MANUAL DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN

DOCUMENTO GENERAL
Radicado: 8-860044445-20180802000017
Fecha: 02/08/2018 09:26:02 a. m.
Usuario: gsousa
Descripción: MANUAL DE POLITICA DE SEGURIDAD DE LA INFORMACION
Almacenar en: 901041401 - MANUAL

Versión 1.0

Leticia, 12 de marzo de 2018

Control del documento

Elaboró	Revisó	Aprobó
Silvia Díaz Ardila	Didier Alberto Zúñiga Palacio	Comité de Control Interno
Directora Administrativa y de Sistemas	**Jefe de Control Interno y Calidad**	**Comité de Control Interno**

Control de cambios

Versión	Fecha de adopción	Descripción de cambios	Solicitó
1.0	12 de marzo de 2018	Se adopta el Manual de Política de Seguridad de la Información. (Aprobado mediante acta Nro. 10)	Directora Administrativa y de Sistemas

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de la Cámara De Comercio del Amazonas. 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.

2. 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.

3. 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 Cámara de Comercio 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.
- Funcionarios de la Cámara de Comercio: Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular sistemas de información.
- Contratistas: se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:
- Colaboradores en Misión; Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos;
  Personas naturales que prestan servicios independientes a la Entidad;
  Proveedores de recursos informáticos.
- Entidades de Control: Procuraduría, Revisoría Fiscal, Contraloría General de la República, Superintendencia de Industria y Comercio.
- Otras Entidades: DIAN

4. DEFINICIONES

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

Activo: Cualquier bien que tenga valor para la organización.

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

Administradores: Usuarios a quienes la Cámara de Comercio ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos y quienes estarán bajo la dirección Administrativa y de Sistemas.

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.

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 de la Cámara y amenazar la seguridad de la información.

Información confidencial (RESERVADA): Información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.

Información confidencial (CONFIDENCIAL): Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO): Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

Información pública: Es la información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.

LAN: Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio 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, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.

Módem (Modulador - Demodulador de señales): Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.

Monitoreo: Verificación de las actividades de un usuario con respecto a los recursos informáticos de La Cámara de Comercio.

OTP (One Time Password): Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

Plan de contingencia: Plan que permite el restablecimiento ágil 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 encripción: Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.

Sistema multiusuario: Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.

Sistema operativo: Software que controla los recursos físicos de un computador.

Sistema sensible: Es aquel que administra información confidencial ó de uso interno que no debe ser conocida por el público en general.
Tercera parte: Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

Usuario: toda persona que pueda tener acceso a un recurso informático de La Cámara de Comercio.

Usuarios de red y correo: Usuarios a los cuales La Cámara de Comercio les entrega un identificador de cliente para acceso a sus recursos informáticos.

Usuarios externos: Son aquellos clientes externos que utilizan los recursos informáticos de La Cámara de Comercio a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.

Usuarios externos con contrato: Usuarios externos con los cuales La Cámara de Comercio establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

5. 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.

6. RESPONSABLE

6.1. Compromiso de la dirección

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

- Mediante el establecimiento de una política de seguridad de la información;

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

6.2. Gestión de los recursos

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento 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.

7. PROCEDIMIENTO

7.1 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.

7.2 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 organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

8. POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO.

La Política de Seguridad de la Información de la Cámara de Comercio se encuentra establecida en el documento MAAS-PL02. (Ver listado de maestro de documentos)

9. POLÍTICA DE ASUNTOS ESPECÍFICOS: IDENTIFICACIÓN BIOMÉTRICA

La Política de Seguridad de la Información de la Cámara de Comercio se encuentra establecida en el documento MAAS-PL03. (Ver listado de maestro de documentos)

10. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

La Política de Seguridad de la Información de la Cámara de Comercio se encuentra establecida en el documento MAAS-PL04. (Ver listado de maestro de documentos)

11. POLÍTICAS DE USO DE LAS CONTRASEÑAS

La Política de Seguridad de la Información de la Cámara de Comercio se encuentra establecida en el documento MAAS-PL05. (Ver listado de maestro de documentos)

12. NORMAS GENERALES DE SEGURIDAD INFORMÁTICA

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

Cumplimiento y Sanciones – Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia Ejecutiva, la Dirección Administrativa y de Sistemas 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 funcionario 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 la sede de La Cámara de Comercio u en ocasión del desarrollo de cualquier actividad por fuera de sus instalaciones, esta podrá suspender la prestación de cualquier servicio de información.

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.

a. 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 Ejecutiva.

b. 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 los funcionarios de sistemas autorizados por la Cámara de Comercio.

c. 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.

d. Responsabilidades del usuario:

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 realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de La Cámara de Comercio.

e. 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 Ejecutiva o de quién él delegue esta función.

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

g. 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.

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

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del funcionario de sistemas y de ser necesario éste dará traslado al comité de seguridad.

i. 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.

j. Traslado de equipos debe estar autorizado.

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de la Cámara de Comercio sin previa autorización. Así mismo, ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de la sede a la cual fue asignado.

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

k. Control de recursos informáticos entregados a los usuarios.

Cuando un funcionario de la Cámara de Comercio inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

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

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

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

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

n. 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.

o. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área Administrativa y de Sistemas. 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 funcionarios solo tienen instalado software legal y autorizado por el jefe de cada área.

p. Apagado de equipos en la noche

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

q. 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.

Uso de contraseñas - Confidencialidad y uso de las contraseñas.

1. La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible.
2. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.
3. Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.
4. 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.

5. 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.
6. No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es "Enero-2004" que según la política "Contraseñas fuertes", es una contraseña válida, pero al mes siguiente pasa a ser "Febrero-2004" y así sucesivamente.
7. 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".
8. 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.
9. 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".
10. Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.
11. Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas.
12. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad.
13. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política "Auditoria periódica a las contraseñas de los usuarios".

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

Bloqueo estación de trabajo: Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 3 min. Por otra parte el escritorio del equipo

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

Reporte de cambio en las responsabilidades de los usuarios al Administrador del Sistema: El Director de cada área debe reportar por medio de un correo electrónico, de manera oportuna al área de sistemas, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

Uso de la información.

Divulgación de la información: 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: 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.

Transferencia de la custodia de información de un funcionario que deja la Cámara de Comercio: Cuando un empleado se retira de la Cámara de Comercio, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico 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.

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 la Directora Administrativa y de Sistemas de la Cámara 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.

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".

Formalidad y uso del correo electrónico institucional:

1. 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.

2. Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.
3. La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.
4. 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.
5. 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.
6. 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.
7. En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas.
8. Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

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.

a. Uso de la Intranet y Sitio Web de La Cámara de Comercio
b. Generales de la Presidencia
c. Administradores de Sistemas.
d. Copias de respaldo.
e. Uso de Firewall.
f. Usuarios previstos en el numeral tercero.
g. Acceso Físico.

Intranet y sitios web de la Cámara de Comercio

Reglas de uso de la Intranet: La Cámara de Comercio utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

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

De la Presidencia Ejecutiva

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 deben guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

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

Se debe realizar una evaluación de riesgos a los recursos informáticos de La Cámara de Comercio por lo menos una vez al año utilizando el procedimiento Interno: "Análisis de riesgos"

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 durante el tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Presidencia Ejecutiva.

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: 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. Además 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.

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.

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.

Para administradores de sistemas

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.

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.

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.

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. 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.

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".

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.

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.

La Directora Administrativa y de Sistemas o quien haga sus veces, 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 Ejecutiva o el Comité de Seguridad.

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.

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

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

Sin autorización escrita La Directora Administrativa y de Sistemas o quien haga sus veces, no debe otorgarle privilegios de administración a ningún usuario.

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.

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 encripción del software como tal.

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.

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.

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

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

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.

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.

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.

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 (Instrusion Detection System), detección de virus y bloqueo de correo no deseado. 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.

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

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

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

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

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

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.

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.

Copias de respaldo

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.

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.

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.

Uso de firewall

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 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.

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.

La dirección Administrativa y de Sistemas 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

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.

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.

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

Usuarios externos

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.

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.

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.

Acceso físico

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.

Ningún equipo electrónico podrá salir de las instalaciones de la Cámara de Comercio sin una orden de salida otorgada por la Directora Administrativa y de Sistemas o quien haga sus veces o sin haber sido registrado en el momento de su ingreso.

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 exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, llaves) y a su vez todos sus privilegios de acceso serán revocados por el área de Sistemas.

Uso de portátiles

1. El antivirus siempre debe estar activo y actualizado
2. No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de La Cámara de Comercio
3. Seguir las políticas de acceso remoto
4. Toda la información que es confidencial debe ir cifrada.
5. 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
6. De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas
7. No dejar el computador móvil en lugares públicos
8. Cuando viaje el computador portátil no debe ir dentro de su maletero siempre debe llevarse en su mano.
9. Cuando vaya en su carro este debe ir en el baúl.
10. No prestar el computador portátil a familiares y/o amigos.

13. 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. La Directora Administrativa y de Sistemas o quien haga sus veces, debe presentar al comité de control Interno para la aprobación 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 podrá ser mediante correo

electrónico u otro medio que se considere pertinente, establecido en la matriz de comunicaciones.

14. COMITÉ DE SEGURIDAD

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 Ejecutiva 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 de la Cámara de Comercio.
- 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.
- 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.