Cámara de Comercio de Manizales por Caldas	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	**VERSIÓN** 2015-12-30

ELABORÓ	REVISÓ	APROBÓ
Comité de Protección de Datos y seguridad de la información Fecha: 2015-12-30	Cesar Augusto Cárdenas Molina Profesional de Sistemas y Telecomunicaciones Fecha: 2015-12-30	Lina María Ramírez Londoño Presidenta Ejecutiva Fecha: 2015-12-30

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de seguridad de la información de la Cámara de Comercio de Manizales por Caldas, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles idóneos de protección y resguardo de la información, definiendo sus lineamientos para garantizar el debido control y minimizar los riesgos asociados.

2. OBJETIVO

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la CCMPC establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance tecnológico y los requerimientos de la Entidad.

El presente documento define los lineamientos que debe seguir la CCMPC con relación a la seguridad de la Información.

Estos lineamientos están escritos en forma de políticas.

3. ALCANCE

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la CCMPC, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar un acuerdo de confidencialidad, que los compromete con el cumplimiento de las políticas de seguridad aquí descritas. Los usuarios de los activos de información de la Entidad se han clasificado así:

- ***Colaboradores de Planta:*** se definen como las personas que han suscrito un contrato laboral con la Entidad.

- ***Funcionarios de la CCMPC:*** Se definen como los empleados de la CCMPC que son susceptibles de manipular sistemas de información.

- ***Contratistas***: se definen como aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:

    - *Colaboradores en Misión*.
    - *Colaboradores por Outsourcing*: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos.
    - *Personas naturales que prestan servicios independientes a la Entidad*.
    - *Proveedores de recursos informáticos.*

- ***Entidades de Control***
    - *Procuraduría.*
    - *Revisoría Fiscal.*
    - *Contraloría General de la República.*
    - *Superintendencia de Industria y Comercio.*

- ***Otras Entidades***
    - DIAN.

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia de seguridad de la información, la CCMPC debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Cámaras de Comercio o entidades que las regulan y aglutinan.

5. DEFINICIONES

Para los propósitos de este documento se aplican los siguientes términos y definiciones:

- *Activo:* cualquier bien que tenga valor para la organización.
- *Acuerdo de Confidencialidad*: es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la CCMPC.
- *Administradores:* usuarios a quienes la CCMPC ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la entidad. Estas personas estarán bajo la dirección de la administración y la presidencia.
- *Amenaza:* causa potencial de un incidente no deseado que puede ocasionar daño a un sistema u organización.
- *Backup*: copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
- *Área de planeación y finanzas*: es el responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos.
- *Comité de protección y seguridad de la información*: conformado por un equipo de funcionarios interdisciplinarios de la CCMPC.
- *Contraseña:* clave de acceso a un recurso informático.
- *Control:* medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- *Directrices*: descripción que aclara lo que se debería hacer y cómo hacerlo para alcanzar los objetivos establecidos en las políticas.
- *Servicios de procesamiento de información*: cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.
- *Seguridad de la Información*: preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- *Evento de seguridad de la información*: es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la

información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

- *Firewall*: conjunto de recursos de hardware y software que protegen los recursos informáticos de accesos indebidos.
- *Incidente de seguridad de la información*: está indicado por un solo evento o serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información.
- *Información confidencial (reservada):* información administrada por la CCMPC en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.
- *Información confidencial*: información generada por la CCMPC en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.
- *Información privada*: información generada por la CCMPC en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.
- *Información pública*: es la información administrada por la CCMPC en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.
- *LAN*: grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio ó una oficina).
- *Licencia de Software*: es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.[1]
- *Copyright:* son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados, se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en ocasiones la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.
- *Propiedad Intelectual:* es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.[2]
- *Open Source* (Fuente Abierta): es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.
- *Software Libre*: software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente en el cual la licencia expresamente específica dichas libertades.

---

[1] Tomado del diccionario Wikipedia. http://es.wikipedia.org/wiki/Licencia_de_software

[2] Tomado de http://www.derautor.gov.co/htm/preguntas.htm#01

- *Software pirata*: es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
- *Software de Dominio Público*: tipo de software en que no se requiere ninguna licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales, estos software son en los que existe una libertad total de usufructo de la propiedad intelectual.
- *Freeware*: software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- *Shareware:* clase de software o programa cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.
- *Módem* (Modulador - Demodulador de señales): elemento de comunicaciones que permite transferir información a través de líneas telefónicas.
- *Monitoreo*: verificación de las actividades de un usuario con respecto a los recursos informáticos de la CCMPC.
- *OTP* (One Time Password): contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este ingreso.
- *Plan de contingencia*: plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la CCMPC en casos de desastres y otros casos que impidan el funcionamiento normal.
- *Política*: toda intención y directriz expresada formalmente por la dirección.
- *Protector de pantalla*: programa que se activa a voluntad del usuario, o automáticamente después de un tiempo en el que no ha habido actividad.
- *Proxy*: servidor que actúa como puerta de entrada a la Red Internet.
- *Recursos informáticos*: son aquellos elementos de tecnología de Información tales como: computadores, servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, y de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.
- *Riesgo*: combinación de la probabilidad de un evento y sus consecuencias.
- *Análisis de Riesgos*: uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- *Evaluación de Riesgos*: todo proceso de análisis y valoración del riesgo.
- *Valoración del riesgo*: proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar su importancia.
- *Gestión del riesgo*: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- *Router*: equipo que permite la comunicación entre dos o más redes de computadores.
- *Sesión*: conexión establecida por un usuario con un Sistema de Información.
- *Sistema de control de acceso*: elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.
- *Sistema de detección de intrusos (IDS)*: es un conjunto de hardware y software que ayuda en la detección de accesos o intentos de acceso no autorizados a los recursos informáticos de la CCMPC.
- *Sistema de encriptación*: elementos de hardware o software que permiten cifrar la información para evitar que usuarios no autorizados tengan acceso.
- *Sistema multiusuario*: computador y su software asociado, que permite atender múltiples usuarios a la vez a través de las redes de comunicación.
- *Sistema operativo*: software que controla los recursos físicos de un computador.

- *Sistema sensible*: es aquel que administra información confidencial o de uso interno que no debe ser conocida por el público en general.
- *Tercera parte*: persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.
- *Usuario*: toda persona que pueda tener acceso a un recurso informático de la CCMPC.
- *Usuarios de red y correo*: usuarios a los cuales la CCMPC les entrega un identificador de cliente para acceso a sus recursos informáticos.
- *Usuarios externos*: son aquellos clientes externos que utilizan los recursos informáticos de la CCMPC a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.
- *Usuarios externos con contrato*: usuarios externos con los cuales la CCMPC establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.
- *Vulnerabilidad:* debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

6. RESPONSABLE

6.1. Compromiso de la dirección

La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

- Mediante el establecimiento de una política de seguridad de la información.
- Asegurando que se establezcan objetivos y planes de seguridad de la información.
- Estableciendo funciones y responsabilidades de la seguridad de la información.
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidades de la mejora continua.
- Asegurando que se realizan auditorías internas.

6.2. Gestión de los Recursos

- Asegurar que las políticas de seguridad de la información brinden apoyo al cumplimiento de la misión y visión de la CCMPC.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
- Procurar que todo el personal tenga conciencia de la importancia de la seguridad de la información.

7. PROCEDIMIENTO

- Comunicación de las políticas de seguridad:

Los miembros del Comité de protección y seguridad de la información, conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

- **Aplicación de las políticas de seguridad:**

Las políticas de seguridad informática se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

7.1. POLÍTICA DE SEGURIDAD DE LA CCMPC.

La CCMPC reconoce abiertamente la importancia de la seguridad de la información así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

La CCMPC dispondrá de los medios necesarios para dar conocer a los funcionarios, terceros y usuarios en general, el presente documento y normas relacionadas. El desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la CCMPC con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- ✓ Políticas de Cumplimiento y Sanciones.
- ✓ Políticas de uso de recursos informáticos.
- ✓ Políticas de contraseñas.
- ✓ Políticas de uso de la información.
- ✓ Políticas del uso de Internet y correo electrónico.
- ✓ Políticas de uso de la Intranet y Sitio Web de la CCMPC.
- ✓ Políticas Generales de la Presidencia.
- ✓ Políticas para Desarrolladores de Software.
- ✓ Políticas para Administradores de Sistemas.
- ✓ Políticas de Copias de respaldo.
- ✓ Políticas de Uso de Firewall.

- ✓ Políticas para Usuarios previstos en el numeral tercero.
- ✓ Políticas de Acceso Físico.

7.3. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

7.3.1. **Seguridad de la información**

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de la CCMPC y al Comité de protección y seguridad de la información.

7.3.2. **incumplimiento de políticas de seguridad**

Todo incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias o contractuales, conforme a lo establecido en el reglamento interno de trabajo de la CCMPC y/o su respectivo contrato.

7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

7.4.1. **Instrucciones para el uso de recursos informáticos**

El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de la CCMPC, debe someterse a todas las instrucciones técnicas, que imparta el Comité de protección y seguridad de la información.

7.4.2. **Manejo de los recursos Informáticos**

Los recursos informáticos de la CCMPC, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización del Oficial de protección y seguridad de la información.

7.4.3. **Acuerdo de confidencialidad**

Para el uso de los recursos tecnológicos de la CCMPC, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.

Prohibición de instalación de software y hardware en los computadores de la CCMPC

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos, solo puede ser realizada por los funcionarios de sistemas autorizados por la CCMPC.

7.4.4. **Uso de aplicativos**

La CCMPC ha suscrito con los fabricantes y proveedores un contrato de “LICENCIA DE USO” para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a la CCMPC Adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

7.4.5. **Uso de recursos y autenticación de usuarios**

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realicen labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la CCMPC.

7.4.6. **Declaración de reserva de derechos de la CCMPC**

La CCMPC usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos la CCMPC se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la CCMPC. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del Comité de protección y seguridad de la información, siempre con el concurso de la Presidencia o su delegado.

7.4.7. **Recursos compartidos**

Está prohibido compartir los discos duros o las carpetas de los computadores de escritorio sin previa autorización del área de sistemas de la CCMPC, quien será el encargado de establecer las medidas de seguridad necesarias..

7.4.8. **Monitoreo de usuarios internos**

Cualquier usuario interno puede ser monitoreado, previa autorización del Comité de protección y seguridad de la información o de la presidencia. El área de sistemas llevará un registro de los monitoreos realizados.

7.4.9. **Acceso no autorizado a los sistemas de información de la Entidad**

Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encripción y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

7.4.10. **Posibilidad de acceso no implica permiso de uso**

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.

7.4.11. **Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.**

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al Comité de protección y seguridad de la información.

7.4.12. Manejo de sesiones en sistemas informáticos

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

7.4.13. Notificación de sospecha de pérdida, divulgación ó uso indebido de información.

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del Comité de protección y seguridad de la información.

7.4.14. Traslado de equipos

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de la CCMPC sin previa autorización del área de sistemas. Así mismo, ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias y por el personal autorizado.

7.4.15. Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con la CCMPC se debe diligenciar el documento de entrega de inventario.

Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

7.4.16. Configuración de sistema operativo de las estaciones de trabajo

Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

7.4.17. Uso restringido de módems en las estaciones de trabajo

Queda prohibido el uso de módems en las estaciones de trabajo dentro de las instalaciones de la CCMPC, que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación del Líder del Área de Sistemas o superior inmediato..

7.4.18. Protección por Defecto de Copyright

Todos los colaboradores de la CCMPC deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.
Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

7.4.19. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área de tecnología. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado.

7.4.20. Apagado de equipos

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina. Se exceptúan los equipos del área de sistemas que por razón de monitoreo deberán permanecer encendidos cuando sea necesario.

7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

7.5.1. Confidencialidad de las contraseñas

La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

7.5.2. Uso de diferentes contraseñas

Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.

7.5.3. Identificación única para cada usuario

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de la CCMPC.

7.5.4.Cambios periódicos de contraseñas

Todos los usuarios deben cambiar su contraseña por lo menos una vez cada 30 días.

7.5.5. Longitud mínima de contraseñas

Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales.

7.5.6. Contraseñas fuertes

Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y caracteres especiales.

7.5.7. Prohibición de contraseñas cíclicas.

No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es “Enero-2004” que según la política “Contraseñas fuertes”, es una contraseña válida, pero al mes siguiente pasa a ser “Febrero-2004” y así sucesivamente.

7.5.8. Las contraseñas no deben ser reutilizadas.

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente.

7.5.9. Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción de lo contemplado en la política “Almacenamiento de contraseñas de administrador”.

7.5.10. Sospechas de compromiso deben forzar cambios de contraseña.

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

7.5.11. Revelación de contraseñas prohibida.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política “Auditoria periódica a las contraseñas de los usuarios”.

7.5.12. Bloqueo estación de trabajo.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min.

7.6. POLÍTICAS DE USO DE LA INFORMACIÓN

7.6.1. Divulgación de la información manejada por los usuarios de la CCMPC

La CCMPC podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales. Se deja claridad que la información pública proveniente de la función registral es administrada exclusivamente para los fines propios de los registros públicos de acuerdo con las normas legales y reglamentarias vigentes sobre la materia. La información proveniente de las demás funciones de la CCMPC es administrada y conservada, observando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información, previamente clasificada, salvo autorización del titular de la misma para su divulgación.

7.6.2. Transferencia de datos solo a organizaciones con suficientes controles.

la CCMPC puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

7.6.3. Registro de las compañías que reciben información privada.

El personal de la CCMPC que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

7.6.4. Transferencia de la custodia de información de exfuncionarios.

Cuando un empleado se retira de la CCMPC, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos, para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la misma.

7.6.5. Eliminación Segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por la CCMPC, antes de su entrega se les realizará un proceso de borrado seguro en la información.

7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

7.7.1. **Prohibición de uso de Internet para propósitos personales.**

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política “Instrucciones para el uso de recursos informáticos”.

7.7.2. **Formalidad del correo electrónico.**

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

7.7.3. **Preferencia por el uso del correo electrónico.**

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

7.7.4. **Uso de correo electrónico.**

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.

7.7.5. **Revisión del correo electrónico.**

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo periódicamente durante su jornada laboral. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

7.7.6. **Mensajes prohibidos.**

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

7.7.7. **Acciones para frenar el SPAM.**

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo, excepto que el origen sea conocido.

7.7.8. **Todo buzón de correo debe tener un responsable.**

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

7.7.9. **Software e información sensible a través de Internet.**

Software e información sensible de la CCMPC que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

7.7.10. **Intercambio de información a través de Internet.**

La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

7.8. POLÍTICAS DE LA INTRANET Y SITIOS WEB DE LA CCMPC

7.8.1. **Reglas de uso de la Intranet.**

La CCMPC utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

7.8.2. **Prohibición de publicitar la imagen de la CCMPC en sitios diferentes a los institucionales.**

La publicación de logos, marcas o cualquier tipo de información sobre la CCMPC o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización de la Presidencia. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

7.8.3. **Conexiones a los sitios Web de la CCMPC**

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de la CCMPC por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización del Comité de protección y seguridad de la información, dependiendo del caso. Particularmente se encuentra

prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

7.9. POLÍTICAS GENERALES DE LA PRESIDENCIA

7.9.1. Evaluación y tratamiento del riesgo

La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados debe guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos de CCMPC al menos una vez cada dos años utilizando la metodología para la administración del riesgo.

7.9.2. Restricción del acceso a la red privada a clientes externos.

No se otorgará acceso a la red privada de la CCMPC a terceros, a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, mediante el uso de los mecanismos de control de acceso establecidos.

7.9.3. Los servidores y equipos de comunicaciones.

Todos los servidores y equipos de comunicaciones que contengan información sensible y software licenciado de propiedad de la Entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

7.9.4. Entrenamiento compartido para labores técnicas críticas.

Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de la CCMPC.

7.9.5. Planes de contingencia

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. La contingencia de sistemas que se acuerdan con terceros deberá disponer de una infraestructura y de un modelo de soporte acorde a las necesidades de la CCMPC.

7.9.6. **Personal competente**

Con el fin de garantizar la continuidad de los sistemas de información, la CCMPC deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

7.9.7. **Chequeo de virus en archivos recibidos en correo electrónico.**

La CCMPC debe procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático.

7.9.8. **Contacto con grupos especializados en seguridad informática**

El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer las nuevas medidas en cuanto a seguridad de la información se van presentando.

7.10. POLÍTICAS PARA DESARROLLADORES DE SOFTWARE

7.10.1. **Ambientes separados de producción y desarrollo.**

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción.

7.10.2. **Cumplimiento del procedimiento para cambios y/o actualizaciones.**

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluados en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

7.10.3. **Documentación de cambios y/o actualizaciones.**

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

7.10.4. **Catalogación de programas.**

Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa prueba por parte del área encargada.

7.10.5. **Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.**

Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.

7.10.6. **Incorporación de contraseñas en el software.**

Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por la CCMPC o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política “Cambios periódicos de contraseñas”.

7.10.7. **Acceso del usuario a los comandos del sistema operativo.**

Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

7.10.8. **Registros de auditoría en sistemas que manejan información sensible.**

Todo sistema que maneje información sensible para la CCMPC debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

7.10.9. **Modificación de información de la entidad en producción.**

La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Presidencia.

7.10.10. **Validación de entradas en los desarrollos.**

El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

7.10.11. **Diseño de seguridad para aplicaciones.**

El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para la CCMPC.

7.10.12. **Personas autorizadas para leer los registros de auditoria.**

Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoria interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

7.11. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

7.11.1. **Soporte para usuarios con privilegios especiales.**

Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

7.11.2. **Terminación privilegios de acceso a los sistemas de información**

Todos los privilegios sobre los recursos informáticos de la CCMPC otorgados a un usuario deben eliminarse en el momento que éste abandone la Entidad y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

7.11.3. **contraseñas de los administradores**

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

7.11.4. **Cambio de contraseñas por defecto.**

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política “Contraseñas fuertes”.

7.11.5. **Brindar acceso a personal externo.**

El Área de Sistemas y Telecomunicaciones velará porque individuos que no sean empleados, contratistas o consultores de la CCMPC no tengan privilegio alguno sobre los recursos tecnológicos de uso privado de la Entidad, a menos que exista una aprobación por parte del Líder del Área de Sistemas o superior inmediato..

7.11.6. **Acceso de terceros a los sistemas de la Entidad**

Antes de otorgarle acceso a un tercero a los recursos tecnológicos privados de la CCMPC se requiere la aprobación del Oficial de protección de datos y seguridad de la información y suscribir el acuerdo de confidencialidad.

7.11.7. **Restricción de administración remota a través de Internet.**

La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para encriptación del canal de comunicaciones.

7.11.8. **Dos usuarios requeridos para todos los administradores.**

Administradores de sistemas multiusuarios deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

7.11.9. **Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.**

Sin autorización de Oficial de protección de datos y seguridad de la información, los administradores no deben otorgarle privilegios de administración a ningún usuario.

7.11.10. **Negación de privilegios de acceso a sistemas**

Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

7.11.11. **Remoción de software para la detección de vulnerabilidades cuando no esté en uso.**

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas o en encripción del software como tal.

7.11.12. **Manejo administrativo de seguridad para todos los componentes de la red.**

Los parámetros de configuración de todos los dispositivos conectados a la red de la CCMPC deben cumplir con las políticas y estándares internos de seguridad.

7.11.13. **Información a capturar cuando un crimen informático o abuso es sospechado.**

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

7.11.14. **Sincronización de relojes para un registro exacto de eventos en la red.**

Los dispositivos multiusuario conectados a la red interna de la CCMPC deben tener sus relojes sincronizados con la hora oficial.

7.11.15. **Revisión regular de los registros del sistema.**

El área de sistemas debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

7.11.16. **Confidencialidad en la información relacionada con investigaciones internas.**

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

7.11.17. **Información con múltiples niveles de clasificación en un mismo sistema.**

Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

7.11.18. **Identificación de vulnerabilidades.**

La entidad dispone de un software de cortafuegos y antivirus con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. Así mismo, se cuenta con un firewall con sistema IDS (Instrusion Detection System), detección de virus y bloqueo de correo no deseado.

7.11.19. **Controles de acceso para sistemas informáticos.**

Todo computador que almacene información sensible de La CCMPC, debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

7.11.20. **Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales**

Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

7.11.21. **Habilitación de Logs en Sistemas y Aplicaciones**

Se debe habilitar la gestión de logs (archivos de transacción) en los sistemas y aplicaciones críticas de la CCMPC

7.11.22. **Mantenimiento de los Sistemas**

Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de la CCMPC

7.11.23. **Verificación física de equipos críticos**

Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.

7.11.24. **Servicios de Red**

Se debe garantizar que el servicio de red utilizado por la CCMPC se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el Comité de protección y seguridad de la información puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

7.11.25. **Revisión de accesos de usuarios**

Se debe realizar por control de auditoría la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

7.12. POLÍTICAS DE BACKUP

7.12.1. **Período de almacenamiento de registros de auditoria.**

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

7.12.2. **Backup de información**

A toda información sensible y software crítico de la CCMPC residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

7.12.3. Copias de información sensible.

Se deben elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

7.13. POLÍTICAS DE USO DE FIREWALL

7.13.1. Detección de intrusos.

Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

7.13.2. Protección conexión externa

Toda conexión a los servidores de la CCMPC proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

7.13.3. Protección conexión a Internet

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

7.13.4. Inventario de conexiones

Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

7.13.5. El sistema interno de direccionamiento de red no debe ser público

Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

7.13.6. Revisión periódica y reautorización de privilegios de usuarios

Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios respectivos.

7.14. POLÍTICAS PARA USUARIOS EXTERNOS

7.14.1. Acuerdos con terceros que manejan información o cualquier recurso informático de la CCMPC

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de la CCMPC por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a la CCMPC ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de la CCMPC.

7.14.2. Definición clara de las responsabilidades de seguridad informática de terceros.

Los aliados, proveedores, clientes y otros usuarios de la CCMPC deben tener conocimiento de sus responsabilidades relacionadas en el presente documento y esta responsabilidad se debe ver reflejada en los contratos y/o acuerdos de confidencialidad de la CCMPC.

7.15. POLÍTICAS DE ACCESO FÍSICO

7.15.1. Reporte de pérdida o robo de identificación

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones.

7.15.2. Orden de salida para equipos electrónicos.

Ningún equipo electrónico podrá salir de las instalaciones de la CCMPC sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

7.15.3. Privilegios de acceso Exfuncionarios

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados.

7.15.4. Ingreso de equipos de grabación y fotografías al Cuarto de servidores

Cualquier miembro de la CCMPC y/o tercero debe estar autorizado por el área de sistemas para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).

8. POLÍTICA DE USO DE PORTÁTILES

8.1.1. Protección de la información

8.1.2. El antivirus siempre debe estar activo y actualizado

8.1.3. Seguir las políticas de acceso remoto. (En los casos que aplique).

8.1.4. Cuando el equipo deba ser entregado para reparación, mantenimiento etc. Se deberá hacer una copia de seguridad y eliminar de éste la información confidencial en los casos requeridos.

8.1.5. Protección del equipo portátil

8.1.6. No dejar el computador móvil en lugares públicos

8.1.7. Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su mano.

8.1.8. Cuando vaya en su carro este debe ir en el baúl.

8.1.9. No prestar el computador portátil a familiares y/o amigos

9. ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACION DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Este documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

El Oficial de protección de datos y seguridad de la información, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

10. COMITÉ DE PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN

El Comité de protección y seguridad de la información está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia con respecto al programa de seguridad de la información dentro de la organización.

El Comité de protección y seguridad de la información debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de protección y seguridad de la información:

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización.
- Revisión y valoración de la Política de Seguridad de la Información.
- Alineación e integración de la seguridad a los objetivos de la entidad.
- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.

- Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.

- Reportar a la Presidencia la necesidad de nuevos proyectos en temas de seguridad de la información.

- Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información

- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información

- Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.

- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.

- Supervisar y controlar de los cambios significativos en la exposición de los activos de información a las principales amenazas.

- Revisar y seguir los incidentes de seguridad de la información.

- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la compañía.

Adicionalmente, el Comité de protección y seguridad de la información tiene la responsabilidad de tratar los siguientes temas (por demanda):

- Mejoras en las actividades inherentes a la Seguridad de la CCMPC y sus procesos.

- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de la CCMPC
- Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.
- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de la CCMPC.
- El Oficial de protección de datos y seguridad de la información convoca al Comité de protección y seguridad de la información con el propósito de evaluar los cambios a la presente política. De este comité se debe levantar Acta como constancia de su evaluación y aprobación de cambios.

Las decisiones del Comité de protección y seguridad de la información son protocolizadas mediante un Acta firmada por las personas designadas.

10.1. **Oficial de protección de datos y seguridad de la información**

Funciones y responsabilidades:

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la entidad.

- Tomar medidas y acciones necesarias para la apropiación y concientización de las políticas de seguridad de la información en la organización.

- Evaluar la efectividad de la seguridad de la información y velar por la mejora continua de la misma.

11. **ANEXOS**

ANEXO 1.

ACUERDO DE CONFIDENCIALIDAD

Ciudad y Fecha:_____

Yo, _____ me comprometo a acatar y dar cumplimiento a cada una de las políticas establecidas en el documento POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN y así mismo mantener estricta confidencialidad sobre toda información que por una u otra razón deba conocer como producto del trabajo que actualmente realizo o realizaré.

Firma: _____

Documento de identificación: _____

Empresa: _____

Área de la CCMPC: _____

_____
Vo. Bo. Recursos Humanos

ANEXO 2.

POLÍTICA DE ASUNTOS ESPECÍFICOS: IDENTIFICACIÓN BIOMÉTRICA

1. ALCANCE

El presente anexo al documento de Política de Seguridad de la Información, reglamenta la protección y uso de los activos de información relacionados con la integración de los servicios de la CCMPC, Confecámaras y la Registraduría Nacional del estado civil, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar previamente un acuerdo de confidencialidad (Anexo 1), que los compromete con el cumplimiento de las políticas de seguridad ya descritas. Los usuarios de los activos se denominan así:

Funcionarios de la CCMPC: Se definen como los empleados de la CCMPC que son susceptibles de manipular el sistema de autenticación biométrica en línea.

2. PROCEDIMIENTO

Los miembros del Comité de protección y seguridad de la información, conscientes que los recursos de información son utilizados de manera permanente por los usuarios de la CCMPC que manipulan el servicio de identificación biométrica, definidos en este anexo, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

3. MEDIDAS POR INCUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD

Todo incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias o contractuales, conforme a lo establecido en el reglamento interno de trabajo de la CCMPC y/o su respectivo contrato.

Si el incumplimiento se origina en una sede, la CCMPC podrá suspender la prestación del servicio de identificación biométrica.

4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

4.1 Instrucciones para el uso de recursos informáticos.

El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica en línea, debe someterse a todas las instrucciones técnicas, que imparta el Comité de protección y seguridad de la información.

4.2 Uso de los recursos informáticos

Los recursos informáticos de la CCMPC, dispuestos para la operación registral, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de la CCMPC, usuaria de este servicio. Cualquier otro uso está sujeto a previa autorización del Oficial de protección de datos y seguridad de la información.

4.3 **Acuerdo de confidencialidad**

Para el uso de los recursos tecnológicos asociados a la solución de autenticación biométrica en línea de la CCMPC, los usuarios de dichos recursos debe firmar un acuerdo de confidencialidad (Anexo 1).

4.4 **Traslado de equipos debe estar autorizado.**

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de la CCMPC sin previa autorización. Así mismo, ningún equipo de cómputo asignado en el kit de identificación biométrica debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

5. **POLÍTICAS DE USO DE LAS CONTRASEÑAS**

5.1 **Identificación única para cada usuario.**

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (Usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. En caso del sistema de autenticación biométrica en línea, el acceso al sistema se realizará mediante un cotejo inicial entre el sistema biométrico y el sistema registral, los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de la CCMPC.

12. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
Versión	Fecha	Revisó	Aprobó	Cambio
1	2015-12-29	Comité de protección y seguridad de la información	Presidencia	Elaboración de documento de Políticas de seguridad de la información.