones para el monitoreo periódico de las acciones y los cambios a las cuentas privilegiadas.

8.1.2. Cuando un tercero o ente externo solicite tener acceso a algún recurso o servicio de la Entidad, se deberá realizar el correspondiente análisis de riesgo con la participación del propietario de la información y de los activos asociados, con el fin de determinar los privilegios a otorgar y definir los mecanismos necesarios para su protección, el cual se documentará en el acta de inicio del contrato o dentro de la documentación de seguimiento de las labores realizadas.

8.1.3. En ningún caso se otorgará a terceros acceso a la información, a las instalaciones, o a centros de procesamiento de información crítica, si previamente no se han cumplido los controles de seguridad establecidos en el procedimiento de seguridad física y del entorno y/o conexión a terceros.

8.1.4. Las asignaciones de privilegios en las aplicaciones para los diferentes usuarios estarán determinadas por el procedimiento de control de acceso a usuarios, estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

8.1.5. Se debe usar una identificación de usuario (ID) para permitir que los funcionarios queden vinculados y sean responsables de sus acciones.

8.1.6. Se debe retirar o bloquear a la mayor brevedad los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado de ser parte de la Entidad. Para esto la Dirección de Talento Humano deberá periódicamente remitir las

COPIA CONTROLADA

novedades de personal para mantener actualizado los derechos de usuario; en el mismo sentido la Dirección Administrativa y Financiera deberá remitir el listado de los contratistas activos en la entidad.

8.1.7. Los privilegios de administración de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red), deben ser asignados exclusivamente a los administradores del sistema designados en la Dirección de Tecnologías de la Información y las Comunicaciones de la Entidad, en ningún caso se debe autorizar estos privilegios de acceso al usuario del equipo.

8.1.8. Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debe suministrar de manera segura una contraseña temporal, la cual se debe forzar a cambiar inmediatamente realice el siguiente ingreso al sistema.

8.1.9. Las contraseñas nunca se deben almacenar en sistemas, medios o formatos no protegidos.

8.1.10. Las contraseñas predeterminadas por el fabricante se deben cambiar inmediatamente después de la instalación de los sistemas o del software.

8.1.11. Toda contraseña es personal e intransferible, y cada usuario es responsable de las acciones que se ejecuten con el usuario que se le ha asignado.

8.1.12. Cuando un funcionario requiera el cambio de contraseña, debe solicitarlo por la Mesa de Servicios, indicando el motivo para el cambio (olvido, falla en el sistema, potencialización de seguridad, entre otros) lo anterior para llevar el registro en con la respectiva justificación y tomar medidas frente a estos registros.

8.1.13. Todos los usuarios deberán cumplir los siguientes lineamientos para la construcción de sus contraseñas:

- Deben estar compuestas mínimo de ocho (8) caracteres que deben ser combinados (mayúsculas, minúsculas, números y caracteres especiales).
- No deben ser idénticas o similares a contraseñas que hayan usado previamente, o al nombre o apellido del usuario.
- La contraseña tendrá una vigencia definida en la Dirección de Tecnologías de la Información y las Comunicaciones, finalizando este periodo el usuario deberá realizar el cambio correspondiente.
- No deben ser fáciles de inferir o adivinar.
- No deben ser susceptibles a ataques de diccionario, es decir, que no incluya palabras que podrían ser encontradas en un diccionario.

8.1.14. Para la selección de controles de las áreas protegidas se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre.

8.1.15. El cableado de energía eléctrica y comunicaciones que transportan datos o brinda apoyo a los servicios de información deben protegerse contra interceptación o daños.

8.1.16. Se debe garantizar la seguridad física de los centros de cableado incluyendo, entre otros, el sistema eléctrico y el control de acceso biométrico.

8.1.17. Todas las puertas que utilicen sistema de control de acceso deben permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados evitar que las puertas se dejen abiertas.

8.1.18. Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado en la Entidad, mientras permanezcan dentro de sus instalaciones.

COPIA CONTROLADA

8.1.19. Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas identificadas como seguras de la Entidad.
8.1.20. Es responsabilidad de todos los usuarios internos y externos acatar los lineamientos de seguridad y mecanismos de control de acceso a las instalaciones de la Entidad.
8.1.21. Todas las áreas que se hayan definido como protegidas y activos de información que la componen, deben ser protegidas de acceso no autorizado mediante controles y tecnologías de autenticación fuerte.
8.1.22. Todo acceso físico a las áreas protegidas deberá estar manejado según los lineamientos definidos por los procedimientos designados para el manejo de estas áreas.
8.1.23. En las áreas seguras donde se encuentren activos de información, se debe cumplir como mínimo con los siguientes lineamientos:

- No se deben consumir alimentos ni bebidas.
- No se deben ingresar elementos inflamables.
- No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario autorizado durante el tiempo que dure su visita.
- No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
- No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- Deberá ser registrado el ingreso y salida de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

8.2. DISPOSITIVOS MÓVILES

El uso de dispositivos móviles, limitando el alcance de estos dispositivos en la entidad a los computadores portátiles (notebooks y laptops) y unidades de almacenamiento externo incluyendo discos de almacenamiento externos, que contengan información de la entidad y que a su vez se utilicen para el manejo de esta información, deben ser controlados de acuerdo con el análisis de riesgo correspondiente, y mitigar el impacto a que se expone la información como su pérdida, alteración y divulgación no autorizada.

Lineamientos:

8.2.1. Se debe contar con un inventario actualizado de dispositivos móviles (computadores portátiles y unidades de almacenamiento externo suministrados por la Entidad, que no sean de consumo) utilizados para almacenar, procesar y/o transmitir información de la Contraloría de Bogotá D.C. inventario que será gestionado y administrado por la Dirección Administrativa y Financiera de la entidad.
8.2.2. La Contraloría de Bogotá D.C., establecerá lineamientos para el acceso a redes inalámbricas, la instalación de software y/o correos electrónicos de la Entidad mediante el uso de este tipo de dispositivos y establecerá las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles objeto de esta política.

COPIA CONTROLADA

8.2.3. En la Contraloría de Bogotá D.C., se adoptarán medidas de apoyo en seguridad de la información para ejercer correctamente la gestión de los riesgos en el acceso a la información, el procesamiento o almacenamiento que se presenten al utilizar los dispositivos móviles en lugares de trabajo remotos, siempre y cuando estos dispositivos sean propiedad de la entidad.

8.2.4. Ante la pérdida del equipo institucional, ya sea por extravío o hurto, deberá informar de manera inmediata a la Dirección Administrativa y Financiera y continuar con el procedimiento administrativo por pérdida de elementos establecido por la Entidad.

8.2.5. Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Contraloría de Bogotá D.C., con el fin de realizar actividades propias de su cargo o funciones asignadas en la Entidad; el uso de estos implementos tecnológicos para cuestiones personales, así como en lugares con algún riesgo de seguridad, no están autorizados por la entidad.

8.2.6. Los dispositivos móviles institucionales deben contar con mecanismos de autenticación para desbloquear el equipo y poder tener acceso a su información y servicios.

8.2.7. Si desde el dispositivo móvil se procesa información se debe contar con un software instalado y actualizado contra códigos maliciosos y firewall personal para prevenir incidentes de seguridad.

8.2.8. El usuario debe propender por el cuidado físico del dispositivo cuando este se encuentre fuera de la entidad, esto es resguardo del dispositivo en lugar seguro y no exposición ni uso en lugares que pueden ser catalogados como inseguros.

8.2.9. Es responsabilidad del usuario realizar periódicamente copias de respaldo a la información que se almacena en el dispositivo.

8.2.10. Los funcionarios y contratistas de la entidad deberán minimizar el uso de dispositivos móviles USB (Universal Serial Bus), son ellos los responsables de su uso y de la información que en ellos transportan y serán los encargados de su almacenamiento y custodia así como de las posibles consecuencias de la perdida de información que contengan estos dispositivos, a los funcionarios que se les proporcione como elemento de consumo dicho dispositivo, es de recordar que la información institucional clasificada como pública reservada y/o pública clasificada no está autorizada para el transporte en estos dispositivos.

8.2.11. La Dirección de Tecnologías de la Información y las Comunicaciones establecerá procedimientos para mantener instalado y constantemente actualizado y configurado software antimalware en todos los equipos institucionales para escanear todas las unidades de almacenamiento externo previamente a su uso.

8.2.12. Es responsabilidad del usuario del dispositivo móvil mantenerlo actualizado con el antivirus y/o software antimalware, en caso de requerir apoyo deberá solicitarlo a la Dirección de Tecnologías de la Información y las Comunicaciones por los medios dispuestos para atención a usuarios.

8.3. ESCRITORIO Y PANTALLA LIMPIOS

La Contraloría de Bogotá D.C., establece las reglas para reducir los riesgos de acceso no autorizado, daño o pérdida, o divulgación no autorizada de la información, en cada uno de los

COPIA CONTROLADA

puestos de trabajo, equipos y servidores de cómputo en términos de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

Lineamientos:

8.3.1. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la Entidad.

8.3.2. Los usuarios siempre al ausentarse del puesto de trabajo físico deberán bloquear el equipo de cómputo, para evitar que otras personas puedan acceder a la información, de la siguiente manera:

- Pulsar simultáneamente (tecla Windows + la tecla L) para bloquear el equipo.
- Pulsar (Ctrl + Alt + Supr) y seleccionar la opción bloquear equipo.

8.3.3. En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar los medios que contengan información clasificada, reservada o confidencial protegida bajo llave.

8.3.4. Los usuarios son responsables por la custodia y las acciones que se realicen sobre los activos de información que le han asignado, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

8.3.5. No se debe dejar en las impresoras documentos expuestos que contengan información sensible, ya que se puede comprometer su confidencialidad.

8.3.6. El usuario no tiene permitido hacer manipulación (traslados, desconexiones) de las estaciones de trabajo, con excepción de los computadores portátiles asignado para el desarrollo de sus funciones.

8.3.7. No publicar o dejar a la vista, documentos o datos clasificados, reservados o confidenciales para la Entidad, como: nombres de usuario, contraseñas, direcciones IP, contratos, números de cuentas, listas de clientes, archivos de propiedad intelectual, datos personales de los funcionarios públicos y/o cualquier información importante para la Entidad que no se desea publicar.

8.3.8. Los funcionarios al ausentarse de su sitio de trabajo deben guardar en un lugar seguro (gabinetes, mobiliario protegido con llave, caja fuerte) cualquier documento físico (hojas impresas, carpetas, cuadernos, libretas de apuntes), medio magnético removible (Memorias Flash, Discos Duros Externos, CD ROM, DVD) que contenga información de la Contraloría de Bogotá D.C.

8.3.9. La estación de trabajo y equipos que están asignados a los usuarios, son activos de la Entidad, por lo mismo el usuario no es dueño del mencionado activo.

8.3.10. Desde el momento en que el usuario firma el formato de asignación de inventario individual, la responsabilidad sobre el estado del equipo es completamente del usuario.

8.4. USO DE INTERNET Y REDES SOCIALES

La Dirección de Tecnologías de la Información y las Comunicaciones, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, en este mismo sentido facilita el acceso a algunas herramientas de redes sociales, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de los funcionarios

COPIA CONTROLADA

y terceros, sin embargo es necesario precisar que será responsabilidad de los funcionarios y contratistas hacer uso de forma correcta y moderada de estas, con el fin de asegurar una adecuada protección de la información institucional.

Lineamientos:

8.4.1. El servicio de Internet debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas para la Contraloría de Bogotá D.C., y no debe utilizarse para ningún otro fin, los usuarios que hacen uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de la Contraloría de Bogotá. D.C.

8.4.2. Todas las comunicaciones establecidas mediante este servicio podrán ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control; en este mismo sentido la Contraloría de Bogotá D.C., se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

8.4.3. No se permite la conexión de módems externos o internos en la red de la entidad, previa solicitud autorizada por la Dirección de Tecnologías de la Información y las Comunicaciones.

8.4.4. Todos los usuarios que usen el servicio de internet son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, la seguridad digital, entre otros.

8.4.5. Los funcionarios y contratistas de la Contraloría de Bogotá D.C., deberán abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.

8.4.6. No es permitido enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida, así como propagar intencionalmente virus o cualquier tipo de código malicioso.

8.4.7. No está permitida la descarga, el uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, herramientas de hacking, información o productos que atenten contra la propiedad intelectual, archivos ejecutables, entre otros, que comprometan la seguridad de la información y la seguridad digital de la entidad.

8.4.8. Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la entidad, no obstante, la Contraloría de Bogotá D.C., se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

8.4.9. Todos los usuarios invitados que requieran acceso a internet dentro de las instalaciones principales de la Contraloría de Bogotá D.C. deben realizarlo por medio

COPIA CONTROLADA

de la red WIFI invitados y cumplir con los requerimientos indicados en el momento que se facilite la conexión, una vez que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes y no se suministrará el servicio.

8.5. USO CORREO ELECTRONICO

El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los funcionarios y contratistas de la Contraloría de Bogotá, D.C., cuyo uso se facilitará bajo las directrices generales del buen uso del correo electrónico.

Lineamientos:

8.5.1. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Dirección de Tecnologías de la Información y las Comunicaciones, cuyo dominio es @contraloriabogota.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

8.5.2. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro, ajeno a los propósitos de la entidad.

8.5.3. En cumplimiento de la Estrategia de Cero Papel liderada por al Plan Institucional de Gestión Ambiental – PIGA, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita y las condiciones lo faciliten.

8.5.4. Se prohíbe el envío de correos masivos (no mayor a 30 destinatarios) internos o externos, con excepción de los enviados por las dependencias expresamente autorizadas, así como de la Dirección de Tecnologías de la Información y las Comunicaciones en caso de ventana de mantenimientos de los servicios de TI. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

8.5.5. Todo mensaje no solicitado o no deseado (SPAM), cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Dirección de Tecnologías de la Información y las Comunicaciones por medio de la Mesa de Servicios como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.

8.5.6. Cuando un funcionario o contratista se retire de la entidad, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo institucional, la Dirección de Talento Humano y/o la Dirección Administrativa y Financiera deberán notificar a la Dirección de Tecnologías de la Información y las Comunicaciones la desactivación de la cuenta.

8.5.7. El tamaño máximo para recibir o enviar mensajes es de 25 MB (incluyendo la suma de todos los adjuntos).

COPIA CONTROLADA

8.5.8. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de la Contraloría de Bogotá D.C., y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.
8.5.9. La cuenta de correo institucional no debe ser utilizada para propósitos personales o para ingreso o suscripción en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.
8.5.10. El correo electrónico institucional en sus mensajes debe contener una sentencia ambiental y de confidencialidad y debe reflejarse en todos los buzones con dominio @contraloriabogota.gov.co.
8.5.11. Es responsabilidad de los usuarios del correo institucional, verificar que los correos cumplan con los estándares determinados por la Oficina Asesora de Comunicaciones para la firma de estos.
8.5.12. La Dirección de Tecnologías de la Información y las Comunicaciones no realiza copias de respaldo de las cuentas de correo institucionales, si un usuario la requiere deberá solicitar el servicio de respaldo por los medios establecidos para soporte a usuarios.
8.5.13. Para las cuentas de correo generalizadas o que le sean asignadas a varios usuarios, estos deberán ser responsables por el manejo y gestión de estas; la Dirección de Tecnologías de la Información y las Comunicaciones no se responsabiliza por el uso inadecuado o perdida de información de estas y al igual que las cuentas personales institucionales, deberán acogerse a los presentes lineamientos.

8.6. USO DE LOS RECURSOS TECNOLÓGICOS

Los recursos tecnológicos de la Contraloría de Bogotá D.C., son herramientas de apoyo a las labores y responsabilidades de los funcionarios y contratistas y se emplearán de manera exclusiva y bajo la completa responsabilidad del funcionario o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Dirección de Tecnologías de la Información y las Comunicaciones, salvo que medie solicitud formal de los Directores, Subdirectores, Jefes de Oficina, a través de la Mesa de Servicios.

Lineamientos:

8.6.1. Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones.
8.6.2. En caso de que el funcionario o contratista deba hacer uso de equipos ajenos a la Contraloría de Bogotá D.C., y requieran ser conectados a la red de la entidad, éstos deberán cumplir con la legalidad del software instalado, sistema operativo y antivirus licenciado y actualizado, y solo podrá conectarse a la red de la entidad una vez esté revisado por la Dirección de Tecnologías de la Información y las Comunicaciones.
8.6.3. Está expresamente prohibido el almacenamiento de archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o

COPIA CONTROLADA

propiedad intelectual de los mismos en los discos duros de computadores de escritorio, portátiles, discos virtuales de red y unidades externas suministrados por la entidad.

8.6.4. No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de la integridad de ésta.

8.6.5. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por la Dirección Administrativa y Financiera de la Entidad.

8.6.6. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la Dirección de Tecnologías de la Información y las Comunicaciones de la entidad.

8.6.7. La Dirección de Tecnologías de la Información y las Comunicaciones es la única dependencia autorizada para la administración del software de la Contraloría de Bogotá D.C., el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

8.6.8. La instalación de software y Sistemas de Información se encuentra bajo la responsabilidad de la Dirección de Tecnologías de la Información y las Comunicaciones y por tanto son los únicos autorizados para realizar esta actividad y toda solicitud debe realizarse por medio de la Mesa de Servicios.

8.6.9. Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por la Dirección de Tecnologías de la Información y las Comunicaciones.

8.6.10. La Dirección de Tecnologías de la información y las Comunicaciones es la responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en la entidad para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

8.6.11. Sólo el personal autorizado por la Dirección de Tecnologías de la Información y Comunicaciones podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la entidad; las conexiones establecidas para este fin, utilizaran los esquemas de seguridad establecidos por la entidad.

8.6.12. Los funcionarios y contratistas de la Entidad son responsables de hacer buen uso de los recursos tecnológicos de la Contraloría de Bogotá D.C. y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, contratistas, terceros, o contra la legislación vigente y políticas y/o lineamientos de seguridad de la información establecidas por la Contraloría de Bogotá D.C.

8.6.13. Cualquier requerimiento que tenga un usuario respecto a instalación, desinstalación, o actualización de sus aplicaciones, deberá solicitarse por medio de la Mesa de Servicios, y estas entrarán a ser evaluadas por la Dirección de Tecnologías de la Información y las Comunicaciones para su aprobación o denegación. (En caso de equipos ubicados en instalaciones de sujetos de control se realizará en coordinación con el área de tecnología de la entidad sujeto de control)

COPIA CONTROLADA

8.6.14. Cada usuario debe ser responsable de realizar el respaldo respectivo de la información que maneja en su equipo de cómputo. La Dirección de Tecnologías de la Información y las Comunicaciones sólo es responsable de respaldar y salvaguardar la información que se encuentra en las unidades de almacenamiento de los servidores del centro de cómputo. En caso de que algún usuario requiera ayuda con sus respaldos, deberá solicitarlo por medio de la Mesa de Servicios, para que se le indique el procedimiento más adecuado y su información pueda estar asegurada.

8.6.15. El uso de dispositivos como unidades de almacenamiento USB, CD o cualquier otro, es de exclusiva responsabilidad de los usuarios, los cuales deberán asegurarse de que estos no contengan ningún medio de contaminación de virus.

8.6.16. Los usuarios solo podrán utilizar software legalmente adquirido y/o autorizado por la Contraloría de Bogotá D.C., en caso de presentarse algún tipo de reclamación por software ilegal y violación de derechos de autor, esta recaerá sobre el usuario responsable en donde se encontrase instalado dicho software. En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información. Los usuarios no pueden realizar copias de software que se encuentre instalado o sea desarrollado por la Contraloría de Bogotá D.C., para su distribución.

8.6.17. Los movimientos o cambios de ubicación de los equipos propiedad de la Contraloría de Bogotá D.C., ubicados en los sujetos de control o que se encuentren fuera de las instalaciones de la entidad se deberán informar a la Dirección de Tecnologías de la información y las Comunicaciones, para realizar limpieza, desinstalación de software que no es propiedad de la entidad y control de ubicación de los equipos, es de aclarar que esta actividad no sustituye la que cada funcionario deberá realizar con la Dirección Administrativa y Financiera para el control propio de los inventarios y bienes de la Contraloría de Bogotá D.C.

8.6.18. No está permitido por parte de los funcionarios aplicar ningún líquido (alcohol, cloro o ácidos) sobre ningún dispositivo asignado (teclado, mouse, monitor) para la desinfección, ya que esta actividad está a cargo del personal de servicios generales de cada dependencia.

8.7. POLÍTICA DE GESTIÓN DE ALMACENAMIENTO

La Contraloría de Bogotá D.C., a fin de proteger la información y preservar la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento, establece los lineamientos para la gestión de la información que se encuentra en unidades compartidas como el Datacontrabog y herramientas como SharePoint y OneDrive.

Lineamientos:

8.7.1. Se restringe el uso de carpetas compartidas desde equipos de escritorio. Si el colaborador no adopta esta política la Dirección de Tecnologías de la Información y las Comunicaciones no se hace responsable de la pérdida o infiltración de la información.

8.7.2. Las carpetas compartidas sobre la infraestructura ofrecida por la Dirección de Tecnologías de la Información y las Comunicaciones como Datacontrabog, serán

COPIA CONTROLADA

gestionadas por cada una de las dependencias quienes velarán por el buen uso de la información y de las carpetas; para esto se debe documentar e informar a la Dirección de Tecnologías de la Información y las Comunicaciones para la administración de los permisos y accesos sobre la carpeta compartida, usando los siguientes criterios:

- Permisos de Lectura
- Permisos de Escritura y modificación
- Permisos de Control Total

Lo cuales serán asignados por la Dirección de Tecnologías de la Información y las Comunicaciones a través de la Mesa de servicios.

Para las herramientas SharePoint u OneDrive, los permisos son concedidos por el propietario del recurso o archivo, por lo tanto, es responsabilidad de cada usuario la gestión de estos permisos.

8.7.3. La información que cada dependencia de la entidad identifique como importante e imprescindible para el desarrollo de sus funciones o soporte de la ejecución de estas, deberá ser almacenada en las carpetas destinadas en el Datacontrabog, para que sean incluidos en las Políticas de respaldo de información (backup).

8.7.4. Cada dependencia tendrá un administrador del espacio asignado en el Datacontrabog que será autorizado con permisos de lectura y escritura, quien gestionará las carpetas y será responsable a que usuarios otorgará permisos sobre esta. Los permisos de administrador serán gestionados por la Dirección de Tecnologías de la Información y las Comunicaciones, a través de la mesa de servicios

8.7.5. Cada administrador de las carpetas del Datacontrabog, deberá realizar semestralmente una depuración de la información y notificar a la Dirección de Tecnologías de la Información y las Comunicaciones los cambios realizados a fin de ajustar las políticas de copias de respaldo.

8.7.6. La información que las dependencias usen para revisión o trabajo colaborativo la podrán almacenar en las unidades de OneDrive o SharePoint, teniendo claridad que este almacenamiento es transitorio y no están cubiertos por los lineamientos de copias de respaldo institucionales de la Contraloría de Bogotá D.C., ya que son herramientas de almacenamiento en la nube y la Dirección de Tecnologías de la Información y las Comunicaciones no las incluye dentro de las políticas de respaldo de información.

8.7.7. Se prohíbe el acceso a las carpetas del Datacontrabog desde equipos de cómputo que no cuenten con una herramienta de antivirus actualizado.

8.7.8. Se prohíbe la publicación de archivo ejecutables (.exe, bat y dll entre otros) en las carpetas del Datacontrabog, si la dependencia requiere usar alguna de las extensiones mencionadas, debe justificarlo a la Dirección de Tecnologías de la Información y las Comunicaciones para ajustar la política, de acuerdo a lo definido por las dos dependencias.

8.7.9. La Dirección de Tecnologías de la Información y las Comunicaciones podrá realizar monitoreo y/o revisiones periódicas, con el fin de asegurar una correcta administración y gestión de las carpetas e información almacenada en el Datacontrabog.

8.7.10. Se prohíbe el uso de carpetas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la función del colaborador.

COPIA CONTROLADA

8.8. USO DE LOS SISTEMAS O HERRAMIENTAS DE INFORMACIÓN

Todos los servidores públicos y contratistas de la Contraloría de Bogotá D.C., son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido.

Lineamientos:

8.8.1. Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelarlas a terceros, ni utilizar claves ajenas.
8.8.2. Todo funcionario y contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.
8.8.3. Todo funcionario y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
8.8.4. En ausencia del funcionario o contratista, el acceso a la estación de trabajo y demás sistemas de información le será bloqueada conforme a los procedimientos vigentes, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. El Grupo Interno de Trabajo de Gestión del Talento Humano debe reportar a la Dirección de Tecnologías de la Información y las Comunicaciones a la mayor brevedad, cualquier tipo de novedad de funcionarios, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.
8.8.5. Cuando un funcionario o contratista cesa sus funciones o culmina la ejecución del contrato con la Contraloría de Bogotá D.C., todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente y el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.

8.9. POLÍTICA DE USO DE DISPOSITIVOS PROPIOS DE FUNCIONARIOS O CONTRATISTAS

La Contraloría de Bogotá D.C., define controles sobre su información mientras se accede a esta a través de dispositivos que no pertenecen o no son provistos por la entidad y que los funcionarios o contratistas utilizarán para manejar o gestionar información institucional; dichos controles aplican a todos los dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información; entre estos dispositivos se incluye a los computadores personales, teléfonos inteligentes, unidades de memoria USB, cámaras digitales, wearables personales, entre otros. En esta política identificará a estos dispositivos como BYOD (Bring Your Own Device tendencia tecnológica cuya traducción es “trae tu propio dispositivo”).

Lineamientos:

8.9.1. Los datos e información de propiedad de la Contraloría de Bogotá D.C., que se almacenan, transfieren o procesan en BYOD siguen perteneciendo a la entidad, y esta

COPIA CONTROLADA

mantiene el derecho a controlar esos datos e información, aunque no sea propietaria del dispositivo.

8.9.2. Las aplicaciones que se tienen autorizadas para esta modalidad de trabajo BYOD, se limitan al correo electrónico, herramientas colaborativas y de integración de los productos Office 365 tales como Teams, OneDrive, aplicaciones de conexión remota como VPN y herramientas de entidades, necesarias para el desarrollo de funciones propias de la Contraloría de Bogotá D.C.

8.9.3. Todos los BYOD deben tener instalado software antivirus, y en la medida de lo posible, software de prevención de intrusiones, programas malignos (malware), software para administración de dispositivos móviles, entre otros.

8.9.4. Los dispositivos BYOD deberán estar protegidos mediante métodos de autenticación como, por ejemplo, claves, contraseñas, lectores biométricos.

8.9.5. La información de propiedad de la entidad no estará compartida para ningún tipo de redes o usuarios (excepto dentro de la intranet de la entidad) o solo podrán compartirse mediante algún método seguro de conexión a la red de la entidad, por ejemplo, VPN.

8.9.6. Cuando se utilicen BYOD fuera de las instalaciones de la entidad, no deben ser dejados desatendidos y, si es posible, deben estar físicamente resguardados bajo llave.

8.9.7. Cuando se utiliza BYOD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

8.9.8. Los funcionarios y contratistas serán los responsables de instalar periódicamente parches, software de protección y actualizaciones, así como de las reparaciones en las fallas técnicas que presenten sus dispositivos y los costos de estos son responsabilidad del propietario.

8.9.9. No está permitido el acceso a personas diferentes a los funcionarios o contratistas propietarios del dispositivo a la información que se esté manejando en el mismo, en caso de evidenciar algún acceso no autorizado el funcionario o contratista será quien asuma la responsabilidad del incumplimiento.

8.9.10. Los funcionarios y contratistas propietarios del dispositivo no exigirán ningún costo por el uso del dispositivo a la Contraloría de Bogotá D.C., ya que es un acuerdo de voluntades con fines laborales.

8.9.11. Costos de telecomunicaciones (cargos de teléfono y datos), licenciamiento y demás costos asociados a los BYOD son asumidos por los funcionarios y contratistas propietarios del dispositivo.

8.10. USO DE HERRAMIENTAS OFIMATICAS Y COLABORATIVAS EN ENTORNOS VUCA[1]

La Contraloría de Bogotá D.C., establece lineamientos y recomendaciones para el uso y aplicación de tecnologías, estrategias y herramientas que permitan contar con una respuesta correcta y eficaz para afrontar los cambios y hacer frente a los problemas y dificultades en un contexto impredecible y cambiante que suponen grandes desafíos para la entidad, a fin de lograr mayor cohesión, eficiencia y dar seguridad a la información que se produce en desarrollo de las funciones que corresponden al cumplimiento de la misionalidad de la entidad.

[1] Volatility (V), Uncertatinty (U), Complexity (C) y Ambiguity (A). - Volatilidad, Incertidumbre, Complejidad y Ambigüedad.

COPIA CONTROLADA

Lineamientos:

8.10.1. **Redes Privadas Virtuales**: Usar la conexión VPN solo para realizar las labores puntuales y luego desconectarse; no se requiere mantener la red activa siempre, puesto que no todas las actividades se hacen directamente sobre el equipo, algunas tareas, se pueden realizar ingresando a la Intranet; esto contribuye con la gestión del canal de la red informática institucional.

8.10.2. **SIGESPRO**: Realizar depuración del Sistema de Gestión de Procesos y Documentos -SIGESPRO-, tramitar y finalizar los procesos, y de esta manera, evitar la cantidad de procesos activos y vencidos.

8.10.3. **Antivirus**: En caso de usar equipos que no son propiedad de la entidad para el desarrollo de las funciones, se solicita a los funcionarios tener activo alguna herramienta de antivirus en sus equipos o dispositivos móviles, a fin de contener la propagación de software malicioso entre los equipos y la red de la entidad.

8.10.4. **Solicitudes de soporte técnico**: Solicitarlo a través de la Mesa de Servicio, ingresando en el botón dispuesto en la Intranet o escribir al correo electrónico mesaservicios@contraloriabogota.gov.co.

8.10.5. **Microsoft TEAMS**: Es una herramienta que puede ser usada por todos los funcionarios de la entidad de manera organizada y para fines laborales; no se debe usar el chat para conversaciones personales; en las videoconferencias, se debe apagar la cámara, usarla solo cuando se va a intervenir; no grabar las sesiones de trabajo, salvo que sea estrictamente necesario y esté autorizado para hacerlo, y participar solo en los canales internos y a los que fue asignado, informar y seguir los protocolos establecidos para su uso en las diferentes actividades institucionales.

8.10.6. **Correo Electrónico**: Todos los funcionarios y contratistas deben depurar los buzones de correo electrónico institucional, para evitar el desbordamiento, debido a que pueden sobrepasar la capacidad de almacenamiento y restringir o limitar la entrada de nuevos mensajes.

8.10.7. **Computadores personales – trabajo en casa**: Cuando se requiera un esquema de trabajo en casa, en lo posible se deberán acoger las políticas de teletrabajo y demás lineamientos de seguridad descritos en este documento a fin de preservar la confidencialidad, integridad y disponibilidad de la información institucional.

8.10.8. **OneDrive y SharePoint**: Son herramientas que proporcionan facilidad en la gestión y colaboración de información y de archivos; los controles de acceso están bajo un entorno de seguridad y confidencialidad aprovisionado por la entidad y el proveedor, la capacidad de almacenamiento de información es limitada y se recomienda su uso moderado y para información estrictamente institucional. Se recuerda a los funcionarios y contratistas que estos espacios son de carácter transitorio y temporal, por tal motivo deberán ser depurados constantemente y eliminados o descargados aquellos documentos de acuerdo con su importancia y naturaleza. Es de mencionar que la cantidad de almacenamiento asignado a cada funcionario es limitada y que, por tanto, de no depurarse puede generarse problemas de espacio que impidan seguir gestionando más información.

8.10.9. **DataContraBog**: Solo el “Administrador de archivo de gestión electrónico” designado mediante memorando en cada una de las dependencias, es quien debe asegurar que el repositorio documental se encuentra acorde con los permisos y la visualización de la información y documentos de los funcionarios que pertenecen a la dependencia, y

COPIA CONTROLADA

que las carpetas e información corresponde a información institucional en el marco de las competencias de cada una dependencias en las cuales ejerce la administración de documentos de archivo. La Dirección de Tecnologías de la Información y las Comunicaciones será responsable de la asignación de permisos de acceso, lectura y modificación según los permisos definidos por la dependencia propietaria del espacio de almacenamiento y de la información en Datacontrabog. El repositorio Datacontrabog-apoyo, es un sitio de almacenamiento de información de apoyo temporal, y es responsabilidad de los funcionarios hacer la depuración, dado que el espacio es limitado.

8.10.10. Todos los recursos dispuestos para atender las contingencias que se presenten en los entornos VUCA, son restringidos y deberán ser utilizados de forma eficiente y cuando sea estrictamente necesario.

9. CONTROL DE CAMBIOS

Versión	R.R. Nº y Fecha Día mes año	Descripción de la modificación
1.0	R.R. No.022 14-jul-2016	Se adoptan las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C., para efectos de obligatoriedad en su cumplimiento, la cual forma parte de la documentación que soporta el Sistema Integrado de Gestión, en el marco del Subsistema de Seguridad de la Información y de la estrategia del Gobierno en Línea.
2.0	R.R. No. 022 19-abr-2018	Se actualizan las Políticas, conforme a lo aprobado en el Comité SIGEL No.3 realizado el día 11 de junio de 2019, a la normatividad legal vigente y a lo establecido en la Norma Técnica Colombiana ISO/IEC 27001:2013, con las directrices para la proteger la información, asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones legales, operativas, tecnológicas y de acuerdo al objetivo estratégico, debiéndose modificar el nombre a Políticas de Seguridad de la Información

COPIA CONTROLADA

Versión	R.R. Nº y Fecha Día mes año	Descripción de la modificación
3.0	R.R. No.038 24-sep-2019	En Comité PG_DIGITAL de diciembre 1 de 2020 se aprueba la actualización de las políticas, en los siguientes aspectos: • Modificar el nombre del documento de "Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C.", a "Políticas de Seguridad de la Información y Seguridad Digital de la Contraloría de Bogotá, D.C." • Modificar y actualizar las políticas con el fin de establecer las directrices para la proteger la información de la Contraloría de Bogotá D.C., asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones legales, operativas, tecnológicas y de acuerdo al objetivo estratégico, manteniendo la confianza de los usuarios internos y externos de los procesos, trámites y servicios que presta la entidad. • Incluir las políticas de Seguridad Digital conforme a los nuevos lineamientos de las políticas institucionales.
4.0	R.R. 012 21-Abril -2021	

COPIA CONTROLADA