



Cámara de
Comercio de
Cartago

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO: TIC-O-002

VERSIÓN: 002

FECHA: SEPT 03 2024



SEGURIDAD DE LA INFORMACIÓN

Política de Seguridad de la información
de la Cámara de Comercio de Cartago

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Tabla de contenido

INTRODUCCIÓN.....

1

OBJETIVO.....

1

ALCANCE.....

1

REQUISITOS LEGALES Y/O REGLAMENTARIOS.....

2

DEFINICIONES.....

2

RESPONSABLE.....

6

COMPROMISO DE LA DIRECCIÓN.....

6

GESTIÓN DE LOS RECURSOS.....

6

PROCEDIMIENTO.....

6

POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO.....

7

POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA.....

7

POLÍTICAS DE CUMPLIMIENTO Y SANCIONES.....

7

Cumplimiento con la seguridad de la información.....

7

Medidas disciplinarias por incumplimiento de políticas de seguridad.....

8

POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS.....

8

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

8

Uso personal de los recursos.....

8

Acuerdo de confidencialidad.....

8

Uso del aplicativo entregado.....

8

El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.....

9

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

9

Recursos compartidos.....

9

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

9

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

9

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

10

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

10

Manejo de sesiones en sistemas informáticos.....

10

Notificación de sospecha de pérdida, divulgación o uso indebido de información.....

10

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

10

Traslado de equipos debe estar autorizado.....

10

Control de recursos informáticos entregados a los usuarios.....

10

Configuración de sistema operativo de las estaciones de trabajo.....

11

Uso restringido de módems en las estaciones de trabajo.....

11

Protección por Defecto de Copyright.....

11

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Custodia de Licencias de Software.....	11
Apagado de equipos en la noche.....	11
Tiempo limitado de conexión en aplicaciones de alto riesgo.....	11
POLÍTICAS DE USO DE LAS CONTRASEÑAS.....	12
Confidencialidad de las contraseñas.....	12
Uso de diferentes contraseñas para diferentes recursos informáticos.....	12
Identificación única para cada usuario.....	12
Cambios periódicos de contraseñas.....	12
Longitud mínima de contraseñas.....	12
Contraseñas fuertes.....	12
Prohibición de contraseñas cíclicas.....	13
Las contraseñas creadas por usuarios no deben ser reutilizadas.....	13
Almacenamiento de contraseñas.....	13
Sospechas de compromiso deben forzar cambios de contraseña.....	13
Revelación de contraseñas prohibida.....	13
Bloqueo estación de trabajo.....	13
Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema.....	13
POLÍTICAS DE USO DE LA INFORMACIÓN.....	14
Divulgación de la información manejada por los usuarios de La Cámara de Comercio.....	14
Transferencia de datos solo a organizaciones con suficientes controles.....	14
Registro de las compañías que reciben información privada.....	14
Transferencia de la custodia de información de un colaborador que deja La Cámara de Comercio.....	14
Transporte de datos sensibles en medios legibles.....	14
Datos sensibles enviados a través de redes externas deben estar encriptados.....	15
Clasificación de la Información.....	15
Eliminación Segura de la Información en Medios Informáticos.....	15
Eliminación segura de la información en medios físicos.....	15
POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO.....	15
Prohibición de uso de Internet para propósitos personales.....	15
Formalidad del correo electrónico.....	15
Preferencia por el uso del correo electrónico.....	16
Uso de correo electrónico.....	16
Revisión del correo electrónico.....	16
Mensajes prohibidos.....	16
Acciones para frenar el SPAM.....	16
Todo buzón de correo debe tener un responsable.....	16
Enviando software e información sensible a través de Internet.....	16
Intercambio de información a través de Internet.....	16
POLÍTICAS DE LA INTRANET Y SITIOS WEB DE LA CÁMARA DE COMERCIO.....	17
Reglas de uso de la Intranet.....	17
Prohibición de publicitar la imagen de La Cámara de Comercio en sitios diferentes a los institucionales.....	17
Prohibición establecer conexiones a los sitios Web de La Cámara de Comercio.....	17
Prohibición de anuncios en sitios Web particulares.....	17
POLÍTICAS GENERALES DE LA PRESIDENCIA.....	17
Evaluación y tratamiento del riesgo.....	17

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.....18

Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.....18

Entrenamiento compartido para labores técnicas críticas.....18

Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.....18

Personal competente en el Centro de Cómputo para dar pronta solución a problemas.....18

Chequeo de virus en archivos recibidos en correo electrónico.....19

Contacto con grupos especializados en seguridad informática.....19

POLÍTICAS PARA DESARROLLADORES DE SOFTWARE.....19

Ambientes separados de producción y desarrollo.....19

Cumplimiento del procedimiento para cambios y/o actualizaciones.....19

Documentación de cambios y/o actualizaciones.....19

Catalogación de programas.....19

Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.....19

Dependencia de la autenticación de usuario en el sistema operativo.....20

Incorporación de contraseñas en el software.....20

Acceso del usuario a los comandos del sistema operativo.....20

Se requieren registros de auditoria en sistemas que manejan información sensible.....20

Registros para los usuarios privilegiados en los sistemas en producción que lo permitan.....20

Los registros del sistema deben incluir eventos relevantes para la seguridad.....20

Resistencia de los registros contra desactivación, modificación y eliminación.....20

Procesos controlados para la modificación de información del negocio en producción.....21

Validación de entradas en los desarrollos.....21

Diseño de seguridad para aplicaciones.....21

Personas autorizadas para leer los registros de auditoría.....21

Archivo histórico de contraseñas.....21

POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS.....21

Soporte para usuarios con privilegios especiales.....21

Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la Entidad.....22

Cuando y como pueden asignar contraseñas los administradores.....22

Límite de intentos consecutivos de ingreso al sistema.....22

Cambio de contraseñas por defecto.....22

Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.....22

Administración de los buzones de correo.....22

Brindar acceso a personal externo.....22

Acceso a terceros a los sistemas de la Entidad requiere de un contrato firmado.....23

Restricción de administración remota a través de Internet.....23

Dos usuarios requeridos para todos los administradores.....23

Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.....23

Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado.....23

Remoción de software para la detección de vulnerabilidades cuando no esté en uso.....23

Manejo administrativo de seguridad para todos los componentes de la red.....23

Información a capturar cuando un crimen informático o abuso es sospechado.....23

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Sincronización de relojes para un registro exacto de eventos en la red.....	24
Revisión regular de los registros del sistema.....	24
Confidencialidad en la información relacionada con investigaciones internas.....	24
Información con múltiples niveles de clasificación en un mismo sistema.....	24
Segmentación de recursos informáticos por prioridad de recuperación.....	24
Software de identificación de vulnerabilidades.....	24
En dónde usar controles de acceso para sistemas informáticos.....	24
Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales.....	25
Habilitación de Logs en Sistemas y Aplicaciones.....	25
Monitoreo de Sistemas.....	25
Mantenimiento de los Sistemas.....	25
Verificación física de equipos críticos.....	25
Servicios de Red.....	25
Revisión de accesos de usuarios.....	25
POLÍTICAS DE BACKUP.....	25
Período de almacenamiento de registros de auditoría.....	25
Tipo de datos a los que se les debe hacer backup y con qué frecuencia.....	26
Copias de información sensible.....	26
POLÍTICAS DE USO DE FIREWALL.....	26
Detección de intrusos.....	26
Toda conexión externa debe estar protegida por el firewall.....	26
Toda conexión hacia Internet debe pasar por el Firewall.....	26
Filtrado de contenido activo en el Proxy.....	26
Firewall debe correr sobre un computador dedicado o appliance.....	26
Inventario de conexiones.....	27
El sistema interno de direccionamiento de red no debe ser público.....	27
Revisión periódica y reautorización de privilegios de usuarios.....	27
POLÍTICAS PARA USUARIOS EXTERNOS.....	27
Términos y condiciones para clientes de Internet.....	27
Acuerdos con terceros que manejan información o cualquier recurso informático de La Cámara de Comercio.....	27
Definición clara de las responsabilidades de seguridad informática de terceros.....	27
POLÍTICAS DE ACCESO FÍSICO.....	28
Reporte de pérdida o robo de identificación.....	28
Orden de salida para equipos electrónicos.....	28
Orden de salida de activos.....	28
Cuando se da una terminación laboral, los privilegios de acceso a la sede de La Cámara de Comercio deben ser revocados.....	28
Ingreso de equipos de grabación y fotografías al Cuarto de servidores.....	28
POLÍTICAS Y PROCEDIMIENTOS DE HABEAS DATA.....	28
POLITICA DE USO DE PORTATILES.....	29
Protección de la información.....	29
Protección del equipo portátil.....	29

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACION DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.....32

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.....32

Oficial de Seguridad de la Información.....33

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de la **CÁMARA DE COMERCIO DE CARTAGO**. En adelante **La Cámara de Comercio**, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información. Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

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 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.

ALCANCE

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

- **Colaboradores de Planta:** Se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.
- **Colaboradores de la Cámara de Comercio:** Se definen como los colaboradores de la Cámara de Comercio que son susceptibles de manipular sistemas de información.
- **Contratistas:** Se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- Colaboradores en misión.
 - **Colaboradores por Outsourcing:** Son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos.
 - Personas naturales que prestan servicios independientes a la Entidad.
 - Proveedores de recursos informáticos.
- **Entidades de Control:**
 - Procuraduría.
 - Revisoría Fiscal.
 - Contraloría General de la República.
 - Superintendencia de Sociedades.
 - **Otras Entidades:**
 - DIAN.

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.

DEFINICIONES

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

- **Tics:** Área encargada de las Tecnologías de la Información y las Comunicaciones.
- **Activo:** Cualquier bien que tenga valor para la organización.
- **Acuerdo de Confidencialidad:** Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de La Cámara de Comercio.
- **Administradores:** Usuarios a quienes la Cámara de Comercio ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la Cámara de Comercio quienes estarán bajo la dirección de la Vicepresidencia de tecnología y soluciones de información de la Entidad.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
- **Backup:** Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- **Coordinación de Planeación e Innovación:** Es el responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.
- **Comité de Seguridad:** Equipo de trabajo conformado por el presidente ejecutivo, coordinador de tecnología o los colaboradores que hagan sus veces.
- **Contraseña:** Clave de acceso a un recurso informático.
- **Control:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **Directrices:** Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- **Servicios de procesamiento de información:** Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- **Evento de seguridad de la información:** Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
- **Firewall:** Conjunto de recursos de hardware y 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 (CONFIDENCIAL):** Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de colaboradores por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de 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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

- **Información pública:** Es la información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.
- **LAN:** Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).
- **Licencia de Software:** Es la autorización o permiso concedido 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 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 específica el uso que se le puede dar al software.
- **Software Libre:** Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
- **Software pirata:** Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
- **Software de Dominio Público:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- **Freeware:** Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- **Shareware:** Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- **Módem (Modulador - Demodulador de señales):** Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.
- **Monitoreo:** Verificación de las actividades de un usuario con respecto a los recursos informáticos de La Cámara de Comercio.
- **OTP (One Time Password):** Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.
- **Plan de contingencia:** Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de La Cámara de Comercio en casos de desastres y otros casos que impidan el funcionamiento normal.
- **Política:** Toda intención y directriz expresada formalmente por la dirección.
- **Protector de pantalla:** Programa que se activa a voluntad del usuario, o automáticamente después de un tiempo en el que no ha habido actividad.
- **Proxy:** Servidor que actúa como puerta de entrada a la Red Internet.
- **Recursos informáticos:** Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.
- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
- **Análisis de Riesgos:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Evaluación de Riesgos:** Todo proceso de análisis y valoración del riesgo.
- **Valoración del riesgo:** Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Router:** Equipo que permite la comunicación entre dos o más redes de computadores.
- **Sesión:** Conexión establecida por un usuario con un Sistema de Información.
- **Sistema de control de acceso:** Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.
- **Sistema de detección de intrusos (IDS):** Es un conjunto de hardware y software que ayuda en la detección de accesos o intentos de acceso no autorizados a los recursos informáticos de La Cámara de Comercio.
- **Sistema de encriptación:** Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.
- **Sistema multiusuario:** Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.
- **Sistema operativo:** Software que controla los recursos físicos de un computador.
- **Sistema sensible:** 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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- **Usuario:** toda persona que pueda tener acceso a un recurso informático de La Cámara de Comercio.
- **Usuarios de red y correo:** Usuarios a los cuales La Cámara de Comercio les entrega un identificador de cliente para acceso a sus recursos informáticos.
- **Usuarios externos:** Son aquellos clientes externos que utilizan los recursos informáticos de La Cámara de Comercio a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.
- **Usuarios externos con contrato:** Usuarios externos con los cuales La Cámara de Comercio establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

RESPONSABLE

COMPROMISO DE LA DIRECCIÓN

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

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

GESTIÓN DE LOS RECURSOS

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de la misión y visión de La Cámara de Comercio.
- 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.

PROCEDIMIENTO

- Comunicación de las políticas de seguridad:

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

- Aplicación de las políticas de seguridad:

Las políticas de seguridad informática se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO

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

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

POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

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

- Políticas de Cumplimiento y Sanciones.
- Políticas de uso de recursos informáticos.
- Políticas de contraseñas.
- Políticas de uso de la información.
- Políticas del uso de Internet y correo electrónico.
- Políticas de uso de la Intranet y Sitio Web de La Cámara de Comercio.
- Políticas Generales de la Presidencia.
- Políticas para Desarrolladores de Software.
- Políticas para Administradores de Sistemas.
- Políticas de Copias de respaldo.
- Políticas de Uso de Firewall.
- Políticas para Usuarios previstos en el numeral tercero.
- Políticas de Acceso Físico.

POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

Cumplimiento con la seguridad de la información

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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 al comité de seguridad.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Todo incumplimiento de una política de seguridad de la información por parte de un colaborador o contratista, así como de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en alguna sede de La Cámara de Comercio, esta podrá suspender la prestación de cualquier servicio de información.

POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

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 el comité de seguridad.

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.

Acuerdo de confidencialidad

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

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

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Uso del aplicativo entregado

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

El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados

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

Declaración de reserva de derechos de La Cámara de Comercio

La Cámara de Comercio usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información 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 comité de seguridad siempre con el concurso de la Presidencia o de quién él delegue esta función.

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 y restringir por Dominio.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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

Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad.

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 encriptación y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

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

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

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.

Notificación de sospecha de pérdida, divulgación o uso indebido de información

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del comité de seguridad.

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 a los niveles establecidos en el presente documento: USO INTERNO y CONFIDENCIAL.

Traslado de equipos debe estar autorizado

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

Control de recursos informáticos entregados a los usuarios.

Cuando un colaborador inicie su relación laboral con La Cámara de Comercio se debe diligenciar el documento de entrega de inventario "GR-F-038 CONTROL ACTIVOS FIJOS". Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario en el formato "GR-F-089 TRASLADO DE ACTIVOS FIJOS" (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

Configuración de sistema operativo de las estaciones de trabajo

Solamente los colaboradores del área de Tics están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

Uso restringido de módems en las estaciones de trabajo

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

Protección por Defecto de Copyright

Todos los colaboradores de La Cámara de Comercio deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.

Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa.

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 colaboradores solo tienen instalado software legal y autorizado por el jefe de cada área.

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 colaboradores en la oficina durante la noche.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

POLÍTICAS DE USO DE LAS CONTRASEÑAS

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.

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.

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 colaboradores contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de La Cámara de Comercio.

Cambios periódicos de contraseñas

Todos los colaboradores de la Cámara de Comercio de Cartago sin excepción alguna deben realizar el cambio de contraseñas **cada seis meses** en los diferentes sistemas de información que gestionan. Esta medida es fundamental para mantener la seguridad de las cuentas, prevenir accesos no autorizados y proteger la información sensible, garantizando que se mantenga actualizada y segura.

Longitud mínima de contraseñas

Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

Contraseñas fuertes

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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

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-XXXX" que según la política "Contraseñas fuertes", es una contraseña válida, pero al mes siguiente pasa a ser "Febrero-XXXX" y así sucesivamente.

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".

Almacenamiento de contraseñas

Ninguna contraseña debe ser guardada de forma legible en archivos "batch", scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción de lo contemplado en la política "Almacenamiento de contraseñas de administrador".

Sospechas de compromiso deben forzar cambios de contraseña

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

Revelación de contraseñas prohibida

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

Bloqueo estación de trabajo

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

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

El ingeniero en soporte y web master debe reportar por medio de un correo electrónico, de manera oportuna al área de Tics, 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.

POLÍTICAS DE USO DE LA INFORMACIÓN

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

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

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.

Registro de las compañías que reciben información privada

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Transferencia de la custodia de información de un colaborador que deja La Cámara de Comercio

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

Transporte de datos sensibles en medios legibles

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

Clasificación de la Información

- 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.
- Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.
- Cualquier uso de servicio de procesamiento de información debe ser autorizado por el Gerente de TI de las cámaras de comercio según el caso, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener conocimiento todos los usuarios involucrados.

Eliminación Segura de la Información en Medios Informáticos

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

Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el comité de seguridad.

POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

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”.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

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.

Uso de correo electrónico

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

Revisión del correo electrónico

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

Mensajes prohibidos

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

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 Tics.

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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Enviando software e información sensible a través de Internet

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

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.

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

Reglas de uso de la Intranet

La Cámara de Comercio podrá utilizar la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el colaborador. Por lo tanto, en caso de existir, el colaborador deberá consultar la intranet permanentemente, así como todos los documentos que en ella se encuentren publicados.

Prohibición de publicitar la imagen de La Cámara de Comercio en sitios diferentes a los institucionales

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

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.

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con La Cámara de Comercio.

POLÍTICAS GENERALES DE LA PRESIDENCIA

Evaluación y tratamiento del riesgo

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

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

Se debe realizar una evaluación de riesgos a los recursos informáticos de La Cámara de Comercio por lo menos una vez al año utilizando el documento Interno: "PE-O-008 GUIA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA CÁMARA DE COMERCIO DE CARTAGO".

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

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

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.

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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

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

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

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.

Contacto con grupos especializados en seguridad informática

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

POLÍTICAS PARA DESARROLLADORES DE SOFTWARE

Ambientes separados de producción y desarrollo

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

Cumplimiento del procedimiento para cambios y/o actualizaciones

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluados en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

Documentación de cambios y/o actualizaciones

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

Catalogación de programas

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

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

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Dependencia de la autenticación de usuario en el sistema operativo

Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

Incorporación de contraseñas en el software

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

Acceso del usuario a los comandos del sistema operativo

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

Se requieren registros de auditoria en sistemas que manejan información sensible

Todo sistema que maneje información sensible para La Cámara de Comercio debe generar registros de auditoría que guarden toda modificación, adición y eliminación de dicha información.

Registros para los usuarios privilegiados en los sistemas en producción que lo permitan

Toda actividad realizada en los sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alternativo de control.

Los registros del sistema deben incluir eventos relevantes para la seguridad

Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

Resistencia de los registros contra desactivación, modificación y eliminación

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

Procesos controlados para la modificación de información del negocio en producción

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

Validación de entradas en los desarrollos

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

Diseño de seguridad para aplicaciones

El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para La Cámara de Comercio.

Personas autorizadas para leer los registros de auditoría

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

Archivo histórico de contraseñas

En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada (ver política "Las contraseñas creadas por usuarios no deben ser reutilizadas") y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

Soporte para usuarios con privilegios especiales

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

Cuando y como pueden asignar contraseñas los administradores

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

Límite de intentos consecutivos de ingreso al sistema

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña válida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados: a) ser suspendido hasta nueva reactivación por parte del administrador; b) ser temporalmente bloqueado (no menos de 5 minutos); c) ser desconectado si se trata de una conexión telefónica.

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”.

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 del mismo 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.

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, mensualmente 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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Brindar acceso a personal externo

El ingeniero de soporte y web master velará porque individuos que no sean empleados, contratistas o consultores de La Cámara de Comercio no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Presidencia o el comité de seguridad.

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

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

Restricción de administración remota a través de Internet

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

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.

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

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

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.

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.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Manejo administrativo de seguridad para todos los componentes de la red

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

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.

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

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

Revisión regular de los registros del sistema

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

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.

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.

Segmentación de recursos informáticos por prioridad de recuperación

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

En dónde usar controles de acceso para sistemas informáticos

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

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

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

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

Monitoreo de Sistemas

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

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

Verificación física de equipos críticos

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

Servicios de Red

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

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.

POLÍTICAS DE BACKUP

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.

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

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

Copias de información sensible

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

POLÍTICAS DE USO DE FIREWALL

Detección de intrusos

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

Toda conexión externa debe estar protegida por el firewall

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

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.

Filtrado de contenido activo en el Proxy

La dirección de TI de la Cámaras de Comercio, debe asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como applets de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información de La Cámara de Comercio.

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.

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.

El sistema interno de direccionamiento de red no debe ser público

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

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de Tics con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios a la Presidencia.

POLÍTICAS PARA USUARIOS EXTERNOS

Términos y condiciones para clientes de Internet

La Cámara de Comercio asume que todos los clientes que usan Internet para establecer relación con Confecámaras o realizan operaciones con las cámaras de comercio aceptan los términos y condiciones impuestos por La Cámara de Comercio en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.

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.

Definición clara de las responsabilidades de seguridad informática de terceros

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

POLÍTICAS DE ACCESO FÍSICO

Reporte de pérdida o robo de identificación

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

Orden de salida para equipos electrónicos

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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.

Orden de salida de activos

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

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 (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (colaboradores autorizados) correo electrónico al área de Tics (tics@camaracartago.org)

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 el área de seguridad de la información para ingresar con equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas etc.).

POLÍTICAS Y PROCEDIMIENTOS DE HABEAS DATA

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo de Cámara de Comercio de Cartago.

Para más información acerca de habeas data consulte el **Manual de Políticas y procedimientos Habeas Data**.

POLITICA DE USO DE PORTATILES

Protección de la información

- El antivirus siempre debe estar activo y actualizado.
- No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de La Cámara de Comercio.
- Seguir las políticas de acceso remoto.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- Toda la información que es confidencial debe ir cifrada.
- Cuando el equipo deba ser devuelto a La Cámara de Comercio para reparación, mantenimiento etc. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo.
- De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de Tics.

Protección del equipo portátil

- No dejar el computador móvil en lugares públicos.
- Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su mano.
- Cuando vaya en su carro este debe ir en el baúl.
- No prestar el computador portátil a familiares y/o amigos.

POLÍTICA DE USO RESPONSABLE DE DISPOSITIVOS MÓVILES

Declaración de Propósito

El propósito de esta política es garantizar la seguridad de la información corporativa accesible y almacenada en dispositivos móviles, ya sean corporativos o personales, utilizados por los colaboradores para fines laborales. Esta política busca minimizar los riesgos asociados con el uso de dichos dispositivos, incluyendo la pérdida de datos, el acceso no autorizado y la exposición a amenazas de seguridad cibernética.

Alcance

Esta política se aplica a todos los colaboradores, contratistas y cualquier otra persona que utilice dispositivos móviles para acceder a recursos y datos de la entidad. Esto es válido tanto si los dispositivos son proporcionados por la entidad como si son de propiedad personal y se utilizan con fines laborales (BYOD - Bring Your Own Device).

Principios

- **Seguridad de la Información:** Proteger la información corporativa frente a accesos no autorizados, pérdida o robo.
- **Disponibilidad:** La información de la empresa debe estar disponible para los usuarios autorizados cuando la necesiten.
- **Responsabilidad:** Cada usuario es responsable del uso seguro de su dispositivo y del cumplimiento de esta política.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- **Privacidad:** Respetar la privacidad de los empleados mientras se aseguran los activos de la compañía.
- **Cumplimiento:** Alinear las prácticas de seguridad con los estándares y regulaciones vigentes, en particular la ISO 27001.

Contenido Obligatorio

I. Registro y Autorización de Dispositivos:

- Todos los dispositivos móviles (celulares y tablets), ya sean propiedad de la entidad o de uso personal con fines laborales (BYOD - Bring Your Own Device), que accedan a información corporativa, deben estar registrados y aprobados por el área de TIC'S.
- Solo dispositivos autorizados y configurados adecuadamente podrán acceder a recursos corporativos.

II. Uso Adecuado de Dispositivos:

- Los dispositivos móviles solo deben usarse para fines laborales.
- Se prohíbe el uso de dispositivos móviles para actividades ilícitas, inapropiadas o que puedan dañar la reputación de la entidad.

III. Configuración de Seguridad Mínima:

- Implementación de políticas de seguridad mediante Google Workspace y Android Device Policy, para controlar configuraciones de seguridad, instalar aplicaciones aprobadas y gestionar permisos de acceso.
- Uso de contraseñas seguras y autenticación multifactor (MFA) en todos los dispositivos.
- Configuración de bloqueo de pantalla con contraseña segura.
- Actualización periódica de sistemas operativos y aplicaciones para mitigar vulnerabilidades.

IV. Gestión de Aplicaciones:

- Restricción y control de aplicaciones instaladas en dispositivos móviles.
- Solo se deben instalar aplicaciones aprobadas por el área de TIC'S.
- Prohibición de aplicaciones que representen riesgos de seguridad.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- Uso de aplicaciones corporativas autorizadas y verificadas.

V. Protección contra Pérdida y Robo:

- Implementación de medidas para la localización y borrado remoto de dispositivos.
- Reporte inmediato de pérdida o robo de dispositivos al área de TIC'S.
- Procedimientos para la restauración de datos y bloqueo de acceso en caso de incidentes.

VI. Educación y Concienciación:

- Programas de formación continua sobre buenas prácticas de seguridad.
- Campañas de concienciación sobre riesgos y amenazas asociados al uso de dispositivos móviles.

Cumplimiento

El incumplimiento de esta política puede resultar en medidas disciplinarias que incluyen, pero no se limitan a, amonestaciones, suspensión de acceso a recursos corporativos y, en casos graves, terminación del contrato laboral. La entidad se reserva el derecho de realizar auditorías y revisiones periódicas para asegurar el cumplimiento de esta política.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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

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

El Jefe de Riesgos o 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.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

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

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

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad de la información, dentro de la Entidad:

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

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

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

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda):

- Mejoras en las actividades inherentes a la Seguridad de La Cámara de Comercio y sus procesos.
- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo de La Cámara de Comercio.
- Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.
- Cambio en los roles del ciclo de certificación.
- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de La Cámara de Comercio El Presidente Convoca al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por todos su miembros.

Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya(n) ejecutado la(s) acción(es) relacionadas.

Oficial de Seguridad de la Información

Oficial de Seguridad de la Información (Coordinador de aseguramiento y Calidad):

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los colaboradores de la compañía.
- Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando con cada proyecto que se implemente como afecta el mapa de riesgos y tomando siempre como base este mapa para cualquier proyecto nuevo que se implemente.
- Dirigir el programa de manejo y seguimiento de incidentes.

 Cámara de Comercio de Cartago	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TIC-O-002
		VERSIÓN: 002
		FECHA: SEPT 03 2024

- Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de la compañía.
Igualmente debe informarla a la compañía y validar que se cumpla. La metodología debe establecer niveles de acceso a la información.
- Crear y mantener un Programa de Concientización en seguridad de la información.
- Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

Integrantes del comité de seguridad de la información:

- Presidenta Ejecutiva.
- Coordinador de Tics.
- Auxiliar Tics.
- Coordinador de Aseguramiento y Calidad.
- Director Administrativo y Financiero.
- Directora Jurídica.
- Directora de Competitividad.

Control de Cambios	
Control de Cambios	Versión 01 - 28 de abril de 2024: Se crea la primera versión de la política, la cual fue aprobada por la Junta Directiva según el Acta No. 934 de la reunión ordinaria realizada el jueves 28 de abril de 2022. Versión 02 - 3 de septiembre de 2024: En la reunión del Comité de Seguridad de la Información realizada el martes 3 de septiembre de 2024, según el Acta No. 2, se realizan cambios en la periodicidad del cambio de contraseñas y se agregan a la presente política los lineamientos para el uso responsable de dispositivos móviles.

ELABORÓ / ACTUALIZÓ	REVISÓ	APROBÓ
Cargo: Coordinador de TICS	Comité de Seguridad de la Información	Comité de Seguridad de la Información
Fecha: junio 14 de 2024	Fecha: septiembre 03 de 2024	Acta No. 2 del Comité de Seguridad de la Información realizado el día Martes 03 de septiembre de 2024
Documento aprobado digitalmente a través del módulo de documentos del aplicativo Binaps		