POLITICAS DE SEGURIDAD DE LA INFORMACION PARA LA CONTRALORIA GENERAL DE CALDAS.

¿Por qué es necesario tener políticas de seguridad?

Las organizaciones, los sistemas y las redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraudes electrónicos, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La información, los procesos, los sistemas y las redes son los activos más importantes y valiosos para cualquier entidad. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del organismo, un plan de continuidad del negocio y atender oportunamente las disposiciones legales.

Requerimientos de seguridad
Existen tres fuentes principales de requerimientos de seguridad:

1. Evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la Contraloría General de Caldas. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad, la probabilidad de ocurrencia y se calcula el impacto potencial.

2. Requerimientos legales, reguladores, estatutarios y contractuales que debe adoptar la Contraloría General de Caldas, contratistas y proveedores de servicio.

3. El conjunto particular de principios, objetivos y requerimientos funcionales para el procesamiento de la información que la Contraloría General de Caldas ha desarrollado para sostener sus operaciones. (Plan de continuidad).

PALABRAS CLAVES

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
Tecnología de la Información: Se refiere al hardware y software operados por los funcionarios de la Contraloría General de Caldas o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin

tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
Riesgo: Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.
Amenaza: Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.
Vulnerabilidad: Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

La seguridad de la información, es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y garantizar el normal funcionamiento de los procesos del organismo. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

La seguridad de la información debe garantizar:
Confidencialidad: que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Integridad: que se salvaguarde la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad: que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Autenticidad: que se asegure la validez de la información en tiempo, forma y distribución. Asimismo, se garantice el origen de la información, validando el emisor para evitar la suplantación.
Auditabilidad: que todos los eventos de un sistema deben poder ser registrados para su control posterior.
Protección a la duplicación: consiste en asegurar que documento sólo se realice una vez, que sea único y no existan múltiples replicaciones, a menos que se especifique lo contrario.
No repudio: garantizar que toda comunicación que se envié o se reciba llegue al destinatario final.
Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta Contraloría General de Caldas.
Confiabilidad: que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

ALCANCE DE LAS POLÍTICAS

Estas Políticas de Seguridad de la Información se presentan con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Contraloría General de Caldas.
Las políticas definidas en el presente documento aplican a todos los funcionarios de la Contraloría General de Caldas, personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la Entidad.

DESCRIPCION DE LAS POLITICAS DE LA SEGURIDAD DE LA INFORMACION EN LA CONTRALORIA GENERAL DE CALDAS.

POLITICA 1.
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Su objetivo es Proteger los recursos de información de la Contraloría General de Caldas y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
Mantener la Política de Seguridad de la entidad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
Los funcionarios de la Contraloría son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Responsables de Hacer cumplir la política de Seguridad de la Información en la Contraloría General de Caldas:

El Líder del **Proceso de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de: notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. (Inducción)
Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El Líder del **Proceso de Recursos Tecnológicos** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Contraloría General de Caldas. Por otra parte, tendrá la función de velar por el cumplimiento del contrato de

mantenimiento de sistemas, que contemple la inclusión de medidas de seguridad en todas las fases.
El Líder del **Proceso de Gestión Jurídica** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Contraloría General de Caldas con sus funcionarios y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.
El Líder del **Proceso de Control Interno**, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

POLITICA 2.
ACCESO PARA AGENTES EXTERNOS QUE GARANTIZA LA SEGURIDAD DE LA INFORMACION

Su objetivo es mantener la seguridad de la información y de los activos de información de la Contraloría General de Caldas cuando sean accedidas por terceros.
Debe controlarse permanentemente el acceso de terceros a los dispositivos de tratamiento de información de la entidad.
Cuando se requiera acceso de terceros, se debe realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que sean pertinentes. Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.

Para mitigar el riesgo de acceso por terceros: Se debe evaluar los riesgos y revisar los controles de seguridad de información existentes respecto a los requerimientos legales.
Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador. En todo caso deberán firmar un acuerdo de buen uso de los Recursos Informáticos.
La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el proceso de Recursos Tecnológicos con el fin de no comprometer la seguridad de la información interna de la entidad.

Responsables de Hacer cumplir la política de acceso para agentes externos que garantiza la seguridad de la información en la Contraloría General de Caldas:

El líder del **proceso de recursos tecnológicos** capacitará al personal de la entidad en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los funcionarios que generan la información, analizará el riesgo de los accesos de terceros a la información de la entidad y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

También cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa

o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

Los **Líderes de cada proceso** cumplirán la función de informar y autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.
El líder de **control interno** será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.
El Líder del **proceso de Gestión Jurídica** notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información de la entidad.

POLITICA 3.
GESTION DE ACTIVOS DE INFORMACION.

Su objetivo es Alcanzar y mantener una protección adecuada de los activos de la Contraloría General de Caldas, además garantizar que los activos de información reciban un apropiado nivel de protección.
La entidad debe tener conocimiento preciso sobre los activos que posee, tales como:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, publicación de contenidos, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, switches de datos, etc.), medios magnéticos (cintas, discos externos, etc.-).
- Otros equipos: ups

Todos los activos deben estar justificados y deben ser asignados a un funcionario. Se deberían identificar a los responsables de cada uno de los activos y asignarles la responsabilidad de notificar acerca de algún inconveniente.

Responsables de Hacer cumplir la política de Gestión de Activos en la Contraloría General de Caldas:

El Líder del **proceso de Recursos Físicos**, y con ayuda del **Encargado del almacén**, deberán construir un inventario actualizado de activos de información, mostrando los funcionarios y sus equipos asignados con especificación y detalle de los mismos (ubicación, número de serie, estado, etc).

POLITICA 4. POLITICA DE SEGURIDAD LIGADA A RECURSOS HUMANOS.

Su objetivo es reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Es por ello que se deben establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.
La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones.
De acuerdo a lo anterior, es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

POLITICA 4.1
Política para los aspirantes a cargos y/o contratos con la contraloría general de caldas.

Su objetivo es asegurar que los futuros funcionarios, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo y/o contrato. (Inducción)
Los contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberán firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad de la información en la Contraloría General de Caldas.

POLITICA 4.2
Política para los funcionarios y/o contratistas activos de la contraloría general de caldas.

Su objetivo es asegurar que los funcionarios, contratistas y terceras personas activas en la entidad, estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.
Se deben definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de La Contraloría General de Caldas.
Todos los empleados los contratistas y los terceros que desempeñen funciones en la entidad, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como su estación de trabajo.
El Líder del **proceso de Recursos Humanos** será el encargado de coordinar las acciones de capacitación que surjan de la presente Política, comunicar los cambios y actualizaciones que se realicen en las mismas.

El líder del **proceso de control interno** deberá revisar el material correspondiente a capacitaciones, políticas, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento, así mismo se hará una auditoria interna para determinar el cumplimiento de las políticas.

POLITICA 4.3
Política para los funcionarios y/o contratistas que dejan o cambian de cargo en la contraloría general de caldas.

Su objetivo es asegurar que los funcionarios, contratistas y terceras personas que salgan de la entidad o cambien de cargo lo hagan de manera organizada y segura con respecto a los activos informáticos, documentos y lineamientos de ley.
Se deben establecer las responsabilidades para asegurar que la salida de la entidad del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo, entrega del cargo con todos los activos informáticos (software, documentos corporativos, equipamiento, dispositivos de computación, etc) y se eliminen todos los derechos de acceso.
Después de que el funcionario deja de prestar sus servicios a la entidad o cambia de cargo se compromete a entregar toda la información respectiva de su trabajo realizado documental (archivos de gestión) electrónica almacenada en el equipo de cómputo o en el correo electrónico corporativo, para esto debe entregar un oficio al proceso de recursos tecnológicos detallando cual y donde está ubicada la información digital en el equipo de cómputo para que desde recursos tecnológicos realicen la copia de seguridad de esta información. Una vez retirado el funcionario de la Contraloría General de Caldas debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios que detecten el mal uso de la información está en la obligación de reportar el hecho al grupo de control interno disciplinario.
Se recomienda que el líder de **recursos tecnológicos** haga un seguimiento del uso del correo institucional de estas personas antes de salir definitivamente de la entidad, con el propósito de identificar si comienzan a extraer información confidencial y propia de la entidad (esto debe ir sujeto a las políticas aplicables y consideraciones legales sobre privacidad).
Los funcionarios que dejen el cargo deberán hacer entrega del mismo al **jefe inmediato**, de igual forma, a quien corresponda deberán hacer la entrega de los bienes asignados a su nombre.

POLITICA 5.
POLITICA DE SEGURIDAD FISICA Y AMBIENTAL EN LA CONTRALORIA GENERAL DE CALDAS.

POLITICA 5.1
Política de seguridad física en la contraloría general de caldas

Sus objetivos son:

- Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y equipos de cómputo de la entidad.

- Prevenir e impedir accesos no autorizados, daños e interferencia a las redes, instalaciones e información de la entidad.
- Proteger el equipamiento de procesamiento de información crítica de la entidad (servidores) ubicándolos en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. (Cuarto de servidores).

La seguridad física brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la entidad. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.
Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

Responsables de Hacer cumplir la política de seguridad física en la Contraloría General de Caldas:

El Líder del **proceso de recursos tecnológicos** en la definición de las medidas de seguridad, velará por implementar la política de áreas protegidas, y coordinará dicha implementación. (Administrador de cuarto de servidores) Asimismo, vigilará el cumplimiento y dará accesos al personal del contrato de mantenimientos correctivos y preventivos.
Todos los funcionarios de la entidad son responsables del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas, también son responsables del manejo de información física en papel.

POLITICA 5.2
Política de seguridad ambiental en la contraloría general de caldas.

Sus objetivos son:
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la entidad. Control de humedades, fugas, etc.
- Evitar transmisión de hongos, virus, agentes propagadores y enfermedades biológicas, esto teniendo aseado y desinfectado constantemente el puesto de trabajo.
- Equipar a los funcionarios de la entidad con escritorios cómodos, sillas confortables, descansa pies, mouse pad, iluminación y ventilación adecuada con el propósito de disminuir los riesgos y enfermedades profesionales.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la entidad como en instalaciones próximas a la sede de la misma que puedan interferir con las actividades.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

- Se debe identificar los sitios de almacenamiento de materiales peligrosos o combustibles. Si existen, deben estar respectivamente señalizados y a una distancia prudente de áreas o cuartos de servidores.
- El archivo central debe ubicarse en una zona aislada, a una gran distancia de cuartos eléctricos, debe ser una zona con acceso restringido, así mismo debe tener deshumidificadores, extintores en zonas estratégicas, visibles y señalizadas. El manejo de papelería debe hacerse con protección (delantal, gorro, guantes y tapabocas) para evitar la propagación de hongos y enfermedades.
- Los puestos de trabajo deben permanecer constantemente aseados, se debe evitar al máximo el consumo de alimentos y el almacenamiento de los mismos en dichas áreas. Esto con el fin de evitar plagas, roedores, insectos, cucarachas.
- Los residuos y manejo de basuras deben hacerse en zonas aptas y por personal capacitado para dicha labor. Esto a una distancia considerable de los puestos de trabajo.

POLITICA 6.
GESTION EN COMUNICACIONES Y OPERACIONES EN LA CONTRALORIA GENERAL DE CALDAS.

Su objetivo es garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
Las comunicaciones establecidas en la entidad permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información.
Los sistemas de información están comunicados, y tienen acceso por los funcionarios y por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan. (Accesos).
La proliferación de software malicioso, como virus, troyano, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas. Es por ello que cada uno de los equipos tiene antivirus licenciado, así mismo restricciones de descargar e instalación de software.

POLITICA 6.1
Procedimientos y responsables de operación en la contraloría general de caldas.

Su objetivo es documentar y mantener actualizados los procedimientos operativos de cada macro proceso y cada sub proceso presente en la entidad.
Los procedimientos deberán tener especificados

1. Responsable de cada proceso (Líder).
2. Procesamiento y manejo de la información.
3. Dependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
4. Restricciones en el uso de atributos del sistema.

5. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

Además de documentar cada proceso se deben desarrollar instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Para la **administración de cambios operativos** se efectuará el procedimiento correspondiente definido por la Contraloría General de Caldas de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica y apoyado en las mejores prácticas para obtener control en cada uno de ellos.
Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.
Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

POLITICA 6.2
Gestión de la provisión de servicios por terceros en la contraloría general de caldas.

Su objetivo es Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio por terceros.
Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los contratos.
La entidad mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte.
La entidad debe verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.
La gestión de cambios en servicios provistos por terceros deberá ir inmerso y especificado en cada contrato, con el fin de asegurar el cumplimiento del mismo.

POLITICA 6.3
Planificación y aceptación del sistema en la contraloría general de caldas.

Su objetivo es minimizar el riesgo de fallas en los sistemas.
Se debe planificar y preparar los cambios y actualizaciones en cada sistema para garantizar la disponibilidad de las operaciones.
Deben realizarse proyecciones de los requisitos de capacidad, almacenamiento y procesamiento para en un futuro para reducir el riesgo de sobrecarga de los sistemas.
Los requisitos operacionales de los nuevos sistemas se deben establecer, documentar y probar, antes de su aceptación.

POLITICA 6.4
Protección contra el código malicioso y descargables en la contraloría general de caldas.

Su objetivo es proteger la integridad del software y la información. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, gusanos, bombas lógicas, etc.
Los funcionarios de la Entidad, deben estar al tanto de los peligros de los códigos maliciosos.
El **líder de recursos tecnológicos** debe introducir controles para evitar, detectar y eliminar los códigos maliciosos. (Antivirus, Servidor de Dominio, Servidor Proxy y Firewall).

Dichos controles, deben establecer políticas y procedimientos formales que contemplen las siguientes acciones:

1. Prohibir la instalación y uso de software no autorizado por la entidad (Derecho de Propiedad Intelectual del Software).
2. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde redes externas, o por cualquier otro medio señalando las medidas de protección a tomar.
3. Instalar y actualizar periódicamente software de detección y reparación de virus, y actualización de base de datos de firma de virus, examinado computadoras y medios informáticos, como medida preventiva y rutinaria.
4. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.
5. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la entidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas, en especial, realizar revisión y análisis de logs.
6. Bloquear todas las descargas de software y música, con el propósito de mantener los equipos protegidos contra las amenazas de la red.
7. Concientizar a los funcionarios de la entidad para borrar archivos temporales, cookies, y registros de navegación web.

POLITICA 6.5
Copias de seguridad y respaldo de la información en la contraloría general de caldas.

Su objetivo es mantener la integridad, disponibilidad de la información y los medios de procesamiento de la misma.
La información que es soportada por la infraestructura de tecnología informática de la Contraloría deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad. Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.
El almacenamiento de la información deberá realizarse internamente en la entidad, esto de acuerdo con la importancia de la información para la operación de la Contraloría.
El proceso de Recursos Tecnológicos será el encargado del respaldo de la información así mismo como del plan (tiempos, personal, recursos) y de la metodología a utilizar para llevarlo a cabo.

Se debe definir un esquema de respaldos y copias de seguridad back-ups, que permita tener acceso a la información en el momento que sea requerida.

1. El proceso de recursos tecnológicos determinará detalladamente a que se le debe sacar copia de seguridad y la periodicidad con la que se debe hacer, teniendo en cuenta la criticidad de la aplicación y el flujo de información que se tienen en un periodo de tiempo razonable.
2. Los medios utilizados para el respaldo deben ser guardados en la oficina de recursos tecnológicos, disponiendo de acceso restringido.
3. Garantizar un nivel de resguardo, seguridad física y ambiental de la información según las normas aplicadas en la entidad.
4. Realizar pruebas periódicas a los medios y dispositivos de respaldo para garantizar el estado de la misma.
5. Cuando un usuario abandone la entidad debe entregar copia de seguridad de la información relevante a la Contraloría General de Caldas que tiene en su equipo de cómputo, adicionando un oficio donde se relacione detalladamente la información corporativa que queda guardada en la copia, para este proceso podrá contar con la colaboración de la empresa contratista de soporte técnico.

POLITICA 6.6
Gestión de la seguridad de las redes en la contraloría general de caldas.

Su objetivo es asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
La gestión segura de las redes, requiere la consideración del flujo de datos, acciones legales, monitoreo y protección. También se pueden requerir controles adicionales para proteger la información confidencial que se transmite a través de red de la entidad.

Toda vez que el cableado estructurado sobre el cual se encuentra sustentada la red de datos de la Contraloría General de Caldas pertenece a la Gobernación de Caldas y son ellos los que se encargan de la gestión del mismo el líder del **proceso de recursos tecnológicos** solicitara colaboración cuando se deba realizar algún cambio es esta infraestructura.

POLITICA 7.
CONTROL DE ACCESOS EN LA CONTRALORIA GENERAL DE CALDAS.

Sus objetivos son:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

- Controlar la seguridad en la conexión entre la red de la contraloría general de caldas y otras redes públicas o privadas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Todos los funcionarios de la Contraloría General de Caldas deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas (Practicantes, funcionarios por contrato) ajenas a la Entidad deberán tener autorización dada por el líder del proceso donde desempeñará sus funciones que indique la información sobre la cual puede tener acceso.
Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad.
Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.
Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución y manejado de acuerdo a su clasificación como incidente o problema.
Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los mismos incurre en la falla de los sistemas.
Cada Funcionario de la contraloría General de caldas posee un nombre de usuario y contraseña para acceder al dominio, dicha configuración se hará inicialmente desde el proceso de recursos tecnológicos, allí mismo se darán los privilegios según el usuario, acceso a las unidades de red, acceso a la información, etc.
De igual manera, las aplicaciones existentes en la entidad, son de acceso restringido, según el perfil de cada funcionario podrán acceder y tendrán privilegios. La administración y mantenimientos de estas aplicaciones se darán en cumplimiento al contrato de adquisición y uso de la misma.
Todos los equipos de la entidad se encuentran conectados a un servidor de dominio, lo que resguarda la información, la configuración y lo que permite programar tareas para todos los equipos de la red.

POLITICA 8.
MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN EN LA CONTRALORIA GENERAL DE CALDAS.

Su objetivo definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible.

El proceso de Recursos Tecnológicos deberá proveer la administración de los sistemas operativos y brindar soporte a los usuarios de los computadores corporativos, con los objetivos de garantizar la continuidad del funcionamiento de las máquinas y del

"software" al máximo rendimiento, y facilitar su utilización a todos los sectores de la entidad.
Esta labor se desarrolla en tareas como:

- Mantenimiento de los equipos, detección y resolución de averías de manera preventiva y correctiva de acuerdo a las solicitudes que haga el usuario por escrito mediante el formato de calidad que se define en el área, de ser un problema mayor se deberá dar aviso a la entidad que provee el servicio de soporte y mantenimiento. (Contrato).
- Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas Back ups.
- Evaluación de necesidades de recursos (memoria, discos) y provisión de los mismos en su caso.
- Instalación y actualización de utilidades de software.
- Atención a usuarios (consultas, preguntas frecuentes, información general, resolución de problemas, asesoramiento).

En general, los mantenimientos de los aplicativos presentes en la Contraloría General de Caldas vienen inmersos en el contrato de la adquisición de los mismos, por lo cual el proceso de recursos tecnológicos tiene como tarea vigilar y supervisar el cumplimiento del objeto del contrato.

POLITICA 9.
GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA CONTRALORIA GENERAL DE CALDAS.

Su objetivo es Garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.
Para estos casos desde el área de recursos tecnológicos y la empresa contratada para prestar el soporte técnico de primer nivel se procederá a diligenciar el formato de requerimiento de soporte técnico el cual sirve como soporte de los incidentes tecnológicos ocurridos en sus equipos de cómputo y los sistemas de información de la entidad. De esta manera se deja un historial de todos los incidentes reportados, para en un futuro minimizar los riesgos de fallas en los sistemas. Los tiempos de respuesta a las solicitudes se establecen de acuerdo a los planes establecidos, para lo cual se debe dar respuesta en un máximo de 4 horas después de recibir la solicitud.

POLITICA 10.
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO EN LA CONTRALORIA GENERAL DE CALDAS.

Sus objetivos son:

- Minimizar los efectos de las posibles interrupciones de las actividades normales de la entidad (sean éstas resultado de desastres naturales, accidentes, fallas en el

equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia de la entidad con el establecimiento de planes que incluyan al menos las siguientes etapas:

    a) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
    b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
    c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
    d) Asegurar la coordinación con los funcionarios líderes de cada proceso y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Se debe implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación.
En este proceso se deben identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones.
Así mismo, se deben analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales.

POLITICA 11.
CUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION EN LA CONTRALORIA GENERAL DE CALDAS.

Sus Objetivos son

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la entidad y/o al funcionario o que incurran en responsabilidad civil o penal como resultado de su incumplimiento. (Proceso de Gestión Jurídica).
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la entidad.
- Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información. (Proceso de recursos tecnológicos).
- Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la entidad. (Cumplimiento contractual).

POLITICA 12. DERECHOS DE PROPIEDAD INTELECTUAL EN LA CONTRALORIA GENERAL DE CALDAS.

Derechos de propiedad intelectual en la información y en el software en la contraloría general de caldas.

Su objetivo es implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
Los funcionarios únicamente podrán utilizar material autorizado por la entidad, así mismo, la entidad solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.
La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deben tener presentes las siguientes normas:

- Ley 23 de 1982, sobre derechos de autor.
- Ley 44 del 1993, "*Por la cual se modifica y adiciona la ley 23 de 1982 y se modifica la ley 29 de 1944*" en relación con los Artículos 51 y 52.

POLITICA 13.
SANCIONES PREVISTAS POR INCUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD EN LA CONTRALORIA GENERAL DE CALDAS.

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias y convencionales que rigen al personal de la Contraloría General de Caldas, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.
Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.
El agente que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial -cuando ocasiona un daño que debe ser indemnizado- y/o en responsabilidad penal -cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.