CONTRALORÍA
GENERAL DE SANTIAGO DE CALI

CONTRALORÍA GENERAL DE SANTIAGO DE CALI

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS

OFICINA DE INFORMÁTICA
GESTIÓN DOCUMENTAL

Santiago de Cali

2022

TABLA DE CONTENIDO

INTRODUCCIÓN

La Contraloría General de Santiago de Cali CGSC, consciente de que la información es el activo más valioso e indispensable para el ejercicio de sus funciones y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de servidores públicos, contratistas y grupos de interés, requiere implementar estrategias que definan los lineamientos y límites que deben cumplir los funcionarios, contratistas y terceros frente a la seguridad y privacidad de la información, independientemente del soporte, propendiendo con ello salvaguardar la integridad, la confidencialidad y la disponibilidad de ésta independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada,

La seguridad y privacidad de la información es una prioridad para la CGSC, teniendo presente que su vulneración puede llegar a tener impactos a nivel legal, de imagen, operacional, en el cumplimiento de la misión y los objetivos estratégicos de la Entidad, se establecen los principios orientadores de seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad y autenticidad, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, de tal manera que se garantice el derecho fundamental al acceso a la información.

Este documento describe las políticas y los lineamientos de seguridad y privacidad de la información definidas por la Contraloría General de Santiago de Cali.

Para la elaboración del mismo, se tomó como base normas aplicables, Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, el COMPES 3854 de 2016 que establece la política nacional de seguridad digital, Decreto 1499 de 2017 de la función pública, el cual modificó el Decreto 1083 de 2015 adopción del MIPG, Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

La Resolución No. 0100.24.03.18.009 del 30 de agosto de 2018 por medio de la cual adoptó el Modelo Integrado de Planeación y Gestión – MIPG, se reglamentaron las disposiciones relativas al sistema institucional de control interno y se creó el Comité Institucional de Coordinación de Control interno, Resolución No. 0100.24.03.19.006 del 28 de enero de 2019 “Por la cual se modifica la Resolución No. 0100.24.03.18.009 del 30 de agosto de 2018, a través de la cual se adopó el

Modelo Integrado de Planeación y Gestión – “MIPG”, se reglamentaron as disposiciones relativas al sistema institucional de control interno y se creo el Comité Institucional de Coordinación de Control Intrno de la Contraloria General de Santiago de Cali”

Las políticas incluídas en este documento se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la Contraloría General de Santiago de Cali y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos, las cuales deben estar alineadas e integradas con el Programa de Gestión documental y sus programa específicos.

1. OBJETIVO

Establecer la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios y definir los lineamientos con respecto al uso y manejo de la información de la CGSC, alineados con el Plan Institucional de Archivo y el Programa de Gestión Documental de la entidad, como plan de acción para afrontar riesgos de seguridad, que permita salvaguardar la integridad, autenticidad, la confidencialidad y la disponibilidad de la información.

2. ALCANCE

Las políticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios son aplicables a todos los niveles de la entidad, son de obligatorio cumplimiento por los funcionarios, contratistas, proveedores y terceros que presten sus servicios o tengan algún tipo de relación con la Contraloría General de Santiago de Cali, y que para el adecuado cumplimiento de sus funciones y las de la entidad: compartan, utilicen, recolecten, procesen, intercambien o consulten su información independientemente de su ubicación, medio o formato de presentación.

3. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos institucionales y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es un documento en los que los funcionarios, contratistas o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos: Es un “almacén” que nos permite guardar grandes

cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales, determinadas o determinables.

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de

las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que o estén sometidas a reservas.

Dato Sensible: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

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

Hoja de Control: Es un instrumento que debe usarse para todos los expedientes producidos por las dependencias de la entidad, en ejercicio de sus funciones misionales y administrativas.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la

organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Plan Institucional de Archivo: Instrumento Archivístico para la planeación de la función archivística, el cual se articula con los demás planes y proyectos estratégicos previstos por la entidad.

Programa de Gestión Documental: Instrumento Archivístico, en él se establecen las estrategias que permitan a corto mediano y largo plazo, la implementación y el mejoramiento de la prestación de servicios, desarrollo de los procedimientos, la implementación de programas específicos del proceso de gestión documental.

SGDEA: una aplicación para la gestión de documentos electrónicos. aunque también se puede utilizar para la gestión de documentos físicos, el cual debe garantizar su integridad. La gestión de documentos electrónicos es compleja y para poder ser implementada correctamente requiere un amplio campo de funcionalidades que cubran las actividades necesarias. Normalmente, un sistema que cumpla estos propósitos-un SGDEA requiere un software especializado, aunque cada vez más se incluyen funciones de gestión documental en los sistemas operativos y en otras aplicaciones.

Información clasificada y reservada: Es el inventario de la información pública generada, obtenida, adquirida o controlada por la entidad, que ha sido calificada como clasificada o reservada.

Documentos Vitales o Esenciales. Son todos aquellos que poseen un valor crítico para la entidad, los cuales son únicos e irremplazables y se requieren de

un cuidado especial a la hora de ser conservados y preservados, por lo anterior poseen un valor intrínseco legal, intelectual y económico.

Documentos Especiales: son aquellos que presentan un formato y soporte diferente a los documentos textuales en papel

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Intención y dirección general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias.

SGSI Sistema de Gestión de la Seguridad de la Información: La parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI Sistema de Gestión de la Seguridad de la Información: La parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Usuario: En este documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la Contraloría General de Santiago de Cali, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la entidad y a quienes se les otorga un nombre de usuario y una clave de acceso.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

Dispositivo móvil: Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria Son ejemplos de estos: celulares inteligentes, tabletas y portátiles.

Cifrado: Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos

Cifrar: Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) que transforma la información, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta.

Datos Personales: información que contiene elementos que al unirse pueden caracterizar a un individuo, por ejemplo, número de cedula, dirección, tipo de sangre, teléfono, etc.

Datos Sensibles: información catalogada como pública clasificada o pública reservada.

Información pública: Es toda información que la Superintendencia de Subsidio Familiar genere, obtenga, adquiera, o controle; corresponde a datos que son de acceso público y que por lo tanto no tienen requerimientos frente a la Confidencialidad. Está en esta clasificación la información denominada como “Pública” en la Ley 1712 de 2014 y como “dato público” en el decreto 1377 de 2013.

Información Pública de Uso Interno: Es toda información que no contiene datos sensibles, que puede encontrarse en proceso de construcción, y que no

requiere su divulgación a terceros, pero es necesaria para las actividades internas de la SSF.

Información pública clasificada: Es aquella información que estando en poder o custodia de la Superintendencia de Subsidio Familiar, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados. Esta corresponde a toda aquella información cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

- El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.
- El derecho de toda persona a la vida, la salud o la seguridad.
- Los secretos comerciales, industriales y profesionales.
- También corresponden a esta categoría los datos que son catalogados como “dato semiprivado o privado” de acuerdo al decreto 1377 de 2013.

Información pública reservada: Es aquella información que estando en poder o custodia de la Superintendencia de Subsidio Familiar es exceptuada de acceso a la ciudadanía por daño a intereses públicos. Esta corresponde a aquella información cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

- La defensa y seguridad nacional;
- La seguridad pública;
- Las relaciones internacionales;
- La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
- El debido proceso y la igualdad de las partes en los procesos judiciales;
- La administración efectiva de la justicia;
- Los derechos de la infancia y la adolescencia;
- La estabilidad macroeconómica y financiera del país;
- La salud pública.
- También corresponde a información de carácter reservado los datos catalogados como sensibles por el decreto 1377 de 2013

Llaves criptográficas: Son códigos (algoritmos) que se generan de forma automática y se guarda en un directorio especial durante la instalación. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

Personal: Es aquella persona que tiene una relación con la SSF, directa o a través de un tercero, bajo cualquier tipo de vinculación: planta, contratistas, proveedores, estudiantes en práctica, etc.

Texto plano: es un archivo informático que contiene únicamente texto formado solo por caracteres que son legibles por humanos, careciendo de cualquier tipo de formato tipográfico. También son llamados archivos de texto llano, simple o sin formato.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS

La Contraloría General de Santiago de Cali, mediante la adopción de la política de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios como parte del Modelo de seguridad y privacidad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad y autenticidad de la información de la Entidad, mediante la gestión integral de riesgos y la implementación de controles tanto físicos como digitales con el fin de dar cumplimiento a requisitos legales y prevenir la materialización de incidentes de seguridad.

La política general de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios tiene los siguientes objetivos:

- Dar cumplimiento a los requisitos normativos y legales con respecto a seguridad y privacidad de la información, seguridad digital y continuidad de los servicios.
- .Mitigar de manera efectiva, eficaz y eficiente, los incidentes de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios.
- Gestionar integralmente los riesgos de seguridad y privacidad de la información y seguridad digital.
- Definir los lineamientos para el manejo de la información tanto física como electrónica de acuerdo al sistema de gestión documental basado en la seguridad y privacidad de la información.
- Establecer mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad y confiabilidad de la información de la entidad.
- Generar conciencia para el cambio organizacional que se requiere para la apropiación de la seguridad y privacidad de información en la entidad.
- Minimizar el riesgo de los procesos misionales de la entidad.

- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y demás partes interesadas.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros y demás partes interesadas de la Contraloría General de Santiago de Cali

- Garantizar la continuidad de la entidad frente a incidentes.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La alta dirección aprobará esta política de seguridad de la información, seguridad digital y continuidad de los servicios como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad como parte fundamental del modelo de seguridad y privacidad de la información.

La alta dirección de la entidad demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios contenidos en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este documento a todos los funcionarios, contratistas, proveedores y demás partes interesadas de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las Políticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios
- La verificación del cumplimiento de las políticas aquí mencionadas.

6. SANCIONES PARA LAS VIOLACIONES DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS

Las Políticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios, pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, contratistas, personal externo y proveedores de la CGSC. Por tal razón, es necesario, que las violaciones a éstas sean clasificadas, con el objetivo de aplicar medidas correctivas conforme a los niveles definidos y mitigar posibles afectaciones contra la seguridad de la información.

El incumplimiento y desacato de las Políticas de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios, se aplicará lo establecido en los procedimientos destinados para tal fin, por los entes de control interno de la Entidad, enmarcados en Ley 1952 de 2019, de acuerdo con las circunstancias, si así lo ameritan.

7. POLITICA DE SEGURIDAD QUE DEBE APLICAR EN LOS RECURSOS HUMANOS

La Contraloría General de Santiago de Cali, debe desplegar esfuerzos para que los servidores públicos y contratistas de la entidad entiendan las responsabilidades frente a la seguridad de la información, con el fin de reducir el riesgo de hurto, fraudes, mal uso de las instalaciones y recursos tecnológicos, y de asegurar la confidencialidad, disponibilidad e integridad de la información.

La Dirección Administrativa y Financiera incluirá en las minutas de los contratos, cláusulas de confidencialidad y obligaciones tendientes a la seguridad de la información y serán divulgadas a los contratistas a través de los supervisores.

La Oficina Asesora Jurídica elaborará un acuerdo de confidencialidad y no divulgación de información, según el tipo de vinculación, que deberá ser firmado por todos los servidores públicos o contratistas, sin importar el nivel jerárquico, en lo que respecta al tratamiento de la información de la Entidad y la autorización de tratamiento de datos personales. Los originales de estos documentos deben ser archivados en la historia laboral de los servidores públicos y en la carpeta del proceso contractual para el caso de los contratistas y proveedores. Para los proveedores de servicios de la Entidad que tienen persona jurídica, estos documentos deben ser firmados por el representante legal.

7.1 Lineamientos antes de asumir el empleo para asegurar que el personal a contratar cumpla con las políticas de seguridad y privacidad de la Información de la Entidad

- La Dirección Administrativa y Financiera, debe definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación de la Entidad y los que dicte la Función Pública.
- La Dirección Administrativa y Financiera, debe definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo a lo que dicta la Ley y la reglamentación vigente.
- Los procesos de selección de personal de servidores públicos y contratistas de prestación de servicios deben contener la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales la Entidad y de acuerdo a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- La Dirección Administrativa y Financiera, debe establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva

de la información contenida en las historias laborales y expedientes contractuales.

- Todo servidor público o contratista debe firmar un documento de acuerdo de confidencialidad y no divulgación de la información con la Entidad, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.
- La Dirección Administrativa y Financiera, debe incluir dentro del manual de funciones las responsabilidades con respecto al cumplimiento de las políticas de seguridad y privacidad de la información, así como todos los lineamientos en el marco del Sistema de Gestión de Seguridad de la Información.
- La Dirección Administrativa y Financiera, debe incluir en el pliego de condiciones y estudios previos para la contratación, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte la Entidad.
- La Dirección Administrativa y Financiera, debe dar a conocer durante la inducción las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites la Entidad y del horario normal de trabajo o de ejecución del objeto contractual.

7.2 Lineamientos durante la ejecución del empleo

- La Dirección Administrativa y Financiera, o el supervisor del contrato deben propender que los colaboradores de la Entidad y usuarios de terceras partes que desempeñen funciones en el mismo, reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.
- La Dirección Administrativa y Financiera, en conjunto con la oficina de informática, deben establecer un curso en cualquier modalidad relacionado con la seguridad y privacidad de la información, teniendo en cuenta oferta académica.
- En lo pertinente al incumplimiento y desacato de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, por los entes de control interno de la Entidad, enmarcados en Ley 1952 de 2019, sus decretos reglamentarios o cualquiera que la modifique, adicione, derogue o subrogue.

7.3 Lineamientos en la Terminación y cambio de empleo

- El jefe inmediato o a quien este delegue debe recoger y custodiar la información propia de la Entidad, que se encuentra en gestión del servidor público, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
- El supervisor del contrato o a quien este delegue deben recoger y custodiar la información de la Entidad bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.

- La Oficina de informática debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
- La Dirección Administrativa y Financiera, o a quienes se deleguen deberán informar a la Oficina de informática, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador; una vez notificada la novedad la Oficina de informática deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los siguientes parámetros:
- Si el buzón pertenece a una cuenta de correo genérica (ejemplo: info@contraloriacali.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados.
- En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes se les entregará en cadena de custodia una copia del buzón garantizando su integridad.
- Se deben inactivar los accesos de tarjetas de proximidad de los sistemas de control de acceso.
- Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con la Entidad.
- Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones.
- Se deben inactivar todos los accesos a los sistemas de información.
- Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir (Chaleco), que lo acredita como colaborador de la entidad.

8. POLÍTICA DE GESTIÓN DE ACTIVOS

El objetivo de esta política es establecer la forma en que se logra y mantiene la protección adecuada de los activos de información, aplica a la alta dirección, funcionarios, contratistas, proveedores y en general a todos los usuarios de la información que cumplan con los propósitos generales de la Contraloría General de Santiago de Cali.

8.1 Lineamientos para la gestión de activos

8.1.1 Identificación de Activos: La Contraloría General de Santiago de Cali dando cumplimiento a la Ley 1712 de 2015 y su Decreto reglamentario 103 de 2015, realizó el proceso de identificación de activos de información la cual se encuentra publicada en la sección de Transparencia y Acceso a la información

pública de la página web. La actualización del inventario de Activos de Información debe hacerse bajo la responsabilidad de cada propietario de información cuando se presenten cambios en la información o en la estructura.

8.1.2 Clasificación de activos: De acuerdo con la normatividad legal vigente, la entidad ha clasificado la información como pública, clasificada y reservada, la cual se encuentra publicada en la sección de Transparencia y Acceso a la información pública de la página web. El dueño o propietario de la información, será el responsable de definir la categoría en la que cada activo de información se encuentra, así como determinar si es necesario un proceso de reclasificación y los controles requeridos para su protección.

8.1.3 Etiquetado de la Información*:* El dueño o propietario de la información, deberá etiquetarla o rotularla, de acuerdo con la clasificación que se le haya dado.

Los documentos con información del tipo "Reservada" deberán ser controlados por medio de copias individuales perfectamente numeradas y registro de las personas que han tenido acceso.

La copia o transferencia de información "Reservada" por cualquier medio (electrónico, magnético, en papel) deberá estar autorizada y controlada.

Todos los documentos del tipo "Reservada" se deberán conservar bajo llave y en lugares seguros.

El envío de documentos con clasificación Reservada, se deberá hacer por medio de canales seguros (correo certificado). En caso de hacerse por medio de forma física, los paquetes deberán estar debidamente cerrados y que sea imposible observar su contenido.

Toda recepción de información Reservada deberá solicitar acuse de recibo.

En caso de ser necesario, se considerará un procedimiento o centro de destrucción de documentos y activos de información que garantice la no reutilización de la información. La destrucción de registros e información de la Contraloría General de Santiago de Cali debe ser formalmente autorizada por el responsable.

La información clasificada o reservada deberá reflejar por medio de una leyenda, la clasificación a la que pertenece, sin importar la forma o medio en la que se encuentre.

Por ningún motivo o circunstancia los documentos impresos de nivel de reserva deben ser reutilizados para impresión, escritura a mano o cualquier otro propósito.

En cada una de las dependencias deben dar tratamiento especial a los documentos marcados con reserva documental por el nivel de confidencial que se le ha conferido.

Los documentos marcados como de reserva documental, que por cualquier circunstancia fueron impresos como copias del sistema de Información Documental y que su uso haya terminado, deberán ser destruidos.

Los documentos desde borradores deben ser tratados con el mismo grado de confidencialidad que los documentos en versión final y deben ser protegidos con controles de Seguridad similares.

La Contraloría General de Santiago de Cali, a través de sus instancias correspondientes, se reserva el derecho de iniciar denuncias, y procesos disciplinarios para sancionar a los funcionarios que divulguen o destruyan ilícitamente la información de la entidad.

8.1.4 Devolución de los Activos de información: De acuerdo con la normatividad legal vigente y atendiendo las directrices del Archivo General de la Nación y teniendo en cuenta que los archivos y documentos son indispensables para garantizar la gestión fiscal, la entidad establece las responsabilidades de los servidores públicos, contratistas o proveedores frente a los documentos y archivos.

El servidor público, contratista o proveedor, será responsable de la adecuada conservación, organización, uso y manejo de los documentos y archivos producto del ejercicio de sus funciones.

Para garantizar la continuidad de la gestión fiscal, todo servidor público o contratista vinculado, trasladado o desvinculado de su cargo, recibirá o entregará según sea el caso, los documentos debidamente inventariados.

La Entidad a través de la Dirección Administrativa y Financiera, implementará la metodología y el formato único de inventario documental de que trata el acuerdo 038 de 2002, para la entrega y recibo de los documentos y archivos.

8.1.5 Gestión de medios removibles*:* El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares) sobre la infraestructura para el procesamiento de la información de la Contraloría General de Santiago de Cali, estará autorizado por el jefe inmediato para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

La Oficina de Informática es responsable de implementar los controles necesarios para asegurar que solo en los equipos de cómputo autorizados de la Contraloría General de Santiago de Cali pueden hacer uso de los medios de almacenamiento removibles.

Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la Contraloría General de Santiago de Cali que éste contiene.

9. POLÍTICA DE RETENCIÓN Y ARCHIVO DE DATOS

El objetivo de esta política es mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información. La entidad propenderá por el uso de tecnologías informáticas y de telecomunicaciones para administración y conservación de archivos.

9.1 Lineamientos de retención y archivo de datos

- Mantener almacenados los archivos en la Contraloría General de Santiago de Cali, de acuerdo al tiempo establecido en las tablas de retención documental.
- Atender las reglas y los principios generales que regulan la función archivística del Estado, que se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
- Utilizar las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos de acuerdo a lo previsto en la Ley y en el Plan Institucional de Archivo ” PINAR y en Programa de Gestión Documental “PGD”.
- Utilizar la herramienta Docunet para la aplicación del “Sistema de Gestión de Documento Electrónico de Archivo”, como sistema de información para la conservación y preservación de los documentos electrónicos de Archivo.

9.2 Nombrado de directorios y archivos o documentos electrónicos

- La longitud máxima del nombre de los archivos incluída la ruta es de 256 caracteres, las carpetas, subcarpetas o documentos deben ser mínimo 4 y máximo 30 caracteres, si el nombre de los archivos es muy extenso y sobrepasa esta longitud, afecta los procesos de búsqueda, backup, copia, migración, restauración, transferencia o compatibilidad entre sistemas de archivos.
- Solo podrán incluir en una carpeta un número máximo de 4 niveles de subcarpetas, si el nivel de subcarpetas supera el máximo de niveles puede afectar los procesos de búsqueda, backup, copia, migración, restauración, transferencia o compatibilidad entre sistemas de archivos.
- No se debe incluir ningún tipo de punto, guion o espacio (.-).

- El nombre del archivo o documento en primer lugar debe identificar el resultado del proceso del cual es producto, debe ser único, preciso, especifico, fácil de recordar, de tal manera que se pueda buscar y ubicar en el menor tiempo por medio de un sistema.

- Usar mayúsculas en la primera letra del nombre del archivo o documento, si el nombre del archivo o documento es compuesto, usar la letra mayúscula en la primera letra de la palabra inicial y en el Inicio de cada palabra compuesta.
- No utilizar caracteres especiales como /%$&*#.\:<>?'" o tildes.
- El archivo o documento debe contener la extensión que identifica el formato o programa donde se generó, seguido de un punto.
- Es recomendable evitar archivos de gran tamaño porque se dificulta su manipulación.
- Relación con Documentación Física, dado el caso que los archivos o documentos electrónicos se encuentren relacionados con documentación física se sugiere nombrar carpetas en los entornos electrónicos y en papel con el mismo título.
- Si el nombre del archivo contiene fecha, esta deberá seguir los lineamientos de la norma ISO 8601 AAAA-MM-DD, AAAA corresponde a los cuatro dígitos del año, MM dos dígitos del número del mes y DD corresponde al día, si el número del mes y el día son de solo un digito, se antecederá el número 0.

10. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La Contraloría General de Santiago de Cali, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán acuerdos de confidencialidad y/o el mismo con las terceras partes con quienes se realice dicho intercambio.

La entidad propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

10.1 *Lineamientos de intercambio de información*

- La Dirección Administrativa y Financiera, en acompañamiento con la Oficina Jurídica, debe definir los modelos de Acuerdos de Confidencialidad y/o de

Intercambio de Información entre la entidad y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar teniendo en cuenta el índice de información clasificada y reservada se debe incluir la prohibición de divulgar la información entregada por la Contraloría General de Santiago de Cali a los terceros con quienes se establecen estos acuerdos, y la destrucción de dicha información una vez cumpla su cometido.

- La Dirección Administrativa y Financiera, debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la entidad.
- Los responsables de los activos de información deben velar porque la información de la Contraloría General de Santiago de Cali sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información teniendo en cuenta el índice de información clasificada y reservada, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.
- Los responsables de los activos de información deben asegurar que los datos requeridos de los funcionarios o contratistas sólo pueda ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los responsables de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Los responsables de los activos de información deben autorizar los requerimientos de solicitud/envío de información de la Contraloría General de Santiago de Cali por /a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Los responsables de los activos de información deben asegurarse que el Intercambio de información (electrónica) solamente se realice si se encuentra autorizada y dando cumplimiento a las políticas de administración de redes, de acceso lógico y de protección de datos personales de la Contraloría General de Santiago de Cali.
- La Oficina de Informática debe velar porque las herramientas de intercambio de información sean seguras, con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

11. POLÍTICA DE USO DE LOS EQUIPOS DE CÓMPUTO

La Contraloría General de Santiago de Cali, establece los siguientes lineamientos para prevenir perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la entidad.

11.1 *Lineamientos para el uso de los equipos de cómputo*

- La instalación de software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la Contraloría General de Santiago de Cali, es una actividad exclusiva de los funcionarios y contratistas designados por la Oficina de Informática.
- No está permitido realizar instalaciones de software en los equipos de la Contraloría General de Santiago de Cali, que viole la leyes de propiedad intelectual, derechos de autor en especial la ley 23 de 1982 y toda la normatividad vigente, la Oficina de Informática desinstalará cualquier software ilegal y registrará este hecho como un incidente de seguridad.

- La Oficina de Informática definirá los perfiles de acceso.

  - ✓ Administradores
  - ✓ Usuarios Generales
  - ✓ Invitados

- No está permitida por parte del usuario, ninguna modificación de los archivos (sistema operativo, aplicaciones y perfil de usuario) que se encuentran en la unidad C:\ del disco duro de los equipos de cómputo.
- La oficina de informática y la Dirección Administrativa y Financiera son las únicas áreas autorizadas para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la entidad.
- Cuando se presente una falla o problema de hardware o software en un equipo de cómputo u otro recurso tecnológico propiedad de la Contraloría General de Santiago de Cali, el usuario responsable debe informar a la Oficina de Informática, con el fin de realizar una asistencia adecuada.
- La instalación, reparación o retiro de cualquier componente de hardware o software de los equipos de cómputo y demás recursos tecnológicos de la entidad, solo puede ser realizado por los funcionarios o contratistas de la Oficina de Informática, o personal de terceras partes autorizados por dicha Oficina.
- Los funcionarios o contratistas de la entidad y el personal provisto por terceras partes deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso a la información de personas no autorizadas.

- Los funcionarios o contratistas de la Contraloría General de Santiago de Cali y el personal provisto por terceras partes no deben dejar encendidas los equipos de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida, daño o robo de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informado de inmediato, a la Dirección Administrativa y Financiera para que esta de inicio a los trámites pertinentes, de acuerdo al procedimiento.
- La dirección administrativa y financiera debe propender porque los equipos de cómputo e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- Se prohíbe expresamente la conexión de aparatos eléctricos diferentes a computadores de escritorio, portátiles o pantallas en los tomas de energía regulada (tomas Naranja) en los puestos de trabajo.
- Se prohíbe el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, de documentos, archivos de video, música, fotos o cualquier otro tipo de archivos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- 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 consiguiente, la perdida de integridad de esta.
- Es los equipos de escritorio o portátiles de la entidad, solo está permitido el uso de software licencia y aquel que sin requerir licencia, sea autorizado por la oficina de informática.

12. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

La Contraloría General de Santiago de Cali, entendiendo la importancia del correo electrónico como herramienta para facilitar la ejecución de funciones y obligaciones de los servidores públicos y contratistas, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

***12.1** Lineamientos para el uso del correo electrónico*

- La Oficina de Informática desactivará las cuentas de correo institucional de funcionarios o contratistas retirados de la entidad, previo reporte de la Dirección Administrativa y Financiera.
- La cuenta de correo electrónico asignada a cada usuario es de carácter individual; por consiguiente, ningún funcionario o contratista de la entidad, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional; por lo cual, no puede ser utilizado para fines personales, económicos, comerciales o de cualquier otro fin ajenos a los propositos de la entidad.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Contraloría General de Santiago de Cali y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido el envío de mensajes o cadenas de mensajes de contenidos ya sea comercial, político, religioso, material audiovisual, discriminatorio, ofensivo, injurioso, obscenos, violatorios de los derechos de autor, pornografía y demás condiciones que degraden la condición humana, o que atenten contra la integridad moral de las personas o instituciones.

- No es permitido el envío de archivos adjuntos que contengan extensiones .exe, .bat, .prg, .bak, .pif, bajo ninguna circunstancia.

- Todo mensaje spam, cadena, que provenga de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Oficina de Informática como incidente de seguridad y deberá acatar las indicaciones que se le den para su tratamiento; lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, ,bat, .prg, .bat, .pif o explicitas referencias no relacionadas con la misión de la Entidad.

- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la Entidad.

- El único servicio de correo electrónico autorizado para el manejo o transmisión de información de la entidad es el asignado por la Oficina de Informática, el cual cuenta con el dominio @contraloriacali.gov.co.

- Se debe preferir el uso del correo electrónico al envió de documentos físicos, siempre que la Ley lo permita, para dar cumplimiento de la iniciativa del uso racional del papel y la eficiencia administrativa.

- Los mensajes de correo electrónico están respaldados por la Ley 527 de 1999 (Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.

- Los mensajes del correo electrónico institucional deben contener una sentencia de confidencialidad, que será diseñada por la Oficina de Informática con el apoyo de la oficina de comunicaciones y debe reflejarse en todos los buzones de correo con dominio @contraloriacali.gov.co.

- Se prohíbe el envío, copia o distribución de información de la entidad a través de correo personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.

- Esta expresamente prohibido distribuir información de la entidad a otras entidades o ciudadanos sin la debida autorización.

- La entidad se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional, de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento, sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información, previa solicitud del nominador del gasto, la dirección administrativa y financiera o el jefe inmediato, a la Oficina de informática.

13. POLÍTICA DE USO ADECUADO DE INTERNET

La Contraloría General de Santiago de Cali, consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar la disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

La Oficina de informática establecerá políticas de navegación, basadas en niveles de usuario por jerarquía, funciones y necesidades del servicio laboral.

13.1Lineamientos para el uso adecuado de internet

Los servidores públicos y contratistas tendrán las siguientes responsabilidades:

- 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 e instituciones.
- El servicio de internet deberá ser usado solo para fines laborales.
- Abstenerse de propagar intencionalmente virus o cualquier tipo de código Malicioso.
- Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
- Abstenerse de descargar software desde internet, así como su instalación en los equipos asignados para el desempeño de sus labores.
- Abstenerse de acceder a páginas relacionadas con pornografía, drogas, alcohol, darkweb, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Skype, Whatsapp, y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la entidad.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La entidad se reserva el derecho de monitorear los accesos y el uso del servicio de internet, además de limitar el acceso a determinadas páginas del mismo, 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.

14. POLÍTICA DE SEGURIDAD EN LAS OPERACIONES

La Oficina de Informática de la Entidad será la encargada de la administración y operación de los recursos informáticos que soportan la operación. De igual manera, velara por la eficiencia en los controles asociados a los recursos informáticos para la protección de la confidencialidad, integridad y disponibilidad de la información y para que los cambios que se realicen sobre los recursos informáticos y sistemas de información en ambientes de pruebas y producción sean controlados y debidamente autorizados. Implementara mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI en la entidad.

14.1 Lineamientos para Respaldo de la información

- La Oficina de informática, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- Los administradores de los servidores, sistemas de información y bases de datos, definirán la frecuencia de los respaldos y el administrador del sistema de respaldo es el responsable de verificar que se efectúen las copias de seguridad según las frecuencias definidas (diarias, semanales y mensuales).
- La información institucional se mantendrá disponible a todas las personas o usuarios autorizados para ello en el momento que la necesiten.
- Los niveles de protección establecidos para la seguridad de la información deben ser mantenidos en todo momento.
- Es responsabilidad de los funcionarios o contratistas de la entidad, identificar la información que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación en la red corporativa, en los lugares o unidades de disco de red lógicas establecidos por la Oficina de Informática.
- Los documentos electrónicos de archivo deberán ser almacenados en formato PDF/A.
- Los expedientes en cualquier soporte deben contener la hoja de control.
- La Oficina de informática debe velar por que se disponga de herramientas tecnológicas para gestionar la información digital de la entidad, la cual debe ser guardada en la red corporativa y asegurar que estas dispongan de copias de respaldo.
- La Oficina de informática debe definir la custodia y almacenamiento de las copias de respaldo.
- La Oficina de informática debe generar mecanismos que mantengan la integridad y confidencialidad de las copias de respaldo.
- Los Funcionarios o contratistas deben utilizar las herramientas tecnológicas dispuesta por la Oficina de informática para gestionar la información de la Entidad.
- Los Funcionarios o contratistas son responsables de la información que resida en el equipo asignado y serán los encargados de mantener copias de respaldo de sus archivos, la Oficina de informática solo se hace responsable de mantener las copias de seguridad de la información que se guarde en la red corporativa.

14.2 Lineamientos para Protección contra códigos maliciosos

- La Oficina de Informática debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.
- La Oficina de Informática realizara campañas de concientización de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.

- La Oficina de Informática debe propender por mantener actualizada la base de datos, base de firmas y parches correspondientes del software antivirus y debe asegurar que esta herramienta no pueda ser deshabilitada de los equipos de la Entidad.
- La Oficina de Informática debe dictar los lineamientos para la instalación del software antivirus con el fin de brindar protección contra códigos maliciosos en todos los recursos informáticos de la Entidad.
- La Oficina de Informática debe aplicar las actualizaciones y parches de seguridad de los sistemas operativos de los equipos y servidores de la Entidad para protegerlos contra códigos maliciosos.
- Todo mensaje sospechoso de procedencia desconocida debe ser inmediatamente reportado a la Oficina de Informática a través de los medios establecidos, tomando las medidas de control necesarias.

14.3 Lineamientos para Control de software operacional.

- La Oficina de Informática debe controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios de la Entidad.
- La Oficina de Informática debe conservar las versiones anteriores del software de aplicación propio de la entidad como medida de contingencia.
- La Oficina de Informática debe usar controles para proteger todo el software implementado y la documentación del sistema.

15. POLÍTICA DE CONTROL DE ACCESO

Con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física por parte de personal no autorizado, y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de la Entidad, los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deben establecer medidas de control de acceso, en aplicaciones, servicios y en general cualquier activo de información de la Entidad.

15.1 Lineamientos de Gestión de Acceso de Usuarios

Todos los recursos de información de la entidad tienen asignados privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario o contratista requiera para el desarrollo de sus funciones, definidos y aprobados por los propietarios de la información y administrados por la Oficina de Informática.

- La Oficina de Informática debe definir un procedimiento para el registro y la cancelación de usuarios en la Entidad, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.
- La Oficina de Informática debe definir un estándar para la identificación de usuarios, teniendo en cuenta los siguientes parámetros:
  Usar la primera letra del primer nombre más el apellido, en caso de homónimos se utiliza, la primera letra del primer nombre más la primera letra del segundo nombre más el apellido, de persistir la situación, se deberá utilizar la primera letra del primer nombre más el apellido, seguido de la primera letra del segundo apellido; si todas las opciones anteriores se encuentra en uso, se utilizará la primera letra del primer nombre más la primera letra del segundo nombre más el primer apellido más la primera letra del segundo apellido.
- El nombre para mostrar debe ser los nombres y apellidos completos. El usuario de correo electrónico, docunet, intranet y mecicalidad debe ser igual al usuario de red, es decir debe existir interoperabilidad entre las diferentes apliciones y el directorio activo (DA).

- Todo funcionario o contratista que requiera tener acceso a los sistemas de información de la Contraloría General de Santiago de Cali, debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la Oficina de Informática. El funcionario o contratista debe ser responsable por el buen uso de las credenciales de acceso asignadas.

- La Contraloría General de Santiago de Cali, proporcionará a los funcionarios y contratistas (personas naturales) los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, Tablet, enrutadores, agendas electrónicas, celulares inteligentes, Access point, que no sean autorizados por la Oficina de Informática.

- La Oficina de Informática, suministrará a los funcionarios y contratistas los usuarios y las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

- La Oficina de Informática, solo deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red, sistema operativo y sistemas de información únicamente a aquellos funcionarios y contratista que cumplan dichas funciones, deben ser cuentas únicas asociadas al usuario de dominio del colaborador; en caso de requerirse usuarios de acceso genérico, éstos deben ser entregados al colaborador de manera

formal por parte del jefe inmediato o supervisor del contrato; en caso de cambiar el titular de la cuenta genérica las credenciales de acceso deben ser modificadas me manera inmediata.

- La Oficina de Informática deberá restringir las conexiones remotas para la administración de la plataforma tecnológica; únicamente deberá permitir el acceso a los funcionarios y contratistas autorizados por la misma.
- La Oficina de Informática debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware y las bases de datos.
- La Oficina de Informática debe mantener un software de gestión de las cuentas actualizado que administren todos los recursos tecnológicos.
- La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.

- Todo trabajo que utilice los servidores de la Contraloría General de Santiago de Cali, con información de la entidad, sus funcionarios o contratistas, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación de la Oficina de Informática.

- Cualquier actividad de adición de un punto de red en el cableado estructurado debe ser acompañado y certificado por funcionarios de la oficina de informática de la contraloría general de Santiago de Cali.

- El acceso al centro de cómputo está controlado mediante chapa de seguridad y restringido sólo a personal autorizado.
- La conexión remota a la red de área local de la entidad, debe ser hecha a través de una conexión VPN segura suministrada por la oficina de informática la cual debe ser aprobada, registrada y auditada.

15.2 *Lineamientos sobre Responsabilidades de los usuarios*

Controlar el acceso a la información para lo cual se debe concientizar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la entidad.
- El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato o supervisor del contrato.
- Cerrar las sesiones activas al finalizar, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

- Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.
- La clave de acceso será desbloqueada sólo luego de la solicitud formal por parte del responsable de la cuenta.

Las claves o contraseñas deben:

- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni el nombre del usuario ni posibles combinaciones, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos o cónyuges, placas de automóvil, números de teléfono, entre otros.
- Tener mínimo ocho caracteres alfanuméricos.
- Cambiarse obligatoriamente cuando lo establezca la oficina de informática. Cada vez que se cambien éstas deben ser distintas por lo menos de las últimas dos anteriores. Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos, combinar mayúsculas con minúsculas, intercalar símbolos como "#", "$", "&" o "%" entre los caracteres de la contraseña. (Pas$w0rd).
- No ser reveladas a ninguna persona, incluyendo al personal de la oficina de informática.
- No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.
- Debe no ser visible en la pantalla, al momento de ser ingresada.
- No se deben almacenar las contraseñas en los navegadores de Internet.

15.3 Lineamientos para Control de Acceso a Sistemas y Aplicaciones.

Para prevenir el acceso no autorizado a sistemas y aplicaciones y servicios de la Entidad, se deben tener en cuenta estos lineamientos:

- La Oficina de Informática debe establecer controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.

- Las sesiones inactivas deben cerrarse después de un período de inactividad definido de10 minutos y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.
- La Oficina de Informática debe establecer controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo programas utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos sin ser debidamente autorizados.
- La Oficina de Informática debe generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información autorizados.
- La Oficina de Informática debe retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información y bloquear su conexión a través de los servicios perimetrales e internos de seguridad informática.
- El acceso al código fuente del programa es limitado, solamente los ingenieros desarrolladores y de soporte autorizados de la Oficina de Informática.

16. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

La Contraloría General de Santiago de Cali, debe adoptar las medidas necesarias para la protección que aseguren el perímetro de sus instalaciones en todas sus sedes, para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, asi como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones). Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

: Establecer lineamientos para prevenir el acceso físico no autorizado, el daño e interferencia de la información e instalaciones de procesamiento de información de la Entidad

16.1 Lineamientos para áreas seguras

Para prevenir el acceso físico no autorizado, el daño e interferencia de la información e instalaciones de procesamiento de información de la Entidad, se establecen los siguientes lineamientos:

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considerarán áreas de acceso restringido.
- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Oficina de Informática; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha oficina durante su visita al centro de cómputo o los centros de cableado.
- La Oficina de Informática debe registrar el ingreso de los visitantes al centro de cómputo o a los centros de cableado que están bajo su custodia, en el formato de control de acceso.
- La Oficina de Informática debe inactivar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- La Dirección Administrativa y Financiera debe garantizar las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la infraestructura tecnológica ubicados en el centro de cómputo y centros de cableado; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas, así como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, entre otros. Estos sistemas se deben monitorear de manera permanente.
- La Oficina de Informática debe velar porque los recursos de la infraestructura tecnológica de la Contraloría General de Santiago de Cali ubicados en el centro de cómputo se encuentren protegidos contra fallas o interrupciones eléctricas.
- La Oficina de Informática debe verificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La Oficina de Informática debe propender por que las labores de mantenimiento de la infraestructura tecnológica, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
- El Subcontralor, Directores Técnicos, Director Operativo, Director Administrativo y Jefes de Oficina que tengan bajo su responsabilidad áreas restringidas deben velar por la efectividad de los controles de acceso físico.
- El Subcontralor, Directores Técnicos, Director Operativo, Director Administrativo y Jefes de Oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

- El Subcontralor, Directores Técnicos, Director Operativo, Director Administrativo y Jefes de Oficina deben velar porque las contraseñas de cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la Entidad.
- La Dirección Administrativa y Financiera debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Contraloría General de Santiago de Cali.
- La Dirección Administrativa y Financiera debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la Entidad.
- La Dirección Administrativa y Financiera debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la Contraloría General de Santiago de Cali.
- La Dirección Administrativa y Financiera debe proveer los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- Los funcionarios deben portar el carné de identificación en un lugar visible mientras se encuentren en las instalaciones de la entidad; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la Dirección Administrativa y Financiera a la mayor brevedad posible.
- Aquellos funcionarios, contratistas o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los funcionarios o contratistas de la Contraloría General de Santiago de Cali y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.
- Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
- Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.
- El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. que ingresen los colaboradores o visitantes.
- El personal de vigilancia debe registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo cómputo (pc o portátil, mouse, teclado, cargador, etc.), servidores, equipos activos de red o cualquier equipo electrónico diferentes a smartphone; en caso de que estos equipos sean propiedad de la Entidad deberán contar con autorización expresa de la Dirección Administrativa y financiera de acuerdo a los procedimientos establecidos para tal fin.

- La Oficina de Informática es responsable de mantener organizado e identificado el cableado en los racks de los centros cableado y centro de datos.
- La Oficina de Informática y la Dirección Administrativa y Financiera, deben mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos y centros de cableado de la Entidad.

- Dirección Administrativa y financiera debe establecer mecanismos de seguridad para el ingreso a las áreas de procesamiento de pagos y debe ser monitoreado mediante circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros, en ningún caso deberá grabarse o monitorear directamente la pantalla o el teclado de los equipos financieros.

- Se prohíbe el consumo de alimentos y bebidas en las áreas seguras de la Entidad.

17. POLÍTICA DE PRIVACIDAD Y CONFIDENCIALIDAD

La Contraloría General de Santiago de Cali ejerce control fiscal de la Administración Central, sus entidades descentralizadas y a los particulares que administren o manejen fondos o bienes del Municipio de Santiago de Cali, procediendo a fijar la política de tratamiento de datos personales que reposan en sus bases de datos y/o archivos, recopilados en el ámbito de su competencia en relación con la vigilancia de los sujetos y puntos de control, los Servidores Públicos vinculados a la entidad, los contratistas y la ciudadanía en general.

Esta política establece los fundamentos para la gestión en la protección de la confidencialidad, privacidad y la intimidad de la información personal que la Entidad ha incorporado en sus bases de datos, permitiendo a los titulares de la misma, conocerla, actualizarla y solicitar su rectificación.

Los lineamientos de esta política se encuentran de manera clara y detallada en la Política de Tratamiento de Datos Personales de la Entidad.

18. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La Contraloría General de Santiago Cali, promoverá entre los funcionarios y contratistas el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La alta dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

18.1 *Lineamientos para el reporte y tratamiento de incidentes de seguridad*

- Los propietarios de los activos de información deben informar a la Oficina de Informática, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
- La Oficina de Informática deben definir un procedimiento para la gestión de incidentes de seguridad de la información.
- La Oficina de Informática debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a la alta dirección aquellos en los que se considere pertinente.
- La Oficina de Informática y la Secretaría General, deben crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
- La alta dirección debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- Es responsabilidad de los funcionarios o contratistas de la Contraloría General de Santiago de Cali y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos a la mayor brevedad posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios o contratistas deben notificarlo a la oficina de informática para que se registre y se le dé el trámite necesario.
- La Oficina de Informática debe definir los canales para que los colaboradores de la Entidad puedan reportar los incidentes de Seguridad de la Información.

19. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

La Contraloría General de Santiago de Cali, proporcionará los recursos suficientes para dar respuesta efectiva a funcionarios, contratistas y procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación acorde con el plan de contingencias al cual estará integrado el Programa de Documentos Vitales o esenciales.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud 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.

La Contraloría General de Santiago de Cali mantendrá canales de comunicación adecuados hacia los funcionarios, contratistas, proveedores y demás partes interesadas.

17.1 *Lineamientos de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información*

- El Comité de gestión y desempeño reconocerá las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- El Comité de gestión y desempeño, liderará los temas relacionados con la continuidad de la entidad y la recuperación ante desastres
- El Comité de gestión y desempeño realizará los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- El Comité de gestión y desempeño, validará que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- El Comité de gestión y desempeño, asegurará la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad del negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
- La Oficina de informática, elaborará 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.
- La Oficina de informática, participará activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité de gestión y desempeño.
- El Subcontralor, Directores Técnicos, Director Operativo, Director Administrativo y Jefes de Oficina identificarán y generarán al interior de sus áreas, la documentación de los procedimientos de continuidad que podrían

ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos serán probados para certificar su efectividad, alineados al programa de documentos vitales esenciales y a la administración del riesgo de la entidad.

20. POLÍTICA DE REDUNDANCIA

La Contraloría General de Santiago de Cali, propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la entidad.

20.1 *Lineamientos para redundancia*

- La Oficina de informática debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la entidad y la plataforma tecnológica que los apoya.
- La Oficina de informática debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Contraloría General de Santiago de Cali.
- La Oficina de informática, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la entidad.

21. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La Contraloría General de Santiago de Cali, velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, razón por la cual propenderá porque el software instalado en los recursos de la infraestructura tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

21.1 Lineamientos de cumplimiento con requisitos legales y contractuales

- La Oficina Asesora Jurídica debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la entidad y relacionados con la seguridad y privacidad de la información.

- La Oficina de Informática velara que el software que se ejecuta en la entidad esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- La Oficina de Informática debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en los equipos de cómputo o computadores portátiles de la entidad para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichos equipos corresponda únicamente al permitido.
- Los usuarios no deben instalar software o sistemas de información en los equipos de cómputo o computadores portátiles suministrados para el desarrollo de sus actividades.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.
- La Oficina Asesora Jurídica, deben definir o actualizar cuando sea necesario la política de tratamiento de datos personales, para la protección de los derechos fundamentales de la información de los ciudadanos en su tratamiento.
- La Dirección Administrativa y Financiera debe incluir los mecanismos para que los supervisores de contrato validen el cumplimiento de las obligaciones generales en materia de seguridad y privacidad de la información.

22. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

La oficina de Informática debe establecer los mecanismos necesarios para proveer la disponibilidad de la red y los servicios que dependen de ella, de igual manera, velara por la disposición y monitoreo de los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la Entidad.

22.1 Lineamientos para la Gestión de la seguridad de las redes.

- La Oficina de Comunicaciones con el apoyo de la Oficina Asesora Jurídica diseñará o actualizara los formatos de autorización de captación y uso de imágenes, videos o cualquier medio audiovisual, para solicitar al propietario la captación y uso, de conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y el Decreto 1074 de 2015, y que autorice de manera libre, expresa e inequívocamente, el uso del recurso audiovisual a la Entidad o a quien esta autorice en el

marco del cumplimiento de su misión. La opción de propietario menor de edad debe ser considerada en los formatos.

- Solo los servidores públicos o contratistas avalados por la Oficina de Comunicaciones o a quien el jefe de esta autorice de manera expresa y en el cumplimiento de las funciones de acompañamiento a programas propios de la Entidad, podrán realizar la toma de material audiovisual los ciudadanos mayores o menores de edad.
- La Oficina de Oficina de Informática debe proporcionar una plataforma Tecnológica que soporte los sistemas de información.
- La Oficina de Informática es la responsable de velar por que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- La Oficina de informática debe establecer la documentación necesaria para la utilización de los servicios de red restringiendo el acceso a los servicios de red y a las aplicaciones.
- La Oficina de informática debe realizar revisiones y monitoreo regularmente a la gestión de los servicios para validar que se encuentran en los acuerdos de servicios de red establecidos con los proveedores.
- El acceso a la red corporativa de la Entidad y a los sistemas de información soportados por la misma, es de carácter restringido. Se deben conceder permisos con base a “la necesidad de conocer” y el “acceso mínimo requerido” conforme a los criterios de seguridad de la información contemplados en la presente política.

23. POLÍTICA DE SEGURIDAD PARA LA RELACION CON PROVEEDORES

La Contraloría General de Santiago de Cali, a través de la Dirección Administrativa y Financiera establecerá los mecanismos de control en su relación con los proveedores, teniendo en cuenta que se debe asegurar la información que se genere, procese, custodie o se tenga acceso, supervisando el cumplimiento de lo establecido en el marco de la seguridad y privacidad de la información.

23.1 Lineamientos para asegurar la protección de los activos de la organización que son accesibles a proveedores de la Entidad

- La Dirección Administrativa y Financiera debe establecer lineamientos para el cumplimiento de las obligaciones contractuales de la dimensión de Seguridad y Privacidad de la Información con terceros o proveedores.
- La Dirección Administrativa y Financiera debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información la Entidad.
- La Dirección Administrativa y Financiera deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- La Dirección Administrativa y Financiera debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica la Entidad.
- La Oficina de informática debe verificar periódicamente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
- Cada dependencia la Entidad que establezca relación con proveedores y su cadena de suministro, debe solicitar acompañamiento periódico a la dimensión de Seguridad y Privacidad de la Información con el fin de dar a conocer las políticas que tiene la Entidad.
- La Dirección Administrativa y Financiera debe incluir en las guías de contratación y supervisión obligaciones generales sobre seguridad y privacidad de la información y los formatos para su cumplimiento y verificación por parte del supervisor de contrato.

24. POLÍTICA DE SEGURIDAD PARA DISPOSITIVOS MÓVILES

Establecer los lineamientos para el manejo de los dispositivos móviles institucionales o personales que acceden a información de la CGSC, y velar por el uso responsable de estos por parte del personal.

Esta política aplica para todo el personal de la CGSC que accede a información de la Red Corporativa a través de dispositivos móviles.

Lineamientos

- La CGSC se reserva el derecho de autorizar o denegar el acceso al servicio de acuerdo con las condiciones de seguridad (https://docs.google.com/forms/d/e/1FAIpQLSdIjN7dkQLGqZK4C7rujTrs_SzVtstkKat0sx8ygzLfg8bV8A/viewform) que se detecten en el dispositivo.

- La Oficina de Informática, debe mantener un inventario actualizado de los dispositivos móviles autorizados.

- Los dispositivos móviles de propiedad de los de Servidores Públicos, contratistas, o terceros no deben estar incluidos en el dominio contraloriacali.gov.co. cualquiera que funcione dentro de la Entidad, para conectarse a los servicios de la red de datos deberán realizar solicitud a la oficina de informática y cumplir con los lineamientos referentes a seguridad de la información.

- Los dispositivos móviles que tengan acceso a la información de la Entidad deben tener instalado un software antivirus, y sistema operativo actualizado.

- En dispositivos móviles entregados por la Entidad, los Servidores Públicos no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica.

- En caso de pérdida o robo de un dispositivo móvil de propiedad de la Entidad, los Servidores Públicos, tendrá que realizar la respectiva denuncia ante la entidad competente, luego debe dar aviso inmediato al personal de la Oficina de Informática, quienes deben realizar las acciones necesarias para la protección de la información almacenada en la red corporativa.

- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.

- Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.

- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.

- Es necesario realizar el cifrado del dispositivo móvil.

25. POLÍTICA DE SEGURIDAD PARA CRIPTOGRAFIA

Con el fin de propender por la confidencialidad e integridad de documentos e información de mayor nivel de sensibilidad, la Entidad debe utilizar sistemas y técnicas criptográficas para la protección de la información.

Esta política aplica para todos los procesos de la CGSC que tratan información pública reservada y pública clasificada, para el personal encargado de implementar los controles de cifrado en los servicios de red, en la plataforma informática y en los sistemas de información de la Entidad en el momento de almacenarse o transmitirse por cualquier medio.

25.1 Lineamientos para el uso de Claves Criptográficas

Se deben implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así como:

- Proporcionar una protección adecuada a los equipos utilizados para generar, almacenar y archivar claves, considerándolos críticos o de alto riesgo.
- Proteger las claves secretas y privadas evitando que sean copiadas o modificadas sin autorización.
- La CGSC, desde la oficina de Informática deberá crear e implantar un procedimiento para administración de llaves de cifrado y protocolos para la aplicación de controles criptográficos.

26. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información institucional física, digital o electrónica que se encuentre a cargo de los servidores públicos, proveedores y partes interesadas, la CGSC debe adoptar buenas prácticas para el manejo y administración de la misma, para lo cual se establecen lineamientos

que los usuarios deben conocer y cumplir, manteniendo comportamientos adecuados mientras están manipulando la información o mientras se ausentan del puesto de trabajo, independientemente del medio en el cual se encuentren almacenados, protegiéndola del acceso no autorizado, pérdidas o daños ocasionados voluntaria o involuntariamente.

Lineamientos

Es responsabilidad de todos(as) os servidores públicos, proveedores y partes interesadas, que tengan acceso a las instalaciones físicas, sistemas de información y equipos de cómputo de la CGSC, salvaguardar los activos que contengan información institucional almacenada en medio físico, digital o electrónico, cumpliendo como mínimo los siguientes lineamientos:

Para el cumplimiento de la Política de Escritorio y Pantalla Limpia, es necesario que todos los equipos de cómputo de la CGSC, se encuentren ingresados al dominio institucional.

- Establecer, a nivel de controlador de dominio, un bloqueo de sesión de usuario, cuando transcurra cierto y determinado tiempo de inactividad.
- Garantizar que la autenticación de usuario sea requerida, cada vez que el equipo de cómputo se encienda, reinicie o bloquee.
- Bloquear la sesión de usuario, cuando se ausente del puesto de trabajo y/o deje los equipos desatendidos, para proteger el acceso a la documentación digital, aplicaciones y servicios.
- Cerrar correctamente la sesión de usuario, apagar el equipo de cómputo y periféricos, cuando finalice la jornada laboral, garantizando con esto, una desconexión satisfactoria de la red institucional y guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.
- Evitar colocar documentos sensibles o accesos directos a los mismos, en el escritorio del equipo de cómputo, manteniendo el mismo, limpio y seguro.
- Retirar de las impresoras, escáneres y fax, toda documentación física, evitando de esta manera la exposición de la información a personal no autorizado.
- Se deben mantener los escritorios físicos y áreas de trabajo libres de todo material o elemento que contenga información clasificada como confidencial, a menos que ésta esté siendo utilizada por personal autorizado, el cual deberá garantizar el aseguramiento adecuado de la misma en todo momento.
- Los funcionarios o contratistas deben mantener el puesto de trabajo y escritorio de los equipos de cómputo, organizado y libre de archivos o información

institucional que pueda ser objeto de consulta, copiado, eliminación por personal no autorizado.

- Se debe evitar el consumo de alimentos o bebidas en áreas de trabajo donde se encuentre ubicada la información institucional en papel, equipos de cómputo, dispositivos electrónicos o cualquier medio de almacenamiento que pueda llegar a ser afectado por el derrame de líquidos o residuos de alimentos.
- Los equipos de escritorio y portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active, ante un tiempo sin uso, el protector definido por la CGSC.
- Si el servidor público o contratista está ubicado cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
- La pantalla de autenticación a la red de la institución debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.
- Los funcionarios o contratistas deben bloquear su sesión de trabajo en el sistema operativo del equipo de cómputo al momento de ausentarse de su puesto de trabajo, sin importar que esté configurado para bloquear la sesión de forma automática después de un tiempo determinado.

	Nombre	Cargo	Firma
Proyectó	Lorena Salgado y Noralba Hoyos Ruiz	Profesional Universitario	
Revisó	Carlos Alfonso Lozano Caicedo	Jefe Oficina de Informática	
Aprobó	Carlos Alfonso Lozano Caicedo	Jefe Oficina de Informática	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			