

RESOLUCION DIRECTIVA No. 09
Fecha: 29 de Marzo de 2016

POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE SEGURIDAD DE LA INFORMACION PARA LA CAMARA DE COMERCIO DE FACATATIVA

La Junta Directiva de la Cámara de Comercio de Facatativá en ejercicio de sus atribuciones legales, estatutarias y en cumplimiento de las disposiciones legales y,

CONSIDERANDO

Que de conformidad con lo establecido en la Ley Estatutaria 1581 de 2012 y reglamentada parcialmente, por el Decreto Nacional 1377 de 2013, se hace necesario y obligatorio, implementar las Políticas de Seguridad de la Información, de la Cámara de Comercio de Facatativá,

Que de acuerdo a lo dispuesto en la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, el cual recoge las medidas de índole técnica y organizativa posibles y necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos de carácter personal que están bajo la responsabilidad de la Cámara de Comercio de Facatativá.

Que nuestro objetivo es que esta política tenga aplicación a las bases de datos que contienen datos de carácter personal que se hallan bajo la responsabilidad de la Cámara de Comercio de Facatativá, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente en protección de datos personales.

Con el ánimo de mejorar la estrategia de Seguridad de la información de la Cámara de Comercio de Facatativá, en adelante la Cámara de Comercio, 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 adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

Que en mérito de lo anteriormente expuesto:

RESUELVE:

ARTICULO 1º: OBJETIVOS: Formalizar el compromiso de la dirección frente a la gestión de la seguridad de la información y presentar de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la Cámara de Comercio 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, en constante cambio y evolución, de acuerdo con el avance de la tecnología y sus requerimientos.

Definir los lineamientos que debe seguir la Cámara de Comercio con relación a la seguridad de la Información, escritos en forma de políticas.

ARTICULO 2º: ALCANCE: La Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la Cámara de Comercio de Facatativá, dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos.

PARAGRAFO PRIMERO: 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;

PARAGRAFO SEGUNDO: Los usuarios de los activos de la información se clasifican así:

Colaboradores de Planta: se definen como aquellas personas que han suscrito un contrato laboral con la entidad.

Funcionarios de la Cámara de Comercio: Se definen como los empleados de la Cámara de Comercio, susceptibles de manipular sistemas de información.

Contratistas: aquellas personas que han suscrito contrato con la entidad y pueden ser: A) Colaboradores en Misión. B) Colaboradores por Outsourcing; aquellas personas que laboran en la entidad y tienen contrato con empresas de suministro de



servicios y que dependen de ellos. C) Personas naturales que prestan servicios independientes a la Cámara de Comercio. D) Proveedores de recursos informáticos.

Entidades de Control: A) Procuraduría General de la Nación. B) Contraloría General de la República. C) Superintendencia de Industria y Comercio. D) Revisoría Fiscal de la Cámara de Comercio.

Otras Entidades: A) DIAN. B) Registraduría Nacional del Estado Civil

ARTICULO 3º: DEFINICIONES. Para los propósitos de este documento se aplican los siguientes términos y definiciones:

Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la Cámara de Comercio.

Activo: Cualquier bien que tenga valor para la organización.

Administradores: Usuarios a quienes la Cámara de Comercio 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 Cámara de Comercio, quienes estarán bajo el amparo de la Dirección de Desarrollo Institucional.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Back up: Copia de la información en un determinado momento que puede ser recuperada con posterioridad.

Coordinación de planeación e innovación: función para garantizar el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas, además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la regulación vigente.

Comité de Seguridad: Equipo de trabajo conformado por el Presidente Ejecutivo, Director de Desarrollo Institucional, Coordinador de Sistemas de Información o los funcionarios que hagan sus veces.

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.

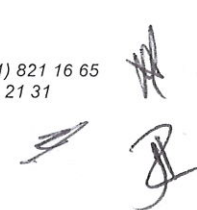
Evento de seguridad de la información: evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.

Incidente de seguridad de la información: indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información confidencial (RESERVADA): información administrada por la Cámara de Comercio 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 (CONFIDENCIAL): información generada por la Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por ésta. 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 (USO INTERNO): información generada por la Cámara de Comercio 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 siendo accesible por todos los usuarios.

Información pública: información administrada por la Cámara de Comercio en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo, la información de Registros Públicos y la 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 o una oficina).

Licencia de Software: 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

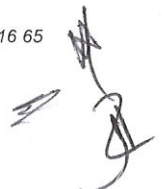
Copyright: Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones 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 muchos de los casos 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,

¹ Tomado de <http://www.derautor.gov.co/htm/preguntas.htm#01>



modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.

Software pirata: 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 ningún tipo de 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 software de dominio público es aquel en el cual 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 su adquisición 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 Cámara de Comercio.

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 acceso.

Plan de contingencia: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la Cámara de Comercio 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: aquellos elementos de tecnología de Información tales como:



computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos 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.p

Valoración del riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

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 Cámara de Comercio.

Sistema de encriptación: Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.

Sistema multiusuario: Computador y su software asociado, que permiten 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: 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 Cámara de Comercio

Usuarios de red y correo: Usuarios a los cuales la Cámara de Comercio 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 Cámara de Comercio 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 Cámara de Comercio 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.

ARTICULO 4º: COMPROMISO DE LA DIRECCIÓN. Es deber de la dirección, la implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información mediante las siguientes acciones:

- a) Establecer una política de seguridad de la información;
- b) Asegurar que se establezcan objetivos y planes de seguridad de la información;
- c) Establecer funciones y responsabilidades de la seguridad de la información;
- d) Comunicar a la Entidad la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidades de la mejora continua;
- e) Asegurar que se realizan auditorías internas.

ARTICULO 5º: GESTIÓN DE LOS RECURSOS. Para el correcto manejo de los recursos la Dirección deberá:

- a) Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de la misión y visión de la Cámara de Comercio de Facatativá.
- b) Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- c) Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
- d) Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.



ARTICULO 6°: COMUNICACIÓN DE LAS POLÍTICAS DE SEGURIDAD. Se deberá socializar y transmitir a los usuarios que acceden a los diferentes servicios de la Entidad y definidos en esta resolución las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

ARTICULO 7°: APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD. Las políticas de seguridad informática estarán orientadas a reducir el riesgo de incidentes de seguridad y minimizar su efecto; establecer las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática se encaminara a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia

ARTICULO 8°: POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO. La Cámara de Comercio 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.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen, según las funciones que realicen para la organización. 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.

La Entidad deberá implementar los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la Cámara de Comercio de Facatativá, con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la entidad, dando cumplimiento al marco jurídico aplicable a los estándares nacionales

ARTICULO 9°: POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA. Las normas establecidas mediante la presente resolución son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se clasifican 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 Cámara de Comercio
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.

ARTICULO 10: CUMPLIMIENTO CON LA 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 Ejecutiva de la Cámara de Comercio y al Comité de Seguridad de la Información.

ARTICULO 11: MEDIDAS DISCIPLINARIAS POR INCUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD.

Todo incumplimiento de la política de seguridad de la información por parte de un funcionario, colaborador o contratista, así como de cualquier estándar o procedimiento es causa para adelantar las acciones disciplinarias de acuerdo a lo establecido en el Reglamento Interno de Trabajo, el Reglamento Disciplinario de la Entidad y demás normas relacionadas, las cuales de acuerdo con su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista. Si el incumplimiento se origina en alguna sede de la Cámara de Comercio, ésta podrá suspender la prestación de cualquier servicio de información.

ARTICULO 12: INSTRUCCIONES PARA EL USO DE RECURSOS INFORMÁTICOS.

El uso de cualquier sistema de información y demás recursos informáticos por parte de los trabajadores, colaboradores, contratistas o usuarios de los sistemas de la Cámara de Comercio de Facatativá, debe someterse a todas las instrucciones técnicas, que imparta el Comité de Seguridad de la Información.

ARTICULO 13: USO PERSONAL DE LOS RECURSOS.

Los recursos informáticos de la Cámara de Comercio dispuestos para la operación, sólo 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 misma. Cualquier otro uso estará sujeto a previa autorización de la Presidencia Ejecutiva.

ARTICULO 14: ACUERDO DE CONFIDENCIALIDAD.

Para el uso de los recursos tecnológicos de la Cámara de Comercio de Facatativá, todo usuario debe firmar un



Acuerdo de Confidencialidad y un Acuerdo de Seguridad de los Sistemas de Información, antes de serle otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.

ARTÍCULO 15: PROHIBICIÓN INSTALACIÓN SOFTWARE Y HARDWARE EN COMPUTADORES DE LA CÁMARA DE COMERCIO. Se prohíbe la instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos de la Entidad, y solo podrá ser realizada por los funcionarios de Sistemas de Información autorizados por la Cámara de Comercio

ARTICULO 16: USO DEL APLICATIVO ENTREGADO. La Cámara de Comercio de Facatativá 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 Cámara de Comercio. Adicionalmente, cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado; de esta forma será controlado el acceso.

ARTICULO 17: EL USUARIO ES RESPONSABLE POR TODA ACTIVIDAD QUE INVOLUCRE SU IDENTIFICACIÓN PERSONAL O RECURSOS INFORMÁTICOS ASIGNADOS. Todo usuario es responsable por todas las actividades relacionadas con su identificación, identificación que no puede ser usada por otro individuo diferente a quien ésta le fue otorgada.

PARÁGRAFO: Los usuarios no deben permitir que ninguna otra persona realice 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 Cámara de Comercio.

ARTICULO 18: DECLARACIÓN DE RESERVA DE DERECHOS DE LA CÁMARA DE COMERCIO. La Cámara de Comercio de Facatativá usará 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 Cámara de Comercio de Facatativá se reserva el derecho y la autoridad de:



- a) Restringir o revocar los privilegios de cualquier usuario;
- b) Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y,
- c) Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la Cámara de Comercio.

PARÁGRAFO: La autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del Comité de Seguridad de la Información, siempre con el concurso de la Presidencia Ejecutiva o en quién se delegue esta función.

ARTICULO 19: RECURSOS COMPARTIDOS. Se prohíbe compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña; cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringiendo el Dominio.

ARTICULO 20: TODO MONITOREO DEBE SER REGISTRADO E INFORMADO AL JEFE INMEDIATO DEL USUARIO. Un usuario puede ser monitoreado bajo previa autorización del Comité de Seguridad de la Información.

ARTICULO 21: ACCESO NO AUTORIZADO A LOS SISTEMAS DE INFORMACIÓN DE LA ENTIDAD. Se prohíbe totalmente 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 encriptación y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

ARTICULO 22: 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.

ARTICULO 23: PROHIBICIÓN A EXPLOTACIÓN DE VULNERABILIDADES DE SEGURIDAD DE 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 caso de encontrar vulnerabilidades, éstas deben ser reportadas de inmediato al Comité de Seguridad.

ARTICULO 24: 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.



ARTICULO 25: NOTIFICACIÓN DE SOSPECHA DE PÉRDIDA, DIVULGACIÓN O USO INDEBIDO DE INFORMACIÓN. Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del Comité de Seguridad de la Información.

ARTICULO 26: ETIQUETADO Y PRESENTACIÓN DE INFORMACIÓN DE TIPO CONFIDENCIAL A LOS USUARIOS DE LOS COMPUTADORES. Toda la información que sea crítica para la organización debe ser etiquetada, de acuerdo con los niveles establecidos en el presente documento: USO INTERNO y CONFIDENCIAL.

ARTÍCULO 27: TRASLADO DE EQUIPOS DEBE ESTAR AUTORIZADO. Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de la Cámara de Comercio, sin previa autorización. 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 por el personal de Sistemas autorizado.

ARTICULO 28: CONTROL DE RECURSOS INFORMÁTICOS ENTREGADOS A LOS USUARIOS. Cuando un usuario inicie su relación laboral con la Cámara de Comercio se debe diligenciar el documento de entrega de inventario, procedimiento que se encuentra en la Dirección Administrativa y Financiera; si el empleado termina su vinculación laboral, es trasladado a otra dependencia o por alguna otra circunstancia deja de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá realizarse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario, debidamente firmado. El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

ARTICULO 29: 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.

ARTICULO 30: USO RESTRINGIDO DE MÓDEMS EN LAS ESTACIONES DE TRABAJO. Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet, a menos que se cuente con aprobación escrita por parte de Presidencia Ejecutiva.

ARTICULO 31: PROTECCIÓN POR DEFECTO DE COPYRIGHT. Todos los colaboradores de la Cámara de Comercio 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, para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la entidad.

ARTICULO 32: CUSTODIA DE LICENCIAS DE SOFTWARE. Las licencias deben ser custodiadas y controladas por el área de Sistemas, la cual debe realizar auditorías de licencia de software como mínimo una vez al año, generando las evidencias respectivas, con el fin de garantizar que los funcionarios solo tengan instalado software legal y autorizado por el Jefe de cada área.

ARTÍCULO 33: APAGADO DE EQUIPOS EN LA NOCHE. 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 durante la noche.

ARTICULO 34: TIEMPO LIMITADO DE CONEXIÓN EN APLICACIONES DE ALTO RIESGO. Si el usuario está conectado a un sistema que contiene información sensible, y éste presenta un tiempo de inactividad corto la aplicación deberá cerrar la sesión iniciada por el usuario.

ARTICULO 35: 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.

ARTICULO 36: USO DE DIFERENTES CONTRASEÑAS PARA DIFERENTES RECURSOS INFORMÁTICOS. Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso; esto involucra los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.

ARTICULO 37: 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; la política rige para aplicativos implementados hasta la fecha de liberación de este documento. Los funcionarios contarán con una identificación única personal y su



respectiva contraseña asignada por el encargado por el área de tecnología de la entidad.

ARTICULO 38: CAMBIOS PERIÓDICOS DE CONTRASEÑAS. Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.

ARTICULO 39: 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. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

ARTICULO 40: CONTRASEÑAS FUERTES. Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y caracteres especiales.

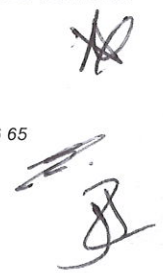
ARTICULO 41: PROHIBICIÓN DE CONTRASEÑAS CÍCLICAS. No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es "Enero-2015" que según la política "*Contraseñas fuertes*", es una contraseña válida, pero al mes siguiente pasa a ser "Febrero-2015" y así sucesivamente.

ARTICULO 42: LAS CONTRASEÑAS CREADAS POR USUARIOS NO DEBEN SER REUTILIZADAS. El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente; esta política es complementada por la política "*Prohibición de contraseñas cíclicas*".

ARTICULO 43: ALMACENAMIENTO DE CONTRASEÑAS. Ninguna contraseña debe ser guardada de forma legible en archivos "batch", scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras 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*".

ARTÍCULO 44: 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.

ARTICULO 45: REVELACIÓN DE CONTRASEÑAS PROHIBIDA. Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas.



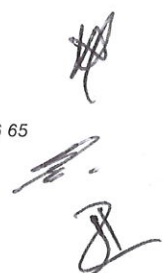
La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política “Auditoria periódica a las contraseñas de los usuarios”.

ARTICULO 46: 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. Por otra parte el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

ARTICULO 47: REPORTE DE CAMBIO EN LAS RESPONSABILIDADES DE LOS USUARIOS AL ADMINISTRADOR DEL SISTEMA. El ingeniero en soporte y web master debe reportar por medio de un correo electrónico, de manera oportuna al área de sistemas, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

ARTICULO 48: DIVULGACIÓN DE LA INFORMACIÓN MANEJADA POR LOS USUARIOS DE LA CÁMARA DE COMERCIO. La Cámara de Comercio 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 Cámara de Comercio 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.

ARTICULO 49: TRANSFERENCIA DE DATOS SÓLO A ORGANIZACIONES CON SUFICIENTES CONTROLES. La Cámara de Comercio 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.



ARTICULO 50: REGISTRO DE LAS COMPAÑÍAS QUE RECIBEN INFORMACIÓN PRIVADA. El personal de la Cámara de Comercio que libere información privada a terceros debe mantener un registro de toda divulgación y éste debe contener qué información fue revelada, a quién y fecha de divulgación.

ARTICULO 51: TRANSFERENCIA DE LA CUSTODIA DE INFORMACIÓN DE UN FUNCIONARIO QUE DEJA LA CÁMARA DE COMERCIO. Cuando un empleado se retira de la Cámara de Comercio, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico institucional como documentos impresos para determinar, quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

ARTICULO 52: TRANSPORTE DE DATOS SENSIBLES EN MEDIOS LEGIBLES. Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD's, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

ARTÍCULO 53: DATOS SENSIBLES ENVIADOS A TRAVÉS DE LAS REDES EXTERNAS DEBEN ESTAR ENCRIPADOS.

Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

ARTÍCULO 54: CLASIFICACIÓN DE LA INFORMACIÓN: Para efectos de la clasificación de la información se deberá tener en cuenta:

- a) Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.
- b) Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser "propiedad"³ de una parte designada de la Cámara de Comercio.
- c) Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.
- d) Cualquier uso de servicio de procesamiento de información debe ser autorizado por el Gerente de TI de las cámaras de comercio según el caso, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener

³ El término "propietario" identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga realmente derechos de propiedad de los activos.



conocimiento todos los usuarios involucrados.

ARTICULO 55: 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 Cámara de Comercio, antes de su entrega se les realizara un proceso de borrado seguro en la información.

ARTICULO 56: ELIMINACIÓN SEGURA DE LA INFORMACIÓN EN MEDIOS FÍSICOS. Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el Comité de Seguridad de la Información.

ARTICULO 57: 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 de 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"*.

ARTICULO 58: 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 de 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"*.

ARTICULO 59: 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.

ARTICULO 60: 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.

ARTICULO 61: 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.

ARTICULO 62: REVISIÓN DEL CORREO ELECTRÓNICO. Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias: así mismo, es su responsabilidad mantener espacio libre en el buzón.

ARTICULO 63: 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.

ARTICULO 64: 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 y avisar inmediatamente al área de sistemas.

ARTÍCULO 65: 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.

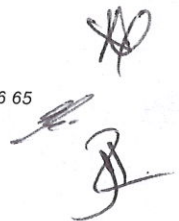
ARTICULO 66: ENVIANDO SOFTWARE E INFORMACIÓN SENSIBLE A TRAVÉS DE INTERNET. Software e información sensible de la Cámara de Comercio que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

ARTICULO 67: 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.

ARTICULO 68: REGLAS DE USO DE LA INTRANET. La Cámara de Comercio 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.

ARTICULO 69: PROHIBICIÓN DE PUBLICITAR LA IMAGEN DE LA CÁMARA DE COMERCIO EN SITIOS DIFERENTES A LOS INSTITUCIONALES. La publicación de logos, marcas o cualquier tipo de información sobre la Cámara de Comercio o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización de la Presidencia Ejecutiva; en consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

ARTICULO 70: PROHIBICIÓN ESTABLECER CONEXIONES A LOS SITIOS WEB DE LA CÁMARA DE COMERCIO. Prohibido establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de la Cámara de Comercio por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización de la



Presidencia, 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.

ARTICULO 71: PROHIBICIÓN DE ANUNCIOS EN SITIOS WEB PARTICULARES.

Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados de la Cámara de Comercio o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con la Cámara de Comercio.

ARTICULO 72: 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 la Cámara de Comercio, por lo menos una vez al año, utilizando el procedimiento interno "Análisis de riesgos"

ARTICULO 73: RESTRICCIÓN POR ACCESO TELEFÓNICO E INTERNET SOBRE RECURSOS TECNOLÓGICOS DE USO INTERNO A CLIENTES EXTERNOS.

No se otorgarán privilegios de acceso telefónico o Internet 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, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Presidencia.

ARTÍCULO 74: LOS COMPUTADORES MULTIUSUARIO Y SISTEMAS DE COMUNICACIÓN DEBEN TENER CONTROLES DE ACCESO FÍSICO APROPIADOS. Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

ARTICULO 75: 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 Cámara de Comercio.



ARTICULO 76: PREPARACIÓN Y MANTENIMIENTO DE PLANES PARA LA RECUPERACIÓN DE DESASTRES Y PARA RESPUESTA A EMERGENCIAS. Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación; 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. Así mismo, debe crear planes de respuesta a emergencia, con el fin de poder dar una pronta notificación de problemas y solución a los mismos en el evento de emergencias informáticas; estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor. 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 entidad.

ARTICULO 77: PERSONAL COMPETENTE EN EL CENTRO DE CÓMPUTO PARA DAR PRONTA SOLUCIÓN A PROBLEMAS. Con el fin de garantizar la continuidad de los sistemas de información, la Cámara de Comercio deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

ARTICULO 78: CHEQUEO DE VIRUS EN ARCHIVOS RECIBIDOS EN CORREO ELECTRÓNICO. La Cámara de Comercio 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, antes de ser transferidos a los computadores de los usuarios.

ARTICULO 79: 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, con el objeto de conocer las nuevas medidas en cuanto a seguridad de la información se van presentando.

ARTICULO 80: 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.

ARTICULO 81: 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.

ARTICULO 82: 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.

ARTICULO 83: 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.

ARTÍCULO 84: 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.

ARTICULO 85: DEPENDENCIA DE LA AUTENTICACIÓN DE USUARIO EN EL SISTEMA OPERATIVO. Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

ARTICULO 86: INCORPORACIÓN DE CONTRASEÑAS EN EL SOFTWARE. Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por la Cámara de Comercio o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política "Cambios periódicos de contraseñas".

ARTICULO 87: 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.

ARTICULO 88: REQUERIMIENTO DE REGISTROS DE AUDITORIA EN SISTEMAS QUE MANEJAN INFORMACIÓN SENSIBLE. Todo sistema que maneje información sensible para la Cámara de Comercio debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

ARTICULO 89: REGISTROS PARA LOS USUARIOS PRIVILEGIADOS EN LOS SISTEMAS EN PRODUCCIÓN QUE LO PERMITAN. Toda actividad realizada en los



sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alterno de control.

ARTÍCULO 90: LOS REGISTROS DEL SISTEMA DEBEN INCLUIR EVENTOS RELEVANTES PARA LA SEGURIDAD. Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

ARTICULO 91: RESISTENCIA DE LOS REGISTROS CONTRA DESACTIVACIÓN, MODIFICACIÓN Y ELIMINACIÓN. Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

ARTICULO 92: PROCESOS CONTROLADOS PARA LA MODIFICACIÓN DE INFORMACIÓN DEL NEGOCIO 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.

ARTICULO 93: 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.

ARTICULO 94: DISEÑO DE SEGURIDAD PARA APLICACIONES. El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para la Cámara de Comercio.

ARTICULO 95: 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.

ARTICULO 96: ARCHIVO HISTÓRICO DE CONTRASEÑAS. En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores; este archivo deberá usarse para prevenir que un usuario seleccione una contraseña ya usada (ver



Política “Las contraseñas creadas por usuarios no deben ser reutilizadas”) y deberá contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

ARTICULO 97: 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.

ARTICULO 98: LOS PRIVILEGIOS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN OTORGADOS A UN USUARIO TERMINAN CUANDO EL USUARIO FINALIZA SU VÍNCULO CONTRACTUAL CON LA ENTIDAD. Todos los privilegios sobre los recursos informáticos de la Cámara de Comercio otorgados a un usuario deben eliminarse en el momento en que éste abandone la entidad, y la información almacenada quede en manos de su jefe inmediato para aplicar procedimientos de retención o destrucción de información.

ARTICULO 99: ASIGNACIÓN DE CONTRASEÑAS POR 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

ARTICULO 100: LÍMITE DE INTENTOS CONSECUTIVOS DE INGRESO AL SISTEMA. El sistema debe limitar el número de intentos consecutivos de introducir una contraseña válida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados: a) Ser suspendido hasta nueva reactivación por parte del Administrador; b) Ser temporalmente bloqueado (no menos de 5 minutos); y c) Ser desconectado si se trata de una conexión telefónica.

ARTICULO 101: 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”.

ARTICULO 102: CAMBIO DE CONTRASEÑAS DESPUÉS DE COMPROMISO DETECTADO EN UN SISTEMA MULTIUSUARIO. Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema deberá asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deberán ser advertidos de cambiar su contraseña en otros

sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

ARTICULO 103: ADMINISTRACIÓN DE LOS BUZONES DE CORREO. Los Administradores deberán establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico; mensualmente se realizará una revisión de control sobre cada uno de los buzones creados con el fin de determinar cuáles requieren depuración para que no alcancen su límite de espacio asignado.

ARTICULO 104: BRINDAR ACCESO A PERSONAL EXTERNO. El Ingeniero de Soporte y web master velará porque individuos que no sean empleados, contratistas o consultores de la Cámara de Comercio no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Presidencia o el Comité de Seguridad.

ARTICULO 105: ACCESO A TERCEROS A LOS SISTEMAS DE LA ENTIDAD REQUIERE DE UN CONTRATO FIRMADO.

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de la Cámara de Comercio se requiere la firma de un formato, acuerdo o autorización de la Presidencia. Es obligatoria la firma del acuerdo de confidencialidad.

ARTICULO 106: 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.

ARTÍCULO 107: DOS USUARIOS REQUERIDOS PARA TODOS LOS ADMINISTRADORES. Los Administradores de Sistemas Multiusuarios deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

ARTICULO 108: PRIVILEGIOS POR DEFECTO DE USUARIOS Y NECESIDAD DE APROBACIÓN EXPLÍCITA POR ESCRITO. Sin autorización escrita de las Direcciones de Área de la Cámara de Comercio, los Administradores no deben otorgarle privilegios de administración a ningún usuario.

ARTICULO 109: NEGACIÓN POR DEFECTO DE PRIVILEGIOS DE CONTROL DE ACCESO A SISTEMAS CUYO FUNCIONAMIENTO NO ES APROPIADO. 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.

ARTICULO 110: 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 encriptación del software como tal.

ARTICULO 111: 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 Cámara de Comercio deben cumplir con las políticas y estándares internos de seguridad.

ARTICULO 112: 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 Back Up y todos los archivos potencialmente involucrados.

ARTICULO 113: SINCRONIZACIÓN DE RELOJES PARA UN REGISTRO EXACTO DE EVENTOS EN LA RED. Los dispositivos multiusuario conectados a la red interna de la Cámara de Comercio deben tener sus relojes sincronizados con la hora oficial.

ARTICULO 114: 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.

ARTICULO 115: 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.

ARTICULO 116: 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.

ARTICULO 117: SEGMENTACIÓN DE RECURSOS INFORMÁTICOS POR

PRIORIDAD DE RECUPERACIÓN. Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero. Todos los departamentos deberán usar el mismo marco para preparar los planes de contingencia a los sistemas de información.

ARTICULO 118: SOFTWARE DE IDENTIFICACIÓN DE VULNERABILIDADES. Para asegurar que el equipo técnico de la Cámara de Comercio ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de Cortafuegos y Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS (*Intrusión Detection System*), detección de virus y bloqueo de correo no deseado.

ARTÍCULO 119: DÓNDE USAR CONTROLES DE ACCESO PARA SISTEMAS INFORMÁTICOS. Todo computador que almacene información sensible de la Cámara de Comercio debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

ARTICULO 120: 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.

ARTICULO 121: 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 Cámara de Comercio.

ARTICULO 122: MONITOREO DE SISTEMAS. Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

ARTICULO 123: MANTENIMIENTO DE LOS SISTEMAS. Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios de la Cámara de Comercio

ARTICULO 124: VERIFICACIÓN FÍSICA DE EQUIPOS CRÍTICOS. Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.



ARTICULO 125: SERVICIOS DE RED. Se debe garantizar que el servicio de red utilizado por la Cámara de Comercio se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el Comité de Seguridad 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.

ARTICULO 126: 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.

ARTICULO 127: PERÍODO DE ALMACENAMIENTO DE REGISTROS DE AUDITORÍA. 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

ARTÍCULO 128: TIPO DE DATOS A LOS QUE SE LES DEBE HACER BACK UP Y FRECUENCIA. A toda información sensible y software crítico de la Cámara de Comercio residente en los recursos informáticos, se le debe hacer back up 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.

ARTICULO 129: COPIAS DE INFORMACIÓN SENSIBLE. Se deben elaborar una copia de cada back up con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

ARTICULO 130: 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.

ARTICULO 131: TODA CONEXIÓN EXTERNA DEBE ESTAR PROTEGIDA POR EL FIREWALL. Toda conexión a los servidores de la Cámara de Comercio 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.

ARTÍCULO 132: TODA CONEXIÓN HACIA INTERNET DEBE PASAR POR EL FIREWALL. 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 él.

ARTÍCULO 133: FILTRADO DE CONTENIDO ACTIVO EN EL PROXY. La dirección de TI de la Cámara de Comercio, debe asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como *applets* de Java, *Adobe Flash Player*, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de la Cámara de Comercio.

ARTÍCULO 134: FIREWALL DEBE CORRER SOBRE UN COMPUTADOR DEDICADO O APPLIANCE. Todo firewall debe correr sobre un computador dedicado o modelo *appliance* para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

ARTICULO 135: 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.

ARTÍCULO 136: 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.

ARTICULO 137: 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 si 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 a la Presidencia Ejecutiva.

ARTICULO 138: TÉRMINOS Y CONDICIONES PARA CLIENTES DE INTERNET. La Cámara de Comercio asume que todos los clientes que usan Internet para establecer relación con CONFECÀMARAS o realizan operaciones con las cámaras de comercio aceptan los términos y condiciones impuestos por la Cámara de Comercio en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.

ARTICULO 139: ACUERDOS CON TERCEROS QUE MANEJAN INFORMACIÓN O CUALQUIER RECURSO INFORMÁTICO DE LA CÁMARA DE COMERCIO. Todos los acuerdos relacionados con el manejo de información o de recursos de informática de la Cámara de Comercio por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados; esta cláusula debe permitirle a

la Cámara de Comercio ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de la entidad.

ARTICULO 140: DEFINICIÓN CLARA DE LAS RESPONSABILIDADES DE SEGURIDAD INFORMÁTICA DE TERCEROS. Socios de negocios, proveedores, clientes y otros asociados a los negocios de la Cámara de Comercio deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con la Cámara de Comercio y verificada por la Presidencia, el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante su estadía en las instalaciones de la Cámara de Comercio, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados

ARTICULO 141: 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.

ARTICULO 142: ORDEN DE SALIDA PARA EQUIPOS ELECTRÓNICOS. Ningún equipo electrónico podrá salir de las instalaciones de la Cámara de Comercio sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

ARTICULO 143: ORDEN DE SALIDA DE ACTIVOS. Todos los activos que afecten la seguridad de la información de la Cámara de Comercio como medios de almacenamiento, CDs, DVDs, entre otros, y que necesiten ser retirados de la entidad, se debe realizar la autorización de salida por medio del formato de autorización de salida de activos dispuesto para estos casos.

ARTICULO 144: PRIVILEGIOS DE ACCESO REVOCADOS A LA TERMINACIÓN LABORAL. Cuando exista una terminación laboral, los privilegios de acceso a la sede de la Cámara de Comercio serán revocados; el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnets, tarjetas de acceso, entre otros); para ello, el Director de Área enviará correo electrónico institucional al funcionario encargado de esta labor en el Área de Sistemas.

ARTICULO 145: INGRESO DE EQUIPOS DE GRABACIÓN Y FOTOGRAFÍAS AL CUARTO DE SERVIDORES. Cualquier miembro de la Cámara de Comercio y/o tercero deberá ser autorizado por la Presidencia o por quien él delegue para ingresar con los equipos con los que pueda obtener información; estos pueden ser videocámaras, celulares, cámaras fotográficas, entre otros.

ARTÍCULO 146: PROTECCIÓN DE LA INFORMACIÓN: Para la utilización de equipos portátiles, se deberá:

El antivirus siempre debe estar activo y actualizado.

- a) No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de la Cámara de Comercio.
- b) Seguir las políticas de acceso remoto.
- c) Toda la información que es confidencial debe ir cifrada.
- d) Cuando el equipo deba ser devuelto a la Cámara de Comercio para reparación, mantenimiento, entre otros, la información confidencial deberá ser borrada y guardada en una copia de respaldo.
- e) De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al Área de Sistemas.

ARTÍCULO 147: PROTECCIÓN DEL EQUIPO PORTÁTIL: Con el fin de proteger los equipos portátiles, se deberá tomar las siguientes medidas:

- a) No dejar el computador móvil en lugares públicos.
- b) Si el funcionario viaja, el computador portátil no debe ir dentro de su maletero; siempre deberá llevarse en su mano.
- c) Cuando vaya en su carro, el equipo deberá ubicarlo en el baúl.
- d) No prestar el computador portátil a familiares y/o amigos.

ARTICULO 148: La POLITICA DE LA SEGURIDAD DE LA INFORMACIÓN: se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Parágrafo 1º: La Junta Directiva de la Cámara de Comercio deberá aprobar el documento. El Comité de Seguridad de la Información delegará al Oficial de Seguridad la responsabilidad de publicación y comunicación a todos los empleados y partes externas pertinentes.

Parágrafo 2º: El mecanismo de notificación y divulgación de los cambios realizados a la Política de Seguridad de la Información será mediante correo electrónico institucional.

ARTICULO 149: COMITÉ DE SEGURIDAD: El Comité de Seguridad de la Información estará conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a Presidencia Ejecutiva, con respecto al programa de seguridad de la información dentro de la Cámara de



Comercio. Responsable de promover la seguridad de la organización mediante compromiso apropiado, contando con los recursos adecuados.

ARTICULO 150: INTEGRANTES DEL COMITE DE SEGURIDAD DE LA INFORMACION. El Comité de Seguridad de la Información estará integrado por:

- a) Presidente Ejecutivo.
- b) Director (a) Administrativo y Financiero o su delegado
- c) Director (a) Desarrollo Institucional o su delegado
- d) Director (a) Jurídico o su delegado.
- e) Coordinador Sistemas de Información.

ARTÍCULO 151: RESPONSABILIDADES COMITÉ DE SEGURIDAD DE LA INFORMACION: El Comité de Seguridad de la Información tendrá las siguientes funciones:

- a) Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización.
- b) Revisión y valoración de la Política de Seguridad de la Información.
- c) Alineación e integración de la seguridad a los objetivos del negocio.
- d) Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.
- e) Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.
- f) Reportar, a través de reuniones semestrales a la Presidencia, el estado de la seguridad y protección de la información en la compañía y la necesidad de nuevos proyectos en temas de seguridad de la información.
- g) Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información.
- h) Preparar y presentar para aprobación el presupuesto designado para el tema de seguridad de la información.
- i) Evaluar la adecuación, coordinación e implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.

- j) Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.
- k) Supervisar y controlar los cambios significativos en la exposición de los activos de información a las principales amenazas.
- l) Revisar y seguir los incidentes de seguridad de la información.
- m) Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la compañía.

ARTÍCULO 152: Comité tiene la responsabilidad de tratar los siguientes temas, según demanda:

- a) Mejoras en actividades inherentes a la seguridad de la entidad y sus procesos.
- b) 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 de la Cámara de Comercio.
- c) Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.
- d) Cambio en los roles del ciclo de certificación.
- e) Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la Política de Seguridad de la Información de la Cámara de Comercio. El Presidente convocará al Comité de Seguridad, con el propósito de evaluar los cambios a la citada política y autorizar su publicación, levantando Acta como constancia de su evaluación y aprobación

PARAGRAFO: Las decisiones del Comité de Seguridad son protocolizadas mediante Acta de Comité de Seguridad, debidamente firmada por todos su miembros. Las Actas de Comité de Seguridad podrán ser anuladas por el Comité de Seguridad mediante el uso de un Acta que invalide el contenido, siempre y cuando no se haya (n) ejecutado la(s) acción (es) relacionada(s)

ARTICULO 153: FUNCIONES OFICIAL DE SEGURIDAD DE LA INFORMACIÓN. Corresponderá al Oficial de Seguridad de la Información (Jefe de Riesgos o persona


designada para los temas de seguridad de la entidad), realizar las siguientes funciones.

- a) Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.
- b) Actualización y seguimiento periódico al mapa de riesgos de la organización, validando con cada proyecto que se implemente cómo afecta dicho mapa.
- c) Dirigir el programa de manejo y seguimiento de incidentes.
- d) Crear y establecer una metodología de clasificación de la información, según su importancia e impacto dentro de la Cámara de Comercio. Igualmente, informarla y validar su cumplimiento. La metodología debe establecer niveles de acceso a la información.
- e) Crear y mantener un Programa de Concientización en Seguridad de la información.
- f) Evaluar en forma continua la efectividad de la seguridad de la información de la organización, con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación

ARTÍCULO 154: ANEXOS. Los formatos adjuntos estarán bajo la custodia de la Oficina de Talento Humano, y reposaran en la Hoja de Vida de cada uno de los Funcionarios.

ARTICULO 155: VIGENCIA. La presente Resolución rige a partir de la fecha de aprobación y expedición y deroga todas aquellas normas que se sean contrarias.

COMUNIQUESE Y CUMPLASE


ROSA HASLEIDY SUÁREZ JIMÉNEZ
Presidente Junta Directiva


CARLOS ROGELIO BOLÍVAR CEPEDA
Secretario Junta Directiva

Proyecto y Reviso: DDI / XGGR 

SEDE PRINCIPAL: Carrera 3 No. 4-60. Tel (s): (091) 842 46 03 – 842 49 57 – Fax: 842 31 51

OFICINA RECEPTORA VILLETA: Calle 4 No. 4-39 Villeta – Tel. (091) 844 63 06

OFICINA RECEPTORA FUNZA: Calle 14 No. 15-04 Centro comercial Bancolombia-Márquez Plaza-. Teléfonos (091) 821 16 65

OFICINA RECEPTORA PACHO: Centro Comercial Pacho Centro Calle 7 No. 16-14 Oficina 202 Teléfono 854 21 31

www.ccfacatativa.org.co - compromiso@ccfacatativa.org.co

