PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTRALORIA GENERAL DE SANTIAGO DE CALI

Fecha del plan: Enero de 2020

VIGENCIA DEL PLAN 2020

DERECHOS DE AUTOR

La Ley No.1915 del 12 julio de 2018 “Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.” determina que en todo proceso relativo al derecho de autor, y ante cualquier jurisdicción nacional se presumirá, salvo prueba en contrario, que la persona bajo cuyo nombre, seudónimo o su equivalente se haya divulgado la obra, será el titular de los derechos de autor. También se presumirá, salvo prueba en contrario, que la obra se encuentra protegida.

Es por ello que el copyright (traducido como derecho de copia que comprende la parte patrimonial de los derechos de autor) del texto, de las tablas y figuras incluidas en este documento es de propiedad de la CONTRALORIA GENERAL DE SANTIAGO DE CALI. Es por ello que si se desea copiar el contenido (texto, tablas o figuras) de más del 40% del documento, debe solicitarse el permiso entrando en contacto con la dirección de sistemas o Secretaría General.

TABLA DE CONTENIDO

INTRODUCCIÓN

La Contraloría General de Santiago de Cali, en su comité directivo del 30 de julio de 2018 aprobó el plan de acción que integro los planes de la entidad, los cuales daban cumplimiento al Decreto 612 de 2018, es por ello que se busca armonizar el presente plan con la política de seguridad aprobada en el 2016, dada la infraestructura digital y segura con que cuenta la entidad.

La Contraloría General de Santiago de Cali es consciente de que la información es el activo más valioso e indispensable para el ejercicio de sus funciones, es por ello que la presentes estrategias buscan definir los lineamientos y límites que deben cumplir los funcionarios, contratistas y terceros frente a la seguridad de la información, propendiendo con ello salvaguardar la integridad, la confidencialidad y la disponibilidad de la información independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada; lo que se resume en reconsiderar puntos estratégicos como las habilidades del talento humano, la cultura, la estructura organizacional y la implementación de tecnologías emergentes, con el claro objetivo de establecer un tratamiento adecuado de la información que se maneja al interior de la entidad asegurando la seguridad y la privacidad de las mismas.

La seguridad de la información es una prioridad para la Contraloría General de Santiago de Cali y por lo tanto, es responsabilidad de todos velar porque no se realicen actividades que vayan en contra de ésta, atendiendo las leyes y demás normas aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

El presente plan es 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.

GLOSARIO

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.

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.

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.

MARCO NORMATIVO:

DECRETO 1078 DE 2015, Ley 1712 de 2015 y su Decreto reglamentario 103 de 2015, realizó el proceso de identificación de activos de información; GEL sección 2 COMPONENTES, INSTRUMENTOS Y RESPONSABLES, Decreto 612 de 2018, POLITICA DE SEGURIDAD ELA INFORMACION 2016, Decreto 2693 de 2012 Decreto 1008 DE 2018.

LINEAMIENTOS CONCEPTUALES Y METODOLÒGICOS

El presente Plan se estructuró sobre la caracterización de causas y agentes que afectan de manera directa e indirecta la seguridad y privacidad de la información, dicho marco conceptual tuvo en cuenta los elementos más importantes que se conocen sobre la materia, buscando la estandarización y el uso de la información recopilada a nivel local, regional o nacional, en el diseño de medidas y acciones de mitigación.

Es así que se identifican algunos conceptos claves que los desarrolladores de estudios caracterización de causas y agentes sobre archivo e informática deben emplear como base para la consolidación de una base de protección de la información.

POLITICA DE OPERACIÓN

La Política de operación de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la alta dirección de la Contraloría General de Santiago de Cali, con respecto a la protección de los activos de información que soportan los procesos de la entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Contraloría General de Santiago de Cali, para asegurar la dirección estratégica de la entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la misma, estos últimos correspondientes a:

- 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 terceros.
- 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 clientes de la Contraloría General de Santiago de Cali
- Garantizar la continuidad de la entidad frente a incidentes.

COMPROMISO DE LA ALTA DIRECCIÓN

La alta dirección aprobó en el 2016 la política de seguridad de la información y en la presente vigencia continuará su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

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

- La revisión de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este plan a todos los funcionarios, contratistas y terceros de la entidad.

- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

SANCIONES PARA LAS VIOLACIONES DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, contratistas, personal externo y proveedores de la Contraloría General de Santiago de Cali. 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.

Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

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, y en general a todos los usuarios de la información que cumplan con los propósitos generales de la Contraloría General de Santiago de Cali.

Normas para la gestión de activos

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.

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.

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 reservado 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.

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 el formato único de inventario documental de que trata el acuerdo 038 de 2002, para la entrega y recibo de los documentos y archivos.

6.1.5 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 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 en los sistemas de información de la Contraloría General de Santiago de Cali sólo los funcionarios, contratistas o terceros autorizados 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.

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.

Normas 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.

- Utilizar la herramienta Docunet como sistema de información para la conservación y preservación del documento electrónico.

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.

Normas 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 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, 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.

POLÍTICA DE USO (de información) DE LOS EQUIPOS DE CÓMPUTO

La Contraloría General de Santiago de Cali, para evitar la pérdida, robo o exposición al peligro de la información alojada en la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre ésta.

Normas de uso de los equipos de cómputo

- La instalación de software en los computadores de la Contraloría General de Santiago de Cali, es una actividad exclusiva de 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 el cual debe ser investigado por el líder de seguridad y analizado en comité de seguridad de la información.
- La Oficina de Informática definirá los perfiles de acceso.

  - ✓ Administradores
  - ✓ Usuarios Generales
  - ✓ Invitados

- En el disco C:\ de los equipos de cómputo encontrarán el sistema operativo, aplicaciones y perfil de usuario, en esta unidad ninguna modificación de los archivos está permitida por parte del usuario.
- El préstamo de bienes informáticos, comunicación y video debe ser registrado en el formato de gestión 1900-15-08-04-38.
- La oficina de informática es la única área autorizada 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 autorizado por dicha Oficina.
- Los funcionarios o contratistas de la entidad y el personal provisto por terceras partes deben bloquear sus equipos en el momento de abandonar

su puesto de trabajo.

- 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 o robo de un equipo de cómputo de la Contraloría General de Santiago de Cali, se debe informar de forma inmediata a la Dirección Administrativa y Financiera para que se inicie el trámite interno y se debe colocar la denuncia ante la autoridad competente.

POLÍTICA DE USO DEL CORREO ELECTRÓNICO

La Contraloría General de Santiago de Cali, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, 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.

Normas de uso del correo electrónico

- La Oficina de Informática proveerá ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- La Oficina de Informática, con el apoyo de la Oficina de Control Interno, programarán campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio 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.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Contraloría General de Santiago

de Cali. El correo institucional no debe ser utilizado para actividades personales.

- 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 cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la entidad y el personal provisto por terceras partes.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Todo funcionario o contratista es responsable de la eliminación de los mensajes cuyo origen sea de dudosa procedencia, por lo tanto asumirá la responsabilidad y consecuencias que pueda ocasionar cualquier archivo adjunto. En estos casos no se debe contestar dicho mensajes, ni abrir los adjuntos, se debe eliminar.
- Todos los mensajes pueden ser sujetos de análisis y conservación permanente por parte de la entidad.
- El servicio de correo electrónico autorizado en la entidad es el asignado por la Oficina de Informática.

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 su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Normas de uso adecuado de internet

- La Oficina de Informática proporcionará los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- La Oficina de Informática debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- La Oficina de Informática debe monitorear continuamente el canal o canales del servicio de Internet.
- La Oficina de Informática debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código

malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- Los usuarios del servicio de Internet de la Contraloría General de Santiago de Cali, deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en los equipos asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, internet invisible u oculto, 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, Kazaa, MSN, Yahoo, Skype, Net2phome 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.

POLÍTICA DE PROTECCIÓN Y RESPALDO DE LA INFORMACIÓN

Esta política define lineamientos que se deben seguir al interior de la Contraloría General de Santiago de Cali (CGSC), para las actividades de almacenamiento en discos duros (internos y externos) y recuperación de información a corto y largo plazo, para responder eficientemente a los requerimientos de los procesos institucionales. Los lineamientos que deben ser cumplidos por toda la entidad para garantizar el respaldo de la información electrónica contenida en los diferentes medios de almacenamiento.

Normas 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.
- La Contraloría General de Santiago de Cali, debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para

permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- 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 realizar 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 carpetas establecidos por la Oficina de Informática (ruta Unidad T:\\CGSCDCB\CARPETAS_AREAS\).
- Los respaldos de información se hacen directamente en la nube Oracle.
- Los documentos electrónicos de archivo deberán ser almacenados en formato PDF/A.
- Los expedientes en cualquier soporte deben contener la hoja de control.

POLÍTICA DE CONTROL DE ACCESO

El acceso a la red corporativa, aplicaciones, servicios y en general cualquier recurso de información de la Contraloría General de Santiago de Cali debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad que se definan por las diferentes dependencias de la entidad, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de la Contraloría General de Santiago de Cali asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por la Oficina de Control Interno de la entidad.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y contratistas e implementada por la Oficina de Informática.

Normas de Control de acceso con usuario y contraseña:

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.

- 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 Contraloría General de Santiago de Cali, 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.

- Solo los funcionarios y contratistas designados por la Oficina de Informática, estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la Contraloría General de Santiago de Cali.

- 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 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.

GESTIÓN DE CONTRASEÑAS

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.

Normas de Gestión de contraseñas

- 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.
- 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 tres 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, alternar mayúsculas con minúsculas,

intercalar símbolos como "#", "$", "&" o "%" entre los caracteres de la contraseña. No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse, ejemplo (Pas$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.

POLÍTICA DE AREAS SEGURAS

La Contraloría General de Santiago de Cali, proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Normas para áreas seguras

- 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 plataforma tecnológica ubicados en el centro de cómputo; 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. Estos sistemas se deben monitorear de manera permanente.

- La Oficina de Informática debe velar porque los recursos de la plataforma 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 asegurar 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 ingresos y egresos de personal a las instalaciones de la Contraloría General de Santiago de Cali deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

- Los funcionarios deben portar el carné que los identifica como tales 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.

POLÍTICA DE PRIVACIDAD Y CONFIDENCIALIDAD

La Contraloría General de Santiago de Cali como organismo de carácter técnico encargado de la vigilancia de la gestión fiscal de la Administración Municipal de Santiago de Cali, fija la presente política de tratamiento de datos personales que reposan en sus bases de datos y 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 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.

ALCANCE

La política de tratamiento de la información, aplica a todas las áreas, funcionarios y contratistas de la entidad que participan en cada una de los procesos institucionales establecidos en el Sistema Integrado de Gestión y a todas las bases de datos y archivos de información personal que reposen en el archivo físico o magnético de la Contraloría General de Santiago de Cali, obtenido en forma presencial, telefónica y/o virtual, verbalmente o por escrito, y que esté en el marco del Artículo 15 de la Constitución Política, la Ley 1581 de 2012, el Decreto N°. 1377 de 2013 y demás normas concordante y pertinente.

Casos en que no es necesaria la autorización.

La autorización del titular no será necesaria cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.

- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el registro civil de las personas.
- Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

Para la debida implementación del presente plan se deberá aplicar los siguientes principios.

Acceso y Circulación Restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución Política. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las previstas en la Ley 1581 de 2012. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a titulares o terceros autorizados confirme a la ley.

Confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales en la Contraloría General de Santiago de Cali que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprenda el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

Finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución Política y la ley, la cual debe ser informada al titular.

Legalidad: El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y en las disposiciones que la desarrollen.

Libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del titular, salvo las excepciones legales. Los datos personales no podrán ser obtenidos ni divulgados sin previa autorización, o en ausencia de mandato legal o, judicial que releve el consentimiento.

Seguridad: La información sujeta a tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias en la medida en que los recursos técnicos, humanos, administrativos, financieros y los estándares mínimos de la entidad así lo permitan para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Transparencia: En el tratamiento se debe garantizar el derecho del titular a obtener del responsable el tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernen.

Veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Sobre la Información personal

Los datos personales de los titulares serán utilizados para el cumplimiento de funciones propias de la Contraloría General de Santiago de Cali, dentro de sus competencias misionales y administrativas establecidas por la Constitución y la ley, en especial, la ley 1581 del 2012, así:

- Los datos personales salvo la información pública como informes de auditorías, estudios y o actuaciones, resoluciones, circulares, videos, invitaciones públicas, boletines, folletos, revistas, informes de gestión, notificaciones de responsabilidad fiscal, entre otros, no podrán estar disponibles en internet u otros medios de divulgación masiva.

- La información personal sobre presuntas responsabilidades fiscales o deudores fiscales incorporados en la bases de datos del Proceso de Responsabilidad Fiscal está sometida a la reserva determinada en la ley.

- La información personal relacionada con los servidores activos y retirados de nuestro Organismo de Control, será utilizada y tratada dentro de los objetivos y alcance fijados en la administración de la planta global de la entidad y para el desarrollo de los programas de bienestar social, salud y seguridad en el trabajado y capacitación con las reservas de ley que sean pertinentes.

- Para cualquiera de los casos los datos personales no podrán ser objeto de actividades con fines comerciales sin la debida autorización del titular.

- En algunos casos, dentro de los mecanismos de participación ciudadana podrán recolectarse datos que reflejen percepciones y opiniones personales sobre aspectos generales o particulares de interés para el ejercicio del control fiscal y el control social, así como sobre el cumplimiento de los objetivos de la Contraloría General de Santiago de Cali, dichos datos están utilizados solamente con fines estadísticos y de conocimiento de la percepción del cliente para efecto de mejora continua en el Sistema

Integrado de Gestión.

Todos los datos antes señalados podrán ser almacenados y procesados en la infraestructura tecnológica de la Contraloría General de Santiago de Cali, o en computadores, o en espacios virtuales institucionales de trabajo asignado para el efecto en las dependencias competentes y tendrán el período de permanencia que se establezca dentro del proceso de gestión documental, de acuerdo con los requerimientos para el cumplimiento de las obligaciones institucionales, bajo estándares de integridad, seguridad, confidencialidad y disponibilidad establecidos por la entidad en sus políticas y procedimientos institucionales.

La Contraloría General de Santiago de Cali cuenta con mecanismos internos de seguridad de la información y protocolos de acceso y administración de las bases de datos para evitar vulneración de la información depositada por manipulaciones ilícitas de terceros. No obstante, nuestra entidad, se exonera de responsabilidad por manipulaciones ilícitas de terceros, fallas técnicas o tecnológicas que se encuentren por fuera de su control como de cualquier situación que no le fuera imputable.

La Contraloría General de Santiago de Cali, podrá comunicar a otras entidades los datos personales de titulares en cumplimiento de disposiciones legales o a solicitud de autoridad competente respetando los principios de confidencialidad y la reserva legal sin que ello constituya vulneración de los derechos de protección de información personal.

Derechos del titular

El titular de la información tiene los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales en la Contraloría General de Santiago de Cali.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la información sobre protección de datos personales.
- Solicitar la suspensión de datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y leales.
- Solicitar información de sus datos personales que hayan sido objeto de tratamiento en la entidad.
- Los demás derechos establecidos en la ley y que le correspondan de acuerdo con la naturaleza jurídica de la entidad.
- Solicitar prueba de la autorización otorgada al responsable del tratamiento, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el Artículo 10 de la Ley 1581 de 2012.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

Obligaciones de la Contraloría General de Santiago de Cali

- Garantizar al titular en todo tiempo, el pleno y efectivo ejercicio del derecho de Habeas Data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre a encargados del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Realizar la actualización, rectificación o supresión de la información en los términos de la ley y/o, comunicar al área encargada del tratamiento, las novedades respecto de los datos suministrados y adoptar las medidas necesarias para que la información reportada se mantenga actualizada.
- Exigir al área encargada del tratamiento el respeto a las condiciones de seguridad y privacidad de la información del titular.
- Garantizar la atención de consultas y reclamos y tramitar los formulados por los titulares en los términos señalados en la ley, a través de la Ventanilla Única de la Contraloría General de Santiago de Cali.
- Cumplir con los mecanismos de seguridad para la protección de la información.
- Cumplir con los tiempos de retención de la información a través del proceso de Gestión Documental.
- Informar cuando determinados datos se encuentran en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo y abstenerse de circular información que esté siendo controvertida por el titular.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- Solicitar y conservar copia de la respectiva autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado.
- Garantizar el adecuado cumplimiento del tratamiento de protección de datos a través de este documento.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

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.

Normas 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.
- El comité de seguridad debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- El comité de seguridad 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.
- El comité de seguridad debe, con el apoyo con la Oficina de Informática y la Secretaría General, 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 al comité de seguridad para que se registre y se le dé el trámite necesario.

POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

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 terceras partes interesadas.

Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

- El Comité de seguridad, 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 seguridad, liderará los temas relacionados con la continuidad de la entidad y la recuperación ante desastres

- El Comité de seguridad, 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 seguridad, validará que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

- El Comité de seguridad, 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 seguridad.

- 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 e documentos vitales esenciales y a la administración del riesgo de la entidad.

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.

Normas 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.

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 (**Ley** 23 de 1982) y propiedad intelectual,(Ley 1915 de 2018) razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Normas 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 seguridad de la información.
- La Oficina de Informática debe verificar 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.

OBJETIVO GENERAL DEL PLAN DE SEGURIDAD YPRIVACIDAD DE LA INFORMACION

La Contraloría General de Santiago de Cali con el presente plan busca planear, organizar, dirigir y controlar actividades que permitan la integridad, disponibilidad y confidencialidad de los activos de información y comunicación,.

OBJETIVOS ESPECÍFICOS

Resguardar los activos de Tecnologías de Información.

Aplicar las mejores prácticas y estándar de seguridad de la información.

Comprometer a todo el personal adscrito a la entidad y terceros interesados, con el proceso de seguridad de la Información.

Establecer y aplicar controles.

Capacitar, concientizar y empoderar a los usuarios de activos de información (digitales, físicos) sobre la seguridad de la información de la Contraloría General de Santiago de Cali.

ALCANCE DEL PLAN DE SEGURIDAD YPRIVACIDAD DE LA INFORMACION

La seguridad de la información es un esfuerzo de equipo, es por ello que se requiere la participación y apoyo de todos los servidores públicos de la Contraloría General de Santiago de Cali, ya sea los que trabajan con sistemas de información o las personas que utilizan la Infraestructura Tecnológica de la entidad.

Por ende el presente plan como las políticas de seguridad que se han definido aplican a todos los funcionarios públicos, contratistas, proveedores y demás usuarios internos y externos de la infraestructura tecnológica de la entidad.

Es por ello que para continuar con su debida articulación e implementación del Sistema de Administración de la Seguridad de la Información. Se deberá continuar con la debida planeación y controles preventivos y correctivos para incidencias de seguridad de la información en: Ataques maliciosos externos, Ataques maliciosos internos, Acceso a la red por personas no autorizadas, acceso físico no autorizado, pérdida o robo de equipo de cómputo, administración de red inadecuada, cambio de datos no intencionado en un sistema de información, copias de seguridad defectuosas, destrucción de archivos, extracción de información, falsificación de archivos, instalación de software no autorizado, Ilegalidad en Licenciamientos, mal uso de sistemas de información, mal uso de recursos de red, pérdidas de conectividad, pérdida de Contraseñas, pérdida de Código fuente de aplicaciones desarrolladas internamente.

DIAGNOSTICO SITUACIONAL

Esta entidad cuenta con unas políticas de seguridad la cual cumple los estándares del Min TIC, conforme a los autodiagnósticos se pudo evidenciar un resultado de 91,3 puntos en la política de Trasparencia y Acceso a la Información y 97 puntos en la de Gestión Documental, lo que permite concluir que existe una debida coherencia frente a los valores para el resultado.

DEFINICIÓN DE ESTRATEGIAS

Para el presente plan se adopta varias estrategias:

Estrategia de liderazgo: busca que el liderazgo en la entidad no se ejerce por una sola persona, se requiere que todo el grupo de gestión de la organización actué con grado de eficacia e influencia, para el desarrollo del presente plan.

Estrategia de apropiación de la gestión del conocimiento, El conocimiento es uno de los mayores activos dentro de la entidad, a través de su gestión se puede lograr una mayor riqueza o valor añadido en la seguridad y privacidad de la información; La gestión del conocimiento es arma con la cual puede uno atacar los problemas organizacionales, ya que el conocimiento individual de cada persona dentro de la empresa se puede convertir en conocimiento colectivo, dando mayor peso a la información y pudiendo así integrar mejores ideas para atacar el problema en cuestión.

El conocimiento que posee una organización puede convertirse en una fuente de ventaja que permita originar acciones innovadoras para generar productos, servicios, procesos y sistemas de gestión que optimicen los recursos y capacidades de la entidad.

Estrategia de comunicación y divulgación. Busca visibilizar y empoderar todos los procesos y resultados de las actividades institucionales de seguridad y privacidad de la información

Estrategia de evaluación y seguimiento. En la ejecución del plan será necesario consolidar informes exactos y basados en pruebas, que proporcionen datos a los responsables de la gestión y de la adopción de decisiones de modo que dirijan la intervención y mejoren sus resultados;

Etapas para la ejecución de las estrategias. La ejecución de las estrategias requiere seguir un proceso metodológico que permita que sean aplicadas adecuadamente:

Desarrollo. Se refiere a la planeación; en ella se diseña la estrategia y se desarrollan las tácticas. Es importante que en esta etapa se consideren todos los factores del macro y microambiente que puedan afectar su aplicación, es decir, se debe visualizar la situación presente.

Aplicación. Es la etapa en la que se integran las tácticas en un solo concepto estratégico; dejan de visualizarse como acciones independientes y se integran en una idea única, que debe corresponder al diseño de la estrategia.

Ejecución. Se pone en marcha la estrategia, siguiendo el calendario y las tácticas

previstas; en su etapa inicial, es posible hacerle algunas modificaciones, de acuerdo con las condiciones que se observen.

Control. Es la etapa en la cual se verifica el correcto funcionamiento de la estrategia, a través de supervisiones y procesos de control; nos ofrecerá retroalimentación para determinar si es necesario establecer acciones alternas.

ALIENACIÓN DE ESTRATEGIAS CON EL PLAN ESTRATÉGICO 2020

La Contraloría General de Santiago de Cali como entidad pública, debe alinearse, con el plan estratégico institucional y los planes de acción; y con esto generar una estrategia para facilitar el logro de los objetivos de la Entidad, apoyando la transformación de la organización y generando valor**.**

Conforme al objetivo Nº 1 GOBERNABILIDAD INSTITUCIONAL EFICAZ – Fortalecer el uso de las tecnologías de información y comunicación- TIC's eje transversal de la política de gobierno digital que permita mayor eficiencia a nivel interno y externo.

PARTES INTERESADAS Y/O CARACTERIZACIÓN DE GRUPOS DE VALOR

IDENTIFICACIÓN DE LAS PARTES INTERESADAS	REQUISITO NECESIDADES Y/O EXPECTATIVAS DE LAS PARTES INTERESADAS	PROCESO Y/O ÁREAS ENCARGADAS DE ATENDER LA NECESIDAD Y/O PARTE INTERESADA	ORIGEN DE LAS PARTES INTERESADAS	CAPACIDAD		INFLUENCIA		MEDIO IDENTIFICACIÓN DEL REQUISITO	PRIORIDAD	ACCIONES Y COMPROMISOS
				NIVEL (Alta - Media - Baja)	JUSTIFICACION	NIVEL (Alta - Media - Baja)	JUSTIFICACIÓN		NIVEL (Alta - Media - Baja)	
Auditoría General de la República	Administracion y Soporte técnico oportuno y confiable brindado acerca de los sistemas SIA Contralorias y SIA Observa a usuarios de la CGSC.	Oficina de Informática	Externo	Alta	Personal entrenado en los sistemas entregados o recibidos mediente convenio.	Alta.	Se pueden Generar sanciones por incumplimientos legales de ley.	Correos Electrónicos. Aplicativo SICIS.	Alta	Administrar los usuarios y atender las solicitudes de los usuarios.
Contraloría General de la República	Administracion y Soporte técnico oportuno y confiable brindado acerca del PNA a usuarios de la CGSC.	Oficina de Informática	Externo	Alta	Personal entrenado en los sistemas entregados o recibidos mediente convenio.	Alta.	Se pueden Generar sanciones por incumplimientos legales de ley.	Correos Electrónicos. Aplicativo SICIS.	Alta	Administrar los usuarios y atender las solicitudes de los usuarios.
Contralorías Territoriales con las cuales se tienen convenios	Aplicativos funcionales entregados mediante convenio que contribuyen al cumplimiento de la labor misional y administrativa de las contralorias Territoriales. -Claridad y precisión en los conceptos transmitidos, capacitaciones y soportes.	Oficina de Informática	Externo	Alta	Personal idoneo en el desarrollo de aplicaciones internas entregadas o recibidas mediente convenio.	Alta	Unificación de procesos en las Contralorías y posicionamiento a nivel nacional de la CGSC.	Documentos soporte de legalización de convenios. -Convenio firmado, instalación configuración, parametrización de los sistemas de acuerdo a cada necesidad. - Certificación de acompañamiento en sitio.	Alta	Cumplir con el convenio haciendo parametrización, entrega, capacitaciones y acompañamiento permanente en el uso de los aplicativos.
Todas las Areas de la CGSC	Información disponible, confiable y segura. - Servicio y mantenimiento oportuno, eficiente y eficáz. Aplicativos funcionales que contribuyen al cumplimiento de la labor misional y administrativa de la Contraloria. -Claridad y precisión en los	Oficina de Informática	Interna	media	No se cuenta con suficiente personal para cubrir con todas las necesidades de los procesos.	Alta	Por ser una oficina trasversal a todos los procesos de la entidad.	Publicación de planes en intranet -Listado de bienes informáticos Hardware, software. -Plan de mantenimiento preventivo. -Aplicación SICIS -Encuesta de satisfacción del cliente interno	Alta	Atención de solicitudes de soporte. Realizar el Mantenimiento Preventivo para el adecuado fucnionamiento de los equipos. Actualizar el aplicativo SICIS para tener el control de los bienes informaticos. Realizar backups para salvaguardar la información.
Contralor, Oficina De Planeación Normalización Y Calidad, Oficina de Control Interno	Información oportuna, confiable y coherente.	Oficina de Informática	Interna	Alta	Informes veraces, coherentes, oportunos y conforme a las disposiciones legales y reglamentarias.	Alta	Incumplimiento a procedimientos internos.	Docunets remisión de informes. - Carpeta Informes de la red corporativa.	Alta	remitir los informes de acuerdo al SGC.
Auditoría General de la República	Información oportuna, confiable y coherente.	Oficina de Informática	Externo	Alta	Informes veraces, coherentes, oportunos y conforme a las disposiciones legales y reglamentarias.	Alta	Se pueden Generar sanciones por incumplimientos legales de ley.	Informe de rendición de la Entidad. Carpeta Informes de la Red corporativa.	Alta	Enviar la información requerida por el ente de control.
Sujetos y Puntos de control	Soporte técnico oportuno, y confiable. Personal entrenado en los sistemas recibidos mediante convenio con la AGR - Claridad y precisión en los conceptos transmitidos	Oficina de Informática	Externo	Alta	Personal entrenado en los sistemas entregados o recibidos mediente convenio.	Alta	Se pueden Generar sanciones por incumplimientos legales de ley.	correos Electronicos. Aplicativo Sicis Registro de convocatoria y asistencia a capacitación	Alta	Atender las solicitudes de soporte, realizados por los usuarios
Proveedores	Claridad y oportunidad en la definición de las necesidades técnologicas requeridas	Oficina de Informática	Externo	Alta	Continuo sondeo del mercado TI, por parte del Jefe de la oficina de Informática	Media	La contratación se hace por subasta publica lo que implica tener varias opciones a la hora de elegir el proveedor que cumpla con todo lo solicitado	Contratos de Prestacion de servicios	Alta	Gestionar la renovacion oportuna de los contratos

INDICADORES Y RESULTADOS DE IMPACTO

Se han definido indicadores de gestión que representan una medida del logro de los objetivos, pero no de manera específica, para final de la vigencia

RIESGOS

Para el Plan de seguridad y privacidad de la información, aplican los riesgos de gestión y corrupción que generarían afectación al proceso de informática y gestión documental, identificados y definidos en el mapa de RIESGOS de la entidad.

RECURSOS

Este plan se lleva a cabo con recursos propios: humanos, físicos, tecnológicos y financieros; con énfasis en aplicación de controles y acciones para fortalecer la seguridad y privacidad de la información.

ESTRATEGIAS PARA COMUNICAR Y DIVULGAR EL PLAN

La eficacia en el tratamiento de los riesgos de seguridad de la información se sustenta, entre otros, en el conocimiento y el trabajo colectivo de los servidores públicos de la entidad. Para ello, tanto el Plan como la información relacionada con el mismo se socializará internamente a través de medios institucionales, tales como Docunet, intranet, carteleras, comités, etc.

ESTRATEGIAS DE EVALUACIÓN Y SEGUIMIENTO

Se propondrá herramientas de seguimiento para medir la ejecución del presente Plan, y el seguimiento se realizará a través de la segunda y tercera línea de defensa de MIPG

RESPONSABLE DEL DOCUMENTO

Secretaria General, Oficina Asesora de Comunicaciones, Oficina de Informática