PLAN DE SEGURIDAD INFORMÁTICA

1. INTRODUCCIÓN

Con el continuo y vertiginoso desarrollo tecnológico en que nos vemos inmersos, se debe prestar mucha atención a los posibles focos vulnerables a los que se pueda estar expuesto en lo relacionado con la seguridad informática, convirtiéndose esta en la figura referente para garantizar la continuidad y el óptimo desempeño de la funciones constitucionales de la Contraloría Departamental del Valle del Cauca.

Es por eso la imperiosa necesidad de establecer y reglamentar las Políticas de Seguridad Informática de la Entidad, estas directrices son de índole técnico y administrativo con el fin de proteger y resguardar todo el componente tecnológico y de telecomunicaciones; y por ende su principal activo, la información. Es necesario que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, estableciendo sus derechos y deberes de cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente la Contraloría Departamental del Valle del Cauca cuenta con una plataforma tecnológica que almacena, procesa y transmite la información institucional, incluye equipos de cómputo de usuario y de servidores de aplicaciones que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Siendo la información institucional un activo valioso para la Entidad, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

Este compendio tiene como finalidad dar a conocer el Plan de Seguridad Informática, que deben aplicar y acatar los funcionarios, contratistas y terceros de la Contraloría Departamental del Valle del Cauca, entendiendo como premisa que

la responsabilidad por la seguridad de la información es de todos los actores que intervienen.

2. OBJETIVO GENERAL

Definir e implementar el Plan de Seguridad Informática, como derrotero con las pautas para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la Contraloría Departamental del Valle del Cauca, para su divulgación, aplicación y revisión permanente.

3. OBJETIVOS ESPECÍFICOS

3.1. Formular el Plan de Seguridad Informática que permita minimizar el impacto en la Entidad debido a la explotación de las vulnerabilidades asociadas a los activos de información.

3.2. Documentar y aplicar los controles y procedimientos necesarios para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información.

3.3. Cumplir con los lineamientos establecidos por el gobierno nacional y su estrategia; Gobierno Digital y Transparencia de la Información.

4. JUSTIFICACIÓN

En los últimos años, las entidades públicas tienden a mejorar la eficiencia, efectividad y eficacia de su gestión a partir de la reducción de costos por diferentes

medios y buscando siempre la mejora del aprovechamiento de sus recursos, para lo cual buscan: optimizar sus procesos misionales, revisar y actualizar políticas de adquisición en la Entidad, automatizar los procesos manuales, dinamizar la integración de los procedimientos de su sistema integrado de gestión, entre otros.

En la actualidad, la seguridad de la información es una de las preocupaciones más grandes que puede llegar a tener una Entidad, ya que se debe a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado, la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para toda organización y en consecuencia necesita ser protegido adecuadamente. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Hoy en día las empresas que manejen sistemas de información han generado la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno en Línea, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y los servicios tecnológicos de la Contraloría Departamental del Valle del Cauca, se hace necesario articular diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

El Plan de Seguridad Informática debe constituirse como una línea de mando sobre la cual se establezcan los parámetros a seguir para garantizar su principal objetivo.

Dando aplicación a la normatividad y a las exigencias que en esta materia establece el Gobierno Nacional.

5. ALCANCE

El Plan de Seguridad Informática, contempla toda la información almacenada, procesada y transmitida en medios electrónicos, los lineamentos establecidos en este documento deben ser conocidos y cumplidos tanto por funcionarios de planta como por los contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la Contraloría Departamental del Valle del Cauca, y por quienes hagan uso de los servicios tecnológicos de la Entidad.

6. DEFINICIONES

Para los efectos del presente documento, se adoptarán las siguientes definiciones:

- **Acceso físico:** La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.
- **Acceso lógico:** Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.
- **Activos de Información:** Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.
- **Aplicaciones o aplicativos:** Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse,

aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

- **Cableado estructurado:** Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.
- **Cifrado de datos:** Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.
- **Configuración Lógica:** conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.
- **Copia de respaldo o backup:** Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.
- **Contenido:** Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.
- **Contraseñas:** Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.
- **Correo electrónico institucional:** Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentra alojado en un hosting de propiedad de la Entidad.
- **Cuenta de acceso:** Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una

contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

- **Dispositivos/Periféricos:** Aparatos auxiliares e independientes conectados al computador o la red.
- **Dominio:** Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.
- **Espacio en disco duro:** Capacidad de almacenamiento de datos en la unidad de disco duro.
- **Herramientas ofimáticas**: Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas. En la Contraloría Municipal de Tuluá se hace uso de la Herramienta Microsoft Office.
- **Información confidencial:** Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.
- **Información/Documento electrónico:** Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Licencia de uso:** Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede

otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.

- **Mantenimiento lógico preventivo:** Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.
- **Mantenimiento físico preventivo:** Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.
- **Medios de almacenamiento extraíble:** Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).
- **Plataforma web:** Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.
- **Propiedad intelectual:** Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.
- **Recurso informático:** Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.
- **Red de datos:** Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

- **Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.
- **Servicio informático:** Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.
- **Servidor:** Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando.
- **Sistema de información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
- **Software antivirus:** Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.
- **Software de gestión:** Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado de los proceso del negocio.
- **Software malicioso:** Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

- **Tráfico de red:** Es la cantidad de datos enviados y recibidos por los usuarios de la red.
- **UPS:** Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

7. MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

7.1. Aplicación

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC de todo el personal comprometido en el uso de los servicios informáticos de la Entidad.

El presente manual se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de la Contraloría Departamental del Valle del Cauca. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, por ende minimizando los riesgos en el uso de las tecnologías de información.

7.2. Evaluación de las Políticas

Las políticas tendrán una revisión periódica, se recomienda que sea anual para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias. Las políticas y estándares de seguridad informática establecidas en

el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de la Entidad.

7.3. Seguridad Institucional

Todo el personal usuario de la infraestructura tecnológica de la Contraloría Departamental del Valle del Cauca debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente Manual de Políticas y Estándares de Seguridad Informática para usuarios.

7.4. Capacitación en Seguridad Informática

Todo servidor o funcionario nuevo en la Contraloría Departamental del Valle del Cauca deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento. Dicha capacitación se impartirá en la jornada de inducción y reinducción institucional.

7.5. Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática establecidos por la Contraloría Departamental del Valle del Cauca.

7.6. Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información

reservada o confidencial de cualquier dependencia, o de que se le declare culpable de un delito informático

7.7. Marco Legal

- **Ley 23 de 1982:** “Derechos de autor”.
- **Ley 87 de 1993:** “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones”.
- **Ley 527 de 1999:** “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- **Ley 594 de 2000:** “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
- **Ley 1266 de 2008**: “Por medio del cual se dictan disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos.
- **Ley 1273 de 2009:** “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- **Ley 1341 de 2009:** “Por la cual se definen principios y conceptos sobre la sociedad de la información y las tecnologías de la información y las telecomunicaciones TIC.
- **Ley 1437 de 2011:** “Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.

- **Ley 1581 de 2012:** “Por la cual se dictan disposiciones generales para la protección de datos personales”. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante Tratamiento) por parte de entidades de naturaleza pública y privada.
- **Decreto 2609 de 2012:** “Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado”.
- **Resolución CRC No 3153 de 2013:** Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI.
- **Decreto 2573 de 2014:** “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.

7.8. Políticas Generales de Seguridad Física

7.8.1. Se destinará un área en la Enditad que servirá como centro de telecomunicaciones en el cual se ubicarán los sistemas de telecomunicaciones y servidores, debidamente protegidos con la infraestructura apropiada, de manera que se restrinja el acceso directo a usuarios no autorizados.

7.8.2. El centro de telecomunicaciones deberá contar con control de temperatura (aire acondicionado) permanente a una temperatura no superior a 18 grados centígrados, así como sistema eléctrico de respaldo (UPS).

7.8.3. Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

7.8.4. Los equipos que hacen parte de la infraestructura tecnológica de la Contraloría Departamental del Valle del Cauca, tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, etc.

7.8.5. La sala o cuarto de servidores, deberá estar separada del área del grupo de sistemas o cualquier otra área o en su defecto mantener una división, esta sala deberá ser utilizada únicamente por servidores que presten servicios informáticos a la Contraloría Departamental del Valle del Cauca.

7.8.6. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica y, proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

7.8.7. La Subdirección Técnica de Informática de la Contraloría Departamental del Valle del Cauca diseñará la red de cableado estructurado de acuerdo con las necesidades institucionales y conforme a la normativa establecida.

7.8.8. La Contraloría Departamental del Valle del Cauca debe contar con un plan de mantenimiento preventivo y correctivo para los equipos de cómputo de su propiedad, incluyendo los servidores, dispositivos de red, eléctrico y seguridad.

7.8.9. Los usuarios de equipos de cómputo que manipulen información crítica, deberán evitar la utilización de medios de almacenamiento externo y que puedan facilitar la pérdida de dicha información.

7.8.10. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

7.9. Políticas Orientadas a los Usuarios Internos

7.9.1. Todo funcionario de planta o contratista que inicie labores en la Contraloría Departamental del Valle del Cauca, relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en las Políticas de Seguridad Informática.

7.9.2. Los funcionarios que se desvinculen y los contratistas que culminen su vínculo contractual con la Contraloría Departamental del Valle del Cauca, deberán hacer entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para expedición de paz y salvo y/o liquidación de contrato.

7.9.3. Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la Contraloría Departamental del Valle del Cauca, por lo tanto no se hará divulgación ni extracción de la misma sin previa autorización de las directivas de la Entidad.

7.9.4. No se realizará por parte de los funcionarios o contratistas copia no autorizada de información electrónica confidencial y software de propiedad de la Contraloría Departamental del Valle del Cauca. El retiro de información electrónica

perteneciente a la Entidad clasificada como confidencial, se hará única y exclusivamente con la autorización del directivo competente.

7.9.5. Ningún funcionario o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

7.9.6. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

7.9.7. Las violaciones de las Políticas para la Seguridad de la Información, serán sancionadas conforme a la Ley 734 del 5 de febrero de 2002 y en especial el artículo 34 numerales 2, 3, 4, 5 y 10, y las normas que lo modifiquen.

7.9.8. El personal de la Contraloría Departamental del Valle del Cauca tiene totalmente prohibido la intervención física sobre los dispositivos que intervienen en la red institucional; cuando surja un inconveniente o necesidad se debe actuar conforme al procedimiento de soporte técnico y funcional y poner la respectiva solicitud por correo electrónico.

7.9.9. El usuario es responsable por la custodia y manejo de los computadores, impresoras u otros equipos que se encuentran asignados a su cargo, y su responsabilidad será determinada mediante un proceso disciplinario siendo extendida a los daños ocasionados a estos dispositivos por uso indebido, siempre que los daños se deban a negligencia o descuido en la operación.

7.9.10. La instalación, mantenimiento, adecuación y modificación del hardware y software instalado en los puestos de trabajo de la Contraloría Departamental del

Valle del Cauca, será permitida solo a los funcionarios del grupo de sistemas autorizados para tal fin, previa asignación o traslado.

7.9.11. La utilización del servicio de Internet está permitido para asuntos institucionales. Se restringirá el acceso a aquellos sitios de streaming y demás que demanden un alto consumo de ancho de banda, además de aquellos que se consideren peligrosos por contenidos relacionados con virus y demás. Se excluyen las solicitudes de visualización de contenidos para la labor institucional.

7.9.12. Los contratistas que por su objeto contractual deban ingresar sus equipos de cómputo u otros equipos tecnológicos a las dependencias de la Contraloría Departamental del Valle del Cauca, deben acogerse a las políticas de seguridad dispuestas por la Entidad.

7.9.13. Es responsabilidad de cada empleado apagar los equipos de oficina que estén a su cargo, al finalizar la jornada diaria de trabajo.

7.9.14. Todos los funcionarios y contratistas de la Contraloría Departamental del Valle del Cauca debe contar y portar con su respectiva identificación o carné corporativo en donde se detalla su nombre, cédula, tipo de vinculación y su fotografía.

7.10. Hardware y Software:

7.10.1. La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del área de la Subdirección Técnica de Informática.

7.10.2. Ningún funcionario podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

7.10.3. No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de la Contraloría Departamental del Valle del Cauca, para actividades que no estén relacionadas con las labores propias de La Entidad.

7.11. Mantenimiento de Equipos de Cómputo

7.11.1. Únicamente el personal autorizado por la Subdirección Técnica de Informática, podrá llevar a cabo los servicios y reparaciones a los equipos informáticos.

7.11.2. Los funcionarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la perdida involuntaria de información, derivada del proceso de reparación.

7.12. Pérdida de Equipos de Cómputo

7.12.1. El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

7.12.2. El préstamo de portátiles, proyectores, escáners, cámaras fotográfica, videocámaras u otro equipo informático, tendrá que solicitarse a la Subdirección Técnica de Informática o dependencia que los tenga asignados.

7.12.3. El servidor o funcionario deberán dar aviso inmediato a la Subdirección Técnica de Informática, y a la Dirección de Gestión Humana de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

7.13. Correo Electrónico

7.13.1. El correo electrónico institucional es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de la Contraloría Departamental del Valle del Cauca, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en la Entidad.

7.13.2. La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de la Contraloría Departamental del Valle del Cauca.

7.13.3. Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

7.13.4. Es responsabilidad del funcionario o contratista depurar su cuenta de correo periódicamente, en todo caso se debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

7.14. Internet

7.14.1. No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades de la Entidad.

7.14.2. El Servicio de internet de la Contraloría Departamental del Valle del Cauca no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Entidad. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

7.14.3. No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Contraloría Departamental del Valle del Cauca o de las personas.

7.14.4. La Contraloría Departamental del Valle del Cauca se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de internet de la Entidad.

7.15. Cuentas de Acceso

7.15.1. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada funcionario y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la Contraloría Departamental del Valle del Cauca.

7.15.2. Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.

7.15.3. La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínimo cada 6 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

7.15.4. Todo funcionario o contratista que se retire de la Entidad de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de la claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

7.16. Seguridad Física

7.16.1. Es responsabilidad de los funcionarios y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la Entidad única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la Contraloría Departamental del Valle del Cauca. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normatividad para tal fin.

7.16.2. Los funcionarios y contratistas deberán reportar de forma inmediata a la Subdirección Técnica de Informática la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros.

Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

7.16.3. Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas que puedan afectar su óptimo desempeño.

7.17. Derechos de Autor

7.17.1. Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

7.17.2. Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Contraloría Departamental del Valle del Cauca, que no esté autorizado por la Subdirección Técnica de Informática.

7.17.3. El control de manejo para las licencias y el inventario de los medios, paquete de CD's, medios virtuales, será responsabilidad de la Subdirección Técnica de Informática.

7.18. Uso de Unidades de Almacenamiento Extraíbles

7.18.1. Los funcionarios y contratistas que tengan información de propiedad de la Contraloría Departamental del Valle del Cauca en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

7.18.2. Toda información que provenga de un archivo externo de la Entidad o que deba ser utilizada tiene que ser analizado con el antivirus institucional vigente.

7.18.3. El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

7.18.4. El servidor o funcionario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.

7.19. Clasificación de la Información

7.19.1. Los documentos electrónicos resultantes de los procesos misionales y de apoyo de la Contraloría Departamental del Valle del Cauca, se tratarán conforme a los lineamientos y parámetros establecidos en el sistema de gestión documental de la Entidad. Los activos de información asociados a cada sistema de información, serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes.

7.20. Personal de sistemas

7.20.1. El control de los equipos tecnológicos deberá estar bajo la responsabilidad de la Subdirección Técnica de Informática, así como la asignación de usuarios y la ubicación física.

7.20.2. La Subdirección Técnica de Informática será la encargada de llevar el control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

7.20.3. La Subdirección Técnica de Informática será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

7.20.4. Las licencias de uso de software estarán bajo custodia de la Subdirección Técnica de Informática. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

7.20.5. El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y contraseña. La Subdirección Técnica de Informática será la encargada de crear y asignar las cuentas de acceso y sus permisos a dominio de red, sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

7.20.6. Todos los equipos de la entidad deben tener instalado un antivirus, en funcionamiento, actualizado y debidamente licenciado.

7.20.7. Se realizará mantenimiento a los equipos de cómputo mínimo una vez al año, de acuerdo a la vida útil de los equipos y a la disponibilidad presupuestal de la entidad. La Subdirección Técnica de Informática deberá elaborar el plan y cronograma de mantenimientos, el cual será notificado a los usuarios, adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos e información.

8. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

La Subdirección Técnica de Informática tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, instalaciones de computo, así como de bancos de datos de información automatizada en general.

8.1. Cláusulas de Cumplimiento

8.1.1. La Subdirección Técnica de Informática realizará acciones de verificación del cumplimiento de este Manual de Políticas y Estándares de Seguridad Informática.

8.1.2. La Subdirección Técnica de Informática podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan.

8.1.3. Los directivos y responsables de los procesos establecidos en la Contraloría Departamental del Valle del Cauca, deben apoyar las revisiones del cumplimiento de los sistemas de las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

9. VIOLACIONES DE SEGURIDAD INFORMÁTICA

9.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

9.2. Ningún usuario o funcionario de la Contraloría Departamental del Valle del Cauca debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por la Subdirección Técnica de Informática.

9.3. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la Contraloría Departamental del Valle del Cauca.