POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: OT-A2-04 Fecha: 2018/07/18 Versión: 01

1. INTRODUCCIÓN

Con el ánimo de mejorar la Seguridad de la información de la CÁMARA DE COMERCIO DE TULUÁ, en adelante La Cámara de Comercio, surge la necesidad de alinear los procesos hacia un mismo objetivo, la seguridad en el manejo de la información.

Para tal fin y teniendo en cuenta el compromiso de la Dirección y Líderes de Proceso, se establece la Política de la Seguridad de la Información, la cual presenta de forma escrita a todos los usuarios, el compendio de normas y lineamientos establecidos para proteger a la Entidad de posibles riesgos de daño, pérdida y uso indebido de la información, equipos y demás recursos informáticos.

2. OBJETIVO

Precisar los lineamientos y directrices establecidas por la organización referente al uso adecuado de los recursos, que permitan mantener el control, protección y resguardo de la información para minimizar los riesgos asociados.

3. ALCANCE

La Política de Seguridad de la Información está dirigida a todos aquellos usuarios que poseen algún tipo de contacto con la información de la entidad.

Estos usuarios se han clasificado de la siguiente forma:

- **Colaboradores de Planta:** Son aquellas personas que han suscrito un Contrato Laboral y tienen relación directa con la Entidad.

- **Contratistas:** Se definen como a aquellas personas que han suscrito un contrato con la Entidad para la prestación de un servicio o la ejecución de una labor específica, estos pueden ser:

    - ✓ **Colaboradores en Misión o por Outsourcing:** Son aquellas personas que laboran en la Entidad, pero dependen y tienen contrato con empresas de suministro de servicios.
    - ✓ **Contratistas de Servicios:** Personas Naturales o Jurídicas que prestan servicios independientes a la Entidad;
    - ✓ **Proveedores de Recursos Informáticos:** Personas Naturales o Jurídicas que ofrecen y prestan servicios informáticos específicos.

- **Entidades de Control:** Son las entidades gubernamentales que tienen como misión ejercer control sobre la gestión de las entidades públicas y particulares que ejerzan funciones públicas, entre ellas:

    - ✓ Procuraduría;
    - ✓ Revisoría Fiscal;
    - ✓ Contraloría General de la República;
    - ✓ Superintendencia de Industria y Comercio.

- **Otras Entidades:** Entidades que por su labor pueden tener acceso a la información de la Cámara de Comercio de Tuluá.

    - ✓ DIAN;
    - ✓ Juzgados;
    - ✓ Registraduría Nacional del Estado;
    - ✓ Registro Único Empresarial y Social – RUES

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la Política de Seguridad de la Información, la Cámara de Comercio se regirá por lo dispuesto en el marco jurídico y normativo aplicable a las Cámaras de Comercio o entidades que las regulan y agrupan.

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 Cámara de Comercio.
- **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.
- **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.
- **Comité de Seguridad de la Información:** Equipo de trabajo integrado por los representantes de todas las áreas de la organización, destinado a definir y/o aprobar las estrategias para el control, protección y resguardo de la información de la Entidad.
- **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.
- **Encripción:** Proceso a través del cual utilizamos software para proteger información sensible mientras se encuentra en tránsito.
- **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 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:** Está 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:** 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. 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.
- **Información 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 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 y es accesible por todos los usuarios.
- **Información Pública:** Es la 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 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 o una oficina).
- **Licencia de Software:** Es la autorización o permiso concedido al usuario por el dueño del programa, para utilizarlo de una forma determinada conforme a unas condiciones convenidas. La licencia precisa los límites y los derechos de uso, modificación o redistribución concedidos a la persona autorizada, además puede señalar el lapso de duración y el territorio de la aplicación.[1]
- **Copyright:** Son el conjunto de derechos de exclusividad con que la ley regula el uso de una idea, una particular expresión 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).
- **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, dentro del cual, su 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. Su licencia expresamente especifica dichas libertades.
- **Software Pirata:** Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.

[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 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, en la que el usuario puede evaluar de forma gratuita el producto 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 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 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 de 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, 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.
- **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 Encripción:** 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:** 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 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 de información que puede ser aprovechada por una o más amenazas.

6. COMUNICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

La Dirección consciente de la importancia de la seguridad de la información y la estabilidad de los recursos informáticos, considera oportuno transmitir a todos los colaboradores y terceros, las normas y lineamientos de comportamiento para la utilización de equipos de cómputo y la administración y uso de la información y demás recursos informáticos.

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico info@camaratulua.org quien lo informará al Comité de Seguridad.

7. APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Las Políticas de Seguridad deberán ser aplicadas por los colaboradores, terceros y usuarios en general una vez publicado el presente documento, con el fin de reducir y mitigar los riesgos o incidentes de seguridad.

El desconocimiento que conlleve a la violación de lo anteriormente mencionado, representará para la persona involucrada las sanciones disciplinarias que apliquen según la omisión cometida.

8. POLÍTICA GENERAL 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, puesto que el uso no adecuado puede poner en peligro el activo estratégico de la organización, la información de las partes interesadas, la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Para ello, se implementarán los controles y acciones pertinentes encaminadas a garantizar la seguridad de los activos de información de La Cámara de Comercio, a fin de lograr un nivel de riesgo aceptable y el cumplimiento al marco jurídico aplicable a los estándares nacionales.

9. COMPROMISO DE LA DIRECCIÓN

La Dirección está comprometida con el establecimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar la información de la entidad, mediante:

- El establecimiento de una Política de Seguridad de la Información, asegurando que esta brinda apoyo al cumplimiento de la misión y visión de La Cámara de Comercio.
- La identificación y atención de los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;
- Asegurando que se establezcan y apliquen correctamente los mecanismos para salvaguardar la información;
- Estableciendo funciones y responsabilidades de la seguridad de la información;
- Comunicando a la organización la importancia de cumplir con las responsabilidades legales y reglamentarias en relación de la seguridad de la información;
- Promoviendo la mejora continua y la toma de conciencia sobre la importancia de la seguridad de la información.
- Asegurando que se realicen auditorías internas.

10. CUMPLIMIENTO Y SANCIONES

10.1. Todos los colaboradores, Contratistas y terceros, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información.

10.2. El Área de Sistemas y el Comité de Seguridad realizarán acciones de verificación del cumplimiento de las Políticas y Estándares de Seguridad Informática.

10.3. El Área de Sistemas y el Comité de Seguridad podrán implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, con el fin de revisar la actividad de los procesos que ejecuta y la estructura de los archivos que se procesan.

10.4. El Área de Sistemas podrá realizar auditorías de licencia de software como mínimo una vez al año, lo anterior para garantizar que los funcionarios solo tienen instalado software legal.

10.5. Todo incumplimiento a la Política de Seguridad de la Información por parte de un funcionario o contratista, es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

11. USO DE RECURSOS INFORMÁTICOS

Del Uso de los Recursos Informáticos

11.1. El uso de cualquier sistema de información y demás recursos informáticos de La Cámara de Comercio, deben estar basados en los lineamientos y directrices establecidos por el Área de Informática y el Comité de Seguridad.

11.2. Los sistemas de información de la Cámara de Comercio deberán ser utilizados con fines institucionales.

11.3. Se encuentra permitido el uso de los recursos tecnológicos de la Cámara de Comercio con fines personales, siempre y cuando no afecte la prestación del servicio, la productividad ni la seguridad de la información corporativa.

11.4. El resultado del uso de dichos recursos tecnológicos, será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad

11.5. Para el uso de los recursos tecnológicos de La Cámara de Comercio, todo usuario debe firmar el Acta de Entrega, además de conocer la Política de Seguridad de la Información.

11.6. El empleado tiene la obligación de proteger los discos, cintas magnéticas, CD-ROM y/o USB que se encuentren bajo su administración.

Del Acceso a los Recursos Informáticos

11.7. Cada usuario contará con un perfil limitado dependiendo de las actividades que realice sobre las aplicaciones.

11.8. Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad o cuando se establezcan cambios internos que así lo ameriten.

11.9. Todo usuario es responsable por 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 realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más.

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

11.11. 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.

11.12. La Cámara de Comercio usará controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información. Para mantener estos objetivos La Cámara de Comercio 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. Esta autoridad se puede ejercer con o sin conocimiento de

los usuarios, bajo la responsabilidad del Comité de Seguridad siempre con el concurso de la Presidencia o de quién él delegue esta función generando un acta de intervención debidamente firmada.

11.13. Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos estos se debe restringir por Dominio.

Cualquier monitoreo debe ser solicitado por la Presidencia Ejecutiva o la Dirección Administrativa.

11.14. Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios, o 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.

11.15. Los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, u 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 Área de Informática.

11.16. 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.

11.17. 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.

11.18. Todas las aplicaciones que contiene información sensible, están parametrizadas para cerrarse al momento de presentarse un tiempo corto de inactividad, por tal razón, cada vez que se presente lo anterior, la aplicación cerrará la sesión iniciada por el usuario.

11.19. Todas las estaciones de trabajo tendrán activado el bloqueo automático de estación, el cual, se activará luego de un período de ausencia o inactividad.

11.20. El escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

11.21. El Director o Jefe del Área debe reportar oportunamente por medio de un correo electrónico al Área de Sistemas, todos los cambios significantes en las responsabilidades de un usuario, su estado laboral y/o su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

11.22. No se otorgarán privilegios de acceso telefónico o conexión a la red local 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 Dirección Administrativa.

De los Equipos

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

11.24. Está terminantemente prohibido copiar o extraer cualquiera de los aplicativos instalados en los computadores de la Entidad.

11.25. El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

11.26. 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.

11.27. El empleado que tenga bajo su custodia algún equipo informático, será responsable de su uso y conservación; en consecuencia, responderá con su propio patrimonio por la pérdida, daño o deterioro que ocurra a los equipos cuando el hecho acontezca por negligencia o culpa del trabajador.

11.28. Mientras se opere los equipos informáticos no se debe consumir alimentos o ingerir líquidos.

11.29. Se debe evitar colocar objetos encima de los equipos informáticos o cubrir los orificios de ventilación.

11.30. El empleado debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

11.31. Los terceros que requieran el uso de un equipo de cómputo, podrán hacer uso de las terminales de autoconsulta o portátiles que están fuera de la red local.

11.32. El empleado deberá dar aviso inmediato de la desaparición, robo o extravío de los equipos informáticos o accesorios bajo su resguardo a la Dirección Administrativa y Financiera.

11.33. Con el fin de proteger la seguridad y funcionamiento de los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios durante la noche.

11.34. Ningún equipo informático debe ser reubicado o trasladado dentro o fuera de las instalaciones de La Cámara de Comercio sin previa autorización. El traslado de los equipos

se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

11.35. 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 o el recurso tecnológico suministrado con carácter permanente, deberá informarlo al Área de Informática.

12. USO DE LA INFORMACIÓN

12.1. La Cámara de Comercio podrá divulgar la información de un usuario almacenada en los sistemas de información, 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 suscritas en la ley de protección de datos personales.

12.2. 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.

12.3. La información proveniente de las demás funciones de la Cámara de Comercio es administrada y conservada, conservando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información, previamente clasificada, salvó autorización del titular de la misma para su divulgación.

12.4. La Cámara de Comercio puede transmitir información privada a terceros siempre y cuando haya la debida autorización previa del Jefe del Área responsable de la misma y el tercero se comprometa a mantener dicha información bajo controles adecuados de protección.

12.5. Es responsabilidad del empleado evitar en todo momento la fuga de la información de la Cámara que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

12.6. Al momento de existir el retiro de un empleado de La Cámara de Comercio, su jefe inmediato debe revisar en conjunto con el colaborador, los archivos magnéticos, correo electrónico y documentos impresos producto de su trabajo, para determinar el tratamiento a realizar según lo dispuesto en la Tablas de Retención Documental (TRD). De igual forma, debe asignar el nuevo responsable de la información.

12.7. Toda destrucción de información debe ser informada al Proceso de Gestión Documental, para garantizar los métodos y el proceso adecuado de eliminación.

12.8. Se debe evitar el transporte de información sensible en medios legibles por el computador (Discos externos, memorias USB, CD), a excepción que dicho medio se encuentre totalmente encriptado y el receptor acepte el intercambio de datos cifrados.

12.9. 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.

12.10. 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 realizará un proceso de borrado seguro en la información.

12.11. Los activos de información de la entidad, serán identificados y clasificados para el adecuado y correcto uso de los mismos.

Los empleados deben acatar las reglas y reglamentos para el uso aceptable de los activos de información.

12.12. Los documentos impresos que contengan información sensible o crítica deben estar siempre almacenados o guardados en lugares que garanticen su seguridad y conservación y protejan su acceso inclusive durante horas no laborales.

12.13. Los empleados deben usar los logos y las marcas de la entidad con moderación y solo con fines laborales.

13. USO DE LAS CONTRASEÑAS

13.1. A cada usuario se le asignará 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.

13.2. 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.

13.3. Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso.

13.4. Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso al sistema. En ese momento, los usuarios deben cambiar su contraseña.

13.5. Las contraseñas deben ser cambiadas una vez cada 30 días o de acuerdo a lo parametrizado en cada recurso informático.

13.6. Todos los usuarios serán automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.

13.7. Las contraseñas deben tener una longitud mínima de ocho (8) caracteres, además de Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales.

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

13.9. El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Un ejemplo de este tipo de contraseñas prohibidas es establecer “Enero-2004” y al mes siguiente pasar a ser “Febrero-2004”, y así sucesivamente.

13.10. Las contraseñas no debe ser guardadas de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas.

13.11. Está totalmente prohibido tener las contraseñas en cualquier medio impreso, con excepción de las contraseñas de administrador, que se almacenan de manera custodiada.

13.12. Los usuarios solo contarán con un límite de tres (3) intentos consecutivos para introducir una contraseña valida, de no ser así, el sistema bloqueará el ingreso del usuario.

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

13.14. 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.

13.15. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.

14. USO DE INTERNET Y CORREO ELECTRÓNICO

Acceso a Internet

14.1. Todos los empleados de la Cámara de Comercio con sistemas de información asignados, tendrán acceso a Internet desde sus estaciones de trabajo. La Cámara se reserva el derecho de retirar o restringir dicho acceso.

14.2. El uso de Internet está limitado exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña; los colaboradores deben tener en cuenta que los recursos tecnológicos generan registros sobre las actividades realizadas.

14.3. Se prohíbe el uso de aplicaciones, programas y/o herramientas que saturen los canales de comunicación o Internet, tales como gestores de descarga, gestores de archivos multimedia (audio y/o videos), entre otros.

14.4. Los Colaboradores pueden intercambiar a través de internet información interna de carácter laboral, con la debida aprobación y usando los mecanismos de seguridad apropiados.

14.5. Queda prohibido el uso de módems o acceso inalámbrico a redes externas en las estaciones de trabajo que estén dentro de la red local.

14.6. Los empleados de la Cámara de Comercio con acceso a Internet deben reportar todos los incidentes de seguridad informática inmediatamente al Área de Sistemas.

14.7. La Cámara de Comercio para el control de la navegación en Internet, restringirá el acceso a sitios de contenido pornográfico, consumo de ancho de banda, contenidos racistas, violencia, ocio, etc. De necesitarse el acceso a una página bloqueada deberá ser autorizado por el Jefe de Área con el concepto del Área de Sistemas.

14.8. La Cámara de Comercio debe contar con los medios adecuados para el escaneo de los archivos descargados de internet y la identificación de virus, antes de ser transferidos a los computadores de los usuarios.

Correo Electrónico

14.9. Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser monitoreada.

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

14.11. Los empleados deben utilizar los buzones institucionales. Está prohibido tramitar información institucional a través de e-mails privados o de uso personal (Yahoo, Gmail, Hotmail, etc.)

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

14.13. Todos los usuarios que dispongan de correo electrónico, tienen la responsabilidad de revisarlo periódicamente y mantener libre el buzón de entrada.

14.14. Se prohíbe el uso del correo electrónico institucional con fines religiosos, humorísticos, pornográficos, publicitarios, políticos, lúdicos, personales o cualquier otro mensaje ajeno a los fines laborales, sin importar el tipo de contenido (Texto, Audio, Video).

14.15. En el caso de recibir un correo no deseado o no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al Área de Sistemas.

14.16. Cualquier 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.

14.17. Los usuarios no deben enviar archivos adjuntos por el correo electrónico que excedan los 15 MB, dado que pueden provocar lentitud en los demás buzones de correo electrónico de la entidad.

14.18. Está prohibido el envío de correos masivos a más de veinte (20) remitentes, en caso de requerirse, se debe realizar el envío a través del software de envío masivo de correos electrónicos.

14.19. Los usuarios podrán almacenar los correos electrónicos de Alta Importancia en su carpeta de trabajo, para ser incluidos dentro de la copia diaria de Backup de Archivos Críticos.

15. RESPALDO Y RESTAURACIÓN (BACKUP)

15.1. Toda la información sensible y los software críticos de La Cámara de Comercio residente en los recursos informáticos, debe contar con el respectivo backup que garantice la protección y disponibilidad de la información.

15.2. El Área de Sistemas es el responsable de respaldar periódicamente la información contenida en los servidores de la Cámara.

15.3. Los usuarios de los recursos informáticos, son los responsables de validar la ejecución de su bakcup diario, de no ejecutarse, deben realizarlo manualmente o informar al Área de Sistemas.

15.4. El Área de Sistemas debe validar periódicamente la ejecución y disponibilidad de los Backup de la información de la entidad.

16. USO DE PORTATILES

16.1. Los equipos de Cómputo Portátiles no deben dejarse sin protección en su lugar de trabajo o cualquier otro lugar.

16.2. Los equipos portátiles deben contar con Antivirus activo y actualizado.

16.3. Cuando los equipos portátiles deban ser enviados para reparación o mantenimiento, la información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo.

17. ADMINISTRADORES DE SISTEMAS

17.1. Todos los sistemas y computadores multiusuarios (servidor) deben contar con dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

17.2. 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.

17.3. En caso de identificarse un compromiso de seguridad en un sistema multiusuario, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata, además de informar a los usuarios la necesidad de cambiar sus contraseñas.

17.4. Al menos dos (2) personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de La Cámara de Comercio.

17.5. El personal involucrado con la seguridad de la información deberá actualizar sus conocimientos periódicamente, con el objetivo de conocer las nuevas medidas, tendencia y controles relacionados con la seguridad de la información

17.6. Toda la información que sea crítica para la organización, debe ser identificada y etiquetada de acuerdo a los niveles establecidos (uso interno o confidencial) como lo establece el documento Índice de información Clasificada y Reservada.

17.7. Las licencias de Software deben ser custodiadas y controladas por el Área de Informática.

17.8. Cada recurso informático y equipo de comunicación (firewall, routers, servidores de control de acceso), deberá contar son su respectiva contraseña de acceso de administrador.

17.9. En caso de identificarse un mal funcionamiento de un sistema de control de acceso, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

17.10. El administrador debe validar que los parámetros de configuración de todos los dispositivos conectados a la red de La Cámara de Comercio, cumplan con las políticas y estándares internos de seguridad.

17.11. El administrador debe velar y garantizar la ejecución regular del mantenimiento preventivo a todos los computadores y sistemas de la entidad.

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

17.13. El Área de Sistemas en conjunto con el Comité de Seguridad Informática, deben velar por la adecuada gestión de los riesgos relacionados con la seguridad informática.

17.14. El Área de Sistemas debe garantizar que el servicio de red utilizado por La Cámara de Comercio se encuentre disponible y operando adecuadamente, para ello debe efectuar escaneos periódicos de la red con la finalidad de resolver problemas, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

17.15. El acceso al centro de cómputo y servidores, debe estar restringido y solamente el personal autorizado podrá acceder a estos lugares.

17.16. La Cámara de Comercio debe contar con una consola de administración de Cortafuegos y Antivirus, en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades.

17.17. Periódicamente el Área de Sistemas debe verificar el estado físico de los equipos informáticos críticos de la entidad.

18. USO DE FIREWALL

18.1. 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.

18.2. 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, con el fin de limitar y controlar las puertas de entrada a la organización.

18.3. 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.

18.4. 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.

18.5. Se debe contar con un diagrama de red de las conexiones a redes externas de la entidad, con el fin de tener una imagen clara de todos los puntos de entrada a la organización.

18.6. 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.

19. REVISIÓN Y ACTUALIZACIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Este documento debe ser revisado y actualizado cada vez que se produzcan cambios significativos relacionados con la seguridad de la información de la entidad o cuando el Comité de Seguridad de la Información así lo considere, de tal forma que se garantice que las políticas aquí contenidas siguen siendo adecuadas, suficientes y eficaces.

El Comité de Seguridad y la Presidencia aprobarán el documento y lo pondrán a disposición de los colaboradores y las partes externas pertinentes.

20. COMITÉ DE SEGURIDAD

El Comité de Seguridad de la Información está conformado por un equipo de trabajo interdisciplinario encargado de brindar apoyo y tomar decisiones con respecto al programa de seguridad de la información de la entidad.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad de la información de la entidad:

- Revisión, actualización y aprobación de la Política de Seguridad de la Información.
- Garantizar la alineación e integración de la seguridad de la información dentro de los objetivos y planeación estratégica de la organización.
- Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la compañía.
- Establecer y respaldar las actividades de concientización de la organización en materia de seguridad y protección de la información.
- Promover explícitamente la seguridad de la información en toda la organización.

- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información
- Evaluar la adecuación, coordinación e implementación de los controles de seguridad específicos para los servicios o sistemas de información.
- Supervisar y controlar los cambios significativos en la exposición de los activos de información de la entidad.
- Revisar y tomar decisiones sobre los incidentes u omisiones relacionados con la seguridad de la información.
- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos críticos fuera de la organización.
- Dejar constancia de las reuniones y decisiones tomadas por el Comité.

Así mismo, el Comité tiene la responsabilidad de tratar los siguientes temas:

- Aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Cámara de Comercio.
- Mejoras propuestas en las actividades inherentes a la Seguridad de la Información de La Cámara de Comercio y sus procesos.
- Acciones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de la información de los procesos.
- Recomendaciones que fortalezcan las políticas, planes o programas de la seguridad de la información de la entidad.

21. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información cuenta con las siguientes responsabilidades:

- Validar la expedición o modificación de las leyes relacionada con la protección de datos personales y protección de la información.
- Hacer seguimiento y validar la ejecución del programa de seguridad de la información de la entidad.
- Crear y mantener en conjunto con el Área de Sistema un Programa de Concientización en seguridad de la información.
- Guiar al cuerpo directivo y a la administración de la organización ante incidentes de seguridad.
- Proponer y coordinar la realización, actualización y seguimiento de la gestión de los riesgos de seguridad de la información de toda la organización.
- Proponer el desarrollo de procedimientos de seguridad detallados que fortalezcan la política de seguridad informática institucional.
- Promover la revisión y actualización de las políticas de seguridad informática.
- Coordinar en conjunto con el Área de Sistema la realización periódica de auditorías a las prácticas de seguridad informática, así como, dar seguimiento de las recomendaciones que hayan resultado de cada auditoria.