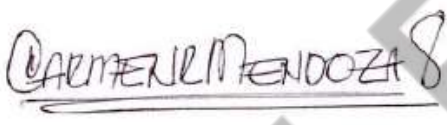
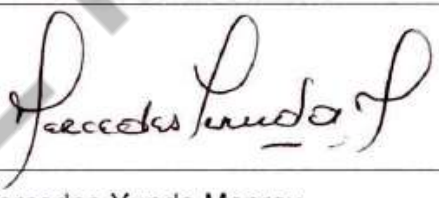
	Aprobación	Revisión Técnica
Firma:		
Nombre:	Carmen Rosa Mendoza Suarez	Mercedes Yunda Monroy
Cargo:	Directora Técnica	Directora Técnica
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	Dirección de Planeación
R.R. No. 038 **Fecha:** 24 SET. 2019		

OBSOLETO

JUAN CARLOS GRANADOS BECERRA
Contralor de Bogotá, D.C.

MARIA ANAYME BARÓN DURÁN
Contralora Auxiliar

MERCEDES YUNDA MONROY
Directora Técnica de Planeación

CARMEN ROSA MENDOZA SUÁREZ
Directora Técnica de Tecnologías de la Información y las Comunicaciones

OBSOLETO

Bogotá, D.C., Septiembre 2019

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO GENERAL DEL SGSI 4
2.1. OBJETIVOS ESPECÍFICOS DEL SGSI 4
3. ALCANCE/APLICABILIDAD 5
4. CUMPLIMIENTO 5
5. TERMINOLOGÍA 6
6. POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACION 7
7. POLÍTICAS ESPECIFICAS DE LA SEGURIDAD DE LA INFORMACION 8
7.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 9
7.2. DISPOSITIVOS MÓVILES 10
7.3. TELETRABAJO 11
7.4. CONTROL DE ACCESO LÓGICO Y FÍSICO 12
7.5. CONTROLES CRIPTOGRÁFICOS 14
7.6. ESCRITORIO LIMPIO Y PANTALLA LIMPIA 15
7.7. COPIAS DE RESPALDO 16
7.8. TRANSFERENCIA DE LA INFORMACIÓN 16
7.9. DESARROLLO SEGURO 17
7.10. RELACIONES CON LOS PROVEEDORES 19
7.11. GESTIÓN DE ACTIVOS 20
7.12. NO REPUDIO 21
7.13. PRIVACIDAD Y CONFIDENCIALIDAD 22
7.14. INTEGRIDAD 23
7.15. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN 23
7.16. REGISTRO Y AUDITORÍA 24
7.17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 25
7.18. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN 26
8. APROBACION Y ACTUALIZACIÓN 27
9. CONTROL DE CAMBIOS. 27

OBSOLETO

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 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.

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, 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 y 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, el cual expresa el compromiso de la alta dirección con la seguridad de la información, 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.

Estas políticas serán revisadas con regularidad, como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, en su estructura, sus objetivos o en alguna condición que la afecte, para asegurar que dichas políticas sigan siendo adecuadas y ajustadas a los requerimientos de la Entidad.

2. OBJETIVO GENERAL DEL SGSI

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.

2.1. OBJETIVOS ESPECÍFICOS DEL SGSI

OBSOLETO

Los siguientes son los objetivos de seguridad de la información para la Contraloría de Bogotá D.C.:

- Aplicar controles de seguridad que permitan proteger los activos de información, buscando mantener la confidencialidad, la disponibilidad e integridad.
- Garantizar la integridad, confidencialidad y el acceso a la información de acuerdo a los niveles y criterios de seguridad que establecidos por la Entidad y a los exigidos por la normatividad vigente.
- Identificar mediante una adecuada evaluación del riesgo, el valor de la información, así como las vulnerabilidades y las amenazas a las que están expuestos los activos de información.
- Minimizar, gestionar y dar tratamiento a los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean asumidos, transferidos, minimizados y/o eliminados de forma eficiente y adaptada a los cambios que se produzcan en la Entidad, el entorno y la tecnología.
- Asegurar el mejoramiento continuo de la seguridad de la información para responder a Los cambios futuros.
- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.

3. ALCANCE/APLICABILIDAD

El alcance del Subsistema de Gestión de la Seguridad de la Información – SGSI, aplica a los activos de información de 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.

4. CUMPLIMIENTO

Tanto la política General del SGSI como las políticas específicas que de esa se desprendan son de obligatorio cumplimiento para todas las personas mencionadas dentro del alcance y deberán dar acatamiento al 100% de las mismas.

El incumplimiento a la política de Seguridad y Privacidad de la Información de la Contraloría de Bogotá D.C., traerá consigo, las consecuencias legales que apliquen a la normativa de la

OBSOLETO

Entidad, incluyendo lo establecido en las Lineamientos que competen al gobierno nacional y territorial en cuanto a seguridad de la Información se refiere.

5. TERMINOLOGÍA

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.
Activo de Información: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Activo de información: Conocimiento o datos que tienen valor para el individuo u organización[1].
Acuerdo de Confidencialidad: Documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Entidad, a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Entidad.
Autenticación: Asegurar que una característica declarada de una Entidad es correcta.
Autenticidad: Propiedad de que una Entidad es lo que dice ser.
Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, Entidades o procesos no autorizados.
Dirección IP: Número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad autorizada.
Incidente de seguridad: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.
Información[2]: Es un activo esencial para el negocio de una organización y por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato físico (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diferentes medios incluyendo: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.
Integridad: Propiedad de exactitud y completitud de la información.
Medios removibles: Dispositivos tecnológico de almacenamiento de información diseñados para ser extraídos del computador.

[1] ISO/IEC 27032:2012
[2] NTC-ISO/IEC27000:2016

OBSOLETO

Mejora Continua: El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de lograr los objetivos relativos a la preservación de la confidencialidad, disponibilidad e integridad de la información. El foco de la mejora continua es buscar oportunidades para la mejora y no asumir que las actividades de gestión existentes son suficientemente buenas o tan buenas como podrían ser.

Política: Declaración de alto nivel que describe la posición de la Entidad sobre un tema específico.

Seguridad de la información: Asegura la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucran la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.

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

6. POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACION

La siguiente es la Política de Seguridad de la Información establecida para la Contraloría de Bogotá, D.C.:

"La Contraloría de Bogotá D.C. reconoce la importancia de la protección de los activos de Información que soportan los procesos de la Entidad, por ello se encuentra comprometida con la implementación de medidas para asegurar su confidencialidad, integridad, disponibilidad y privacidad de acuerdo con las Lineamientos legales vigentes, para lo cual, adopta políticas, procedimientos, lineamientos y asigna responsabilidades para la adecuada gestión de la seguridad de la información".

La alta dirección de la Contraloría de Bogotá D.C., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un subsistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Distrito y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la Contraloría de Bogotá D.C., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, las políticas del SGSI estarán determinadas por las siguientes premisas:

OBSOLETO

- 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.
- 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, aprendices, practicantes y grupos de interés de la Contraloría de Bogotá D.C.
- Garantizar la continuidad del negocio frente a incidentes.

7. POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACION

A continuación, se establecen las políticas específicas de la seguridad de la información que soportan el SGSI de la Contraloría de Bogotá D.C.:

- La Contraloría de Bogotá D.C., ha decidido definir, implementar, operar y mejorar de forma continua un Subsistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Entidad y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.
- La Contraloría de Bogotá D.C., protegerá la información generada, procesada o resguardada por los procesos misionales y activos de información que hacen parte de los mismos.
- La Contraloría de Bogotá D.C., protegerá la información creada, procesada, transmitida o resguardada por sus procesos misionales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Contraloría de Bogotá D.C., protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Contraloría de Bogotá D.C., controlará la operación de sus procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Contraloría de Bogotá D.C., implementará control de acceso a la información, sistemas y recursos de red.
- La Contraloría de Bogotá D.C., garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Contraloría de Bogotá D.C., garantizará a través de una adecuada gestión de los incidentes de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

BORRADOR

- La Contraloría de Bogotá D.C., garantizará la disponibilidad de sus procesos misionales y la continuidad de su operación basado en el impacto que pueden generar los incidentes.
- Contraloría de Bogotá D.C., garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, Contraloría de Bogotá D.C., desarrollará e implementará controles de seguridad de la información, los cuales serán establecidos en los procedimientos del Sistema Integrado de Gestión.

A continuación, se describen en detalle las políticas específicas de la seguridad de la información que soportan el SGSI de la Contraloría de Bogotá D.C.

7.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En la Contraloría de Bogotá D.C., se definen los roles y responsabilidades los cuales ejecutan actividades de administración, operación y gestión de la Seguridad de la Información, para prevenir que se presenten conflictos de intereses que conlleven 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 están definidos en el numeral 7.4.6. Roles y Responsabilidades del manual del Sistema Integrado de Gestión – SIG de la Entidad.

7.1.2. El Comité Técnico de Seguridad de la Información y Gobierno en Línea – SIGEL 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 nuevos lineamientos del orden Nacional y Distrital relativos a la seguridad de la información, 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. Los proyectos desarrollados en la Contraloría de Bogotá D.C deberá incorporar dentro de la planeación y desarrollo, el cumplimiento de la política de seguridad de la información, valoración de riesgos y los controles a estos.

7.1.4. Se debe asignar al responsable de cada activo o proceso de Seguridad de la Información, y se deben documentar los detalles de esta responsabilidad.

7.1.5. Se deben definir las responsabilidades para las actividades de gestión del riesgo de la Seguridad de la Información

7.1.6. La estructura de organización de Seguridad de la Información debe ser publica y clara en sus responsabilidades para cada uno de los roles definidos.

OBSOLETO

7.1.7. 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.

7.2. DISPOSITIVOS MÓVILES

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

Lineamientos:

7.2.1. 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.

7.2.2. 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.

7.2.3. 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.

7.2.4. 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.

7.2.5. 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, se debe evitar hacer uso de estos para cuestiones personales, así como en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

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

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

7.2.8. 7.2.8. Se deben generar recomendaciones del uso y cuidado de tipo físico cuando el dispositivo se encuentre fuera de las instalaciones de la entidad. El usuario debe

OBSOLETO

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

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

7.3. TELETRABAJO

La Contraloría de Bogotá D.C., según lo establecido en los procedimientos de la Entidad debe proteger la información a la que tienen acceso los funcionarios, por razón y motivo de su cargo, en consecuencia y respecto a los teletrabajares se indica, 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:

7.3.1. 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.

7.3.2. 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.

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

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

7.3.5. 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.

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

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

7.3.8. La administración, mantenimiento y soporte de equipos que son propiedad de los teletrabajadores, es responsabilidad de los mismos, en ningún momento la Contraloría

OBSOLETO

de Bogotá D.C., se hace responsable por estas actividades; la entidad las asume, para los equipos que suministre al teletrabajador.

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

7.4. 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 a la clasificación de la información, las funciones y cargos que desempeñen los funcionarios, contratistas y terceros. Siempre se brindarán accesos de acuerdo al 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:

7.4.1. La Contraloría de Bogotá D.C, se 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.

7.4.2. Cuando se 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.

7.4.3. En ningún caso se otorgará acceso a terceros, 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.

7.4.4. 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.

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

7.4.6. Se debe retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado de ser parte de la Entidad.

7.4.7. 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

OBSOLETO

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.

7.4.8. 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.

7.4.9. Las contraseñas nunca se deben almacenar en sistemas de computador o en otro medio en un formato no protegido.

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

7.4.11. 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.

7.4.12. 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 máxima de 90 días, 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.

7.4.13. 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.

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

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

7.4.16. 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.

7.4.17. 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.

7.4.18. Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas identificadas como seguras de la Entidad.

7.4.19. Es responsabilidad de todos los usuarios internos y externos acatar las Lineamientos de seguridad y mecanismos de control de acceso a las instalaciones de la Entidad.

7.4.20. 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.

7.4.21. Todo acceso físico a las áreas protegidas deberá estar manejado según los lineamientos definidos por los procedimientos designados para el manejo de estas áreas.

OBSOLETO

7.4.22. 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 empleado 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.
- No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

7.5. CONTROLES CRIPTOGRÁFICOS

La política de seguridad de controles criptográficos 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:

7.5.1. 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.

7.5.2. Se deben establecer mecanismos para el manejo y la administración de llaves de cifrado; y estándares para la aplicación de controles criptográficos.

7.5.3. Se deben implementar controles respecto de la administración de llaves, recuperación de información cifrada en caso de pérdida, compromiso o daño de las llaves y reemplazo de las llaves de cifrado.

7.5.4. Al implementar esta política en materia criptográfica, se deben considerar los controles aplicables al cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.

7.5.5. 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.

7.5.6. Todas las llaves serán protegidas contra modificación y destrucción y las llaves privadas serán protegidas contra uso indebido, copia o divulgación no autorizada.

OBSOLETO

7.5.7. A fin de reducir la probabilidad de compromiso, las llaves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por un lapso de tiempo definido, no mayor a 12 meses.

7.5.8. La pérdida, robo o posible divulgación no autorizada de la llave de cifrado o mecanismo criptográfico debe de ser reportado inmediatamente a la Dirección de Tecnologías de la Información y las Comunicaciones para su revocación.

7.5.9. Para la generación de contraseña para las llaves o mecanismos criptográficos deberán cumplir lineamientos establecidos en el lineamiento 7.4.12. de este documento, para la construcción de contraseñas seguras.

7.5.10. La Dirección TIC será responsable y encargada de la activación y revocación de las llaves criptográficas asignadas por la Contraloría de Bogotá, D.C., a los usuarios autorizados.

7.6. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

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

Lineamientos:

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

7.6.2. Los usuarios siempre al ausentarse del puesto de trabajo 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.

7.6.3. 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.

7.6.4. 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.

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

7.6.6. 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.

7.6.7. 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.

OBSOLETO

7.6.8. 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.

7.6.9. 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.

7.6.10. 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.

7.7. COPIAS DE RESPALDO

La Contraloría de Bogotá D.C., debe realizar copias de respaldo de la información misional 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 aclara que cada usuario es responsable de la información que maneja en su equipo de cómputo, en consecuencia, es el responsable de realizar las copias de respaldo de la misma.

Lineamientos:

7.7.1. Los medios de copias se deben almacenar en custodia externa en una sede alterna de la Contraloría de Bogotá D.C., asegurando que tenga implementado mecanismos de protección ambiental.

7.7.2. Realizar pruebas de restauración de la información, de acuerdo a un plan de restauración de copias de respaldo establecido, para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.

7.7.3. 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.

7.7.4. 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.

7.7.5. Se debe contar con registros exactos y completos de las copias de respaldo.

7.7.6. Definir la frecuencia y tipo de copias de respaldo a realizar.

7.7.7. Las pruebas de restauración se deberían hacer en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que se cause un daño o pérdida de la información.

7.8. TRANSFERENCIA DE LA INFORMACIÓN

OBSOLETO

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 que pueda copiar, modificar, o eliminar la información por parte de terceros.

Lineamientos:

7.8.1. Usar técnicas de cifrado de la información para garantizar la confidencialidad e integridad de la información durante la transferencia de la información.

7.8.2. 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.

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

7.8.4. Cuando proceda, la oficina responsable de dar respuesta legal a un requerimiento de información clasificada, deberá verificar previamente entre otros temas y sin limitarse a:

- 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.

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

7.9. 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, los desarrolladores 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:

OBSOLETO

7.9.1. 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.

7.9.2. Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.

7.9.3. El cambio de versión de las aplicaciones implementadas en el ambiente de producción se debe hacer de acuerdo a lo definido en el procedimiento para el control de cambios, 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.

7.9.4. 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.

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

7.9.6. El paso de software de un ambiente a otro debe ser controlado y gestionado de acuerdo a lo definido en el procedimiento de control de cambios.

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

7.9.8. 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 tenga cumpla los requisitos definidos por la Dirección de Tecnologías de la Información y las Comunicaciones.

7.9.9. 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, del mismo modo se debe aplicar el procedimiento para el control de cambios, 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.

7.9.10. 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.

7.9.11. 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.

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

7.9.13. 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 como resultado de proyectos o programas que se encuentran en la Entidad.

7.9.14. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Dirección de Tecnologías de la Información y las Comunicaciones.

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

OBSOLETO

7.9.16. Se encuentra prohibido el uso e instalación de juegos en los computadores de la Contraloría de Bogotá D.C.

7.10. 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:

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

7.10.2. 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 al 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.

7.10.3. La Entidad debe incluir dentro de los acuerdos a firmar con el proveedor, todos los controles de seguridad aplicables.

7.10.4. 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

7.10.5. 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.

7.10.6. 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, éste junto con los encargados de la infraestructura tecnológica, aprobarán y autorizarán el acceso y uso de la información.

7.10.7. 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

OBSOLETO

- 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.
- 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.

7.10.8. 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.

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

7.10.10. 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.

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

OBSOLETO

7.11. 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 a 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:

7.11.1. 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.

7.11.2. 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 a la presente política y el procedimiento establecido para la gestión de activos.

7.11.3. La identificación, clasificación y valoración de los activos de información se debe realizar de acuerdo al procedimiento establecido.

7.11.4. 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.

7.11.5. Se debe mantener un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, de acuerdo a lo establecido en el procedimiento para la gestión de activos.

7.11.6. Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.

7.11.7. 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 a lo establecido en el procedimiento para la gestión de activos.

7.11.8. 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.

7.11.9. 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.

7.11.10. 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.

7.11.11. La Contraloría de Bogotá D.C. empleará procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos.

7.11.12. 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.

7.12. 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:

OBSOLETO

7.12.1. Para los procesos que se consideren se deben implementar mecanismos en los que no exista la posibilidad de desafiar su validez de una acción por parte de quien la generó.
7.12.2. Algunos mecanismos a implementar deberán contar con un tercero en que todos confíen y quien permita avalar la integridad y origen de los datos.
7.12.3. 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.
7.12.4. Estos registros se deben proteger contra perdida o modificación de tal manera que se garantice su disponibilidad e integridad.
7.12.5. Se deben realizar auditorías continuas a los mecanismos de control y a los procesos, para asegurarse que las partes implicadas nieguen haber realizado una acción.
7.12.6. Los servicios de intercambio electrónico de información deben incorporar mecanismos que sean garantía de no repudio.

7.13. 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 a su nivel de clasificación.

Lineamientos:

7.13.1. 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.
7.13.2. 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 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.
7.13.3. 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 los mismos.
7.13.4. 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.
7.13.5. Este acuerdo de confidencialidad debe indicar la vigencia del mismo, el cual debe mantenerse por un tiempo adicional que considere Contraloría de Bogotá D.C., luego de terminada la vinculación con la Entidad.
7.13.6. El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.

OBSOLETO

7.13.7. La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

7.13.8. 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.

7.13.9. Presentar quejas ante el área administrativa encargada de la protección de los datos personales.

7.14. 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:

7.14.1. 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.

7.14.2. 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.

7.14.3. 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.

7.15. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Contraloría de Bogotá D.C., 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; así mismo, responderá de manera efectiva ante eventos adversos según la dimensión y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la Seguridad de la Información durante dichos eventos, de igual manera se mantendrán canales de comunicación adecuados hacia los funcionarios y demás partes interesadas.

Para esto La Contraloría de Bogotá D.C., deberá evaluar el impacto de eventos que afectan los procesos de la Entidad y que tienen soporte en la infraestructura tecnológica y en la prestación de terceros, igualmente, deberá desarrollar planes de contingencia y de recuperación ante desastres (DRP) para aquellos servicios que son críticos y misionales, dichos planes deben

OBSOLETO

considerar medidas tanto técnicas como administrativas y deberán probarse y revisarse de manera periódica.

Lineamientos:

7.15.1. La Contraloría de Bogotá D.C., conforme a su misionalidad, establece que debe contar con un Plan de Recuperación ante Desastres (DRP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

7.15.2. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, deben estar incorporados y definidos en el Plan de Recuperación ante Desastres (DRP).

7.15.3. Los responsables de los procesos de la recuperación serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio a todos los interesados.

7.15.4. 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, esta labor debe ser coordinada por el oficial de Seguridad de la Información, la Dirección de Planeación con el apoyo de los dueños de procesos críticos y la Dirección de Tecnologías de la Información y las Comunicaciones.

7.15.5. 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.

7.15.6. Los procesos críticos deben soportarse en aplicaciones e infraestructura técnica robusta, software y hardware confiable y en instalaciones alternas o duplicadas.

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

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

7.15.9. Se debe identificar, acordar y documentar todas las responsabilidades y los procedimientos para la recuperación de los servicios informáticos.

7.15.10. Se debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados identificados como críticos y misionales dentro de la Entidad.

7.15.11. Se debe realizar los análisis de impacto a la operación y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia, con las consideraciones de Seguridad de la Información a que haya lugar.

7.16. REGISTRO Y AUDITORÍA

BORRADOR

Esta política de Registro y Auditoría define lo pertinente a las auditorías que se realizan a los procesos que incluyen activos del Sistema 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:

7.16.1. 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.
7.16.2. 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 Tecnología y que se conserva información documentada como evidencia de la implementación del programa de auditoria.
7.16.3. Como parte del programa de auditoria se deben incluir auditorias periódicas al Subsistema de Gestión de Seguridad de la Información.
7.16.4. 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.
7.16.5. Las auditorias se deben realizar acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
7.16.6. Se debe definir a qué es necesario hacer seguimiento y medición dentro del Subsistema de Gestión de Seguridad de la Información.
7.16.7. 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.
7.16.8. 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.
7.16.9. El almacenamiento de los registros de las auditorías internas realizadas al Sistema de Gestión de Seguridad de la Información se debe realizar de acuerdo a lo establecido en el procedimiento de Auditorías Internas.

7.17. 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:

7.17.1. En la Contraloría de Bogotá D.C., se aplicarán procedimientos y responsables de gestión que permita evaluar y decidir cuándo un evento de seguridad, corresponde a un

OBSOLETO

incidente de seguridad de la información, así como asegurar una atención que brinde respuesta rápida, eficaz y metódica a los incidentes detectados.

7.17.2. Todo evento de seguridad ocurrido en la Contraloría de Bogotá D.C., deberán ser comunicados mediante canales de gestión apropiados.

7.17.3. 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.

7.17.4. Se debe reportar al Oficial de Seguridad de la Información los incidentes de seguridad de la información, quien tendrá la responsabilidad de investigar y solucionar los incidentes de acuerdo con su criticidad, junto con la Dirección de Tecnologías de la Información y las Comunicaciones y el equipo de respuesta ante incidentes de seguridad de la información - CSIRT.

7.17.5. 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 al procedimiento “Gestión de Incidentes de Seguridad de la Información”.

7.17.6. 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”.

7.17.7. Se deben analizar los incidentes de seguridad para identificar cuáles serán escalados y proceder a realizar el contacto con las autoridades, cuando se estime necesario.

7.17.8. Todo aquel 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 al procedimiento de Gestión de Incidentes de Seguridad de la Información.

7.17.9. 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 establecerá un procedimiento para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.

7.18. 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 empleados 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:

7.18.1. 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.

OBSOLETO

7.18.2. 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.

7.18.3. A partir de los resultados de pruebas de ingeniería social y/o de análisis de riesgo se deberán 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.

7.18.4. Se debe definir un mecanismo de inducción en Seguridad de la Información para todos los funcionarios que sean destinados a recibir un nuevo cargo, bien sea por nombramiento, traslado o por disposiciones internas.

7.18.5. Se debe definir y desarrollar un programa de capacitación y sensibilización de tal forma que de manera periódica se refuercen los conceptos y amenazas de seguridad para que los funcionarios cuenten con información actualizada y sepan cómo actuar ante incidentes y como reportarlos.

7.18.6. La Contraloría de Bogotá D.C., deberá incluir dentro del Plan Institucional de Capacitación – PIC, los programas de capacitación y sensibilización en seguridad de la información.

7.18.7. La asistencia a las sesiones de capacitación y sensibilización en seguridad de la información son de carácter obligatorio.

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

7.18.9. Se debe evaluar a todos los funcionarios de manera periódica, los niveles de sensibilización en temas de seguridad de la información.

Las anteriores políticas se complementan con cada uno de los procedimientos, guías, manuales y demás documentación establecidos por la Contraloría de Bogotá D.C. para la gestión del Subsistema de Gestión de la Seguridad de la Información.

8. APROBACION Y ACTUALIZACIÓN

Las políticas de seguridad de la información, serán aprobadas en sesión del Comité SIGEL o quien haga sus veces y las actualizaciones a que haya lugar, serán aprobadas por la misma instancia y se realizaran cuando se requiera.

9. CONTROL DE CAMBIOS

Versión	R.R. No.	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

OBSOLETO

		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
3.0	R.R. No.038 24-sep-2019	

OBSOLETO