

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 1/52
--	--	---

Políticas de Seguridad de la Información de la Cámara de Comercio de Huila

1.1.1.1.1 Versión 7 - 2021

Actualización: Noviembre, 2021

**Elaborado Por:
Dirección Área de TIC**

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 2/52
---	---	--

TABLA DE CONTENIDO

1. INTRODUCCION	8
2. ALCANCES Y AREAS DE ACCIÓN	9
3. OBJETIVO.....	10
4. REQUISITOS LEGALES Y/O REGLAMENTARIOS	10
5. DEFINICIONES	10
6. RESPONSABLES	15
6.1 Compromiso de la Dirección.....	15
6.2 Gestión de los Recursos	15
7. ANALISIS DE RIESGOS.....	15
7.1 Análisis de Amenazas	16
7.1.1 Identificación de Activos	16
7.1.2 Usuarios	16
7.1.3 7.1.2 Identificación de Amenazas	16
7.1.3.1 Desastres del Entorno	16
7.1.3.2 Amenazas en el Sistema	16
7.1.3.3 Amenazas en la Red	17
8. PROCEDIMIENTO.....	18
8.1 POLITICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO DE HUILA	18
8.1.1 Propiedad de la información	19
8.1.2 Responsabilidad Individual.....	19
9. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN.	20
9.1 POLÍTICAS DE CUMPLIMIENTO Y SANCIONES	20
9.1.1 Cumplimiento con la seguridad de la información.....	20
9.1.2 Medidas disciplinarias por incumplimiento de políticas de seguridad.....	20

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 3/52
--	--	--

9.2	POLÍTICAS DE MANEJO DE OPERACIONES Y COMUNICACIONES	21
9.2.1	Control de cambios	21
9.2.2	Segregación de responsabilidades	21
9.2.3	Separación de ambientes Desarrollo, pruebas y Productivo	21
9.2.4	Manejo de la capacidad y esquemas de alta disponibilidad	21
9.3	POLÍTICAS DE DESARROLLO DE SOFTWARE	22
9.4	POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS	22
9.4.1	Instrucciones para el uso de recursos informáticos.....	22
9.4.2	Uso personal de los recursos	22
9.4.3	Acuerdo de confidencialidad	23
9.4.4	Uso del aplicativo entregado.	23
9.4.5	El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.....	23
9.4.6	Declaración de reserva de derechos de la Cámara de Comercio de Huila.	24
9.4.7	Recursos compartidos.	24
9.4.8	Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.....	24
9.4.9	Acceso no autorizado a los sistemas de información de la Entidad.	24
9.4.10	Posibilidad de acceso no implica permiso de uso.	25
9.4.11	Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.	25
9.4.12	Manejo de sesiones en sistemas informáticos.....	25
9.4.13	Impresoras y escáner.	25
9.4.14	Dispositivos móviles, PDAS (Agendas personales digitales), Tablets	25
9.4.15	Notificación de incidentes de seguridad de la información o de datos personales.....	26
9.4.16	Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores.	27
9.4.17	Traslado de equipos debe estar autorizado.....	27
9.4.18	Control de recursos informáticos entregados a los usuarios.	27

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 4/52
--	--	--

9.4.19	Configuración de sistema operativo de las estaciones de trabajo.	28
9.4.20	Uso restringido de dispositivos de red en las estaciones de trabajo.	28
9.4.21	Protección por Defecto de Copyright.....	28
9.4.22	Custodia de Licencias de Software	28
9.4.23	Apagado de equipos en la noche	29
9.4.24	Tiempo limitado de conexión en aplicaciones de alto riesgo.....	29
9.5	POLÍTICAS DE USO DE LAS CONTRASEÑAS	29
9.5.1	Confidencialidad de las contraseñas.	29
9.5.2	Uso de diferentes contraseñas para diferentes recursos informáticos.	29
9.5.3	Identificación única para cada usuario.	29
9.5.4	Cambios periódicos de contraseñas.....	30
9.5.5	Longitud mínima de contraseñas.	30
9.5.6	Contraseñas fuertes.	30
9.5.7	Prohibición de contraseñas cíclicas.	30
9.5.8	Las contraseñas creadas por usuarios no deben ser reutilizadas.	30
9.5.9	Almacenamiento de contraseñas.	30
9.5.10	Sospechas de compromiso deben forzar cambios de contraseña.	30
9.5.11	Revelación de contraseñas prohibida.....	31
9.5.12	Bloqueo estación de trabajo.	31
9.5.13	Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema.	31
9.6	POLÍTICAS DE USO DE LA INFORMACIÓN	31
9.6.1	Divulgación de la información manejada por los usuarios de la Cámara de Comercio	31
9.6.2	Transferencia de datos solo a organizaciones con suficientes controles.....	32
9.6.3	Registro de las compañías que reciben información privada.	32
9.6.4	Transferencia de la custodia de información de un empleado que deja la Cámara de Comercio de Huila.....	32

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 5/52
--	--	--

9.6.5	Transporte de datos sensibles en medios legibles.	32
9.6.6	Datos sensibles enviados a través de redes externas deben estar encriptados.....	32
9.6.7	Clasificación de la Información.	32
9.6.8	Eliminación Segura de la Información en Medios Informáticos ..	34
9.7	POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO	34
9.7.1	Prohibición de uso de Internet para propósitos personales.	34
9.7.2	Formalidad del correo electrónico.....	34
9.7.3	Preferencia por el uso del correo electrónico.	34
9.7.4	Uso de correo electrónico.....	34
9.7.5	Revisión del correo electrónico.....	35
9.7.6	Mensajes prohibidos.	35
9.7.7	Acciones para frenar el SPAM.	35
9.7.8	Todo buzón de correo debe tener un responsable.....	35
9.7.9	Enviando software e información sensible a través de Internet.	35
9.7.10	Intercambio de información a través de Internet.....	36
9.8	POLÍTICAS DE SITIOS WEB DE LA CÁMARA DE COMERCIO	36
9.8.1	Prohibición de publicitar la imagen de la Cámara de Comercio de Huila en sitios diferentes a los institucionales.	36
9.8.2	Prohibición establecer conexiones a los sitios web de la Cámara de Comercio	36
9.8.3	Prohibición de anuncios en sitios Web particulares.....	36
9.9	POLÍTICAS GENERALES DE LA PRESIDENCIA	37
9.9.1	Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.....	37
9.9.2	Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.	37
9.9.3	Entrenamiento compartido para labores técnicas críticas.	37
9.9.4	Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.....	37
9.9.5	Personal competente en el Centro de Cómputo para dar pronta solución a problemas.	38
9.9.6	Chequeo de virus en archivos recibidos en correo electrónico..	38

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 6/52
--	--	--

9.9.7	Contacto con grupos especializados en seguridad informática.	38
9.10	POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS.	38
9.10.1	Soporte para usuarios con privilegios especiales.	38
9.10.2	Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad.....	38
9.10.3	Cuándo y cómo pueden asignar contraseñas los administradores	38
9.10.4	Cambio de contraseñas por defecto.	39
9.10.5	Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.	39
9.10.6	Administración de los buzones de correo.	39
9.10.7	Brindar acceso a personal externo.....	39
9.10.8	Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado.....	39
9.10.9	Administración remota a través de Internet.....	40
9.10.10	Dos usuarios requeridos para todos los administradores.	40
9.10.11	Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.	40
9.10.12	Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado.....	40
9.10.13	Remoción de software para la detección de vulnerabilidades cuando no esté en uso.	40
9.10.14	Manejo administrativo de seguridad para todos los componentes de la red.	40
9.10.15	Información a capturar cuando un crimen informático o abuso es sospechado.....	41
9.10.16	Sincronización de relojes para un registro exacto de eventos en la red.	41
9.10.17	Revisión regular de los registros del sistema.	41
9.10.18	Confidencialidad en la información relacionada con investigaciones internas.	41
9.10.19	Información con múltiples niveles de clasificación en un mismo sistema.	41

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 7/52
--	--	--

9.10.20 Segmentación de recursos informáticos por prioridad de recuperación.	42
9.10.21 Software de identificación de vulnerabilidades.....	42
9.10.22 Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales.....	42
9.10.23 Habilitación de Logs en Sistemas y Aplicaciones.....	43
9.10.24 Monitoreo de Sistemas.....	43
9.10.25 Mantenimiento de los Sistemas.....	43
9.10.26 Verificación física de equipos críticos.	43
9.10.27 Servicios de Red	43
9.10.28 Revisión de accesos de usuarios	44
9.11 POLÍTICAS DE BACKUP.....	44
9.11.1 Período de almacenamiento de registros de auditoría.	44
9.11.2 Tipo de datos a los que se les debe hacer backup y con qué frecuencia.....	44
9.11.3 Copias de información sensible.	44
9.11.4 En dónde usar sistemas de respaldo para sistemas informáticos.	44
9.12 POLÍTICAS DE USO DE FIREWALL	44
9.12.1 Detección de intrusos.....	45
9.12.2 Toda conexión externa debe estar protegida por el firewall.....	45
9.12.3 Toda conexión hacia Internet debe pasar por el Firewall.	45
9.12.4 Firewall debe correr sobre un computador dedicado o appliance.	45
9.12.5 Inventario de conexiones.	45
9.12.6 El sistema interno de direccionamiento de red no debe ser público.	45
9.12.7 Revisión periódica y reautorización de privilegios de usuarios.	45
9.13 POLÍTICAS PARA USUARIOS EXTERNOS.....	46
9.13.1 Términos y condiciones para clientes de Internet.	46
9.13.2 Acuerdos con terceros que manejan información o cualquier recurso informático de la Cámara de Comercio	46

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 8/52
--	--	--

9.13.3	Definición clara de las responsabilidades de seguridad informática de terceros.....	46
9.14	POLÍTICAS DE ACCESO FÍSICO.....	46
9.14.1	Reporte de pérdida o robo de identificación.....	46
9.14.2	Orden de salida para equipos electrónicos.	47
9.14.3	Orden de salida de activos.....	47
9.14.4	Cuando se da una terminación laboral, los privilegios de acceso a la sede de la Cámara de Comercio deben ser revocados.	47
9.14.5	Ingreso de equipos de grabación y fotografías al Cuarto de servidores.....	47

1. INTRODUCCION

En una organización los requerimientos de seguridad que involucran las tecnologías de información pueden tornarse complejos y difíciles de realizar, dadas las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. Esto ha llevado a que muchas organizaciones, mediante la integración del recurso humano y tecnológico, hayan desarrollado normas y directrices que permitan sensibilizar y proteger la información y los recursos críticos de la misma.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 9/52
--	--	--

En este sentido, el presente documento pretende ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la Cámara de Comercio del Huila prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias.

Toda persona que utilice los recursos y servicios informáticos de la entidad, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información.

Las normas y políticas expuestas en este documento, están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

2. ALCANCES Y AREAS DE ACCIÓN

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

- **Colaboradores de 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 aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:
 - Colaboradores por convenio: son aquellas personas que laboran en la Entidad y tienen un contrato para la ejecución de un convenio;
 - 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 sociedades.
 - Superintendencia de Industria y Comercio.
- **Otras Entidades**
 - DIAN.
 - Confecamaras.
 - UGPP.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 10/52
--	--	---

3. OBJETIVO

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

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

Estos lineamientos están escritos en forma de políticas.

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia 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 o entidades que las regulan y aglutinan.

5. DEFINICIONES

- **Activo:** Recurso del sistema de información o relacionado con éste, necesario para que la entidad funcione correctamente y alcance los objetivos propuestos.
- **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 del área de TIC.
- **Amenaza:** Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o perdidas de información.
- **Área Crítica:** Es el área física donde se encuentran instalados los equipos de cómputo y de telecomunicaciones, que requieren de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de información y de comunicación de la entidad.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 11/52
--	--	---

- **Backup:** Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
- **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.
- **Control de Acceso:** Una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.
- **Contraseña:** Clave de acceso a un recurso informático.
- **Desastre o Contingencia:** Interrupción de la capacidad de acceso a la información y procesamiento de la misma, necesarias para la operación normal de la entidad.
- **Directrices:** Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- **Riesgo:** Es una amenaza. El riesgo mide el nivel de exposición que tiene un activo ante una amenaza. Dentro de los tipos de riesgos tenemos:
 - Los Riesgos Estratégicos: tienen que ver con el mercadeo, las compras, cambios en el comportamiento de los usuarios, cambios reglamentarios, etc.
 - Los Riesgos Financieros: se relacionan con la parte de tesorería, evaluación de proveedor, fraudes, acceso a ciertos datos de seguridad, control de los inventarios, etc.
 - Los Riesgos Operativos: se refieren a los errores de operación, practicas inseguras como el sabotaje, rutinas en los empleados, destrucción voluntaria, etc.
 - Los Riesgos Técnicos: se relacionan con las fallas en los equipos, incendios, explosiones, inundaciones, sabotajes, contaminación y otros fenómenos naturales.
- **Internet:** Es una red de computadores alrededor de todo el mundo, que comparten información unas con otras por medio de página o sitios, implementada en un conjunto de protocolos denominados TCP/IP.
- **Intranet:** Es un sitio Web interno y privado de la empresa, a la que los usuarios pueden acceder mediante un navegador y que permite múltiples funcionalidades organizacionales.
- **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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 12/52
--	--	---

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 (RESERVADA):** Información administrada por la Cámara de Comercio en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.
- **Información confidencial:** Información generada por la Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.
- **Información privada (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 ó una oficina).
- **Licencia de Software:** Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.
- **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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 13/52
--	--	---

términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.

- **Propiedad Intelectual:** Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.
- **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 especifica 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 exigida por ley.
- **Software de Dominio Público:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- **Freeware:** Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- **Shareware:** Clase de software o programa, cuyo propósito es evaluar por un determinado tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.
- **Monitoreo:** Verificación de las actividades de un usuario con respecto a los recursos informáticos de La Cámara de Comercio.
- **OTP (One Time Password):** Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.
- **Plan de contingencia:** Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la Cámara de Comercio en casos de desastres y otros casos que impidan el funcionamiento normal.
- **Política:** Toda intención y directriz expresada formalmente por la dirección.
- **Protector de pantalla:** Programa que se activa a voluntad del usuario, ó automáticamente después de un tiempo en el que no ha habido actividad.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 14/52
--	--	---

- **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.
- **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 detección de intrusos (IDS):** Es un conjunto de hardware y software que ayuda en la detección de accesos o intentos de acceso no autorizados a los recursos informáticos de la Cámara de Comercio.
- **Sistema de encriptación:** Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.
- **Sistema 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 de Huila.
- **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 de Huila establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.
- **Vulnerabilidad:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 15/52
--	--	---

- **Arquitectura de software:** Una arquitectura de software describe los componentes básicos de un sistema de software y su combinación interna, por tanto, define la estructura que debe de tener un software, las piezas que debemos construir y el modo en el que se deben de juntar y trabajar entre ellas.

6. RESPONSABLES

6.1 Compromiso de la Dirección.

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

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

6.2 Gestión de los Recursos

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento del propósito superior de la Cámara de Comercio de Huila.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información

7. ANALISIS DE RIESGOS

Para que un sistema sea seguro, se deben identificar las posibles amenazas, las cuales nos llevan a tomar medidas que anulen la acción de dicho riesgo sobre la operación del servicio de la Cámara de Comercio.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 16/52
--	--	---

7.1 Análisis de Amenazas

7.1.1 Identificación de Activos

La identificación de activos se relaciona en el anexo: Inventario de activos de información.xlsx

7.1.2 Usuarios

El Anexo 1. de la presente política, lleva la relación de los usuarios que interactúan con los activos de información de la entidad.

7.1.3 7.1.2 Identificación de Amenazas

Conociendo los recursos que debemos proteger, se deben identificar las vulnerabilidades y amenazas a las cuales ellos están expuestos.

De acuerdo con la forma en que se pueden producir tenemos:

7.1.3.1 Desastres del Entorno

Se incluyen todos los posibles problemas con la ubicación del entorno de trabajo informático o de la entidad, así como de las personas que de una u otra forma están relacionadas con el mismo.

Dentro de estas amenazas identificamos las siguientes:

- Pérdida por fraude o hurto.
- Pérdidas por causas accidentales (cortes del fluido eléctrico, sobrecargas, derrame de sustancias en equipos, etc.)
- Pérdidas por desastres naturales (incendio, inundación, terremotos, descargas eléctricas).
- Pérdidas por caídas en los sistemas de comunicación.
- Pérdidas a causa del personal interno o externo.

7.1.3.2 Amenazas en el Sistema

Se contemplan todas las vulnerabilidades de los equipos y su software, que pueden acarrear amenazas a la seguridad de la información.

Dentro de estas amenazas identificamos las siguientes:

- Fallos en los equipos de cómputo

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 17/52
--	--	---

- Fallos en el Sistema Operativo
- Fallos en los programas
- Programas no autorizados
- Pérdidas por decisiones erróneas de los usuarios.

7.1.3.3 Amenazas en la Red

La interconexión de equipos mediante redes locales, intranet, e internet, acarrea nuevas y peligrosas amenazas de seguridad.

Dentro de estas amenazas identificamos las siguientes:

- Pérdidas por virus y software malicioso.
- Pérdidas por un intruso o Hacker.
- Pérdidas por la utilización deliberada de dispositivos externos de almacenamiento electrónico.
- Pérdidas por los usuarios internos de la red.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 18/52
--	--	--

Valoración de las Amenazas

AMENAZAS		PROBABILIDAD/IMPACTO								Riesgo total %
		Servidores		Estac. Trabajo		Datos		Infraestructura		
		P	I	P	I	P	I	P	I	
Desastres del Entorno	Fraude o hurto	1	20	2	10	1	10	1	20	17.5
	Causas Accidentales	1	20	1	10	1	10	1	10	12.5
	Desastres Naturales	1	20	1	20	1	20	1	20	20
	Caídas de Comunicación	1	20	1	5	1	10	1	10	11.2
	Personal	1	20	1	10	1	10	1	20	15
Amenaz. en el Sistema	Fallos Equi. Computo	2	10	2	10	1	20	-	-	15
	Fallos S.O.	2	5	1	5	1	5	-	-	5
	Fallos Progr.	2	10	1	10	2	5	-	-	10
	Prog. No Aut.	1	10	2	5	2	10	-	-	10
	Usuarios	1	20	1	10	2	5	-	-	10
Amenazas en la Red	Virus, Software Malicioso	1	10	1	5	2	20	-	-	13.7
	Intruso, Hacker	1	20	1	5	1	5	-	-	7.5
	Dispo. Exter.	1	10	1	5	1	10	-	-	6.2
	Usuarios	1	20	1	10	1	20	-	-	12.5

8. PROCEDIMIENTO

La Dirección del área de TIC, consciente que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

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

8.1 POLITICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO DE HUILA

La Cámara de Comercio de Huila reconoce abiertamente la importancia de la seguridad de la información, así como la necesidad de su protección por

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 19/52
--	--	---

constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos y la reputación misma de la entidad.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen, según las funciones que realicen para la organización. El desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

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 planeación y estrategia de la compañía, dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

8.1.1 Propiedad de la información

Todos los recursos tecnológicos e informáticos suministrados por la CCH a los empleados son propiedad exclusiva de la CCH.

Toda la información y propiedad intelectual creada por los empleados que laboren para la CCH son propiedad exclusiva de la CCH y no deben ser duplicadas, sustraídas o compartidas con ninguna persona excepto bajo una autorización expresa de la misma.

8.1.2 Responsabilidad Individual

Cada empleado o usuario es responsable por el cumplimiento de la política de seguridad de la información, uso y de las demás políticas, lineamientos, procesos, procedimientos etc. emitidos por la CCH.

Los empleados o usuarios tienen la responsabilidad de mantener en sus computadores únicamente la información mínima requerida para poder realizar los trabajos a los cuales se encuentren asignados.

Los empleados o usuarios no deberán permitir que nadie coloque en riesgo los recursos tecnológicos o la información de la CCH o de sus clientes.

Los empleados o usuarios deben ser conscientes que la CCH, para los propósitos especificados en el presente documento, podrá monitorear toda

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 20/52
--	--	---

comunicación electrónica, así como también el uso de los recursos tecnológicos o información almacenada en dichos recursos.

9. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN.

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 manejo de operaciones y comunicaciones.
- Políticas de desarrollo de software.
- Políticas de uso de recursos informáticos.
- Políticas de contraseñas.
- Políticas de uso de la información.
- Políticas del uso de Internet y correo electrónico.
- Políticas de sitios Web de La Cámara de Comercio
- Políticas Generales de la Presidencia
- Políticas para Administradores de Sistemas.
- Políticas de Copias de respaldo.
- Políticas de Uso de Firewall.
- Políticas para Usuarios Externos.
- Políticas de Acceso Físico.

9.1 POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

9.1.1 Cumplimiento con la seguridad de la información.

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de la Cámara de Comercio y la Dirección del área de TIC.

Todos los empleados recibirán formación apropiada sobre las políticas y procedimientos de seguridad de la entidad, que les permita concientizarse sobre el valor de la información y los servicios críticos.

9.1.2 Medidas disciplinarias por incumplimiento de políticas de seguridad

Todo incumplimiento de una política de seguridad de la información por parte de un empleado o contratista, así como de cualquier estándar o procedimiento es

	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 21/52
---	--	---

causa para iniciar acciones disciplinarias, las cuales, de acuerdo con su gravedad serán evaluadas, según el reglamento interno de trabajo.

9.2 POLÍTICAS DE MANEJO DE OPERACIONES Y COMUNICACIONES

9.2.1 Control de cambios

El control de cambios es un procedimiento que asegura que todos los cambios son controlados, en los que se incluye el planteamiento, análisis, pruebas, aprobaciones e implementación de estos.

La gestión del cambio está contemplada en el documento: Lineamientos para la gestión de cambios TI y en la Plantilla Control Gestión de Cambios

9.2.2 Segregación de responsabilidades

Los deberes y las áreas de responsabilidad deben estar segregados para reducir el riesgo de la oportunidad de uso, abuso, modificación accidental o no autorizada. En caso de no poder realizar la segregación de deberes, se deberán establecer controles compensatorios con dichas actividades o roles.

9.2.3 Separación de ambientes Desarrollo, pruebas y Productivo

- En los sistemas productivos no se deben almacenar compiladores o utilitarios que puedan usarse para actividades de desarrollo o programación.
- En el ambiente productivo solo se debe instalar productos que cumplan satisfactoriamente el ciclo de pruebas y aprobación del mismo (Procedimiento de Construcción de Software)
- La fecha y hora de todos los sistemas conectados a la red de la CCH deben permanecer sincronizados.
- La infraestructura física de los sistemas de producción, Calidad y desarrollo debe estar separada.

9.2.4 Manejo de la capacidad y esquemas de alta disponibilidad

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 22/52
--	--	---

La infraestructura de TI que soporte los sistemas de información críticos para la operación del negocio debe poseer en lo posible topologías de redundancia o alta disponibilidad.

9.3 POLÍTICAS DE DESARROLLO DE SOFTWARE

Los sistemas de información que se desarrollen al interior o con terceros deben cumplir con los lineamientos, estándares y tecnologías especificados por el área de TI. Documentos tales como: Lineamientos de Arquitectura de Referencia, Plantilla de Diseño y Arquitectura de Software, Procedimiento de Construcción de Software, plantillas de casos de uso entre otros establecidos por el área de TI.

El ambiente de desarrollo debe estar lógicamente separado del ambiente productivo, en caso de configuraciones de pasos productivos los desarrolladores tendrán acceso especial por un tiempo limitado, permisos que deben ser removido cuando entre en operación el software desarrollado.

9.4 POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

9.4.1 Instrucciones para el uso de recursos informáticos

El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de la Cámara de Comercio, debe someterse a todas las instrucciones técnicas, que imparta la Dirección del área TIC.

Todo empleado de la Cámara de Comercio, que utilice algún elemento de cómputo para el desarrollo de sus labores, deberá estar capacitado en el uso correcto del recurso físico o el uso del software, antes de tener acceso al mismo.

9.4.2 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. Cualquier otro uso está sujeto a previa autorización de la Presidencia.

Los usuarios deberán conocer claramente los activos que están bajo su responsabilidad para su correcto manejo y custodia. Así mismo le corresponderá

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 23/52
--	--	---

notificar el movimiento de este a la coordinación de compras, bienes y servicios del área administrativa y financiera.

9.4.3 Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos de La Cámara de Comercio, todo usuario debe firmar un acuerdo de confidencialidad (Anexo 2) antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.

- *Prohibición de instalación de software y hardware en los computadores de La Cámara de Comercio de Huila.*

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 empleados de sistemas autorizados por la Cámara de Comercio de Huila.

9.4.4 Uso del aplicativo entregado.

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

9.4.5 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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 24/52
--	--	---

de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Cámara de Comercio de Huila.

9.4.6 Declaración de reserva de derechos de la Cámara de Comercio de Huila.

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

9.4.7 Recursos compartidos.

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 esto se debe hacer con autorización previa.

9.4.8 Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.

Un usuario puede ser monitoreado bajo previa autorización de la Presidencia y la dirección del área de TIC.

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

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

Ningún usuario evadirá y vulnerará los sistemas de seguridad, ni intentará obtener palabras claves asignadas a otros usuarios. Siendo este acto considerado de mala fe y causal de llamado de atención con copia a la hoja de vida.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 25/52
--	--	---

9.4.10 Posibilidad de acceso no implica permiso de uso.

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

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

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

9.4.12 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.

Es responsabilidad de cada usuario verificar su salida de los programas o aplicaciones activas, antes de retirarse del equipo, con el objeto de evitar que cualquier usuario pueda ingresar a las aplicaciones y modificar la información.

9.4.13 Impresoras y escáner.

- La información que se imprima o se escanee, y que esté clasificada como confidencial, no debe dejarse desatendida en áreas públicas.

9.4.14 Dispositivos móviles, PDAS (Agendas personales digitales), Tablets

El empleado o usuario que hace uso de dispositivos móviles o medios mencionados en este aparte debe cumplir con:

- Solo se debe almacenar información en este tipo de dispositivos previa autorización de directores o coordinadores propietarios de la información e informando al rol de seguridad de la información
- Proteger la confidencialidad y disponibilidad de la información de la CCH que almacene en cualquier dispositivo móvil.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 26/52
--	--	---

- Notificar al área de TI en caso de pérdida o robo del dispositivo donde tenga almacenada información de la CCH
- Los medios removibles no deben tratarse como medios de almacenamiento permanente o de respaldo (backup) de información.

9.4.15 Notificación de incidentes de seguridad de la información o de datos personales.

Un incidente de seguridad es cualquier evento que comprometa o amenace la confidencialidad, integridad y la disponibilidad de información, aplicaciones o recursos tecnológicos, como, por ejemplo:

- Accesos no autorizados
- Virus informáticos
- Cadenas en el correo electrónico
- Vulnerabilidades en programas de software instalados
- Robo de computadores
- Instalación de software prohibido
- Consulta de sitios web no autorizados

Cualquier incidente de Seguridad debe reportarse de acuerdo con el PL - Procedimiento de Gestión de Incidentes

Ante un incidente de seguridad se debe tener en cuenta lo siguiente:

- Los empleados o usuarios tienen la responsabilidad de reportar al oficial de protección de datos a través de la mesa de ayuda a la mayor brevedad, cualquier incidente de seguridad, vulnerabilidad, problemas u oportunidades de mejora que se identifiquen.
- Cualquier robo o pérdida de información, capital intelectual, recurso tecnológico, software etc., debe reportarse a la mayor brevedad a través de la plataforma de mesa de ayuda y el auxiliar administrativo de seguridad de la información y protección de datos personales hará el respectivo análisis del evento y será el encargado de reportarlo en los tiempos requeridos a la SIC.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 27/52
--	--	---

- Los empleados o usuarios tienen la responsabilidad de reportar cualquier problema real o sospecha de virus que se presenten por fuentes internas o externas (Ejemplo mail de terceros), a través de la mesa de ayuda al área de TIC.

9.4.16 Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores.

Toda la información que sea crítica para la organización debe ser etiquetada de acuerdo con los niveles establecidos en el presente documento: USO INTERNO y CONFIDENCIAL.

9.4.17 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 el responsable del bien, el coordinador de bienes y servicios y si es necesario, con el apoyo del soporte técnico de la oficina de TIC tomando las medidas de seguridad necesarias.

9.4.18 Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con La Cámara de Comercio se debe diligenciar el documento de movimiento de activos fijos. Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de entrega de activos. El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado al hardware.

La Dirección de Talento Humano y SGSST notificará a través de email o por escrito al área de TIC cualquier novedad con relación al ingreso o retiro de personal para la creación o inactivación de usuarios (login) de acceso indicando fecha de ingreso o retiro. Para ello se deberá tener en cuenta los siguientes puntos:

- Ausencia Temporal: Cuando se trate de vacaciones, licencias, incapacidades (mayor a 5 días hábiles), se deberá inactivar usuarios a los aplicativos centralizados. Anexo 1 de activos de información.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 28/52
--	--	---

- Ausencia Definitiva: Cuando se trate de retiro definitivo de la entidad, se deberá inactivar usuarios de los aplicativos centralizados (Anexo 1 de activos de información), cuentas de email corporativas.
- Incorporaciones: Cuando se trate de ingreso de personal nuevo, se deberán crear los usuarios correspondientes en los aplicativos centralizados (si este lo requiere) para el buen desempeño de sus actividades y cuenta de correo corporativo.

9.4.19 Configuración de sistema operativo de las estaciones de trabajo.

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

9.4.20 Uso restringido de dispositivos de red en las estaciones de trabajo.

Queda prohibido el uso de dispositivos de red en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de Presidencia y la Dirección de TIC.

9.4.21 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 mínimo una vez al año, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

9.4.22 Custodia de Licencias de Software

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 29/52
--	--	---

9.4.23 Apagado de equipos en la noche

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de empleados en la oficina durante la noche.

9.4.24 Tiempo limitado de conexión en aplicaciones de alto riesgo

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

9.5 POLÍTICAS DE USO DE LAS CONTRASEÑAS

9.5.1 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.

9.5.2 Uso de diferentes contraseñas para diferentes recursos informáticos.

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

9.5.3 Identificación única para cada usuario.

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. Los empleados contarán con una identificación única personal y su respectiva contraseña generada por el sistema ó asignada por el encargado de tecnología de La Cámara de Comercio, solicitando cambio de la misma en el primer inicio de sesión.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 30/52
--	--	---

9.5.4 Cambios periódicos de contraseñas.

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

9.5.5 Longitud mínima de contraseñas.

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

9.5.6 Contraseñas fuertes.

Las contraseñas no deben ser nombres propios ni palabras del diccionario, ni fechas de nacimiento, ni números consecutivos; debe ser una mezcla de números, letras (con minúsculas y mayúsculas) y caracteres especiales.

9.5.7 Prohibición de contraseñas cíclicas.

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

9.5.8 Las contraseñas creadas por usuarios no deben ser reutilizadas.

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Esta política es complementada por la política “Prohibición de contraseñas cíclicas”.

9.5.9 Almacenamiento de contraseñas.

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

9.5.10 Sospechas de compromiso deben forzar cambios de contraseña.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 31/52
--	--	---

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

9.5.11 Revelación de contraseñas prohibida.

En 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 empleados de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.

9.5.12 Bloqueo estación de trabajo.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 5 min. Por otra parte, el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

9.5.13 Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema.

La Dirección de Talento Humano y SGSST debe reportar por medio de un correo electrónico, de manera oportuna al área de TIC, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

9.6 POLÍTICAS DE USO DE LA INFORMACIÓN

9.6.1 Divulgación de la información manejada por los usuarios de la Cámara de Comercio

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 32/52
--	--	---

personales, garantizando la privacidad de la información, previamente clasificada, salvo autorización del titular de la misma para su divulgación.

9.6.2 Transferencia de datos solo a organizaciones con suficientes controles.

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

9.6.3 Registro de las compañías que reciben información privada.

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

9.6.4 Transferencia de la custodia de información de un empleado que deja la Cámara de Comercio de Huila

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

9.6.5 Transporte de datos sensibles en medios legibles.

Si se transporta información sensible en medios legibles por el computador (CD's, DVD's, memorias extraíbles, D.D. Externos), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

9.6.6 Datos sensibles enviados a través de redes externas deben estar encriptados.

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.

9.6.7 Clasificación de la Información.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 33/52
--	--	---

- Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.
- Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser “propiedad” de una parte designada de la Cámara de Comercio de Huila.
- Cualquier uso de servicio de procesamiento de información debe ser autorizado por la Dirección de TIC de las Cámaras de Comercio según el caso, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener conocimiento todos los usuarios involucrados.

Para dar manejo a la información la de CCH se definen los siguientes roles:

- **Propietario:** Determina el valor de la información y las medidas de protección requeridas, así mismo determina el grado de acceso a la misma.
- **Custodio:** Administra el acceso y la disponibilidad de la información de acuerdo con lo establecido por el propietario.
- **Usuario:** Tiene acceso y uso de la información de acuerdo con lo establecido por el propietario.

Algunas de las consideraciones a tener en cuenta son:

- Toda la información de la CCH, de sus clientes, o de terceros debe ser identificada y clasificada por el propietario de acuerdo con su nivel de confidencialidad.
- Los usuarios de la información deben cumplir con la política de seguridad de la información y la de protección de datos personales.
- Los usuarios no deben utilizar los servicios de terceros (no autorizados) para manejar o procesar información confidencial de la CCH, ejemplo uso de DropBox, correos electrónicos personales no autorizados, etc.

9.1.1 Información confidencial en Reuniones

Si información con clasificación de confidencial es divulgada oralmente en seminarios, diplomados, lecturas, video conferencias, el orador debe comunicar de manera clara el carácter de la información y debe recordar a los participantes su responsabilidad de protegerla.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 34/52
--	--	---

9.6.8 Eliminación Segura de la Información en Medios Informáticos

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

9.7 POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

9.7.1 Prohibición de uso de Internet para propósitos personales.

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

9.7.2 Formalidad del correo electrónico.

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

9.7.3 Preferencia por el uso del correo electrónico.

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

9.7.4 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.
- Los empleados o usuarios son responsables de tomar medidas necesarias para prevenir el uso no autorizado de su correo electrónico y en consecuencia son responsables de todas las actividades que se hagan con su cuenta de correo.
- Está prohibido que los empleados o usuarios hagan uso de la cuenta de correo electrónico que ha sido asignada a otra persona.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 35/52
--	--	---

- El sistema de correo electrónico es un activo valioso que se debe utilizar para propósitos de la entidad.
- Cuando un usuario se ausente de sus labores por un tiempo prolongado debe activar la notificación de ausencia. (Ejemplo en vacaciones, licencias etc.)
- El aviso legal aprobado y la correspondiente firma corporativa deben utilizarse en todos los mensajes salientes de los buzones de correo.

9.7.5 Revisión del correo electrónico.

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

9.7.6 Mensajes prohibidos.

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

9.7.7 Acciones para frenar el SPAM.

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

9.7.8 Todo buzón de correo debe tener un responsable.

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

9.7.9 Enviando software e información sensible a través de Internet.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 36/52
--	--	---

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

9.7.10 Intercambio de información a través de Internet.

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

9.8 POLÍTICAS DE SITIOS WEB DE LA CÁMARA DE COMERCIO

9.8.1 Prohibición de publicitar la imagen de la Cámara de Comercio de Huila en sitios diferentes a los institucionales.

La publicación de logos, marcas o cualquier tipo de información sobre la Cámara de Comercio de Huila o sus actividades en Internet solo deben ser realizada o autorizada a través de las páginas institucionales de la misma por la dirección de comunicaciones y relaciones corporativas y previa autorización de la Presidencia. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

9.8.2 Prohibición establecer conexiones a los sitios web de la Cámara de Comercio

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios web de la Cámara de Comercio por parte de los empleados y de sus sitios web o páginas particulares, salvo previa autorización de la Presidencia, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales o como meta-etiquetas.

9.8.3 Prohibición de anuncios en sitios Web particulares.

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 37/52
--	--	---

9.9 POLÍTICAS GENERALES DE LA PRESIDENCIA

9.9.1 Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.

No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por el director de departamento quien lo solicite.

9.9.2 Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.

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

9.9.3 Entrenamiento compartido para labores técnicas críticas.

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

9.9.4 Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 38/52
--	--	---

9.9.5 Personal competente en el Centro de Cómputo para dar pronta solución a problemas.

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

9.9.6 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.

9.9.7 Contacto con grupos especializados en seguridad informática.

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

9.10 POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS.

9.10.1 Soporte para usuarios con privilegios especiales.

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

9.10.2 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 queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

9.10.3 Cuándo y cómo pueden asignar contraseñas los administradores

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 39/52
--	--	---

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. El usuario debe realizar el cambio de su contraseña ó el sistema debe obligar al usuario a cambiar su contraseña.

9.10.4 Cambio de contraseñas por defecto.

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

9.10.5 Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas de este sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

9.10.6 Administración de los buzones de correo.

Los administradores deben establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico, trimestralmente se realizará una revisión de control sobre cada uno de los buzones creados para determinar cuáles requieren una depuración para que no alcancen su límite de espacio asignado.

9.10.7 Brindar acceso a personal externo.

El área de TIC velará porque individuos que no sean empleados, contratistas o consultores de La Cámara de Comercio no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Presidencia y excluyendo las pantallas de auto-consulta que disponga la entidad para los usuarios.

9.10.8 Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado.

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de la Cámara de Comercio, la dirección de TIC verificará que exista una relación contractual o convenio que obligue a que este tercero deba tener acceso a los recursos tecnológicos para el cumplimiento del objeto contratado/convenido.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 40/52
--	--	---

9.10.9 Administración remota a través de Internet.

La administración remota desde Internet es permitida por tiempo determinado para el cumplimiento de alguna labor específica y bajo supervisión permanente del área de TIC. Culminada la labor, se realizarán los cambios de clave asignados temporalmente y desinstalación de software si es requerido.

9.10.10 Dos usuarios requeridos para todos los administradores.

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

9.10.11 Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.

Sin autorización escrita de la Dirección del área de TIC de la Cámara de comercio, los administradores no deben otorgarle privilegios de administración a ningún usuario.

9.10.12 Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado.

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

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

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

9.10.14 Manejo administrativo de seguridad para todos los componentes de la red.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 41/52
--	--	---

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.

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

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

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

Los dispositivos multiusuario conectados a la red interna de la Cámara de Comercio deben tener sus relojes sincronizados con la hora legal Colombiana.

9.10.17 Revisión regular de los registros del sistema.

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

9.10.18 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.

9.10.19 Información con múltiples niveles de clasificación en un mismo sistema.

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 42/52
--	--	---

9.10.20 Segmentación de recursos informáticos por prioridad de recuperación.

Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero.

9.10.21 Software de identificación de vulnerabilidades.

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

9.10.22 Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales

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

El mantenimiento preventivo de equipos deberá realizarse en las instalaciones de la Cámara de Comercio, en el lugar asignado como laboratorio para tal fin en la sede principal. El auxiliar operativo de sistemas se desplazará a las sedes de la entidad a realizar dicho mantenimiento.

Cuando un equipo es enviado a mantenimiento correctivo fuera de la entidad y posee información crítica, se deben tomar medidas especiales para salvaguardar la información de este.

Todos los equipos de cómputo deben estar amparados con un seguro adecuado que los proteja contra robo, o cualquier evento siniestro.

Los equipos de cómputo que cumplan con su tiempo de servicio deben ser reemplazados. El tiempo de obsolescencia será el siguiente:

- Equipos de Cómputo: 3 años
- Cableado Estructurado: 20 años.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 43/52
--	--	---

- Tendido eléctrico: 15 – 20 años.
- Equipos de Comunicaciones: 5 años

Nota: Cumplido los tiempos, deberá considerarse lo indicado en el manual de almacén.

9.10.23 Habilitación de Logs en Sistemas y Aplicaciones

Se debe habilitar la gestión de logs (archivos de transacción) en los sistemas y aplicaciones críticas de la Cámara de Comercio de Huila.

9.10.24 Monitoreo de Sistemas

Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

9.10.25 Mantenimiento de los Sistemas

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

9.10.26 Verificación física de equipos críticos.

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

9.10.27 Servicios de Red

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

Los visitantes no deben conectar sus computadores a la red interna de la CCH, sin previa autorización del área de TIC.

Se prohíbe el uso de programas o software utilizados para investigar o explorar el ambiente de seguridad de la información de la CCH por parte de empleados o usuarios no autorizados. Las excepciones serán validadas en coordinación con el área de TI por ejemplo para realizar auditorías internas o externas dentro de la red o sistemas de información de la CCH.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 44/52
--	--	---

9.10.28 Revisión de accesos de usuarios

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

9.11 POLÍTICAS DE BACKUP

9.11.1 Período de almacenamiento de registros de auditoría.

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

9.11.2 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 soportado en el/los manual(es) de copias de seguridad.

9.11.3 Copias de información sensible.

Se deben elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y/o cinta, según el/los manual(es) de copias de seguridad y almacenado en un lugar externo.

9.11.4 En dónde usar sistemas de respaldo para sistemas informáticos.

Todo computador que almacene información sensible de la Cámara de Comercio del Huila debe tener un sistema de respaldo para garantizar su protección y que no sea modificada y borrada.

9.12 POLÍTICAS DE USO DE FIREWALL

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 45/52
--	--	---

9.12.1 Detección de intrusos.

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

9.12.2 Toda conexión externa debe estar protegida por el firewall.

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

9.12.3 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.

9.12.4 Firewall debe correr sobre un computador dedicado o appliance.

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

9.12.5 Inventario de conexiones.

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

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

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

9.12.7 Revisión periódica y reautorización de privilegios de usuarios.

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 46/52
--	--	---

9.13 POLÍTICAS PARA USUARIOS EXTERNOS

9.13.1 Términos y condiciones para clientes de Internet.

La Cámara de Comercio asume que todos los clientes que usan Internet para establecer relación con la Cámara de Comercio aceptan los términos y condiciones de uso impuestos por la Cámara de Comercio en sus términos y condiciones de uso del portal web, antes de realizarse cualquier transacción.

9.13.2 Acuerdos con terceros que manejan información o cualquier recurso informático de la Cámara de Comercio

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

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

Socios de negocios, proveedores, clientes y otros asociados a los negocios de la Cámara de Comercio deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con la Cámara de Comercio y verificada por la supervisión asignada para tal fin, 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.

9.14 POLÍTICAS DE ACCESO FÍSICO

9.14.1 Reporte de pérdida o robo de identificación.

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

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 47/52
--	--	---

9.14.2 Orden de salida para equipos electrónicos.

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

El retiro de los equipos de las dependencias de la Cámara de Comercio para mantenimiento correctivo se efectuará a través de una orden de salida firmada por el Director área de TIC o en su defecto quien esté a cargo de la oficina y la persona que retira el equipo.

9.14.3 Orden de salida de activos

Todos los activos que afecten la seguridad de la información de la Cámara de Comercio como medios de almacenamiento, CDs, DVDs., Memorias extraíbles, entre otros, y que necesiten ser retirados de la entidad, debe tener una autorización por parte del director de departamento/área.

9.14.4 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, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnet, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (empleados autorizados) al correo electrónico del área de Sistemas por parte de la Dirección de Talento Humano y SGSST.

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

Cualquier miembro de la Cámara de Comercio y/o tercero debe estar autorizado por la Presidencia ó el área de TIC para ingresar con equipos donde puedan obtener información. Estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).

10. DATA PRIVACY

La CCH debe establecer y comunicar la política de protección de datos personales para cualquier información de carácter personal que la organización pueda recolectar y procesar en sus aplicativos de TI

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 48/52
--	--	---

La política de protección y privacidad de datos personales no debe entrar en conflicto con las leyes locales donde opera la CCH (Colombia)

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

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

La persona designada por la Presidencia debe aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 49/52
--	--	---

12. ANEXOS

ANEXO 2.

ACUERDO DE CONFIDENCIALIDAD

Ciudad y Fecha: _____

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

Firma: _____

Documento de identificación: _____

Sede: _____

Área de la Cámara de Comercio: _____

Vo. Bo. Dirección Talento Humano y SGSST

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 50/52
--	--	---

ANEXO 3.

POLÍTICA DE ASUNTOS ESPECÍFICOS: IDENTIFICACIÓN BIOMÉTRICA PARA SIPREF.

1. ALCANCE

El presente anexo al documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información relacionados con la integración de los servicios de la Cámara de Comercio de Huila, Certicámara, Confecámaras y la Registraduría Nacional del estado civil, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar previamente un acuerdo de confidencialidad (Anexo 2), que los compromete con el cumplimiento de las políticas de seguridad ya descritas. Los usuarios de los activos que se denominan así:

Empleados de la Cámara de Comercio: Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular el sistema de autenticación biométrica en línea.

2. PROCEDIMIENTO

Los miembros de la Dirección del área de TIC, conscientes que los recursos de información son utilizados de manera permanente por los usuarios de la Cámara de Comercio que manipulan el servicio de identificación biométrica, definidos en este anexo, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información, compartidas de igual forma por Certicámara y Confecámaras.

3. MEDIDAS DISCIPLINARIAS POR INCUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo con su gravedad serán evaluadas con el reglamento interno de trabajo.

4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 51/52
--	--	---

4.1 Instrucciones para el uso de recursos informáticos.

El uso del computador personal, periféricos y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica en línea, debe someterse a todas las instrucciones técnicas, que imparta la dirección del área de TIC.

4.2 Uso personal de los recursos

Los recursos informáticos de la Cámara de Comercio, dispuestos para la operación registral, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de la Cámara de Comercio usuaria de este servicio. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad. Cualquier otro uso está sujeto a previa autorización de la Presidencia y Dirección Jurídica.

4.3 Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos las Cámaras de Comercio, todo usuario debe firmar un acuerdo de confidencialidad (Anexo 2) 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 de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware.

4.4 Traslado de equipos debe estar autorizado.

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

5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

5.1 Identificación única para cada usuario.

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (Usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores. Esta política rige para

 Cámara de Comercio del Huila	MANUAL DE PROCEDIMIENTOS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	FECHA 11-2021 VERSIÓN 7 PAGINA 52/52
--	--	--

aplicativos implementados hasta la fecha de liberación de este documento. En caso del sistema de autenticación biométrica en línea, el acceso al sistema se realizará mediante un cotejo inicial entre el sistema biométrico local, la plataforma de Certicámara y el sistema registral, los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de la Cámara de Comercio.