SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS

CÁMARA DE COMERCIO DE CÚCUTA

Contenido

1. INTRODUCCIÓN....6
2. OBJETIVO....6
3. ALCANCE....6
4. REQUISITOS LEGALES Y/O REGLAMENTARIOS....7
5. DEFINICIONES....7
6. RESPONSABLE....10
6.4. APROBACIÓN Y GESTIÓN DE LOS RECURSOS....10
6.4.1 APROBACIÓN DE LOS RECURSOS....10
7. PROCEDIMIENTO....11
7.1. POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO....11
7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA....11
7.3. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES....12
7.3.1. Cumplimiento con la seguridad de la información....12
7.3.2. Medidas disciplinarias por incumplimiento de políticas de seguridad....12
7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS....12
7.4.1. Instrucciones para el uso de recursos informáticos.....12
7.4.2. Uso personal de los recursos....12
7.4.3. Acuerdo de confidencialidad....12
7.4.4. Prohibición de instalación de software y hardware en los computadores de La Cámara de Comercio. ...12
7.4.5. Uso del aplicativo entregado.....13
7.4.6. El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.....13
7.4.7. Declaración de reserva de derechos de La Cámara de Comercio....13
7.4.8. Todo seguimiento debe ser registrado e informado al jefe inmediato del usuario.....13
7.4.9. Acceso no autorizado a los sistemas de información de la Entidad.....13
7.4.10. Posibilidad de acceso no implica permiso de uso.....13
7.4.11. Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.....14
7.4.12. Manejo de sesiones en sistemas informáticos....14
7.4.13. Traslado de equipos debe estar autorizado.....14
7.4.14. Control de recursos informáticos entregados a los usuarios.....14
7.4.15. Protección por Defecto de Copyright....14
7.4.16. Custodia de Licencias de Software....14
7.4.17. Tiempo limitado de conexión en aplicaciones críticas....14
7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS....15

7.5.1. Confidencialidad de las contraseñas....15
7.5.2. Identificación única para cada usuario. 15
7.5.3. Cambios periódicos de contraseñas....15
7.5.4. Contraseñas fuertes. 15
7.5.5. Las contraseñas creadas por usuarios no deben ser reutilizadas. 15
7.5.6. Almacenamiento de contraseñas. 15
7.5.7. Sospechas de compromiso deben forzar cambios de contraseña. 15
7.5.8. Revelación de contraseñas prohibida. 15
7.5.9. Reporte de cambio en las responsabilidades de los usuarios a la Dirección de TI. 15
7.6. POLÍTICAS DE ACTIVOS INFORMÁTICOS 16
7.6.1. Transferencia de la custodia de información de un funcionario que deja La Cámara de Comercio....16
7.6.2. Transporte de datos sensibles en medios legibles....16
7.6.3. Clasificación de activos informáticos....16
7.6.4. Eliminación Segura de la Información....16
7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO 16
7.7.1. Prohibición de uso de Internet para propósitos personales. 16
7.7.2. Formalidad del correo electrónico....16
7.7.3. Uso de correo electrónico....17
7.7.4. Revisión del correo electrónico....17
7.7.5. Acciones para frenar el SPAM. 17
7.7.6. Todo buzón de correo debe tener un responsable....17
7.7.7. Intercambio de información a través de Internet....17
7.8. POLÍTICAS DE LA INTRANET Y SITIOS WEB DE LA CÁMARA DE COMERCIO 17
7.9. POLÍTICAS GENERALES DE SEGURIDAD....17
7.9.1. Restricción sobre recursos tecnológicos de uso interno....17
7.9.2. Los Servidores y sistemas de comunicación deben tener controles de acceso físico apropiados. 17
7.9.3. Entrenamiento compartido para administración de los sistemas. 17
7.9.4. Ejecución del plan de contingencia para la recuperación ante desastres. 18
7.9.5. Personal competente en la Dirección de TI para dar pronta solución a problemas. 18
7.9.6. Chequeo de virus en archivos recibidos en correo electrónico. 18
7.10. POLÍTICAS PARA DESARROLLADORES DE SOFTWARE....18
7.10.1. Ambientes separados de producción y desarrollo....18

7.10.2. Documentación de sistemas de información. 18
7.10.3. Se requieren registros de auditoria en sistemas críticos. 18
7.10.4. Los registros del sistema deben incluir eventos relevantes para la seguridad. 18
7.10.5. Personas autorizadas para leer los registros de auditoría. 19
7.11. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS 19
7.11.1. Soporte para usuarios con privilegios especiales. 19
7.11.2. Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad. 19
7.11.3. Cuando y como pueden asignar contraseñas los administradores. 19
7.11.4. Administración de los buzones de correo. 19
7.11.5. Brindar acceso a personal externo. 19
7.11.6. Restricción de administración remota a través de Internet. 19
7.11.7. Manejo administrativo de seguridad para todos los componentes de la red. 19
7.11.8. Sincronización de relojes para un registro exacto de eventos en la red. 20
7.11.9. Revisión periódica de las vulnerabilidades de los sistemas de información. 20
7.11.10. Confidencialidad en la información relacionada con investigaciones internas. 20
7.11.11. Software de identificación de vulnerabilidades. 20
7.11.12. En dónde usar controles de acceso para sistemas informáticos. 20
7.11.13. Mantenimiento preventivo en computadores y sistemas de redes. 20
7.11.14. Registro de Logs en Sistemas y Aplicaciones 20
7.11.15. Monitoreo de Sistemas de información. 20
7.11.16. Servicios de Red 20
7.11.17. Revisión de accesos de usuarios 21
7.12. POLÍTICAS DE COPIAS DE RESPALDO 21
7.12.1. Período de almacenamiento de copias de respaldo. 21
7.12.2. Tipo de datos a los que se les debe hacer backup y con qué frecuencia. 21
7.13. POLÍTICAS DE USO DE FIREWALL 21
7.13.1. Detección de intrusos. 21
7.13.2. Toda conexión externa debe estar protegida por el firewall. 21
7.13.3. Toda conexión hacia Internet debe pasar por el Firewall. 21
7.13.4. Filtrado de contenido. 21
7.13.5. Firewall debe correr sobre un servidor dedicado o appliance. 21
7.13.6. El sistema interno de direccionamiento de red no debe ser público. 22

7.14. POLÍTICAS PARA USUARIOS EXTERNOS....22
7.14.1. Definición clara de las responsabilidades de seguridad informática de terceros....22
7.15. POLÍTICAS DE ACCESO FÍSICO....22
7.15.1. Reporte de pérdida o robo de identificación....22
7.15.2. Orden de salida para servidores y equipos de telecomunicaciones....22
7.15.3. Cuando se da una terminación laboral, los privilegios de acceso a la sede de La Cámara de Comercio deben ser revocados....22
7.15.4. Ingreso a los centros de datos....22
8. POLITICA DE USO DE PORTATILES....22
8.1. Protección de la información....22
8.2. Protección del equipo portátil....23
9. ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN. 23
10. VIGENCIA....23
11. CONTROL DE CAMBIOS....23

1. INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de **LA CÁMARA DE COMERCIO DE CÚCUTA**, en adelante La Cámara de Comercio, surge la necesidad de documentar la política que contiene los lineamientos en lo referente al uso adecuado de los recursos tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo parámetros y directrices que orienten a los colaboradores y permitan asegurar la integridad, confidencialidad, veracidad y disponibilidad de la información en la Entidad.

2. OBJETIVO

Este documento formaliza el compromiso de la Alta dirección frente a la gestión de la seguridad de la información y presenta a los usuarios de los sistemas de información de la Entidad, los lineamientos establecidos para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, de los equipos y demás recursos informáticos, los cuales están en constante evolución de acuerdo con el avance de la tecnología y las buenas prácticas en materia de seguridad de la información.

3. ALCANCE

La Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la Cámara de Comercio y por tanto está dirigido a todos los usuarios del ente cameral que posean algún tipo de contacto con estos activos. Los usuarios deberán firmar un acuerdo de confidencialidad, que los compromete con el cumplimiento de las políticas de seguridad aquí descritas.

Los usuarios de los activos de información de la Entidad se han clasificado así:

- Colaboradores de Planta: se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.

- Colaboradores de la Cámara de Comercio: Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular sistemas de información.

- Contratistas: se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:
  - Colaboradores en Misión;
  - Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos;
  - Personas naturales que prestan servicios independientes a la Entidad;
  - Proveedores de recursos informáticos.

- Entidades de Control
  - Procuraduría;
  - Revisoría Fiscal;

- Contraloría General de la República;
- Superintendencia de Industria y Comercio.

- Otras Entidades
  - DIAN;

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la política de seguridad de la información, la Cámara de Comercio debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Cámaras de Comercio y/o entidades que las regulan, entre los que se encuentran:

- Resolución 1519 de 2020 del MinTIC
- Circular 18 de la PGN de 2021
- Circular 100-00002 de 2022 de la SuperSociedades
- Ley 1581 de 2012
- NTC ISO 27001 de 2013

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 sobre los recursos informáticos de la Cámara de Comercio quienes estarán bajo la Dirección de tecnología de la información.
- **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 y protección de datos personales**: Equipo de trabajo conformado por la resolución de creación del comité.
- **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**: Un 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/o software que protegenrecursos 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 reservada**: Información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que debido a aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de esta.
- **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 colaboradores por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de esta y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad.
- **Información privada:** 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 autorizadano 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.
- **Licencia de Software**: Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.[1]
- **Copyright**: Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. 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.
- **Open Source** (Fuente Abierta): Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.
- **Software Libre**: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
- **Software pirata**: Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigidapor 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, o con unas

funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago.

- **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 que impidan el funcionamiento normal.
- **Política:** Toda intención y directriz expresada formalmente por la Alta dirección.
- **Recursos informáticos**: Son aquellos elementos de tecnología de Información tales como: equipos de cómputo, servidores, elementos de comunicaciones, elementos de almacenamiento de información, sistemas de información y bases de 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.
- **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/o 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 accesos indebidos a la información.
- **Sistema operativo**: Software que controla los recursos físicos de un computador.
- **Usuario**: toda persona que pueda tener acceso a un recurso informático de La Cámara de Comercio
- **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.
- **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

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

6. RESPONSABLE

6.1. COMPROMISO DE LA PRESIDENCIA EJECUTIVA

- Liderar el compromiso de la Entidad con la implementación, revisión y mejora de los mecanismos para asegurar la información.
- Asignar los recursos necesarios para garantizar la seguridad de la información, incluyendo recursos humanos y herramientas físicas y tecnológicas.
- Respaldar e incentivar actividades tendientes al cumplimiento de funciones y responsabilidades en materia de la seguridad de la información.
- Asegurar que la seguridad de la información brinda apoyo al cumplimiento de la misión y visión de La Cámara de Comercio.

6.2. COMPROMISO DE LA DIRECCIÓN DE TI

- Asegurar y evidenciar la implementación, operación, seguimiento, revisión y mejora de los controles informáticos y mecanismos tecnológicos para asegurar la información.
- Establecer planes y actividades relacionados con la seguridad de la información
- Adelantar las acciones del plan de sensibilización de la política de seguridad de la información
- Realizar las revisiones y actualizaciones pertinentes de manera periódica de la política de seguridad de la información y socializar.

6.3. COMPROMISO DE LA GERENCIA DE DESARROLLO ESTRATÉGICO

- Comunicar a todos los colaboradores la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua, como parte de la estrategia de la Cámara.
- Realizar la planeación de auditoría internas relacionadas con los sistemas de gestión integrados que se encuentren implementadas
- Documentar los procedimientos que sean requeridos en el marco de la seguridad de la información.

6.4. APROBACIÓN Y GESTIÓN DE LOS RECURSOS

6.4.1 APROBACIÓN DE LOS RECURSOS

La Presidencia Ejecutiva de la Cámara de Comercio de Cúcuta aprobará los recursos para gestionar los programas y proyectos para asegurar la información de la Entidad, en el marco de las posibilidades dentro del presupuesto anual, teniendo en cuenta las prioridades para la seguridad de la información.

6.4.2 GESTIÓN DE LOS RECURSOS

Teniendo en cuenta que la presente política se encuentra a cargo del proceso de Tecnología de la Información, la Dirección de TI solicitará y gestionará los recursos destinados para la seguridad de la información teniendo presente los requerimientos para la implementación y/o mantenimiento de los controles de seguridad informáticos necesarios.

7. PROCEDIMIENTO

- Comunicación de la Política de seguridad:

  Los miembros del Comité de Seguridad de la información y Protección de datos, conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los recursos tecnológicos y de información.

- Aplicación de la Política de seguridad:

  La política de seguridad informática se orienta a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establece las reglas básicas con las cuales la organización debe operar sus recursos informáticos.

7.1. 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 uso inadecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños importantes que afecten el normal funcionamiento de los procesos.

Los colaboradores y usuarios en general deberán conocer el presente documento, directrices, estándares y procedimientos que apliquen según las funciones que realicen para la organización, las acciones que conlleven a la violación de lo anteriormente mencionado representarán para las personas involucradas las sanciones que apliquen según el incidente presentado.

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

7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

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

- Políticas de Cumplimiento y Sanciones
- Políticas de Uso de Recursos Informáticos.
- Políticas de Contraseñas.
- Políticas de Activos de Informáticos.
- Políticas del Uso de Internet y Correo Electrónico.
- Políticas de Uso de la Intranet y Sitio Web de La Cámara de Comercio
- Políticas Generales
- Políticas para Desarrolladores de Software
- Políticas para Administradores de Sistemas.

- Políticas de Copias de Respaldo.
- Políticas de Uso de Firewall.
- Políticas para Usuarios Externos.
- Políticas de Acceso Físico.

7.3. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

7.3.1. Cumplimiento con la seguridad de la información

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar la política de la seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia Ejecutiva de La Cámara de Comercio de Cúcuta y al Comité de Seguridad de la información y protección de datos personales.

7.3.2. Medidas disciplinarias por incumplimiento de políticas de seguridad

El incumplimiento de la política de seguridad de la información por parte de un colaborador o contratista es causa para iniciar acciones disciplinarias, las cuales de acuerdo con su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

7.4.1. Instrucciones para el uso de recursos informáticos.

El uso de cualquier sistema de información y demás recursos informáticos por parte de los usuarios de los sistemas de la Cámara de Comercio, estará sujeto a los lineamientos dados en la presente política y las guías de buen uso de la Dirección de Tecnología de la Cámara de Comercio.

7.4.2. Uso personal de los recursos

Los recursos informáticos de La Cámara de Comercio, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad.

7.4.3. Acuerdo de confidencialidad

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

7.4.4. Prohibición de instalación de software y hardware en los computadores de La Cámara de Comercio.

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

7.4.5. Uso del aplicativo entregado.

La Cámara de Comercio ha suscrito con los proveedores contratos de licenciamiento para los aplicativos que utiliza. Está terminantemente prohibido hacer uso de la información de la Cámara de Comercio que se gestione con dichos aplicativos y/o se aloja en los equipos de cómputo de la Entidad. Esto se asegura con las cláusulas incluidas en los contratos realizados. Adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

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

7.4.7. Declaración de reserva de derechos de La Cámara de Comercio

La Cámara de Comercio usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información generada y almacenada en los sistemas y aplicativos de la Entidad. Para mantener estos objetivos La Cámara de Comercio se reserva el derecho y la autoridad de:

1. Restringir, modificar o revocar los privilegios de cualquier usuario;
2. Inspeccionar, copiar y revisar cualquier programa u otro recurso que vaya en contra de los objetivos antes planteados; y,
3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Cámara de Comercio.

Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad de la Presidencia Ejecutiva o de quién él delegue esta función.

7.4.8. Todo seguimiento debe ser registrado e informado al jefe inmediato del usuario.

Un usuario puede ser supervisado bajo previa autorización del Presidente Ejecutivo y/o Líderes de área.

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

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

7.4.10. Posibilidad de acceso no implica permiso de uso.

Los usuarios no deben modificar o eliminar información perteneciente a otro usuario sin la debida autorización de este.

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

En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato a la Dirección de Tecnología de la Cámara de Comercio.

7.4.12. Manejo de sesiones en sistemas informáticos

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

7.4.13. 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. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias.

7.4.14. Control de recursos informáticos entregados a los usuarios.

Cuando un empleado termine su vinculación laboral con la Entidad, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que porsu negligencia haya ocasionado a los equipos de hardware.

7.4.15. 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, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

7.4.16. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área de tecnología. Esta área debe realizar revisiones de software como mínimo una vez al año generando los informes correspondientes, para garantizar que los colaboradores tienen instalado software legal.

7.4.17. Tiempo limitado de conexión en aplicaciones críticas

Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad definido la aplicación cerrará la sesión iniciada por el usuario.

7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

7.5.1. Confidencialidad de las contraseñas.

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

7.5.2. 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.

7.5.3. Cambios periódicos de contraseñas.

Todas las aplicaciones críticas deben estar configuradas para solicitar a los los usuarios cambiar su contraseña periódicamente.

7.5.4. Contraseñas fuertes.

Todas las contraseñas deben tener un nivel de complejidad mínimo, cumpliendo con algunas características: Incluir combinación de números, letras mayúsculas, minúsculas y/o caracteres especiales.

7.5.5. 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.

7.5.6. Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario en ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso.

7.5.7. Sospechas de compromiso deben forzar cambios de contraseña.

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

7.5.8. Revelación de contraseñas prohibida.

La contraseña personal no debe ser digitada en presencia de terceras personas, así sean colaboradores de la Entidad y ningún usuario deberá intentar obtener contraseñas de otros usuarios.

7.5.9. Reporte de cambio en las responsabilidades de los usuarios a la Dirección de TI.

La Gerencia responsable del cambio y/o Talento humano debe informar mediante un radicado del Sistema de Gestión Documental, de manera oportuna al área de tecnología todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral o de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

7.6. POLÍTICAS DE ACTIVOS INFORMÁTICOS

7.6.1. 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, la Dirección de tecnología resguarda la información del usuario obtenida de las herramientas dispuestas para almacenar información como el correo electrónico, OneDrive y equipo de cómputo. Esta información será respaldada en un servidor bajo la custodia de tecnología, y esta copia es entregada al jefe inmediato en caso de ser solicitada para su conocimiento y fines pertinentes.

7.6.2. Transporte de datos sensibles en medios legibles.

Para los equipos que manejen información de tipo jurídico - legal y de control interno, se realizará la encriptación del disco duro mediante una aplicación licenciada por la Entidad para la protección de éste en caso de pérdida y/o hurto del equipo.

7.6.3. Clasificación de activos informáticos

- Todos los activos informáticos deben estar claramente identificados y se debe elaborar y mantener un inventario detodos los activos importantes.
- Se deben identificar, documentar e implementar las reglas de uso adecuado los activos asociados con los servicios de procesamiento de la información.

7.6.4. Eliminación Segura de la Información

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.

7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

7.7.1. Prohibición de uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas.

7.7.2. Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto, se debe dar un buen uso al correo electrónico.

7.7.3. Uso de correo electrónico.

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

7.7.4. Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo diariamente.

7.7.5. 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 tecnología.

7.7.6. Todo buzón de correo debe tener un responsable.

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

7.7.7. Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet, pero exclusivamente para propósitos laborales y usando las herramientas disponibles por la Entidad para ello.

7.8. POLÍTICAS DE LA INTRANET Y SITIOS WEB DE LA CÁMARA DE COMERCIO

7.8.1. Reglas de uso de la Intranet.

La Cámara de Comercio utiliza la intranet como un recurso de publicación de documentos de interés para todos los colaboradores de esta. Por lo tanto, el empleado puede consultar la intranet periódicamente o cuando lo requiera,así como todos los documentos que en ella se encuentran publicados.

7.9. POLÍTICAS GENERALES DE SEGURIDAD

7.9.1. Restricción sobre recursos tecnológicos de uso interno

No se otorgarán privilegios de accesos representativos y/o específicos a no ser que la solicitud sea aprobada por medio de la ruta y procedimiento de Gestión de acceso a los sistemas.

7.9.2. Los Servidores y sistemas de comunicación deben tener controles de acceso físico apropiados.

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

7.9.3. Entrenamiento compartido para administración de los sistemas.

Al menos dos personas deben tener el mismo conocimiento para la adecuada administración de los sistemas de información críticos de La Cámara de Comercio.

7.9.4. Ejecución del plan de contingencia para la recuperación ante desastres.

La infraestructura informática de la Entidad debe tener un plan de contingencia para la restauración de la operación en caso de emergencia. Se debe mantener documentado el plan comprobado que permita que los sistemas de información críticos puedan estar operativos en la eventualidad de un desastre. El plan de contingencia para la infraestructura tecnológica de la Entidad deberá contar con el debido soporte que sea acorde a las necesidades y posibilidades de la Cámara de Comercio de Cúcuta. Para el caso de los sistemas de información contratados como SaaS, el proveedor debe informar a la Entidad el plan de contingencia establecido para garantizar la operatividad de estos.

7.9.5. Personal competente en la Dirección de TI para dar pronta solución a problemas.

Con el fin de garantizar la optimización de los recursos informáticos, el buen uso de las herramientas adquiridas y la continuidad de los sistemas de información, la Cámara de Comercio debe asegurar la actualización de los conocimientos para contar con personal profesional y competente que pueda administrar, planear, gestionar, detectar y buscar soluciones con eficiencia y efectividad.

7.9.6. 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.

7.10.POLÍTICAS PARA DESARROLLADORES DE SOFTWARE

7.10.1. Ambientes separados de producción y desarrollo.

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

7.10.2. Documentación de sistemas de información.

Todos los sistemas de información que se encuentren en producción deben tener la documentación respectiva.

7.10.3. Se requieren registros de auditoria en sistemas críticos.

Todo sistema crítico para La Cámara de Comercio debe generar registros de auditoría que guarden modificaciones, adiciones y eliminación de en los sistemas de información por un periodo de tiempo especificado en la configuración de la aplicación.

7.10.4. Los registros del sistema deben incluir eventos relevantes para la seguridad.
Los sistemas críticos de la Entidad deben contener log de eventos de seguridad relevantes.

7.10.5. Personas autorizadas para leer los registros de auditoría.

Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado.

7.11. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

7.11.1. Soporte para usuarios con privilegios especiales.

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

7.11.2. 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 que éste abandone la Entidad y la información almacenada en las herramientas OneDrive, correo electrónico y equipo de cómputo queda respaldada en un servidor a cargo de la Dirección de TI para este fin.

7.11.3. Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema, posteriormente el usuario debe cambiarla.

7.11.4. Administración de los buzones de correo.

Los administradores realizarán la creación y el mantenimiento a los buzones de correo electrónico para los usuarios de la Entidad por medio del procedimiento de gestión de acceso a los sistemas.

7.11.5. Brindar acceso a personal externo.

El área de Tecnología de la Cámara de Comercio velará porque individuos que no sean colaboradores de La Entidad no tengan accesos sobre los recursos tecnológicos de uso interno a menos que exista una solicitud escrita por parte del usuario que lo requiere con su debida justificación y esta haya sido aprobada por tecnología y la presidencia ejecutiva.

7.11.6. Restricción de administración remota a través de Internet.

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

7.11.7. 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.

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

Los equipos de cómputo conectados a la red interna de La Cámara de Comercio deben tener sus relojes sincronizados con la hora oficial.

7.11.9. Revisión periódica de las vulnerabilidades de los sistemas de información.

El área de tecnología debe revisar periódicamente las vulnerabilidades de los sistemas de información por medio del aplicativo Nessus para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

7.11.10. Confidencialidad en la información relacionada con investigaciones internas.

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

7.11.11. Software de identificación de vulnerabilidades.

Para garantizar que la Entidad cuenta con niveles óptimos y buenas prácticas en el ejercicio del aseguramiento de los recursos informáticos, todos los sistemas de información y equipos de cómputo conectados a la red deben ser analizados con un software de detección de vulnerabilidades por lo menos dos veces al año. Adicionalmente, la Entidad cuenta con un software Cortafuegos y una plataforma de Antivirus que permiten visualizar reportes de eventos relacionados con incidentes de seguridad.

7.11.12. En dónde usar controles de acceso para sistemas informáticos.

Todo sistema 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.

7.11.13. Mantenimiento preventivo en computadores y sistemas de redes

Se debe realizar mantenimiento preventivo regularmente en todos los equipos de cómputo y sistemas de redes, para minimizar riesgos de fallas.

7.11.14. Registro de Logs en Sistemas y Aplicaciones

Se debe permitir el registro de logs en los sistemas y aplicaciones críticos de La Cámarade Comercio.

7.11.15. Monitoreo de Sistemas de información

Se debe mantener monitoreo periódico de los servidores y aplicaciones que puedan identificar y solucionar cualquier requerimiento de manera oportuna.

7.11.16. Servicios de Red

Se debe garantizar que el servicio de red utilizado por La Cámara de Comercio se encuentre disponible y operando adecuadamente. El área de tecnología 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 incidentesde seguridad.

7.11.17. Revisión de accesos de usuarios

Se debe realizar la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos una vez por año.

7.12. POLÍTICAS DE COPIAS DE RESPALDO

7.12.1. Período de almacenamiento de copias de respaldo.

De acuerdo con la criticidad de cada servidor o aplicación, se debe establecer una periodicidad de ejecución del backup a realizar, así como su tiempo de almacenamiento (semanal, mensual, anual).

7.12.2. Tipo de datos a los que se les debe hacer backup y con qué frecuencia.

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

7.13. POLÍTICAS DE USO DE FIREWALL

7.13.1. Detección de intrusos.

El Firewall implementado para la Cámara de Comercio debe incluir un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

7.13.2. Toda conexión externa debe estar protegida por el firewall.

Toda conexión a los servidores de La Cámara de Comercio proveniente del exterior debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

7.13.3. 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 el firewall.

7.13.4. Filtrado de contenido.

Dentro de las definiciones de políticas del firewall se debe filtrar el contenido que pueda comprometer la seguridad de los sistemas de información de La Cámara de Comercio.

7.13.5. Firewall debe correr sobre un servidor dedicado o appliance.

El firewall debe correr sobre un servidor dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

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

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

7.14. POLÍTICAS PARA USUARIOS EXTERNOS

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

Proveedores de tecnología 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, 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.

7.15. POLÍTICAS DE ACCESO FÍSICO

7.15.1. Reporte de pérdida o robo de identificación.

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnets de identificación.

7.15.2. Orden de salida para servidores y equipos de telecomunicaciones.

Ningún servidor o equipo de telecomunicación podrá salir de las instalaciones de La Cámara de Comercio sin una aprobación de salida otorgada por la GAF o sin haber sido registrado en el momento de su ingreso.

7.15.3. Cuando se da una terminación laboral, los privilegios de acceso a la sede de La Cámara de Comercio deben ser revocados.

Cuando exista una terminación laboral, todos los privilegios de acceso a los sistemas deberán ser revocados al momento de que el Líder del área o talento humano informe a la Dirección de TI.

7.15.4. Ingreso a los centros de datos

Cualquier miembro de La Cámara de Comercio y/o tercero debe estar autorizado por la Dirección de TI para ingresar a los centros de datos.

8. POLITICA DE USO DE PORTATILES

8.1. Protección de la información

8.1.1. El antivirus siempre debe estar activo y actualizado
8.1.2. 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
8.1.3. El usuario es responsable de la salvaguarda de la información almacenada en su equipo ya que la

Entidad presta las herramientas de respaldo para ello con el uso del OneDrive.

8.2. Protección del equipo portátil

8.2.1. No dejar el computador móvil en lugares públicos

8.2.2. Las herramientas tecnológicas facilitadas por la Entidad a sus funcionarios son para el uso exclusivo de estos en el ejercicio de sus funciones.

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

Este documento se debe revisar cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz. De igual forma, la disponibilidad de recursos para la implementación y actualización de la Política de Seguridad de la Información de la Cámara de Cúcuta, estarán sujetos al presupuesto establecido para cada vigencia con las disposiciones emitidas por la Alta Dirección.

El mecanismo de notificación y divulgación de los cambios realizados a la Política de la Seguridad de la Información será mediante correo electrónico, sistema de gestión documental, intranet o cualquier medio de comunicación oficial aprobado por la entidad.

10. VIGENCIA

La presente política rige a partir de su expedición y deroga todas las disposiciones internas que le sean contrarias.

11. CONTROL DE CAMBIOS

FECHA	VERSIÓN	RAZÓN DEL CAMBIO	Elaboró	Revisó	Aprobó
14/07/14	1	Versión original – Revisó CERTICÁMARA			
19/11/15	2	Separación de modelo para Biometría. Modificación Anexo 1: generalización del formato. Creación: Anexo 2 para política de asuntos específicos. Revisado por Jesús Davis Tabares Rendón – Aprobado por Rodrigo Mejía Nova.	Área de tecnología	Comité de seguridad de la información	Acta número 05 del comité de Seguridad de la Información 07/06/17
27/12/2022	3	Ajuste de políticas establecidas, modificación o eliminación de ítems no aplicables	Director de TI	Comité de Seguridad de la información Acta 02 del 2022	Presidencia Ejecutiva Acta de Junta Directiva extraordinaria Número 393 del 27 de diciembre 2022