CONTRALORIA
DISTRITAL DE CARTAGENA DE INDIAS

PLAN DE SEGURIDAD

Y PRIVACIDAD DE LA INFORMACION

2019

TABLA DE CONTENIDO

Pág.

INTRODUCCION

La seguridad informática según lo establece la **ISO/IEC 27001** fija las bases para preservar la confidencialidad, integridad y disponibilidad de la información, así como la de los sistemas utilizados para su procesamiento.

El Manual de Políticas para la Seguridad de la Información de la Contraloría Distrital de Cartagena de Indias (Resolución 198 del 14 de octubre del 2014) es el documento oficial necesario para el control y la seguridad en el uso de las tecnologías de información y las comunicaciones.

Todas las acciones y medidas establecidas en el presente Plan de Seguridad y Privacidad de la Información, son de obligatorio cumplimiento para todo el personal que labora en la Contraloría Distrital de Cartagena de Indias ya sean funcionarios públicos o contratistas y que usen las tecnologías de información y las comunicaciones.

La seguridad informática se basa en la preservación de los siguientes principios.

- **Confidencialidad:** La información debe ser accesible solo para las personas autorizadas para autenticarse en los sistemas de información.

- **Integridad:** La información se debe conservar exacta y completa en los sistemas de información.

- **Disponibilidad:** Los usuarios autorizados tienen acceso a la información con todos sus recursos cuando se requiera.

  La definición de estos tres conceptos permite ampliar el espectro para tener una idea más clara de lo que se pretende con el siguiente documento; y es, proteger la infraestructura física y lógica de la Contraloría Distrital de Cartagena de Inidas contra daños que alteren la información contenida en esta infraestructura, e identificar ¿contra qué clase de daños?, ¿Causados por quién? y ¿en dónde?.

Para lograr la protección de la información, existe una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información de la Contraloría Distrital de Cartagena de Indias.

La seguridad informática comprende proteger el software, base de datos, archivos, hardware y todo lo que la Contraloría Distrital de Cartagena de Indias valore como un activo y que significa un riesgo si esta información termina en manos de otras personas.

OBJETIVO

Por medio de este documento, se pretende que la Contraloría Distrital de Cartagena de Indias cuente con los lineamientos que le permitan mantener en óptimas condiciones de funcionamiento de los recursos Tecnológicos (equipos de cómputo, software, información, entre otros) asegurando el control y seguridad de la información. Controlar y soportar los recursos de datos de cómputo, software y hardware en la entidad, buscando una adecuada administración ante amenazas técnicas, físicas, tecnológicas y de inoperancia que las afecte.

ALCANCE

Este documento cubre las acciones que deben adoptar y cumplir todos los funcionarios sin importar su tipo de vinculación y contratistas de la Contraloría Distrital de Cartagena de Indias, para lograr la seguridad de la información en los equipos informáticos al máximo.

CERTIFICACION ISO 27001[1]

¿En qué consiste?

El Sistema General de Seguridad Informática (SGSI) basado en ISO/IEC 27001 permite la gestión y control de los riesgos de la seguridad de la información en las organizaciones para las cuales la información y la tecnología son activos importantes de su negocio.

Mediante las mejores prácticas de seguridad de la información, las organizaciones que certifican su SGSI demuestran ante sus accionistas, clientes, autoridades, proveedores y demás partes interesadas, la debida diligencia en este importante aspecto y garantizan la aplicación adecuada de los recursos en las áreas de mayor impacto potencial, optimizando así sus inversiones y costos de seguridad.

¿A quiénes está dirigida?

- Empresas de servicios.
- Prestadores de servicios
- Empresas del sector de tecnología de la información.
- Empresas de comunicaciones.
- Empresas de seguridad y custodia.
- Entidades públicas.
- Todo tipo de empresas de cualquier sector económico o industrial, públicas o privadas que hagan uso intensivo de la tecnología de la información.

¿Qué beneficios trae su implementación?

- Habilita y potencializa el uso de las más actuales herramientas de colaboración y de gestión de la información, protegiendo el valor de la confidencialidad, la integridad y la disponibilidad de la información para el negocio.

- La implementación del sistema de gestión de seguridad de la información se constituye en una herramienta para la comunicación eficaz entre la alta dirección empresarial, los responsables de la gestión y custodia de la información y los clientes y demás interesados.

- Previene y reduce eficazmente el nivel de riesgo, mediante la implantación de los controles adecuados; de este modo, prepara a la organización ante posibles emergencias y garantiza la continuidad del negocio.

- Permite a la dirección monitorear, evaluar, asignar y gestionar los recursos necesarios para la seguridad de la información.

- Incrementa el nivel de conciencia del personal respecto a los tópicos de seguridad de la información."

1http://www.icontec.org/Ser/EvCon/Paginas/PCS/ci27001.aspx **Icontec Colombia.**

1. USO DE INTERNET, CORREO ELECTRÓNICO Y SERVICIOS INFORMÁTICOS

1.1. SOLICITUD Y AUTORIZACIÓN DE SERVICIOS

Para la asignación de cualquier servicio informático, inicialmente se debe diligenciar el formato de la solicitud del servicio establecido por la Dirección Administrativa y Financiera de acuerdo a los siguientes servicios:

SERVICIO	¿QUIÉN LO AUTORIZA?
Internet	Director Administrativo y Financiero
Correo electrónico	Director Administrativo y Financiero
Software administrativo	Director Administrativo y Financiero

Por lo tanto, el Director Administrativo y Financiero de la Contraloría Distrital de Cartagena de Indias es responsable de:

- Velar por el cumplimiento de las normas en este procedimiento.
- Informar al Profesional Universitario del Proceso de Recursos Tecnológicos por medio del formato establecido de las novedades de cambio o rotación del personal que tiene asignado el servicio para su desactivación o reasignación.

1.2. ASIGNACION Y CONDICIONES DEL SERVICIO

Para la asignación de los servicios, el Proceso de Recursos Tecnológicos tendrá en cuenta la viabilidad técnica y asignara el servicio de acuerdo a la demanda y disponibilidad de los mismos. Se debe tener en cuenta:

- Capacidad y disponibilidad del ancho de banda para asignar un punto de conexión a internet.
- Viabilidad física o inalámbrica para la conexión.
- Cantidad de accesos asignados a la oficina.
- Disponibilidad y cantidad de correos asignados a la oficina.
- Validar la importancia y necesidad de la creación del correo electrónico.

- Validar el módulo y perfil del usuario para establecer los permisos de acceso en los aplicativos requeridos.

Los usuarios al utilizar estos servicios deben tener en cuenta:

- Lo establecido en el manual de Políticas para la Seguridad de la Información de la Contraloría Distrital de Cartagena de Indias.

- Los servicios asignados al funcionario deben ser para uso exclusivo de sus actividades labores y/o capacitaciones del personal de la Contraloría Distrital de Cartagena de Indias.

- El servicio a utilizar por los funcionarios es personal e intransferible, cada uno deberá firmar un acta de compromiso y buen uso del servicio en los equipos.

- Todos los funcionarios de la Contraloría Distrital de Cartagena de Indias que requieren el uso de equipos tecnológicos, deberán firmar y aceptar las normas de confidencialidad, buen uso y manejo de los recursos informáticos, igualmente, acatar, cumplir y respetar las políticas de seguridad de la Información establecidas en este Plan o cualquier otro documento relacionado emanado por la Contraloría Distrital de Cartagena de Indias.

- Para los nuevos funcionarios y/o contratistas deberán tramitar ante la Dirección Administrativa y Financiera la solicitud de la cuenta de correo electrónico, posteriormente el funcionario deberá firmar y aceptar las condiciones del servicio y recibir su usuario y contraseña del correo institucional. En este documento se debe dar constancia que la persona conoce y acepta las normas, reglamentos, seguridad y buen uso de los recursos informáticos.

- Cada funcionario y/o contratista una vez finalice la utilización de un servicio, debe asegurarse de cerrar la sesión de trabajo para evitar que otra persona tenga acceso a su perfil. Por lo tanto, si un funcionario o usuario encuentra abierta la sesión de trabajo de otra persona, su deber es cerrarla y no hacer uso de ella.

- Si llegase a ocurrir que una persona es sorprendida trabajando en una sesión que no le pertenece, puede haber un llamado de atención, proceso por la Secretaria General de la Contraloría Distrital de Cartagena de Indias o en caso extremo la entidad puede establecer acciones judiciales.

- La Dirección Administrativa y Financiera a través del Proceso de Recursos Tecnológicos, se reserva el derecho de hacer monitoreo y seguimiento a la utilización del servicio por parte de los usuarios y reportara al Contralor (a) Distrital de Cartagena para que tomen las medidas tendientes a mejorar su utilización cuando haya lugar.

- La conexión a servicios como internet de equipos tecnológicos como portátiles, tabletas, Smartphone u otros dispositivos tecnológicos que no pertenecen a la Contraloría Distrital de Cartagena de Indias, deben ser avalados por el Director Administrativo y Financiero de la Contraloría Distrital de Cartagena de Indias mediante solicitud a al Profesional Universitario del Proceso de Recursos Tecnológicos.

1.3. USO DE LOS SERVICIOS

1.3.1 Actividades aceptables

Internet

- Deben Operar todos los sistemas de información Web incluyendo el acceso a portales que permitan el normal desarrollo de las actividades laborales.

- Toda la información descargada de internet debe ser almacenada en una misma carpeta, con el fin de facilitar la búsqueda o seguimiento de archivos ante amenaza de infecciones.

- Se debe evitar al máximo el envío o descargas de archivos demasiado grandes (> 5 Mb) que saturen o ralenticen el sistema.

Correo Electrónico

- Los correos electrónicos recibidos de dudosa procedencia, primero deben ser analizados con los antivirus y de ser necesario dejarlos en cuarentena hasta garantizar su confiabilidad. De no ser posible su desinfección debe ser eliminado.

- El buen uso del correo electrónico institucional e internet es una política de la entidad, por lo tanto los funcionarios se deben abstener de utilizar cuentas libres de correo electrónico para evitar la difusión de spam, correo no deseado y la proliferación de virus. El correo electrónico debe ser revisado como mínimo dos veces al día, el no hacerlo no lo exime de sus responsabilidades de estar enterado de la información contenido en su buzón de correo electrónico.

- los equipos de cómputo deben contar con antivirus que permitan escanear en tiempo real cualquier archivo abierto o descargado de internet.

- Los correos enviados y recibidos se deben conservar como mínimo tres (3) meses para garantizar su conservación ante cualquier eventualidad.

- Se debe mantener depurado los buzones del correo electrónico eliminando periódicamente los mensajes innecesarios.

- Todos los correos electrónicos salientes, deben incluir la firma digital que debe contener el logo de la Contraloría, Nombre, cargo, oficina, Dirección física y teléfono de contacto.

- Se debe evitar al máximo el envío o descargas de archivos demasiado grandes (> 5 Mb) que saturen o ralenticen el sistema, el envío de archivos adjuntos superiores a 1 Mb deben ser comprimidos.

- Al utilizar el correo institucional @contraloriadecartagena.gov.co los usuarios deben velar por mantener la buena imagen de la entidad.

1.3.2 Actividades inaceptables

Internet

- En horas laborales se debe evitar desarrollar cualquier actividad que sea lucrativa o comercial de carácter individual, independiente de las funciones labores asignadas.

- Crear ambiente de trabajo hostil.

- Publicar en internet, redes sociales o página web institucional información que vulnere los derechos de los demás personas, involucrando la imagen y buen nombre de la Contraloría Distrital de Cartagena de Indias.

- Acceder, publicar o compartir contenido ofensivo, ocioso o pornográfico.

- Compartir información confidencial de la entidad.

- Descargar e instalar software, archivos o programas ejecutables que pueden ser potencialmente peligrosos para la integridad de la información.

- Descargar e instalar software, archivos o programas ejecutables sin la autorización de la Dirección Administrativa y Financiera.

- Usar programas espía para vulnerar la política de seguridad implementada en la Contraloría Distrital de Cartagena de Indias.

- Monitorear la red de transmisión de datos para buscar huecos de seguridad que les permita acceder a la información privada y privilegiada de los usuarios, contrario a la moral y las buenas costumbres.

- Introducir, ejecutar, distribuir o almacenar en los equipos de cómputo, software que puede ser utilizado para capturar lo escrito en teclado (Keylogger) y así obtener información como claves y contraseñas.

- Alojar en los servidores páginas web diferentes a las oficiales de la entidad.

Correo Electrónico

- Envío individual o masivo de cadenas que permitan la proliferación de spam.

- Enviar mensajes de correo electrónico utilizando la cuenta institucional que comprometan el buen nombre de la Contraloría Distrital de Cartagena de Indias.

- Deshabilitar o desinstalar el antivirus instalado en los equipos de cómputo.

- Habilitar la funcionalidad que deja reconocer la vista previa de cada uno de los correos, lo anterior debido a que permite la activación y propagación de virus y códigos maliciosos.

- Utilizar el servicio de mensajería con fines comerciales o publicitarios no institucionales.

- Permitir que personas ajenas a la entidad utilicen el servicio.

- Utilizar el correo electrónico para fines personales.

1.3.3 Desactivación de cuentas de correo electrónico

Las cuentas de correo electrónico pueden ser desactivadas o eliminadas por la Dirección Administrativa y Financiera en los siguientes casos.

- Cuando el funcionario ya no esté vinculado laboralmente con la Contraloría Distrital de Cartagena de Indias, ya sea como empleado o funcionario público, contratista, consultor o asesor. En este caso el Profesional Universitario del área administrativa oficiará a al Profesional Universitario del Proceso de Recursos Tecnológico para reportar la novedad.

- Por inactividad, después de dos (2) meses se puede inhabilitar la cuenta.

- Al funcionario que infrinja las normas descritas anteriormente.

1.3.4 Políticas de Seguridad

Todos los funcionarios sin importar su tipo de vinculación laboral y/o contratistas de la Contraloría Distrital de Cartagena de Indias que hagan uso de las tecnologías de la información y las comunicaciones deberán cumplir las políticas de seguridad del Manual de Políticas para la Seguridad de la Información, adoptadas mediante Resolución 198 del 14 de octubre de 2014 por la Contraloría Distrital de Cartagena de Indias.

1.3.5 Aspectos técnicos

- La Dirección Administrativa y Financiera a través del Proceso de Recursos Tecnológicos definirá el acceso a la red de datos. Para mayor control sobre su administración y uso se debe configurar la asignación de IP dinámica mediante el protocolo DHCP.

- Se debe establecer un sistema de autenticación de usuarios bajo un dominio controlado que permita unas directivas de seguridad para el internet, seguridad y servicios de correo.

- El servicio de internet debe ser administrado por la Dirección Administrativa y Financiera a través del Proceso de Recursos Tecnológicos será quienes definirán los equipos autorizados, horarios, acceso a páginas y ancho de banda asignado.

- Para el soporte técnico a los usuarios se dispone la cuenta sistemas@contraloriadecartagena.gov.co.

2. ADMINISTRACION DEL SOFTWARE

2.1. LINEAMIENTOS GENERALES

- La Dirección Administrativa y Financiera a través del Proceso de Recursos Tecnológicos debe velar por que todo el software instalado en los equipos de cómputo de la Contraloría Distrital de Cartagena de Indias, cumpla con la normatividad de propiedad intelectual, igualmente, llevará un control sobre las licencias adquiridas, tipo de licencia, vigencia, instalaciones y número de usuarios.

- Ningún usuario sin la autorización de la Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos podrá instalar software en los equipos de cómputo de la Contraloría Distrital de Cartagena de Indias, igualmente ningún usuario podrá copiar software de los equipos con fines personales o comerciales.

- Cualquier nuevo software a ser instalado en la Contraloría Distrital de Cartagena de Indias, debe ser supervisado por la Dirección Administrativa y Financiera a través del Proceso de Recursos Tecnológicos con el fin de proteger la integridad de la información en la entidad.

- Cada usuario es responsable del software que se encuentre instalado en su equipo, por lo tanto, es responsable de su uso y utilización.

2.2. ADQUISICIÓN DE SOFTWARE

Criterios mínimos para la adquisición de software.

2.2.1. Adquisición de sistemas de información

Para la adquisición de Sistemas de Información, por parte de la Contraloría Distrital de Cartagena de Indias se puede recurrir a la adquisición de software comercial o adquirir aplicativos desarrollados a la medida. En todo caso, la adquisición de cualquier tipo de sistema de información debe cumplir con los siguientes criterios.

- Debe llevar la autorización y visto bueno de la Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos.

- El Profesional Universitario del Proceso de Recursos Tecnológicos emitirá concepto técnico sobre las necesidades de software presentadas, evaluando que los requerimientos tanto de hardware como de software estén acordes con la necesidad planteada.

En la relación contractual, el proveedor debe cumplir como mínimo con los siguientes compromisos:

- Declarar compromiso de confidencialidad del sistema y la información.
- Constituir a favor de la Contraloría Distrital de Cartagena de Indias un documento que exprese la licencia de uso o autorización del mismo, incluyendo como mínimo: Nombre del software, versión del producto, número de licencias y tiempo de licenciamiento.
- Brindar actualización y soporte técnico, por el término de un (1) año como mínimo.
- Capacitar y entrenar al personal involucrado en la instalación, operación, administración y desinstalación del sistema.
- Informar a la Contraloría Distrital de Cartagena de Indias, a través de la Dirección Administrativa y Financiera, cuando el fabricante genere alguna nueva versión del sistema de información, y hacer entrega de medios magnéticos sin costo alguno para su respectiva instalación, durante la vigencia del licenciamiento.
- Entregar en idioma castellano, el manual técnico, de operación y del usuario.
- Instalar las licencias adquiridas y entregar los instaladores de las mismas a la Dirección Administrativa y Financiera de la Contraloría Distrital de Cartagena de Indias.

Si el software requerido no se encuentra disponible en el mercado, se optara por la adquisición de software desarrollado a la medida, teniendo en cuenta los siguientes criterios:

- Las personas naturales o jurídicas a contratar el servicio, deben demostrar experiencia e idoneidad en el desarrollo de software.
- Se debe disponer de un estudio de factibilidad técnica y económica.
- Exigir una metodología formal de desarrollo, que incluya requerimientos o especificaciones, diseño (de programas y de datos), desarrollo (en donde se tenga en cuenta los parámetros de integridad, seguridad, disponibilidad y desempeño del nuevo sistema), pruebas e implementación; cualquier

metodología que se implemente para el desarrollo de software debe contener como mínimo las siguientes etapas en estricto orden:

1.- Planeación y/o Análisis

2.- Diseño

3.- Codificación

4.- Compilación

5.- Pruebas

6.- Implementación

Dejando evidencia de cada una de las etapas.

- La plataforma tecnológica a utilizar debe ser avalada por la Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos permitiendo la compatibilidad con los sistemas operativos y aplicativos utilizados.

- En los estudios previos, dentro de las "obligaciones del contratista": La realización del procedimiento de inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor a favor de la Contraloría Distrital de Cartagena de Indias. Entiéndase como soporte lógico a: el programa de computador, la descripción de programa y el material auxiliar y entregar el código fuente y código objeto debidamente documentados.

2.2.2. Adquisición de software de Ofimática

La Contraloría Distrital de Cartagena de Indias para el normal funcionamiento de sus actividades, requiere el uso de diferentes software específico de uso ofimático cuyo licenciamiento debe cumplir las siguientes directrices:

- Siempre se debe adquirir la última versión del producto disponible en el mercado compatible con los utilizados actualmente.

- Continuamente se debe actualizar el software para garantizar su seguridad y contar con las novedades más recientes del producto.

- La Contraloría Distrital de Cartagena de Indias debe apoyar la producción de software libre, se debe empezar a migrar paulatinamente al uso de estas herramientas de uso y libre licenciamiento.

2.2.3. Software producido en la Contraloría Distrital de Cartagena de Indias

- Se debe incentivar la producción de software al interior de la Contraloría Distrital de Cartagena de Indias.

- Todo software, base de datos o aplicativo, desarrollado por cualquier funcionario sin importar el tipo de vinculación, pasa a ser propiedad de la Contraloría Distrital de Cartagena de Indias, la cual adquiere los derechos de propiedad intelectual (previa inscripción del registro en la dirección de derechos de autor del Ministerio del interior). Diferente que este pactado lo contrario en una minuta contractual.

- Estos aplicativos desarrollados por la entidad, se realizarán con las herramientas de desarrollo disponibles y también deberán estar licenciadas por la Contraloría Distrital de Cartagena de Indias.

2.3. DERECHOS DE AUTOR

Es responsabilidad de la Dirección Administrativa y Financiera de la Contraloría Distrital de Cartagena de Indias que todo el software instalado en los equipos de cómputo cumpla con las leyes de propiedad intelectual. Igualmente el software desarrollado al interior de la entidad debe ser registrado ante la entidad encargada de estas licencias en el ministerio del interior.

Debe ser una política al interior de la Contraloría Distrital de Cartagena de Indias, que todo software que se utilice en beneficio de la función misional de la entidad, debe estar debidamente licenciado y legalizado.

Se recomienda utilizar licencias corporativas que cubran todos los equipos de la entidad para abaratar costos de uso.

2.4. OPERACIÓN

La operación y utilización del software en las instalaciones de la Contraloría Distrital de Cartagena de Indias, estará abierta a todos los funcionarios que lo requieran, de acuerdo a la disponibilidad de equipos de cómputo y con sus licencias respectivas. La Dirección Administrativa y Financiera con el Profesional universitario del Proceso de Recursos Tecnológicos debe garantizar la debida operación de estos equipos, con un plan de mantenimiento preventivo y correctivo periódico que minimice daños, desgaste o deterioro de los mismos.

Las políticas de uso de los equipos de cómputo y telecomunicaciones deben ser muy claras, la utilización de estos elementos debe ser exclusivamente para labores propias de cada oficina, no para uso privado y menos comercial que atente contra el buen nombre y racionalización de los bienes de la entidad. La

Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos debe coordinar y controlar los accesos a los aplicativos.

Es responsabilidad de cada usuario velar por la integridad y seguridad de su información, se debe manejar los datos de forma responsable para garantizar un uso eficiente de los sistemas informáticos.

2.4.1. Normas de buen Uso

- la cuenta de acceso a los sistemas informáticos es personal e intransferible, por lo tanto cada usuario debe hacer buen uso de su usuario y contraseña ya que es dueño de la información procesada bajo su perfil.

- Este perfil de cada usuario debe ser usado para para llevar a cabo en forma eficiente todas las labores asignadas por la entidad.

- Es responsabilidad de cada usuario que su equipo de cómputo nos sea infectado por virus, gusanos, troyanos o archivos maliciosos que pongan en riesgo o vulneren la seguridad de la información, para esto se debe contar con los software de seguridad (antivirus, antispyware) legalizados y actualizados, teniendo especial cuidado en no abrir o descargar archivos de origen desconocido, malicioso o sospechoso, igualmente se debe evitar el traspaso de información por medios extraíbles como memorias USB sin el chequeo preventivo. Cualquier anomalía de este tipo o sospecha de virus informático, debe ser avisado inmediatamente al Profesional Universitario o al Técnico Operativo del Proceso de Recursos Tecnológicos de la Contraloría Distrital de Cartagena de Indias.

- Todos los funcionarios deben acatar las normas de seguridad, guías de buen uso y manuales instructivos que regulen el buen uso de los equipos de cómputo.

- Se debe mantener en reserva el acceso a la información privilegiada, no se debe filtrar ni compartir información vital para la entidad, en estos casos cada usuario debe firmar un documento de confidencialidad de la información.

2.4.2. No está permitido

- Facilitar el acceso de personas no autorizadas a los sistemas de información de la entidad.

- Instalar software en los equipos de cómputo sin la autorización de la Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos, esta dependencia debe certificar la autenticidad y legalidad de estos aplicativos en relación con los objetivos y misión de la entidad. Igualmente no se permite descargar software que

atente contra la integridad de la información y que además violen los derechos de autor.

- Eliminar, desinstalar o modificar software de la entidad alojado en los equipos de cómputo.
- Tratar de violar los sistemas de seguridad para acceder a sistemas de información, o facilitar que otros lo hagan.
- Adueñarse de los recursos compartidos, evitando que otros funcionarios hagan uso de los mismos.
- Hackear o intentar acceder a otros sistemas utilizando software espía para vulnerar los accesos y alterar la información.
- Acceder a los archivos *.log para Hackear los registros de uso del sistema.
- Intentar descifrar las claves de acceso.

2.5. ADMINISTRACIÓN

La Contraloría Distrital de Cartagena de Indias, como parte de su actividad pública, genera una considerable cantidad de información electrónica, que se constituye en registros oficiales y que por ende, necesitan de una administración específica y de procedimientos y prácticas de manipulación que se adecuen a las reglamentaciones existentes en la Entidad y a la normativa vigente a nivel nacional. De igual forma, dispone de servidores desde donde brinda determinados servicios a los funcionarios y mantiene en operación diversos sistemas de información y software. Todo sistema de información deberá tener asignado un administrador dentro de la Entidad, quien se encargará de realizar tareas técnicas propias del aplicativo y garantizar el funcionamiento del mismo.

La Dirección Administrativa y Financiera con el Profesional Universitario y Técnico de Soporte del Proceso de Recursos Tecnológicos deberá:

- Brindar soporte técnico, mantenimiento y configuración a todos los sistemas de información que hagan parte del sistema informático de la entidad, donde se utilicen servidores, equipos de cómputo o equipos de telecomunicaciones.
- Estar atento ante cualquier contingencia y responder en el menor tiempo posible.
- Coordinar la capacitación del personal en el uso eficiente de los recursos informáticos.

- Prueba, instalación, capacitación y actualización de software administrativo y de gestión a implementar en la entidad.
- Mantener actualizada la documentación de las configuraciones del sistema.
- Hacer cumplir los protocolos establecidos para el buen uso y manejo de la información, incluyendo la generación, resguardo y restauración de los Backup (Copias de seguridad).
- Mantener actualizadas las bases de datos y parametrización de los sistemas de información.
- Definir y establecer los privilegios en los accesos de los usuarios a los sistemas de información.
- Llevar un registro de los antecedentes ocurridos en los sistemas de información que alteren su buen desempeño y rendimiento.
- Poner en marcha los planes de contingencia ante cualquier eventualidad.
- Administrar y monitorear las cuentas de usuario para su autenticación en los sistemas de información.
- Garantizar la integridad de la información y la seguridad física y lógica de los datos almacenados en los sistemas informáticos.
- Mantener la confidencialidad en el acceso privilegiado a los datos.
- Reportar cualquier incidente de seguridad informática ocurrido en la entidad.

2.6. SEGUIMIENTO A LA SEGURIDAD INFORMATICA EN LA ENTIDAD

La Dirección Administrativa y Financiera es la encargada de diseñar y ejecutar todas las políticas de seguridad informática al interior de la Contraloría Distrital de Cartagena de Indias para garantizar la funcionalidad, integridad y seguridad de la información. La Contraloría Distrital de Cartagena de Indias debe garantizar todos los recursos económicos y técnicos requeridos para este fin.

Para garantizar la disponibilidad e integridad de los sistemas de información, se debe adecuar a las siguientes prácticas y medidas de seguridad:

- Tanto los sistemas operativos como las aplicaciones de tipo general o administrativo deben permanecer funcionales y actualizadas constantemente con los script o parches para garantizar su operatividad.

Esto garantiza utilizar los sistemas con las últimas versiones que minimizan la ocurrencia de errores o huecos de seguridad.

- Cualquier cambio ejecutado en el sistema debe ser supervisado para garantizar que este estaba autorizado e igualmente debe quedar documentado.

- Si el sistema está trabajando muy bien, igualmente se debe llevar un registro y evidenciar su correcto funcionamiento.

- Los aplicativos o sistemas multiusuario deben tener activado el registro automático de las acciones ejecutadas por todos los usuarios (*.log), se debe tener un historial cronológico que indique los cambios en el sistema, accesos no permitidos y huella recorrida por cada usuario. Este registro debe ser monitoreado periódicamente como una acción preventiva para buscar posibles fallas que alteren el sistema.

- Todo el sistema de fecha y hora de los equipos de cómputo debe ser sincronizado con la hora local.

- La ubicación de los servidores debe ser en un sitio seguro, área protegida y el acceso debe ser restringido.

- Los cambios al software realizado por terceros deben ser amparados por un documento de confiabilidad, no divulgación y utilización no permitida del mismo.

3. ADMINISTRACION DEL HARDWARE

3.1. ADQUISICIÓN

Al momento de adquirir equipos tecnológicos, es muy importante desde la etapa precontractual tener en cuenta los siguientes aspectos.

- Se debe exigir equipos de marcas reconocidas en el mercado, estos fabricantes deben cumplir con lo siguiente:

    - Reconocimiento internacional, amplia red de distribuidores, garantía a nivel nacional y presencia en el mercado colombiano.

    - Solo se deben adquirir equipos nuevos de excelente calidad y marcas reconocidas.

    - La garantía de fábrica mínimo debe ser de tres (3) años y una póliza de seguro del equipo mínimo por un año.

- Si es un equipo de escritorio, todos los periféricos deben ser de la misma marca.

- El proveedor de los equipos de cómputo debe entregar los equipos instalados, configurados, brindar el soporte y la garantía necesaria, además si incluye software debe registrar las licencias ante el fabricante del equipo y si es hardware realizar los trámites para efectos de las garantías respectivas. Además, se debe entregar en el sitio en el cual se va a utilizar.

- Cualquier adquisición de hardware o software realizada por la Contraloría Distrital de Cartagena de Indias, debe contar con el visto bueno y concepto técnico de la Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos.

3.2. OPERACIÓN

Los equipos de cómputo disponibles en la Contraloría Distrital de Cartagena de Indias, deben ser para uso exclusivo de los funcionarios para el desempeño propio de sus labores, totalmente prohibido su uso con fines privados, personales o con fines de lucro.

Para utilizar un equipo de cómputo con fines diferentes al deber misional de la entidad, este debe ser autorizado por el Contralor Distrital de Cartagena y la Dirección Administrativa y Financiera.

Cualquier reparación o servicio que se requiera en estos equipos de cómputo, debe ser realizado y/o supervisado por el personal técnico calificado del Proceso de Recursos Tecnológicos. Ninguna persona ajena está autorizada para reparar y mucho menos destapar un equipo de estos.

La Dirección Administrativa y Financiera con el Profesional Universitario del Proceso de Recursos Tecnológicos impartirá las instrucciones para garantizar el buen uso de los equipos de cómputo y todos sus periféricos.

3.2.1. Usos requeridos

- Al concluir la jornada laboral, todos los equipos deben quedar apagados completamente y desconectados de la red eléctrica, salvo los equipos de comunicaciones activos de la red, servidores o equipos de seguridad que deben permanecer 24 horas encendidos.

- Debido a factores atmosféricos como rayos o tormentas eléctricas, los equipos tecnológicos deben ser apagados y desconectados de las tomas de energía eléctrica, a excepción de equipos que por extrema necesidad

deban seguir funcionando, tomando todas las medidas de seguridad necesarias para su protección.

- Ante el evento de instalación o reparación de instalaciones eléctricas, los equipos tecnológicos deben ser apagados y desconectados de las tomas de energía eléctrica, a excepción de equipos que por extrema necesidad deban seguir funcionando, tomando todas las medidas de seguridad necesarias para su protección.

- Para la limpieza de los equipos de cómputo y sus accesorios, nunca debe realizarse con paños húmedos, debe reemplazarse por espuma para limpieza.

- Cumplir a cabalidad las instrucciones e indicaciones dadas por el Proceso de Recursos Tecnológicos, que buscan garantizar el buen uso de los equipos y elementos de cómputo.

- Proteger los equipos ante los riesgos generados por el ambiente y velar por su conservación en buen estado.

- Todo funcionario responsable de manejo o custodia de equipos de cómputo, debe reportar de forma inmediata a la Dirección Administrativa y Financiera o al Profesional Universitario del proceso de recursos tecnológicos cualquier daño o falla presentado por el equipo.

Para servidores:

- No debe exceder la capacidad máxima de almacenamiento asignada para los servicios informáticos; si llegase a ocurrir, cada funcionario es responsable de la salvaguarda y protección de su información. El Proceso de recursos Tecnológicos programará visitas periódicas para medir la capacidad de almacenamiento utilizada.

- El almacenamiento utilizado por los usuarios, debe ser única y exclusivamente para las labores propias de la entidad; por lo tanto, esta información solo debe ser de carácter laboral, administrativo o investigativo; si llegase a ocurrir, esta podrá ser eliminada de los sistemas informáticos previa comunicación dirigida al responsable del equipo.

Para estaciones de trabajo:

- Todos los funcionarios deben hacer buen uso de las recomendaciones dadas por la Dirección Administrativa y Financiera para el manejo de contraseñas.

- El único medio de autenticación (usuario y contraseña) en el sistema debe ser el asignado por el Proceso de Recursos Tecnológicos de la Dirección Administrativa y Financiera.

- Ningún usuario podrá modificar la configuración de su equipo de trabajo ni mucho menos la de sus compañeros, para este caso la Dirección Administrativa y financiera y el Proceso de Recursos Tecnológicos implementará las acciones necesarias para los permisos y acceso de los usuarios al sistema.

- Para el traslado de cualquier equipo de cómputo, este debe ser autorizado por la Dirección Administrativa y financiera, quien debe evaluar su operación, compatibilidad y conectividad en el nuevo puesto de trabajo.

- Cualquier daño a equipo de cómputo debido al mal uso o acción deliberada a propósito. Será asumida por el funcionario responsable, quien deberá cancelar de su propio pecunio el daño causado.

- Es deber de cada empleado realizar las copias de seguridad respectiva para mantener la integridad de su información. Por lo tanto, ni la Contraloría Distrital de Cartagena ni la Dirección Administrativa y financiera ni el Proceso de Recursos Tecnológicos se hacen responsables de la perdida de información personal en los equipos de cómputo. En el evento que el equipo sufra un daño y deba ser reparado, con anterioridad el usuario responsable deberá realizar el Backup de su información.

- Ante cualquier evento de pérdida o robo de algún componente de hardware o de software, este debe ser reportado a la Dirección Administrativa y financiera de forma inmediata.

- Apagar y encender los equipos de acuerdo a los procedimientos establecidos por el Proceso de Recursos Tecnológicos de la Dirección Administrativa y financiera.

3.2.2. Usos inaceptables

- Permitir o facilitar que personas ajenas a la Contraloría Distrital de Cartagena de Indias hagan uso de los recursos informáticos.

- Modificar la configuración de los equipos establecida por la Contraloría Distrital de Cartagena de Indias.

- Intentar cualquier tipo de daño (físico o lógico) a los recursos informáticos.

- Ingerir comidas o bebidas en el mismo puesto de trabajo mientras se está usando el equipo de cómputo.

- Fumar en el mismo puesto de trabajo mientras se está usando el equipo de cómputo.

- Instalar software sin autorización de la Contraloría Distrital de Cartagena de Indias, instalar software adquirido por el propio usuario para uso personal.

- Desatender las impresoras mientras se imprime.

- Compartir información por la red interna de la entidad violando los principios y recomendaciones de buen uso impartidas por la Dirección Administrativa y Financiera. Igualmente conectar equipos tanto a la red de datos como a internet sin la autorización de la Contraloría Distrital de Cartagena de Indias.

3.3. ADMINISTRACIÓN

La Contraloría Distrital de Cartagena de Indias dispone de hardware y software que requiere ser administrado, como son servidores, dispositivos de red, equipos de cómputo y estaciones de trabajo, para un mejor servicio. Por tanto, la Dirección Administrativa y Financiera y el Proceso de Recursos Tecnológicos deberán:

- Definir los recursos que se requieran para que los equipos administrados funcionen continua, eficaz y oportunamente.

- Definir y diseñar todos los protocolos de uso de los recursos informáticos y su recuperación ante posibles fallos. Igualmente definir los pasos a seguir ante inconvenientes o fallos con los equipos.

- Garantizar la operatividad de los equipos y elementos de cómputo, redes de datos y comunicaciones para que estén disponibles para los usuarios.

- Establecer procesos y actividades programadas para los mantenimientos de hardware y software solicitados por los usuarios. Periódicamente se deben programar mantenimientos preventivos generales a todos los equipos de la Contraloría Distrital de Cartagena de Indias, estos deben realizarse cada 6 meses. En el caso que un equipo requiera acción correctiva, este debe realizarse de inmediato por el personal técnico de la Contraloría Distrital de Cartagena de Indias.

- El personal técnico del Proceso de Recursos Tecnológicos de la Dirección Administrativa y Financiera debe realizar los Backup periódicos respectivos a los servidores que almacenan información administrativa, el Backup de los equipos de usuario debe ser realizado por cada uno de ellos.

- Se debe mantener actualizada una bitácora o registro de las acciones desarrolladas como mantenimientos, cambio de repuestos, recuperaciones, falla en equipos etc.; que permitan mantener un insumo para establecer posibles causas de fallos en los sistemas.

- Aplicar en forma estricta las normas de seguridad y control establecidas.

- Planificar la instalación, eliminación o actualización de software y hardware en los equipos que cumplen funciones administrativas.

- Configurar todos los entornos de red con sus protocolos y puertos que garanticen el acceso a recursos compartidos.

- La ubicación de servidores y equipos activos de la red debe ser un lugar restringido para el acceso de personal que no cuente con autorización del Proceso de Recursos Tecnológicos de la Dirección Administrativa y Financiera.

- Se deben coordinar y programar jornadas de capacitación, actualización y entrenamiento dirigido a todos los funcionarios o áreas específicas en temas de ofimática, software administrativo y aplicativo utilizado por los funcionarios de la Contraloría Distrital de Cartagena de Indias.

- Todas las oficinas que utilicen equipos y elementos tecnológicos que manejen información muy importante para la entidad, deben contar con controles de acceso y cierre. Al final de la jornada laboral estas deben quedar cerradas y se deben extremar las medidas de seguridad.

4. ADMINISTRACION DE LA RED DE DATOS

4.1. ADQUISICIÓN

Para la adquisición de equipos y elementos de cómputo, la Dirección Administrativa y Financiera será la única dependencia responsable de la adquisición de este tipo de soluciones, para lo cual deberá:

- En lo posible utilizar tecnología de punta administrable que permita:
  - Segmentar la red para la creación de VLAN y la configuración de servicios de impresión y compartir recursos en red.
  - Permitir el servicio de Redes Privadas Virtuales – VPN.
  - La arquitectura debe ser escalable, es decir que se permita actualizar.
  - Emisión de alertas ante ataques, accesos no autorizados o broadcast.
  - Redireccionar o balancear tráfico de datos para evitar cuellos de botella.
  - Clasificar paquetes de datos.

- Autenticación y control de acceso a los recursos.
- Clasificación de paquetes.
- Bloqueo de aplicaciones.
- Alto nivel de redundancia y tolerancia a fallas.
- Compatibilidad en los sistemas, fácil migración tecnológica y comunicación transparente.

- El cableado estructurado y las redes inalámbricas deben ser certificadas cumpliendo las normas internacionales.

4.2. SOLICITUD Y ASIGNACIÓN DEL SERVICIO

Para la prestación del servicio técnico y soporte a usuarios, la Dirección Administrativa y Financiera a través del Proceso de Recursos Tecnológicos facilitará los formatos para que la persona interesada en configurar un equipo para acceder a la red, acceder a internet, etc., diligencien el formato respectivo para hacer la solicitud.

Cada funcionario será responsable del buen uso y custodia de estos elementos y equipos de cómputo, por lo tanto, cada Secretaría u oficina responderá por:

- Velar por el cumplimiento de las normas establecidas.
- Informar a la Dirección Administrativa y Financiera cualquier cambio en la asignación de funciones y equipos, para las reasignaciones o cambios respectivos.

Dependiendo de la disponibilidad, la Dirección Administrativa y Financiera asignará el servicio o soporte Solicitado y realizará el seguimiento para su buen uso.

4.3. OPERACIÓN

4.3.1. Actividades requeridas

- La red de datos se debe utilizar para compartir recursos, archivos, carpetas, servicios de impresión, conexión a bases de datos y sistemas de información.
- Los equipos de cómputo solo deben ser usados como clientes de servicios.

- Las carpetas compartidas deberán contar con contraseña de acceso.

- Cualquier falla en los sistemas de cómputo deberá ser reportada inmediatamente a al Proceso de Recursos Tecnológicos de la Dirección Administrativa y Financiera.

- Se debe mantener un estricto control con los sistemas antivirus para evitar daños en la información y su propagación.

- Se debe respetar el derecho a la intimidad y la seguridad de la información, se debe respetar el derecho a la privacidad de todos los usuarios del sistema.

- Los únicos dispositivos conectados a la red de datos deben ser los autorizados por la Dirección Administrativa y Financiera o por el Contralor Distrital de Cartagena.

4.3.2. Restricciones en la Red

- Conectarse a la red de datos interna de la Contraloría Distrital de Cartagena de Indias utilizando otros medios o sistemas no implementados por la Dirección Administrativa y Financiera de la Contraloría Distrital de Cartagena de Indias.

- Que los usuarios intenten acceder a los sistemas de información por medios diferentes a los asignados.

- Intentar acceder a los servidores o manipular las conexiones para impedir el normal funcionamiento de las redes de datos.

- Acceder al centro de cómputo y telecomunicaciones sin la debida autorización de la Dirección Administrativa y Financiera o del Contralor Distrital de Cartagena.

- Intentar dañar o violentar física o lógicamente cualquier dispositivo de la red de datos de la Contraloría Distrital de Cartagena de Indias.

- Adueñarse de recursos compartidos para uso exclusivo, no permitiéndole a otros usuarios utilizarlos en la red.

- Instalar servicios de comunicaciones como correo electrónico, Servidores Web, FTP, escaneadores de puertos, etc., sin la autorización de la Dirección Administrativa y Financiera ni del Contralor Distrital de Cartagena.

- Instalar o configurar tarjetas o equipos de comunicaciones para acceso remoto como: módems, RDSI, ADSL, Router o cualquier otro dispositivo de comunicaciones sin la respectiva autorización de la Dirección Administrativa y Financiera ni del Contralor Distrital de Cartagena.

4.4. ADMINISTRACIÓN

La Dirección Administrativa y Financiera junto al Proceso de Recursos Tecnológicos de la Contraloría Distrital de Cartagena de Indias deberá:

- Definir los recursos necesarios para que las redes de datos operen correcta y continuamente.
- Monitorear constantemente el tráfico en la red, así como diseñar y formular recomendaciones de uso del recurso y recuperación ante fallas.
- Atender los inconvenientes o fallas de las redes.
- Ejecutar los procesos asignados conforme a las solicitudes de los usuarios o a las actividades programadas en calendarios preestablecidos de revisión, dejando el registro correspondiente en las solicitudes de proceso.
- Revisar los resultados de los procesos e incorporar acciones correctivas.
- Realizar las copias de respaldo (back-up) de la configuración de los servicios habilitados en los servidores de red (DHCP, Filtrados, etc.), conforme a parámetros preestablecidos en el procedimiento para la realización de copias de seguridad.
- Supervisar los procesos de mantenimiento que se les realice a las redes de datos de la Contraloría Departamental del Vichada.
- Documentar la configuración de los servidores de red y de la topología de las mismas.
- Establecer los requisitos de infraestructura física para restringir el acceso a las áreas en que están los servidores de red, rack y equipos activos.
- Administrar las direcciones IP reales o virtuales.
- Poner en marcha los planes de recuperación ante contingencias.
- Formular estrategias para el crecimiento o adecuación de las redes de datos de la entidad.

4.5. MANTENIMIENTO

Con el fin de garantizar la continua operación de las redes de datos de la Contraloría Distrital de Cartagena de indias, la Dirección Administrativa y Financiera con el Proceso de Recursos Tecnológicos deberá:

- Establecer los procedimientos de mantenimiento preventivo y correctivo de equipos de cómputo y redes los cuales deberán realizarse mínimo dos veces al año.

- Mantener actualizado la hoja de vida para cada equipo de cómputo.

- Programar jornadas de capacitación para los funcionarios y contratistas de la Contraloría Distrital de Cartagena de Indias, buscando una mayor eficiencia laboral y actualización en el área de desempeño.

- Documentar los procedimientos para configurar los servicios de red en los servidores y los dispositivos de comunicaciones.

- Presentar las solicitudes de recursos económicos necesarios para la actualización y mantenimiento de las redes.

4.6. ASEGURAMIENTO

La Dirección Administrativa y Financiera con el Proceso de Recursos Tecnológicos deberán velar por la seguridad de las redes de datos de la Contraloría Distrital de Cartagena de Indias así:

- Se debe garantizar que el centro de cómputo debe ser independiente con su propia red eléctrica, aire acondicionado, UPS de respaldo, mecanismos de detección y extintores de incendios, sistema de monitoreo y control de acceso.

- El tendido de cables y líneas de comunicación deberán cumplir con todas las normas de seguridad para evitar su contacto e impedimento de movilidad con los usuarios. A su vez que se debe garantizar la no presencia de roedores en las cajas y cableado estructurado.

- Cualquier contingencia relacionada con la red de datos debe ser atendida de manera inmediata por el personal técnico.

- Sebe garantizar la presencia de extintores en las áreas críticas de la red, como cuartos de máquinas, racks, entre otros.

- Realizar mantenimiento periódico a los ductos por donde circula el cableado estructurado para minimizar la presencia de roedores.

5. USUARIOS Y PASSWORD

Cada computador o equipo de cómputo registrado a un usuario del sistema debe tener un usuario y contraseña para autenticarse en la red de la siguiente forma.

- **Usuario:** Se compone con el primer nombre en minúscula y el primer apellido en minúscula. Si ya existe ese usuario, se agregara la letra inicial en minúscula del segundo apellido y si persiste se adiciona un consecutivo numérico empezando en 1.

  Ej: Si el usuario se llama Pedro García Lopez, el nombre de usuario sería. pedrogarcia

- **Contraseña:** La contraseña o Password se genera con el número de identificación del usuario, el cual la cambiara en el siguiente inicio de sesión con el siguiente formato: Longitud mínimo de ocho (8) caracteres alfanuméricos con al menos una letra mayúscula y un carácter especial ($ % & #). Esta contraseña debe ser cambiada por el usuario mínimo cada 90 días para garantizar mayor seguridad en la información.

  - Es de resaltar que la contraseña es personal e intransferible.
  - La contraseña nunca debe escribirse en ningún sitio, papel o paredes para recordarla, debe ser fácil de recordar al momento de escribirla.
  - Al momento de teclear su contraseña, asegurarse que nadie este mirando su teclado.
  - La contraseña no deber ser enviada por correo electrónico ni mencionarse en conversaciones, mucho menos hacerlo explícitamente diciendo “Mi clave es XXXXX”.
  - Debe ser obligatorio el uso de protector de pantalla con contraseña para bloquear la cuenta y así evitar intrusos en momentos de inactividad.

Cada Sistema de Información dentro de la Contraloría Distrital de Cartagena de Indias debe tener su administrador o funcionario responsable delegado por el Jefe de área quien informara mediante oficio a la Dirección Administrativa y Financiera con copia al despacho del Contralor Distrital de Cartagena para su autorización y será el único responsable del sistema,

para lo cual debe cambiar su clave periódicamente y por lo tanto mantener las mismas normas y condiciones para sus usuarios.

6. OPERACIÓN Y FUNCIONAMIENTO DE LA PÁGINA WEB

- La Oficina Participación Ciudadana de la Contraloría Distrital de Cartagena de Indias o en su defecto el Contralor Distrital de Cartagena serán los responsables del control y publicación de todo el material, contenidos e imagen gráfica de carácter institucional.

- La Dirección Administrativa y Financiera con el Proceso de Recursos Tecnológicos son los responsables de la operación de los servidores web que albergan la publicación de la página, a su vez, se ocupa de la programación y desarrollo de contenido a la medida utilizando tecnología y lenguajes de programación de vanguardia teniendo en cuenta los lineamientos de la entidad y la Política de Gobierno Digital de MINTIC.

- Todos los contenidos que aparecen en los diferentes sitios y micrositios, portales o páginas electrónicas de cada una de las dependencias de la Contraloría Distrital de Cartagena de Indias con presencia en la página web, son responsabilidad del área que los emite incluyendo su actualización.

- La Dirección Administrativa y Financiera con el Proceso de Recursos Tecnológicos deben garantizar el funcionamiento y operatividad del hosting de la página web de la entidad.

6.1. RESPONSABILIDAD DE LA INFORMACIÓN

- Todos los archivos y/o documentos a publicar deben estar en formato pdf y cumpliendo con la guía de estilo y usabilidad de la Contraloría Distrital de Cartagena de Indias.

- La actualización de la información publicada por cada área es responsabilidad de la misma.

- En todo lo relacionado a movimientos de personal con presencia en la página web, será el Área administrativa la instancia responsable de actualizar y/o notificar de manera inmediata.

6.2. RESPONSABILIDAD DE LOS CONTENIDOS

- Los contenidos publicados en la página web de la Contraloría Distrital de Cartagena de Indias deberán reflejar la actividad del despacho del Contralor y de cada Área u oficina respetando y reflejando siempre la Misión, Visión, Objetivos, Filosofía y Principios de la entidad.

- No se podrá realizar ningún tipo publicación que involucre proselitismo de ideas políticas, religiosas, raciales o gremiales.

- No se debe permitir publicación de contenidos que promuevan la violencia, intolerancia, racismo o vicios.

- Quedan prohibidos los links o vínculos a páginas externas a la Contraloría Distrital de Cartagena de Indias que vayan en contra de la Misión, Visión, Objetivos, Filosofía y Principios de la misma.

- Totalmente prohibido la publicación de material pornográfico, contenido sexual y pornografía infantil.

- No se permite la comercialización de espacios o publicidad dentro de la página web de la entidad.

7. MEDIDAS DISCIPLINARIAS

La Contraloría Distrital de Cartagena de Indias es consciente de la importancia de la continuidad de los servicios informáticos, por tal razón, aplicará todas las medidas disciplinarias del caso para todos los funcionarios de la entidad que infrinjan todo lo dispuesto en este documento. La infracción por parte de cualquiera de los funcionarios sin tener en cuenta el tipo de vinculación implicara los llamados de atención y procesos respectivos hasta las acciones judiciales necesarias para garantizar la seguridad de los sistemas informáticos al interior de la entidad.

8. DIVULGACIÓN

La Dirección Administrativa y Financiera establecerá las estrategias para el conocimiento y difusión de la presente política a todos los funcionarios de la Contraloría Distrital de Cartagena de Indias.