

# CORPORACION AUTONOMA REGIONAL DEL CAUCA

## RESOLUCIÓN No.

( )

Por la cual se establece **PLAN ESTRATÉGICO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN PETIC** para la Corporación Autónoma Regional del Cauca.

EL DIRECTOR GENERAL DE LA CORPORACION AUTONOMA REGIONAL DEL CAUCA C.R.C, en el ejercicio de sus facultades estatutarias y legales y

### **CONSIDERANDO:**

Las estructuras sociales y la economía de todas los países han venido transformándose en el transcurso del tiempo, incorporando una manera de ver el mundo distinto a como la percibían los anteriores profesionales, se ha pasado del paradigma de la sociedad industrial a la del conocimiento.

La riqueza y la capacidad de supervivencia de las naciones en el mundo actual ya no dependen de la cantidad de recursos naturales, ni del acopio de información, sino de su capacidad para contar con capital humano suficiente y con la educación adecuada para discriminar y seleccionar lo relevante de la información disponible y agregarle valor, innovándola, mejorándola, o creando nuevas técnicas, productos y servicios.

La Corporación Autónoma Regional del Cauca CRC no puede estar a espaldas de estos cambios, el funcionamiento de esta entidad se realiza de forma similar al cualquier organización, por eso la importancia de poseer estrategias para creación y manipulación de información y conocimiento.

La CRC cumple un papel importante en el medio ambiente colombiano, es por eso que esta entidad debe funcionar por medio de las mejores practicas, nacionales e internacionales. Para ello, la tecnología es imprescindible en la operatividad de la organización, las tecnologías de la información y comunicación (TIC's), brindan la rapidez, facilidad y confiabilidad a la información además de realizar procedimientos que para las personas llegan a ser complejas y demoradas, reduciendo la eficiencia de la entidad.

A medida que la Corporación se ha vuelto cada vez más dependiente de las computadoras y las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de los grupos de trabajo de la entidad necesitan un nivel alto de disponibilidad y algunos requieren incluso un nivel continuo, ya que resultaría extremadamente difícil funcionar sin los recursos informáticos. Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo.

Para garantizar que la entidad pueda cumplir de manera oportuna y eficiente su papel de regular el mercado, facilitar la competitividad, impulsar la transparencia, la democratización y asegurar el bienestar de los ciudadanos con equidad y sostenibilidad en el largo plazo, debe promover el desarrollo de un entorno adecuado para modernizarse utilizando las nuevas tecnologías de información y comunicación para lograr su propia transformación y ser capaz de gestionar mas eficientemente sus recursos y, mejorar su relación y los servicios que presta a los ciudadanos y las empresas.

Con la implementación del Plan Estratégico de Tecnologías de la Información y Comunicación PETIC, la Corporación Autónoma Regional del Cauca CRC realizara una gran inversión en conocimiento para

la mejora de los recursos tecnológicos que se poseen. Esta mejora en los recursos tanto físicos, humanos, financieros, entre otros, conlleva a la ampliación de los servicios y de la necesidad de que estos se encuentren disponibles para todos los procesos requeridos para una excelente operatividad. Con el objetivo de garantizar la disponibilidad de los servicios y resguardar la información que es vital en una organización, se pretende brindar protección a los equipos de cómputo instalados, todos aquellos equipos que hagan parte de la CRC.

Por otra, al ejecutar el PETIC, se garantizara que los recursos se administraran de la mejor manera, de una forma que genere sinergia en la organización y que para llegar a esto, es necesario un cuestionamiento en los aspectos administrativos y técnicos.

Al contar con PETIC, se asegura que la organización cuente con un organigrama adecuado a las necesidades específicas de esta, garantizando el mejor flujo de información entre los miembros de un grupo de trabajo de Sistemas, Esto hace el PETIC, formular una propuesta de formación del Grupo de trabajo de Sistemas, considerando las necesidades prioritarias de la empresa, teniendo en cuenta que responsabilidades comunes se agrupen en una sola persona y enfatizando que como todo grupo o equipo de trabajo, debe tener un líder, una persona que represente dicho equipo de trabajo ante las directivas de la organización, en este caso un responsable del Área de Sistemas.

En mérito de lo expuesto,

## **RESUELVE:**

### **DE LA ESTRUCTURA DE TRABAJO DEL GRUPO DE SISTEMAS**

**ARTICULO PRIMERO:** Es importante tener en cuenta la ubicación del Grupo de Trabajo de sistemas en la estructura de la organización; al realizar trabajo de soporte a procesos administrativos, el grupo está bajo la dirección de la Subdirección Administrativa.

**PARAGRAFO PRIMERO: MISION** Apoyar y dar solución oportuna, eficiente y con calidad en la Corporación Autónoma Regional del Cauca CRC a los requerimientos de computo relacionado con Hardware, Software, Redes de Comunicaciones y Soporte Técnico, para el normal procesamiento de la Información en todas las áreas o dependencias de la Entidad, facilitando la incorporación y uso eficiente de las Tecnologías de la Información y Comunicación TIC's/I para un optimo funcionamiento de la organización.

**PARAGRAFO SEGUNDO: VISION** Ser una Oficina líder en la administración de las tecnologías de información que sirva de modelo a los demás entes autónomos ambientales del país, incorporando uso y adopción de las tecnologías de información a la vanguardia en el proceso de gestión ambiental y en los procesos administrativos propios de la organización.

**ARTICULO SEGUNDO:** El responsable del Grupo de Trabajo de Sistemas de la Corporación Autónoma Regional del Cauca -CRC, debe evaluar continuamente la existencia de controles adecuados, para cerciorarse de un seguro y eficiente funcionamiento en todo lo relacionado con esta dependencia ante cambios tecnológicos y otros que se puedan presentar; esto incluye la revisión en los siguientes aspectos:

- 1 Estructura del grupo de trabajo de Sistemas
- 2 Administrativos
- 3 Equipos
- 4 Software (Incluyendo los SI que se han desarrollado)
- 5 Copias de seguridad
- 6 Seguridad física
- 7 Seguridad lógica
- 8 Red de Comunicaciones
- 9 Soporte.

**ARTIULO TERCERO:** **Políticas de definición de cargos.** Analizadas las necesidades en su totalidad del grupo de Sistemas de la Corporación Autónoma Regional del Cauca, se definen los cargos así:

- 1 Responsable del Grupo Trabajo de Sistemas
- 2 Administrador de los Sistemas de Información de la corporación y el soporte de estos.
- 3 Administrador de Bases de Datos y copias de seguridad. (Backup)
- 4 Administrador de la red de comunicaciones y servidores (Incluye portal Web)
- 5 DOS (2) Técnico operativo para el mantenimiento Hardware y Software
- 6 Diseñador de aplicaciones

## DE LOS ASPECTOS ADMINISTRATIVOS

**ARTICULO CUARTO:** **Comité de Sistemas.** En este comité se discuten los aspectos relacionados al área de sistemas de la Corporación que tienen que ver con toda la Entidad. El Comité de Sistemas es un órgano de gestión que tiene como objetivo primordial, el establecer, conducir y evaluar las políticas internas para el crecimiento ordenado y evolutivo de la Tecnología de la Información en la Corporación, así como apoyar en la materia a todas las dependencias de la organización.

**PARAGRAFO PRIMERO:** El Comité de Sistemas debe estar conformado por:

Lo presidirá el Jefe de Plantación de la Corporación y hará parte de él los Subdirectores de cada área o sus delegados, el responsable del grupo de trabajo de Sistemas y responsables de programas y/o proyectos que se estén llevando a cabo en el momento de las las sesiones del comité.

**PARAGRAFO SEGUNDO:** Entre las Funciones del Comité esta:

1. Promover el establecimiento de políticas y normas en materia de uso de tecnología de la información en la Corporación según las necesidades de cada Subdirección.
2. Determinar acciones para solucionar las necesidades de servicios y equipos de informática y telecomunicaciones en cada una de las áreas de la corporación.

3. Promover el aprovechamiento de nuevas tecnologías de la información y fomentar la adecuada capacitación de los servidores públicos en materia de informática.
4. Proponer los parámetros que sirvan para determinar el funcionamiento y los requerimientos de servicios de Tecnología de la Información, conforme a la estructura jurídica, orgánica y programática de la Corporación.
5. Proponer medidas de tipo administrativo y jurídico que permitan la coordinación en materia de Tecnología de la Información
6. Fomentar la formulación de un plan de integración y desarrollo de un sistema integral de servicios informáticos, con base en las normas aplicables.
7. Supervisar y evaluar el Plan Estratégico de Tecnologías de la Información y Comunicación de la corporación.
8. Formular sugerencias respecto del presupuesto para la adquisición y contratación de bienes y servicios informáticos;
9. Recomendar el empleo de formularios estandarizados, claros y sencillos para la recolección y captura de información, así como la simplificación y optimización de los procedimientos en cada una de las áreas de la Corporación;
10. Elaborar y expedir su Reglamento Interno.

**ARTICULO QUINTO: Plan de trabajo del Comité.** El Plan Estratégico de TIC`s nos conducirá a desarrollar planes de trabajo detallado de los proyectos donde intervengan el grupo de sistemas. Para el eficiente trabajo del comité se dispone:

- 1 Realizar una (1) sesión ordinaria por mes y sesiones extraordinarias cuando estar se requiera.
- 2 Estas sesiones extraordinarias serán programadas por el jefe de plantación y este mismo notificara a todos los integrantes del comité.
- 3 Los planes o proyectos que se discutan en el comité, deberán estar acompañados por cronogramas de trabajo, presupuestos, personal involucrado en su desarrollo, indicadores y otros factores que se consideren necesario.

## DEL SOFTWARE

**ARTICULO SEXTO: Plataforma tecnológica estándar de trabajo.** Para una mejor armonía entre los sistemas de información, estos deben ser compatibles bajo la Plataforma ORACLE.

**PARAGRAFO PRIMERO: Inventario del software.** Es indispensable llevar un inventario detallado y actualizado del *software* que tiene la Entidad. Esto implica que cada vez que se realice una compra, instalación o desinstalación de software se tenga en cuenta que la plataforma para base de datos es ORACLE y además, debe reflejarse en el inventario. Se debe manejar una relación del software instalado en los equipos vs. licencias adquiridas, donde siempre debe ser igual o superior el número de licencias adquiridas, con respecto al software instalado, esto con el fin de dar cumplimiento a la legislación correspondiente. La persona encargada de llevar el control del inventario software es el Responsable del Grupo de Sistemas. (*Ver Formato Inventario Software*)

**PARAGRAFO SEGUNDO: Legislación del *software*.** La legislación de derechos de autor en Colombia está respaldada por la ley 23/1982 y ley 603/2000. Esta legislación convierte e ilícita la copia de los programas sin el consentimiento de los titulares de los derechos de autor, con excepción de la copia de seguridad.

La ley 44/1993 impone multas al que realice copias ilegales de programas de computador.

Para dar cumplimiento a la legalización del *software* se debe tener en cuenta aspectos tales como:

- 2 Asegurar que solo se encuentre instalado *software* legalizado en todos los equipos de la Entidad.
- 3 Asignar a una persona como responsable del inventario del *software* el cual debe siempre estar actualizado, detallando los equipos donde se encuentra instalado.
- 4 Las licencias se deben encontrar inventariadas.
- 5 Prohibir a los usuarios la instalación de *software* en los equipos, dando lugar a sanciones disciplinarias contra el empleado que infrinja dicha disposición.

**PARAGRAFO TERCERO: Manuales.** Para cada aplicación que posea la organización, deben existir manuales de usuario, técnico y de procedimientos para la administración de los mismos. Dichos manuales deben estar completos y actualizados. Los manuales brindan la información esencial para la solución de fallas hardware y software. Al igual que las licencias e inventario software, se deben resguardar en un lugar seguro, siendo el responsable del grupo de sistemas el encargado de dicha labor.

**PARAGRAFO CUARTO: Registro de fallas en el *software*.** Llevar por cada aplicación (especialmente las más críticas para el funcionamiento de la Entidad), un registro de las fallas que se presentan, documentando la solución dada y la persona que dio la solución. Debe diligenciarse el formato de fallas al igual que las fallas Hardware (*FORMATO DISPONIBLE EN LA INTRANET*).

**PARAGRAFO QUINTO: Políticas de Adquisición o desarrollo de *software*.** Los sistemas operativos, las herramientas de desarrollo, los manejadores de bases de datos, los paquetes ofimáticos o cualquier otra herramienta de software que permita capturar, manipular y procesar datos, tienen como característica particular el que su adquisición está sujeta a un amplio conjunto de variables que involucran al desarrollador de sistemas, al analista de sistemas, al usuario final y a la estructura de procesos afectados por tales herramientas.

A diferencia de otro tipo de bienes que adquieren las organizaciones, la adquisición de software se asemeja mucho más a la adquisición de bienes con alto contenido intelectual. El software está sujeto a las leyes de propiedad intelectual o derechos de autor.

Además, la adquisición de un producto de software casi nunca finaliza. Aparecen nuevas versiones que contienen mejoras a la anterior y en muchos casos nuevas herramientas o

utillerías. Para el caso del software adaptado o desarrollado a la medida, nunca se alcanza un producto final pues constantemente se hacen variaciones de forma o de fondo, a solicitud de los usuarios o por cambios en los procedimientos de la Organización.

Todo lo anterior se refleja obviamente en grandes inversiones iniciales y costos fijos en muchos casos difíciles de manejar.

Debe por lo tanto implementarse una política clara y amplia a seguir para la adquisición y desarrollo de herramientas de Software para la Corporación. Esta política se describe a continuación:

1. La adquisición y desarrollo de herramientas de software se harán de acuerdo a las metas programadas en el Plan Operativo de la Corporación.
2. Todo software o sistema operativo que se quiera adquirir debe ser compatible con la plataforma de trabajo ORACLE.
3. La adquisición y desarrollo de herramientas de software se harán cumpliendo con los requerimientos del plan de compras de la Corporación para cada período.
4. La adquisición de herramientas de software tiene que seguir todos los pasos exigidos por la Ley de contratación que cubre las Corporaciones Autónomas Regionales. (Ley 80 de 1993, decreto 2170 de 2002)
5. La decisión de qué herramienta adquirir no debe ser una decisión unilateral de la oficina de sistemas ni del área usuaria.
6. La consecución, instalación, adecuación y modificación del software instalado en los equipos de la Corporación, será permitida sólo a los funcionarios de la oficina de sistemas autorizados para tal fin y sólo podrán hacerlo con los instaladores originales.
7. El área usuaria y la oficina de sistemas deben hacer un levantamiento de los requerimientos dentro del marco de los procesos y procedimientos propios de las áreas implicadas. El resultado de este proceso será documentado e incluirá el alcance, definición de futuras etapas y análisis de costos del proyecto. Además la oficina de sistemas llevará una estadística del software de la Corporación.
8. Para la adquisición o desarrollo de herramientas hechas a la medida o adaptadas a las necesidades de la Corporación, ellas deben ajustarse al modelo de datos de la Corporación y a los estándares de desarrollo de la oficina de sistemas que apuntan a que la información sea alimentada de forma colectiva en el sistema de información Corporativo.
9. Para la adquisición de otro tipo de herramientas de software ofrecidas por el mercado informático, los criterios predominantes no pueden ser el precio y la acuciosa necesidad de las áreas usuarias. Aspectos como plataforma multiusuario, capacidad de procesamiento distribuido, escalabilidad, interoperabilidad con el modelo de datos y la plataforma teleinformática de la Corporación, plataforma de desarrollo abierta, desarrollo orientado a objetos con contenido de elementos OLE y herramientas orientadas a entornos WEB, son algunos de los criterios que deben primar al momento de hacer la selección.
10. Las herramientas de software opcionadas deben ser probadas por las áreas usuarias antes de su compra. De no ser posible lo anterior deben ser vistas en operación

donde se encuentren instaladas. El resultado de este proceso será documentado e incluirá cuadros comparativos de los aspectos técnicos básicos y análisis de costos.

11. Todo producto de software debe incluir capacitación para el área usuaria y la oficina de sistemas.
12. Todo producto de software debe especificar el período de garantía, derechos a actualizaciones por nuevas versiones o cambios por ley.
13. La adquisición de los programas fuente de las herramientas de software estará condicionada a la capacidad presupuestal de la Corporación y a las políticas de desarrollo de aplicaciones de la oficina de sistemas.
14. La actualización o adquisición de nuevas versiones estará sujeta a la evaluación de las áreas usuarias y de la oficina de sistemas y deberán estar acordes con las metas del plan operativo de la Corporación.

La Corporación Autónoma Regional del Cauca, trabaja bajo la plataforma ORACLE, por tanto las aplicaciones que se encuentren no deberán crear conflictos funcionales.

Para los procesos administrativos, se trabajara por medio de las versiones de la suite de oficina de Microsoft Office.

Alguna modificación para el software estándar de trabajo, debe ser discutida y analizada por el grupo de Sistemas y el comité de sistemas, para determinar cual es la opción más favorable para la organización.

Hay que resaltar que ORACLE es la plataforma de trabajo y no un software en específico que pueda ser cambiado.

**ARTICULO SEPTIMO: Políticas de seguridad, uso y administración del software:** A continuación se describen los aspectos que se incluyen en las políticas de seguridad, uso y administración del *software*:

El software está regulado por las leyes de derecho de autor de cada país. Para el caso de Colombia la ley que regula los derechos de propiedad del software es la Ley No 44 de derechos de autor. El hecho de no cumplir con tales disposiciones acarrea sanciones graves tales como multas y cárcel para el representante Legal y encargados de la administración del software en las Organizaciones.

Con el ánimo de hacer una mejor administración de los recursos de software de la Corporación y con el fin de garantizar que lo requerido por la Ley No 44 de 1993 se cumpla, la siguiente política de manejo de software ha sido elaborada:

1. El *software* adquirido de terceros por la Entidad debe estar amparado por las respectivas licencias de funcionamiento y debe contener la documentación técnica y operativa necesaria para permitir su operación y mantenimiento o la capacitación respectiva sobre el manejo del mismo.
2. Los sistemas operativos, herramientas de desarrollo, manejadores de bases de datos, paquetes ofimáticos u otra herramienta de software que se encuentre instalada en cualquier microcomputador, servidor o cualquier otro tipo de equipo teleinformático, deben cumplir con todos los requerimientos de la Ley No 44 de 1993

- o aquellas que la deroguen. Será obligación de los funcionarios de la Corporación conocer lo establecido en la Ley 44 de 1993.
3. Todo el software con que cuenta la Corporación y sus respectivas licencias, serán salvaguardados por la oficina de sistemas, para ello se coordinará con la subdirección administrativa la entrega y recibido a satisfacción de cada una de ellas.
  4. La copia, venta, distribución de *software* y manuales de *software*, están estrictamente prohibidas y puede dar lugar a sanciones disciplinarias contra el empleado que infrinja esta disposición.
  5. El *software* que sea prioridad exclusiva de la Entidad, desarrollado o adquirido, no puede ser reproducido ni utilizado por terceros, bajo ningún pretexto. Solo se puede hacer copia de dicho *software* para copias de seguridad y para uso exclusivo de la Entidad.
  6. Cuando un equipo es retirado de la Entidad con autorización el usuario que retira el equipo se compromete a no sacar copias del *software* instalado en el equipo, para uso personal o de terceros.
  7. Todos los disquetes o medios de almacenamiento que se utilizan deben pasar primero por el antivirus, el cual es definido por el Área de Sistemas
  8. El desarrollo de *software*, al igual que la selección, evaluación y adquisición de nuevos productos debe acogerse al procedimiento y normas establecidas por la Entidad.
  9. Los usuarios no pueden copiar en sus equipos *software* bajado de Internet, así sea de uso gratuito, esto debido al gran riesgo de contagio de virus. Si el usuario requiere de un determinado *software* debe hacer la solicitud al Área de Sistemas.

## DE LAS COPIAS DE SEGURIDAD O BACKUP

**ARTICULO OCTAVO: Contenido de Copias.** Las copias de se deben hacer completas, incluyendo todo lo que necesita la aplicación para poder responder ante cualquier contingencia:

- 1 Datos
- 2 Programas fuente
- 3 Programas objeto (ejecutables)

**PARAGRAFO PRIMERO: Periodicidad.** La Entidad debe realizar como mínimo una copia de respaldo semanal, periodo que dependerá del flujo de la información de ésta; adicionalmente se recomienda mensualmente hacer una copia de respaldo completa para ser guardada en un lugar externo a la oficina del grupo de Sistemas.

Hay que tener en cuenta la rotación de los medios magnéticos de acuerdo al método utilizado (Incremental, diferencial o total). Esto con el fin de tener varias alternativas en caso de necesitar recuperar información y el medio magnético donde se ha realizado la copia haya sufrido un daño o pérdida.

**PARAGRAFO SEGUNDO: Responsabilidad.** En el Grupo de sistemas, la persona asignada para la ejecución y custodia de las copias de respaldo de los datos y programas almacenados en los equipos servidores que posee la Entidad. es el administrador de la base de datos.

**PARAGRAFO TERCERO: Almacenamiento.** Los medios magnéticos utilizados para el respaldo deben ser guardados en la caja fuerte dispuesta por la dirección de la Corporación junto con el Grupo de Sistemas, en el centro de documentación, donde se tengan las seguridades apropiadas tales como:

- 1 Acceso restringido
- 2 Controles de humedad, humo y temperatura (Cuarto Frio)
- 3 Condiciones de limpieza e iluminación del lugar
- 4 Existencia de extintor con fecha vigente

Es importante tener en cuenta los anteriores aspectos de seguridad para el lugar donde se guardan las copias de respaldo tanto internas como externas.

Las copias de respaldo internas no se deben guardar en el sitio de trabajo del grupo de sistemas. Esto con el fin de disminuir el riesgo de daño, en caso de ocurrencia de un siniestro en el mismo.

## **ARTICULO NOVENO: Procedimiento para la realización de las copias de respaldo.**

**PARAGRAFO PRIMERO: Objetivo** Contar con una copia de respaldo de toda la información importante para la Corporación, para así evitar la pérdida de información en caso de suceder algún percance o siniestro.

**PARAGRAFO SEGUNDO: Proceso** Backup de las Bases de Datos en ORACLE , consiste en realizar una copia de seguridad de todas las Bases de Datos de la Corporación.

1. La configuración del Servidor de Base de Datos Oracle, nos garantiza en nuestro servidor la seguridad de recuperar información en caso de alguna eventualidad o siniestro hasta 1 minuto antes de sucedido, aun si no se hubiera hecho un backup hace un mes.
2. Todo Backup se realizará en Tapes (Cintas de almacenamiento) y de manera automática para lo cual se ha programado en lenguaje Host del Oracle Script que realizan estos procedimientos como tareas programadas, el administrador de la base de datos solo debe recordar poner los Tapes respectivos.
3. De Lunes a Jueves se realizará un Export Full Database y el Viernes se realizará un Export Full Database por duplicado de los cuales uno será almacenado en el área de trabajo del Grupo de Sistemas y otro se enviará a una Bóveda de Backups externa ubicado donde lo considere la Subdirección Administrativa. El Export Full Database respalda la información de todas las transacciones realizadas, este sirve para hacer recuperaciones parciales.
4. El ultimo día del mes se realizará un Backup Completo de la Base de Datos por duplicado (un consolidado del mes), el cual reemplazará a los backups del mes correspondiente, uno de

ellos será almacenado en el área de trabajo del Grupo de Sistemas y otro se enviará a una Bóveda de Backups externa ubicado donde lo considere la Subdirección Administrativa. El Backup Completo de la Base de Datos respalda la estructura y las transacciones de la Base de Datos, en caso de pérdida obtendríamos la recuperación total de la Base de Datos.

5. Los tapes son reemplazados en su totalidad cada 3 meses aproximadamente para asegurar que los respaldos realizados sean confiables

## DE LOS EQUIPOS

**ARTICULO DECIMO:** **Inventario de equipos.** Se debe contar con un inventario detallado y actualizado de los equipos de computo pertenecientes al Área de sistemas (servidores, PC's, impresoras, Scanner etc.).

El inventario contiene aspectos (Ver Formato Inventario de Equipos) como:

- 1 Código del equipo.
- 2 Descripción detallada de la configuración del equipo.
- 3 Responsable del equipo.
- 4 Ubicación Especifica (Área, SubArea, Oficina ).
- 5 Fecha de compra.
- 6 Proveedor.
- 7 Tiempo de la garantía.
- 8 Software instalado en el equipo.

**ARTICULO DECIMO PRIMERO:** **Procedimientos para comunicar fallas en los equipos.** Es importante que cuando los usuarios necesiten comunicar un problema presentado en su equipo, se cuente con un procedimiento formal que para el caso sería el uso de la aplicación ya existente en la entidad, discriminando si dicho problema es físico o lógico para dar un servicio oportuno y eficiente a los usuarios.

La solicitud contiene la siguiente información Ver Formato Reporte de Fallas):

Código del equipo

- 1 Persona que detectó el problema
- 2 Fecha y hora
- 3 Problema detectado
- 4 Solución dada
- 5 Persona que solucionó el problema
- 6 Fecha y hora en que se solucionó el problema

Este informe de fallas debe ser entregado al responsable del Grupo de sistemas o algún integrante del mismo para que se asigne una persona que realice la reparación.

**ARTICULO DECIMO SEGUNDO: Procedimiento para la instalación y configuración de equipos.** La instalación, adecuación y modificación del hardware instalado en los puestos de trabajo de la Corporación, será permitida sólo a los funcionarios del grupo de sistemas autorizados para tal fin.

Los funcionarios del grupo de sistemas autorizados para la instalación, adecuación y modificación del hardware llevarán un registro riguroso de las instalaciones y modificaciones realizadas.

Proceso para instalación o modificación del Hardware y Software

1. Requerimientos del cargo al cual el equipo va brindar soporte informático.
2. Análisis de requerimientos por parte del responsable de la red de comunicaciones.
3. Verificaciones de licencias vigentes para el software que se va a instalar en el o los equipos.
4. Verificación de existencia y óptimo estado de componentes hardware para cumplir los requerimientos solicitados.
5. Instalación de los componentes software y hardware.

En el caso de no contar con los componentes lógicos o físicos necesarios para el óptimo funcionamiento de los equipos, se debe informar de forma escrita al responsable del grupo de sistemas para que este a su vez, informe al área de adquisiciones.

Los registros que se realicen para llevar el control de instalación y modificación de la configuración hardware y software son: (Ver Formato de Mantenimiento):

- 1 Software o hardware antiguo.
- 2 Software o Hardware actual.
- 3 Observaciones de por qué el cambio (fallas u optimización).

**ARTICULO DECIMO TERCERO: Bitácora para cada uno de los servidores.** Se debe llevar una bitácora por cada servidor, donde se registren las actividades realizadas y los problemas presentados, persona que realizó la actividad, fecha y hora. En caso de alguna falla se debe documentar la solución.

Lo anterior garantiza que se genere un repositorio de fallas junto con su respectiva solución que a futuro agilice la solución de problemas.

**ARTICULO DECIMO CUARTO: Procedimiento para el retiro de los equipos.** Siempre que se requiera retirar de la entidad un equipo de cómputo, debe diligenciarse una orden de salida, la cual debe ir firmada por el almacenista de la Corporación. La persona que retira el equipo, debe responsabilizarse del buen uso y manejo del mismo, comprometiéndose a no instalar software ni realizar copias de los programas y datos que se encuentran en el equipo al igual que entregar el equipo en las mismas condiciones con las que fue retirado.

**PARAGRAFO PRIMERO: Documentación.** Mantener una copia del software y los manuales de operación de los equipos de cómputo, manuales técnicos, manuales de usuario etc. Estos manuales y software deben ser inventariados y estar bajo la responsabilidad y custodia del Grupo de Sistemas en cabeza del responsable del grupo, el cual llevará un control correspondiente sobre las entradas y salidas.

Es importante que todos los procesos de manipulación de los equipos de cómputo, sean documentados para evidenciar el trabajo que se hizo en estos y para el control y la solución de conflictos similares en el futuro.

En el caso de solución de problemas debe dejar registro de:

- 1 Problema presentado.
- 2 Análisis de conclusión de por que se presenta el fallo
- 3 Procedimiento de solución.

Con esto se da la posibilidad de resolver problemas más rápido en un futuro.

**PARAGRAFO SEGUNDO: Estándares de Desempeño.** Existencia y evaluación de los estándares de desempeño, tales como tiempo de respuesta, velocidad, volúmenes de información, etc.

Estos indicadores son analizados por todos los integrantes del Grupo de sistemas con la coordinación del responsable del Grupo.

**PARAGRAFO TERCERO: Mantenimiento de Equipos.** Las políticas de mantenimiento de equipos se realiza con el fin de garantizar su óptimo funcionamiento especialmente en los servidores, equipos de comunicaciones y aquellos otros equipos, por ejemplo, computadores e impresoras que sean de criticidad alta cuenten con un mantenimiento preventivo, correctivo y predictivo. Se debe verificar que dichos mantenimientos sean oportunos y de buena calidad: además, contar con un cronograma anual de los mantenimientos preventivos planeados para el control y monitoreo del mantenimiento a cualquier equipo se debe diligenciar el formato de mantenimiento

Los objetivos del mantenimiento son:

- 1 Evitar, reducir, y en su caso, reparar, las fallas sobre los bienes precitados.
- 2 Disminuir la gravedad de las fallas que no se lleguen a evitar.
- 3 Evitar detenciones inútiles o para de máquinas.
- 4 Evitar accidentes.
- 5 Evitar incidentes y aumentar la seguridad para las personas.
- 6 Conservar los bienes productivos en condiciones seguras y preestablecidas de operación.
- 7 Balancear el costo de mantenimiento con el correspondiente al lucro cesante.
- 8 Alcanzar o prolongar la vida útil de los bienes.

**PARAGRAFO CUARTO: Políticas de uso de los equipos informáticos.**

A continuación se describen las políticas con respecto a los equipos de cómputo:

1. 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.

2. Es responsabilidad de cada empleado apagar los equipos de oficina que estén a su cargo, al finalizar la jornada diaria de trabajo.
3. El encendido y apagado del equipo servidor es función exclusiva de la Oficina de Sistemas.
4. Los usuarios no deben abrir los computadores, impresoras, reguladores de voltaje u otros equipos de cómputo, para retirar o instalar partes.
5. Es responsabilidad de cada usuario realizar la limpieza exterior de los equipos a su cargo.
6. Los equipos de computación son par uso exclusivo en Oficinas de la Entidad y no deben ser utilizados para beneficio propio o de terceros, sin la debida autorización del jefe de área.
7. El jefe de almacén es el único autorizado para el traslado físico de equipos, tanto interna como externamente.
8. Se prohíbe el consumo de alimentos en zonas de instalación de equipos de cómputo. El equipo dañado por ingerir bebidas o alimentos en la zona de instalación será cobrado al empleado responsable.
9. No se debe colocar elementos tales como plantas, alimentos o líquidos, sobre los equipos ni bloquear sus rejillas de ventilación con papeles u otros objetos.
10. En los multitomas (marcados de color rojo) que provean corriente regulada destinados a alimentar eléctricamente los equipos de cómputo, no deben ser conectados equipos diferentes como calculadoras, ventiladores, aspiradoras, etc.
11. Los equipos de cómputo deben protegerse con cubiertas plásticas especiales al finalizar las labores diarias, para evitar la acumulación de polvo en su interior.
12. Toda operación irregular del hardware debe ser reportada al funcionario encargado para tal fin en la oficina de sistemas.
13. El usuario de cada equipo debe eliminar archivos innecesarios del disco duro para liberar espacio e incrementar la eficiencia en la ejecución de los programas.

## **PARAGRAFO QUINTO: Políticas y criterios de compra de elementos Teleinformaticos**

Este tipo de adquisiciones que nunca culmina es de elementos teleinformáticos, tales como microcomputadores, servidores y equipos de telecomunicaciones entre otros. Al igual que el software, siempre habrá un modelo nuevo, un modelo mejor y más potente; y siempre el usuario deseará tener el último modelo, pues el que tiene ya es demasiado "lento" o no le sirve.

Las inversiones iniciales en hardware son altas y deben ser actualizadas en períodos demasiado cortos que promedian entre los tres y cinco años.

La siguiente es la política que debe seguirse para la adquisición y renovación de los elementos teleinformáticos de la Corporación:

1. La adquisición y renovación de elementos teleinformáticos se hará de acuerdo a lo programado en las metas del Plan Operativo de la Corporación.
2. La adquisición y renovación de elementos teleinformáticos se hará cumpliendo con los requerimientos del plan de compras de la Corporación para cada período.
3. La adquisición y renovación de elementos teleinformáticos tiene que seguir todos los pasos exigidos por la Ley de contratación que cobija las Corporaciones Autónomas Regionales. (Ley 80 de 1993, decreto 2170 de 2002)
4. La decisión de qué elemento adquirir no deberá ser una decisión unilateral de la oficina de sistemas ni del área usuaria.

5. El área usuaria y la oficina de sistemas deben hacer un levantamiento de los requerimientos a nivel de hardware que permitan que las áreas implicadas alcancen los objetivos programados. El resultado de este proceso será documentado e incluirá el alcance, definición de futuras etapas y análisis de costos del proyecto.
6. La adquisición de equipos teleinformáticos debe ajustarse a la infraestructura de hardware y software de la Corporación y a estándares de mercado abiertos.
7. En la adquisición de equipos teleinformáticos ofrecidos por el mercado informático, los criterios predominantes no pueden ser el precio y la acuciosa necesidad de las áreas usuarias. Aspectos como capacidad de procesamiento y de almacenamiento, escalabilidad, interoperabilidad con el modelo de datos de la Corporación, estándares abiertos y gestión remota, son algunos de los criterios que deben primar al momento de hacer la selección.
8. Los equipos teleinformáticos opcionados deben ser probados por las áreas usuarias antes de su compra. De no ser posible lo anterior deben ser vistas en operación donde se encuentren instalados. El resultado de este proceso será documentado e incluirá cuadros comparativos de los aspectos técnicos básicos y análisis de costos.
9. La adquisición de equipos teleinformáticos tales como servidores y equipos de telecomunicaciones deberá incluir la capacitación para los funcionarios de la oficina de sistemas encargados de operarlos.
10. Todo elemento teleinformático debe especificar el período de garantía y las características de los mantenimientos preventivos y correctivos.
11. La actualización o adquisición de nuevos equipos estará sujeta a la evaluación de las áreas usuarias y de la oficina de sistemas y deberán estar acordes con las metas del Plan Operativo de la Corporación.

## **DE LA SEGURIDAD DE LAS CUENTAS**

**ARTICULO DECIMOQUINTO:** 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.

## **ARTICULO DECIMOSEXTO: DESCRIPCION DE LAS POLITICAS PARA LA ELECCION DE CLAVES DE ACCESO**

Una clave de acceso (Contraseña/Password) es un código o una palabra que se utiliza para acceder a datos restringidos de un sistema software o hardware.

Las claves de acceso son la protección más común en contra de accesos no autorizados a cualquier sistema.

Para poder utilizar correctamente las claves de acceso, se definen las siguientes políticas:

1. No colocar como clave de acceso su nombre, apellido o algún otro dato personal o familiar.
2. No utilizar palabras simples, que puedan ser encontradas en un diccionario.
3. No utilizar palabras de otros idiomas.

4. Utilizar combinaciones de letras y números en la clave de acceso.
5. No comentar a nadie su clave de acceso al sistema.
6. La clave debe tener como mínimo 8 caracteres de longitud.
7. Se debe cambiar periódicamente la clave de acceso (máximo 1 mes) utilizando el mismo sistema como base.

**ARTICULO DECIMOSEPTIMO:** Agregándose a las políticas de seguridad se proponen formas de claves de acceso:

- La clave puede poseer tres letras, seguidas de dos números y luego por lo menos otras tres letras.
- La clave puede estar compuesta de 2 números, cuatro letras y luego por lo menos otros dos números.
- La clave puede poseer 2 números y luego por lo menos 6 letras.
- La clave puede ser las primeras letras de una estrofa de su canción favorita sumada a su año de nacimiento.

**PARAGRAFO:** Todos los usuarios bloquearán su teclado cada vez que dejen sin atención su sistema.

## **DEL LICENCIAMIENTO CORPORATIVO**

**ARTICULO DECIMONOVENO :** Los empleados de la Corporación Autónoma Regional del Cauca utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

**ARTICULO VIGÉSIMO :** Para la utilización de programas de licencias de uso libre tipo GNU GPL o similares se debe tener autorización explícita del Área de Sistemas.

**ARTICULO VIGÉSIMO PRIMERO :** Los empleados de la Corporación Autónoma Regional del Cauca no descargarán ni ejecutarán programas informáticos no autorizados a través de Internet.

**ARTICULO VIGÉSIMO SEGUNDO :** Los empleados de la Corporación Autónoma Regional del Cauca que se enteren de cualquier uso inadecuado que se haga en la organización de los programas informáticos o la documentación vinculada a estos, deberán notificar al Área de Sistemas.

**ARTICULO VIGÉSIMO TERCERO :** Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos

pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. La Corporación Autónoma Regional del Cauca no permite la duplicación ilegal de programas informáticos. Los empleados de la Corporación Autónoma Regional del Cauca que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo a las circunstancias.

**ARTICULO VIGÉSIMO CUARTO** : Cualquier duda respecto a si cualquier empleado puede copiar o utilizar un determinado programa informático, debe plantearse al Área de Sistemas.

**ARTICULO VIGÉSIMO QUINTO** : La actualización de sistemas antivirus y actualizaciones de seguridad de los sistemas operativos que buscan la reducción de virus informáticos dentro de la organización deberá ser realizada única y exclusivamente por el personal de sistemas. En los casos en los que el usuario tenga los conocimientos para realizar estas actualizaciones deberá tener la autorización explícita del Área de Sistemas.

**ARTICULO VIGÉSIMO SEXTO** : **Utilización del Antivirus** Se hace prioritario la utilización para cualquier proceso en red (local o Internet) el uso del antivirus. Se debe ejecutar por lo menos una vez por semana a todo el disco duro de su equipo, se recomienda ejecutarlo inmediatamente al llegar a su sitio de trabajo, esto es fácil debido a que los antivirus se pueden configurar para que se ejecuten al iniciar el equipo, además se debe hacer verificaciones de virus en cada disquete que se utilice en su equipo, así sea de su propiedad o de algún origen confiable. Recuerde que si ya ha sido revisado el disco y fue utilizado en otro equipo debe revisarlo nuevamente. No olvide que la actualización de los antivirus es una labor del administrador, pero es su deber como usuario final estar atento a esto.

## DE LA RED CORPORATIVA

**ARTICULO VIGÉSIMO SÉPTIMO** : **Red Local** En ningún caso se podrá abandonar la estación de trabajo dejando abiertas las sesiones de los programas informáticos en los que este trabajando. Debe cerrar la aplicación y cuando regrese deberá entrar al sistema nuevamente digitando su clave de acceso. Para los equipos con Windows 98 se debe colocar el protector de pantalla protegido por contraseña, esta debe ser colocada en el mismo instante que colocó el protector de pantalla y no debe ser igual a las anteriormente utilizadas, debido a que existen programas que logran descifrar la contraseña de los protectores de pantalla y además la de acceso a la red

**ARTICULO VIGÉSIMO OCTAVO** : No compartir carpetas de archivos de su computador. Las carpetas nunca se deben compartir. En caso que sea estrictamente

necesario se deberán compartir las carpetas con autorización del área de sistemas, solo con permisos de lectura e inmediatamente se termine la transferencia del archivo se deberá dejar de compartir la carpeta. Preferiblemente dentro del correo institucional se compartirá la utilidad de MALETIN.

**ARTICULO VIGÉSIMO NOVENO** : Si maneja información confidencial de la Empresa, lo mejor es mantenerla cifrada en su disco duro local con una copia respectiva en el servidor indicado por el Área de Sistemas. Uno de estos productos es el PGP (Pretty Good Privacy). No olvide asegurar su llave privada, si la pierde es probable que su información pueda ser descifrada. En caso de no utilizar el anterior sistema, utilizar la comprensión zip con contraseña y las utilidades de Office (Documentos doc y xls) para restringir y envíe la información al Área de Sistemas con el fin de resguardarla.

**ARTICULO TRIGÉSIMO** : No basta mantener copia de la información cifrada en el servidor o en el equipo que el Área de Sistemas adecue. Recuerde realizar copias de respaldo actualizadas de la información vital que maneje en su disco duro y colocarla en un lugar seguro bajo llave y cifrada.

## DE LA COMUNICACIÓN INSTITUCIONAL

**ARTICULO TRIGÉSIMO PRIMERO** : Utilice el sistema de mensajería instantánea INTRANET, CORREO INSTITUCIONAL solo para asuntos de la organización, no para comunicación personal, envíe de insultos y acosos.

**ARTICULO TRIGÉSIMO SEGUNDO** : La utilización del servicio de Internet solo esta permitido para asuntos institucionales. Procure ser muy efectivo en su navegación, busque exclusivamente lo necesario y al descargar un archivo mayor a 1.5 MB hágalo en horas no laborales o comuníquese con el Área de Sistemas. Recuerde que el uso indiscriminado del Internet puede generar un retardo en el tráfico de la información y producir inconvenientes innecesarios en los procesos de la Corporación Autónoma Regional del Cauca.

**ARTICULO TRIGÉSIMO TERCERO** : Mantener la información de la organización en la misma y no transportarla a otro sitio diferente de ésta. Se corre el riesgo de no tener las mismas precauciones de seguridad en otro sitio y por ende se estará atentando contra la seguridad de toda la Corporación Autónoma Regional del Cauca. La información que necesariamente deben salir de la organización lo deben hacer bajo las mas estrictas medidas de seguridad y se deberá reportar al Área de Sistemas.

**ARTICULO TRIGÉSIMO CUARTO** : Absténgase de instalar programas descargados

de Internet no autorizados por el administrador de la red, usted puede convertirse en el responsable del caos en materia de seguridad para toda la red de la empresa. Estos programas pueden ser troyanos (Son aquellos programas que prometen ser algo y realmente realizan otra cosa que compromete la seguridad del usuario), virus o puertas traseras (Programa que le permite al vándalo informático entrar al sistema que ya ha vulnerado de manera más sencilla y reiterativa) que le dan acceso a los vándalos informáticos para realizar alguna labor concreta.

**ARTICULO TRIGÉSIMO QUINTO** : La utilización de la INTRANET y del CORREO INSTITUCIONAL esta permitido en la organización solo para comunicación de la organización y bajo autorización del Área de Sistemas, por favor absténgase de utilizarlo para conversaciones personales. Las actualizaciones de este software de mensajería instantánea solo están permitidas por el Área de Sistemas.

**ARTICULO TRIGÉSIMO SEXTO** : El uso del sistema de correo electrónico de la Corporación Autónoma Regional del Cauca es para el uso exclusivamente de asuntos relacionados con la empresa. Bajo ninguna circunstancia se deberá utilizar en forma privada o para el beneficio único del trabajador.

**ARTICULO TRIGÉSIMO SÉPTIMO** : El sistema de correo electrónico de la Corporación Autónoma Regional del Cauca cuenta con un sistema antivirus que bloqueará y le avisará a usted como usuario de un equipo cuando el correo que desea ver pueda contener virus o algún tipo de programa peligroso, por favor acate estas disposiciones y no descargue estos correos.

**ARTICULO TRIGÉSIMO OCTAVO** : La Corporación Autónoma Regional del Cauca se reserva el derecho de vigilar o monitorear el uso del sistema de correo electrónico de acuerdo con las leyes y reglamentaciones aplicables, y si se comprueba que existe un uso indebido de éste, se puede estar sujeto a sanciones. El uso indebido del correo electrónico incluye, pero no se limita a:

- Enviar o recibir deliberadamente material pornográfico, indecente u otro material sexual.
- Enviar información confidencial de la Corporación Autónoma Regional del Cauca, o secretos comerciales sin la autorización pertinente.
- Utilizar el correo electrónico para acoso sexual.
- Enviar correo electrónico con insultos.
- Enviar cartas en cadena.
- Enviar correo electrónico vulgar.
- Enviar correo electrónico que incluya discriminación sexual o racial.
- Enviar correo electrónico “basura” (Spam) (Ejemplo: correo no relacionado con el negocio enviado a amplias listas de distribución).

- Enviar correo electrónico religioso o político.
- Utilizar el correo electrónico de la Corporación Autónoma Regional del Cauca para actividades comerciales privadas o publicidad no oficial.
- Enviar todo tipo de correo electrónico que pueda crear responsabilidad alguna para la Corporación Autónoma Regional del Cauca (Ejemplo: uso indebido de sus facultades firmantes, divulgación de información confidencial, secretos comerciales y de negocios, etc.).

**ARTICULO TRIGÉSIMO NOVENO** : Los usuarios no deben enviar correos electrónicos cuando:

- Contiene información que sea comercialmente sensible o contenciosa o que pueda tener otras implicaciones contractuales o legales para la Corporación Autónoma Regional del Cauca, a menos que sea para efectos específicos, autorizados y mediante codificación aprobada.
- Puede dañar la reputación de la Corporación Autónoma Regional del Cauca o su relación con otras entidades, o cuando puede afectar a los socios de la Corporación Autónoma Regional del Cauca.
- Puede infringir derechos de autor y otros derechos de propiedad intelectual.

**ARTICULO CUADRAGÉSIMO** : Usted no debe dirigir ni responder correo electrónico basura, acosador o cartas en cadena, si se recibe este tipo de correos, éstos deben borrarse.

**ARTICULO CUADRAGÉSIMO PRIMERO** : La responsabilidad del uso del correo electrónico es de cada usuario y cualquier inconveniente que surja por el mal uso de este, deberá ser asumido por el usuario.

**ARTICULO CUADRAGÉSIMO SEGUNDO** : Sea consciente que al comunicarse con correo electrónico vía Internet, usted será considerado por los receptores como representante de la Corporación Autónoma Regional del Cauca. Tenga cuidado al comunicarse en todo momento de una manera profesional y cortés.

**ARTICULO CUADRAGÉSIMO TERCERO** : Absténgase de adjuntar archivos muy grandes a su correo electrónico. Los mensajes largos y voluminosos aumentan considerablemente el tráfico de la red, representan mas carga para los recursos tecnológicos y son difíciles de leer. Los anexos deben comprimirse utilizando herramientas como Winzip o equivalentes.

**ARTICULO CUADRAGÉSIMO CUARTO** : Es fácil enviar mal los mensajes, **revise siempre el nombre del receptor antes de hacer el envío de su correo.**

**ARTICULO CUADRAGÉSIMO QUINTO** : Se deben borrar periódicamente los correos viejos del buzón de correo, las copias de correos enviados si ya no los necesita, sobre todo los que tienen archivos adjuntos. Es muy importante no sobrepasar el tamaño de almacenamiento que se le ha asignado a su correo porque esto causa que sus correos dejen de llegar.

**ARTICULO CUADRAGÉSIMO SEXTO** : Proporcione siempre un tema, asunto o subject significativo y acorde para su correo.

**ARTICULO CUADRAGÉSIMO SÉPTIMO** : Revise la claridad y el profesionalismo de su correo.

**ARTICULO CUADRAGÉSIMO OCTAVO** : No utilice el correo para discusiones emocionales, acosadoras, o insultantes.

**ARTICULO CUADRAGÉSIMO NOVENO** : No digite mensajes en letras mayúsculas implica mal genio o que está gritando a la otra persona.

**ARTICULO QUINCUAGÉSIMO** : Utilice las casillas “CC (copia a) y CCO (copia oculta a)” y la opción “Responder a todos” con moderación. Informe sólo a quienes necesitan saberlo. Cada copia creada para una persona crea un mensaje adicional en la red.

**ARTICULO QUINCUAGÉSIMO PRIMERO** : El correo electrónico no debe reemplazar el contacto personal. Existe la tendencia a ser menos formal o cuidadoso lo cual algunas veces genera malestar. Recuerde que el contacto directo persona a persona es lo mejor para manejar asuntos difíciles, complejos o emocionales.

**ARTICULO QUINCUAGÉSIMO SEGUNDO** : Todas las leyes que rigen los derechos de autor, difamación, discriminación y otras formas de comunicación escrita, también se aplican al correo electrónico.

**ARTICULO QUINCUAGÉSIMO TERCERO** : Los correos electrónicos que usted envía pueden reenviarse o imprimirse y distribuirse sin su conocimiento; no asuma que el receptor mantiene confidencialmente su correo.

**ARTICULO QUINCUAGÉSIMO CUARTO** : El correo electrónico es un documento de validez legal y prueba de evidencia de acuerdo a la validez jurídica que le otorga la ley 527 del 1999 a los mensajes de datos digitales. Por consiguiente, tiene el mismo efecto legal que otro medio de correspondencia escrita.

**ARTICULO QUINCUAGÉSIMO QUINTO** : Recuerde revisar con el software antivirus

todos los archivos adjuntos a sus correos y aquellos que descargue de la red.

**ARTICULO QUINCUAGÉSIMO SEXTO :** No abra correos que tengan archivos adjuntos con doble extensión o imágenes jpg muy grandes mayores a 700Kb.

**ARTICULO QUINCUAGÉSIMO SÉPTIMO :** El correo spam se define como correo no deseado, es decir, correo que el usuario no desea recibir como noticias o publicidad indeseada. Se pueden presentar casos en los que un correo electrónico es no deseado para un usuario pero deseado para otros. Por esto se recomienda seguir las siguientes recomendaciones para controlar el spam:

**ARTICULO QUINCUAGÉSIMO OCTAVO :** Utilice la casilla asunto o subject de sus correos adecuadamente, solo ponga frases en español cortas y precisas.

**ARTICULO QUINCUAGÉSIMO NOVENO :** No se suscriba a listas de distribución que no conozca plenamente.

**ARTICULO SEXAGÉSIMO :** Tenga cuidado de donde escribe su correo electrónico, procure no escribirlo en sitios Web que no sean de su confianza.

**ARTICULO SEXAGÉSIMO PRIMERO :** Evite reenviar los correos masivos o los correos que solicitan enviarse a más personas para conceder cosas como deseos. Estos correos están hechos para capturar direcciones de correo electrónico de usuario.

**ARTICULO SEXAGÉSIMO SEGUNDO :** **Vigencia y derogatorias.** La presente resolución rige a partir de su publicación, modifica y deroga todas las disposiciones que le sean contrarias.

**PUBLÍQUESE Y CÚMPLASE**

Dada en Popayán, a los

**JESUS HERNAN GUEVARA**  
Director General CRC

Proyecto dgi