MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

Contenido

INTRODUCCIÓN

El presente Manual muestra la manera en que la Cámara de Comercio Aburrá Sur hace gestión y está comprometido con su Sistema de Gestión de Seguridad de la Información, con el fin de velar por la confidencialidad, integridad y disponibilidad de la información que se guarda, se procesa o se transmite dentro y fuera de la organización.

Por lo tanto, en este documento se reúnen todos los lineamientos y direccionamientos enfocados en los controles definidos por la alta gerencia para mantener el Sistema con base en la Norma ISO 27001:2013, para fortalecer el mejoramiento continuo frente a todos los aspectos y actividades de la gestión de la Seguridad de la Información en la compañía.

Este documento formaliza el compromiso de la Alta Dirección frente a la Gestión de la Seguridad de la Información y presenta por escrito a los usuarios el compendio de acciones con las cuales la Cámara 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 en relación con la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

1. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de la Política de Seguridad Información consiste en establecer unos criterios, directrices y estrategias que le permitan a la Cámara de Comercio Aburrá Sur proteger su información, así como la tecnología para el procesamiento y administración de la misma.

La Política de Seguridad Información proporciona la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades del sistema.

El propósito de estructurar Políticas de Seguridad de Información es, por tanto, garantizar que los riesgos para la Seguridad de Información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La Seguridad de Información consiste en garantizar la Confidencialidad, Integridad y Disponibilidad de la Información, así como de los sistemas implicados en su tratamiento dentro de la Cámara.

Al aclarar las responsabilidades de los usuarios y las medidas que deben adoptar para proteger la información y los sistemas informáticos, la Cámara evita pérdidas graves o divulgación no autorizada.

Por otra parte, el buen nombre de la Organización se debe en parte a la forma como protege su información y sus sistemas informáticos.

Por último, la Política de Seguridad de la Información puede ser útil como prueba en los litigios, en las negociaciones del contrato con el cliente, en las ofertas de adquisición y en las relaciones de negocios en general.

1.1 Objetivos de la seguridad de la información

- Ejecutar y monitorear actividades que aseguren la sostenibilidad y disponibilidad del Sistema de Gestión de Seguridad de la Información.

- Implementar programas de sensibilización a los colaboradores sobre la importancia y aplicación de la seguridad de la información.

- Garantizar y velar porque los riesgos de seguridad de la información sean identificados, valorados y tratados eficientemente.

- Dar cumplimiento y apoyo a los requerimientos legales, regulatorios, contractuales, apoyados en la estrategia de seguridad de la información.

2. MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Todas las políticas y procedimientos que figuran en este documento están aprobados, apoyados y respaldados por la Alta Dirección de la Cámara de Comercio Aburrá Sur.

Para la entidad está claro que la información depositada en los sistemas informáticos debe ser protegida de acuerdo con su criticidad, valor y sensibilidad de esta.

Las medidas de Seguridad de la Información deben ser tomadas, independientemente de los medios de almacenamiento donde se guarda la información, los sistemas utilizados para procesarla o los métodos usados para la transferencia de la misma.

La información que reposa en los sistemas informáticos debe ser protegida de acuerdo con su clasificación de seguridad.

3. DEFINICIONES

Para efectos del presente documento se entiende por:

Ataque: Evento, exitoso o no que atenta sobre el buen funcionamiento del Sistema Informático.

Amenaza: Es un evento que puede desencadenar un incidente en el sistema informático, produciendo daños materiales o pérdidas inmateriales en sus activos.

Análisis de Riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Buzón: También conocido como Cuenta de correo electrónico o de E-Mails.

Contraseña o Clave (Password): Es una forma de autenticación o control de acceso que utiliza información secreta para controlar el acceso hacia algún recurso informático. Puede está conformado por números, letras y/o caracteres especiales

Confidencialidad: Es asegurar que la información es accesada sólo por las personas autorizadas para ello.

Disponibilidad: Es asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando éstos sean requeridos.

Dispositivos USB: Es un dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías (pilas).

FTP: (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos): En informática es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Integridad: Mantenimiento de la exactitud e integralidad de la información y sus métodos de proceso.

Incidente de Seguridad de la Información: Es un evento atribuible a una causa de origen humano.

Esta distinción es particularmente importante cuando el evento es el producto de una intención dolosa de hacer daño.

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, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

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 y basado en el principio del menor privilegio.

Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad.

Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad.

Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO): Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general.

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

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

Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Impacto: Medición de los efectos que se generan en el Sistema Informático cuando se materializa una amenaza.

Plan de Contingencia: Disponibilidad de recursos para atender oportunamente una eventualidad en el Sistema Informático.

Política de Seguridad de la Información: Es el conjunto de directrices, lineamientos, medidas preventivas y reactivas de la organización y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma, generando valor agregado para la empresa y confiabilidad por parte del cliente interno y externo.

Política de Seguridad informática: Consiste en asegurar que los recursos y la información soportada en la plataforma informática (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. Toda intención y directriz expresada formalmente por la alta dirección.

Red Privada Virtual o VPN (siglas en inglés de Virtual Private Network): Es una tecnología de red que permite una extensión de la red local sobre una red pública.

Riesgo: Es la probabilidad de ocurrencia de un hecho favorable o desfavorable que pudiera afectar la Seguridad de la Información.

Sistema de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).

Sistema Multiusuario: Se refiere a un concepto de sistemas operativos, pero en ocasiones también puede aplicarse a programas de ordenador de otro tipo (e.j. aplicaciones de base de datos).

En general se le llama Multiusuario a la característica de un Sistema Operativo o Programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente.

Software Malicioso: Programa o parte de un programa destinado a perturbar, alterar o destruir la totalidad o parte de los elementos de la lógica esencial para el funcionamiento de un sistema de procesamiento de la información.

Estos programas se pueden dividir en cuatro clases: los virus informáticos, gusanos, troyanos y bombas lógicas.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un Sistema Informático.

Unidad Central de Procesamiento o CPU: Es el componente en un ordenador o computador que interpreta las instrucciones y procesa los datos contenidos en los programas de la computadora.

Virus: Es un programa de ordenador que puede copiarse a sí mismo e infectar un ordenador.

Vulnerabilidad: Son aspectos que influyen negativamente en la Seguridad de la Información y que posibilitan la materialización de una amenaza.

4. ALCANCE

El manual de seguridad de la información y todos sus aspectos están dentro del siguiente alcance para la compañía:

Los Empleados

La Seguridad de la Información es un esfuerzo grupal. Esto requiere de la participación y el esfuerzo de todos los miembros de la organización que trabajan con los sistemas de información.

Así, cada empleado deberá comprometerse en el cumplimiento de los requisitos de la Política de Seguridad de la Información y de los documentos asociados a la misma.

Los Sistemas (Hardware y Software)

Esta Política aplica para todos los computadores, redes, aplicaciones y sistemas operativos que son propiedad o son operados por la Cámara. La Política cubre únicamente la información manejada por los computadores y las redes institucionales.

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.
- Registraduría Nacional del Estado.
- Registro Único Empresarial y Social – RUES.

5. DIVULGACIÓN DE LA INFORMACIÓN

Acceso de información por parte de Terceros

El acceso a terceros de la información de la Institución será permitido siempre y cuando haya la debida autorización previa del Jefe del Área responsable de la misma.

Cuando el suministro de la información involucre aspectos tecnológicos deberá contarse adicionalmente con el visto bueno previo del Jefe Departamento TIC, quien deberá validar los riesgos de la seguridad de la información requerida.

Requerimiento de información por parte de terceros

Las solicitudes de información registral, informes financieros, documentos de políticas internas, actas, manuales, estudios económicos, procedimientos, y, en general, todo tipo de información, se encuentran amparados por los lineamientos de la Política de Seguridad de la Información.

Divulgación de la seguridad de la información a personal externo

La información relativa a las medidas de seguridad, a los sistemas de procesamiento de información y a las redes es confidencial y no debe ser divulgada a usuarios no autorizados a menos que se cuente con la autorización del Jefe Departamento TIC.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

6.1 Política general de seguridad de la información

La Cámara de Comercio de Aburrá Sur está comprometida con la custodia y protección de la información, garantizando la confidencialidad, integridad y disponibilidad de la misma, mediante actividades, procedimientos y estrategias definidas, que generen valor agregado para el cliente interno y externo, apoyados en un comprometido y excelente equipo humano que trabaja cada día para proteger la información, administrando de manera transversal y efectiva los riesgos de seguridad de la información y sus controles necesarios para la mejora continua, y de esta forma dar cumplimiento a la normatividad y requerimientos legales y contractuales vigentes.

6.2 Política de organización de la seguridad

Todos los funcionarios y terceros que prestan servicios a Cámara de Comercio de Aburrá Sur hacen parte de una estructura organizacional de Seguridad donde se debe contar con roles y responsabilidades formalmente definidas y comunicadas, teniendo en cuenta lo anterior, se debe dar cumplimiento a procedimientos y controles que garanticen el logro de los objetivos de Seguridad de la Información en la entidad.

En dicha estructura se deben considerar todos los proyectos o procesos que se ejecuten en la entidad y los medios o dispositivos de acceso a la información tanto internos como externos.

Como parte de esta política hacen parte todos los proyectos de la Cámara de Comercio Aburrá Sur desde sus etapas iniciales en las cuales se consideran todos los aspectos de seguridad de la información y sus riesgos, de igual manera se incluyen los aspectos de seguridad de la información para el teletrabajo, con el fin de proteger la información y su manejo en estas condiciones.

6.2.1. Organización Interna

Para la gestión de la seguridad de la información se definen roles y responsabilidades, los cuales pueden ser consultados en el documento Roles Y Responsabilidades de Seguridad de la Información.

Direcciones o áreas responsables de la Seguridad de la Información

El Comité de Seguridad de la Información, gestionado, conformado y respaldado por la Alta Dirección de la Cámara, es el responsable de establecer y mantener las Políticas de Seguridad de la Información, las normas, directrices y procedimientos de la Organización.

Declaración de reserva de derechos de La Cámara de Comercio

La Cámara 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 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;

3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Cámara.

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.

Contacto con grupos especializados en Seguridad de la Información. 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.

6.2.2. Dispositivos para la movilidad y teletrabajo

Sólo los empleados autorizados por la Presidencia Ejecutiva tendrán acceso remoto único y exclusivamente a través de una VPN (Red Privada Virtual) a los sistemas de la Cámara, no está permitido el acceso remoto utilizando conexiones diferentes a una VPN.

Esta autorización deberá estar expresamente formalizada y documentada y de la misma el Departamento TIC guardará copia.

El Departamento TIC llevará un registro de los empleados autorizados por la Presidencia Ejecutiva para acceder de manera remota a los sistemas de la Cámara y asistirá en la configuración de la conexión VPN a aquellos usuarios que hayan sido autorizados. De estos accesos deberán llevarse un Log.

La continuidad de estas autorizaciones estará sujeta al cumplimiento de las Políticas de Seguridad de la Información y la revocatoria de la autorización estará a cargo de la Presidencia Ejecutiva.

Dispositivos Móviles.

Las nuevas tecnologías, en su constante evolución, han permitido que se desarrollen nuevas herramientas para desempeñar labores profesionales de forma más eficaz.

Se ha evolucionado, del ordenador como principal herramienta de trabajo, a utilizar dispositivos móviles como smartphones o tablets en entornos de trabajo donde la movilidad es fundamental.

Sin embargo, esa movilidad conlleva unos riesgos asociados a la posibilidad de pérdida o robo del dispositivo, produciéndose una pérdida de confidencialidad de la información contenida en el mismo.

A continuación, se enumerarán algunas buenas prácticas o medidas disponibles que se pueden llevar a cabo para incrementar la seguridad en los dispositivos móviles.

- **Seguridad Lógica: Bloqueo por Contraseña.**

  La gran mayoría de dispositivos dispone de medidas de bloqueo al entrar en modo suspendido.

  Este recurso garantiza que el acceso al uso del dispositivo móvil sólo puede efectuarse por la persona autorizada que conoce la clave.

  En caso de extravío o robo, la única manera de poder utilizar el dispositivo es restaurando los valores de fábrica, por lo que toda la configuración y datos almacenados se perderían.

  Existen varios métodos para restringir el uso del dispositivo. Éstos varían en función del fabricante.

  Los más utilizados son la contraseña con pin de 4 dígitos, contraseña alfanumérica o patrón de desbloqueo.

  Es importante, igualmente, configurar el dispositivo móvil para que pasado un tiempo de inactividad pase automáticamente a modo de suspensión y se active el bloqueo de la pantalla.

  Si no se usara esta medida, la técnica de bloqueo perdería prácticamente toda su efectividad.

- **Cifrado de Memoria.**

Esta práctica se suele complementar con la técnica anterior. Consiste en cifrar la memoria de almacenamiento, haciendo imposible la copia o extracción de datos si no se conoce la contraseña de desbloqueo.

Según el modelo o fabricante, se permite cifrar tanto la memoria interna como la memoria de almacenamiento externo, como las tarjetas de memoria flash.

Una vez cifrado, solo se podrá acceder a los datos almacenados al encender el dispositivo con la contraseña de bloqueo de pantalla.

Si no se conociese la clave no sería posible recuperar la información, aunque se utilicen técnicas forenses de extracción y copia de datos.

La única forma posible sería con técnicas de fuerza bruta, que consisten en probar automáticamente todas las combinaciones posibles de contraseña, hasta encontrar aquella que permite el acceso.

Por tanto, es importante que para que este ataque sea muy difícil de llevarse a cabo, se utilice una contraseña compleja, que combine letras con dígitos, mayúsculas y caracteres especiales.

- **Borrado Remoto.**

Con esta práctica se podrán borrar los datos del dispositivo y restaurarlos a los valores de fábrica, todo ello de forma remota.

Puede ser muy importante tener a mano este recurso en caso de pérdida o robo del dispositivo, en el supuesto de que la información almacenada sea sensible.

Esta función depende del tipo de dispositivo, del fabricante o de la operadora, y es posible que el servicio sea de pago.

- **Copias de Seguridad.**

Si la información utilizada en el dispositivo es importante, y su pérdida ocasionara graves problemas, entonces sería conveniente utilizar alguna solución de copias de seguridad.

Hay programas que sincronizan los datos almacenados con el ordenador de escritorio, o en alguna aplicación online ofrecida por el fabricante, de forma que los datos están siempre disponibles y actualizados.

En caso de pérdida del dispositivo, la información seguiría estando disponible y a salvo.

Se recomienda que, si se utilizan este tipo de opciones, de sincronizar los datos con alguna aplicación online externa a nuestra organización, no se sincronice la información confidencial si la hubiera, puesto que dejaría de 'estar en nuestras manos'.

Lo recomendable es encontrar soluciones de copias de seguridad controladas por la Cámara, para que la información no viaje fuera de ella.

- **Los Peligros del Malware**

El uso cada día más frecuente de smartphones y tablets ha derivado en que la creación de malware apunte hacia estas plataformas.

Hoy día el riesgo de que un smartphone pueda ser infectado por un virus es una realidad.

Éstos se basan principalmente en el robo de documentos, contraseñas, datos bancarios e información personal.

Por eso es conveniente adoptar unas políticas de seguridad para evitar en la medida de lo posible infecciones de malware que haga peligrar la confidencialidad, integridad y disponibilidad de la información.

A continuación, se presentan algunas recomendaciones que apuntan a la mitigación de este riesgo:

- **Fuentes Confiables.**

El principal problema de infecciones en dispositivos móviles es por causa de la instalación de programas desde fuentes desconocidas.

Es muy importante instalar aplicaciones únicamente desde los repositorios oficiales del dispositivo, como App Store o Google Play y App Word, para iPhone/iPad o Android y BlackBerry respectivamente.

Se debe evitar siempre instalar aplicaciones descargadas directamente de P2P, o foros.

Se corre el serio riesgo de que estos programas contengan algún troyano y tras su instalación, infecten el dispositivo.

- **Jailbreak/root**

Los términos Jailbreak o root de un dispositivo se refieren a conceder privilegios de administración a las aplicaciones, saltándose la protección que tiene por defecto los sistemas operativos.

Esta característica puede añadir funcionalidades extra al dispositivo, pero también es un riesgo extra al que se expone, ya que se está eliminando la barrera de protección que sin jailbreak o root se mantiene.

Salvo que sea absolutamente necesario para el funcionamiento de una aplicación concreta, no se permite habilitar esta característica a los dispositivos.

- **Sólo las aplicaciones necesarias**

Llenar el dispositivo de aplicaciones innecesarias no sólo ralentiza su funcionamiento, sino que aumenta el riesgo de que una de estas aplicaciones tenga una vulnerabilidad que pueda ser aprovechada por un atacante y conseguir el control del dispositivo.

Por eso es recomendable desinstalar toda aplicación que no sea estrictamente necesaria para el desempeño del dispositivo, y así minimizar el riesgo de exposición por una aplicación vulnerable.

Además, es importante leer los permisos y condiciones tiene que deben ser aceptados antes de instalar una aplicación y comprobar la reputación de la misma.

- **Protección antivirus**

Se recomienda disponer de un antivirus en el dispositivo móvil como medida extra de protección contra el malware.

- **Actualizaciones de software**

Los sistemas operativos de los dispositivos incluyen un sistema de actualización de aplicaciones.

Mediante una notificación, informan que existe una nueva versión de una aplicación instalada.

Estas actualizaciones, además de añadir funcionalidades, corrigen fallos de seguridad.

Siempre que el sistema notifique de una actualización disponible, se debe aceptar y aplicar la nueva versión.

Manteniendo el sistema actualizado se evitan posibles infecciones por aplicaciones vulnerables.

Otras Recomendaciones.

Otras recomendaciones importantes, además del sentido común a la hora de usar los dispositivos móviles y pensar siempre en lo que se está haciendo, son las siguientes:

- **No almacenar información sensible**

La información más delicada de la empresa u organización no debe ser almacenada en dispositivos móviles, aunque estén cifrados puesto que los dispositivos móviles suponen riesgos

- **WIFIS públicas**

Las redes inalámbricas de uso público, o compartido, como las disponibles en hoteles o cafeterías pueden suponer un riesgo.

A pesar de que tenga contraseña para poder utilizarse, un atacante podría conectarse y capturar el tráfico de todas las personas que se encuentran conectadas a esa red inalámbrica.

Podría entonces analizar el tráfico capturado y recopilar contraseñas o datos confidenciales.

Si se va a hacer uso de redes inalámbricas de uso público, se recomienda no acceder a ningún servicio que requiera contraseña, realizar operaciones bancarias o descargar documentos confidenciales.

- **Desactivar comunicaciones inalámbricas**

Es muy importante desactivar las redes inalámbricas si no se van a utilizar a corto plazo. Las redes más usuales suelen ser WIFI, Bluetooth, o infrarrojos.

Es posible realizar ataques contra redes inalámbricas, utilizando puntos de acceso falsos, y engañando al dispositivo para que se conecte automáticamente a una red de supuesta confianza.

El usuario navegaría entonces sin tener constancia de que el tráfico está siendo monitoreado por un atacante.

- **Cargadores públicos**

Se han dado casos de fugas de información en dispositivos móviles por haber sido conectados en cargadores públicos.

Se debe evitar conectar el dispositivo por USB a cualquier ordenador público, como hoteles o cibercafés, y cualquier otro aparato que no tengamos total confianza en él.

Pueden haber sido manipulados para extraer información de cualquier dispositivo USB al que se conecten.

6.3. Política de seguridad de los recursos humanos

Todos los colaboradores contratados directamente o por un proceso de tercerización de la entidad deben velar por el cumplimiento de los objetivos y las políticas de la Seguridad de la Información de Cámara de Comercio de Aburrá Sur.

Para ello se deben considerar los mecanismos que garanticen un nivel de seguridad aceptable en el proceso de contratación, formación, procesos disciplinarios, cambios de cargo y demás controles de seguridad definidos durante el periodo de ejecución del contrato laboral y posterior a su terminación.

Para más información consultar los Procedimientos de Selección y Contratación de Personal y Gestión del Recurso Humano.

6.4 Política de Administración de activos de información

La información de la entidad constituida por aquella, suministrada por los clientes y la concerniente a los procesos propios de negocio es considerada como esencial para la Cámara de Comercio de Aburrá Sur y por lo tanto debe ser protegida.

Es responsabilidad de los funcionarios de la entidad y en especial de los Gerentes, Directores y Líderes, identificar claramente los activos de información con los que tiene relación, identificar su rol como dueños o custodios, clasificarse a fin de definir su importancia para la organización y protegerse independientemente del medio en el que se encuentre o transmita por medio de mecanismos de identificación y tratamiento del riesgo.

De igual manera se deberá garantizar llevar a cabo una adecuada gestión, disposición y transferencia de los medios removibles que contengan información que deben estar igualmente clasificados y tener responsabilidad por dichos activos.

Si algún área por requerimiento muy específico tiene la necesidad de contar con un dispositivo especial o específico, su instalación deberá ser autorizada por la Presidencia Ejecutiva, con el apoyo técnico del Departamento TIC.

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.

6.4.1 Responsabilidad sobre los activos

Tener en cuenta que los activos pueden ser (Recursos de Información, Recueros de software, activos físicos y servicios), de acuerdo a su criticidad y sensibilidad los activos deben ser clasificados y por ello es de mucha importancia tenernos identificados e inventariados, teniendo claridad los riesgos asociados a los mismos.

Este documento Inventario y Clasificación de Activos de Información, contiene la información de los activos identificados para la Cámara de Comercio Aburrá Sur.

Todo lo relacionado a la gestión de activos lo encuentra disponible en el documento Procedimiento Gestión de Activos Tecnológicos.

El uso con fines personales de los recursos tecnológicos de la Cámara está permitido siempre y cuando sea en tiempo no laboral y no afecte la productividad ni la seguridad de la información corporativa.

6.4.2 Clasificación de la información

El detalle del uso aceptable de los activos de información y la metodología de identificación y clasificación de estos se encuentran en el Procedimiento Clasificación y etiquetado Activos de información.

6.4.3 Manejo de los soportes de almacenamiento

Los medios de almacenamiento deben ser controlados y protegidos adecuadamente.

De acuerdo con el manejo que se debe dar a los medios de almacenamiento, se establece la siguiente política de manejo de medios:

Todos los medios que guarden información de la organización deben tener autorización y revisión de uso por parte del Departamento TIC, con el fin de instalar los mecanismos y controles necesarios para proteger la información, tales como cifrado de información, control de acceso a través de contraseñas, entre otros.

De igual forma ningún funcionario está autorizado para utilizar los medios removibles sin el visto bueno y autorización del Departamento TIC.

Para ello, y como parte de esta Política, todos los equipos de cómputo de los usuarios en la Cámara de Comercio Aburrá Sur se encuentran bloqueados para el retiro de información en medios removibles.

Solo están autorizados los roles y cargos que por parte de la alta gerencia sean aprobados.

El empleado tiene la obligación de proteger los discos, cintas magnéticas, CD-ROM y otros medios de almacenamiento como memorias USB que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

En el Procedimiento Gestión de Activos Tecnológicos en el Subproceso 5.1.3 se define cuando un activo es dado de baja, en el cual se requiere la eliminación segura de datos, por lo cual se debe seguir lo dispuesto por el Instructivo de Destrucción de Datos.

6.5 Política de control de acceso

Los aplicativos, sistemas operativos, redes y demás recursos tecnológicos de Cámara de Comercio de Aburrá Sur deben contar con esquemas de control de acceso confiables.

Por lo anterior es importante que cada colaborador o tercero resguarde apropiadamente las credenciales que le son suministradas considerando que son de carácter personal e intransferible.

Así mismo se establecen procesos de gestión de usuarios y perfiles que se deben aplicar en todo el ciclo de vida de la relación contractual tanto de los empleados, como de terceros de la entidad.

El detalle de los controles definidos para el acceso a los sistemas de información y elementos informáticos se encuentra en el documento Procedimiento Gestión de Accesos de Usuarios.

El personal con acceso privilegiado debe tener en cuenta sus obligaciones y responsabilidades de acuerdo con el apartado **Usuarios Administradores de Sistemas del documento Roles y Responsabilidades SGSI**.

Cada empleado es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y password o claves necesarios para acceder a la información y a la infraestructura tecnológica de la Cámara, por lo cual deberá mantenerlo de forma confidencial.

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

El acceso a Internet provisto a los usuarios de la Cámara es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

La asignación del servicio de Internet se tramita con el Departamento TIC. Esta solicitud se debe hacer a través de ticket y deberá tener el visto bueno del Jefe Inmediato.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la Cámara.

En caso de necesitar una conexión especial a Internet, ésta tiene que ser notificada y aprobada por el Jefe Departamento TIC.

El uso de módem para acceso a Internet está prohibido, en caso de requerir su uso, debe ser previamente solicitado a través de ticket y autorizado por el Jefe Departamento TIC y para realizar labores exclusivas de la organización.

Se prohíbe el uso de aplicaciones, programas y/o herramientas que saturen los canales de comunicación o Internet, tales como gestores de descarga de archivos multimedia (audio y/o videos), P2P, Torrent entre otros.

Se prohíbe la utilización de los computadores y recursos de la Cámara para ejecutar juegos de cualquier índole. Estas actividades darán lugar a acciones y sanciones disciplinarias.

Gestión de contraseñas de usuario

- La Cámara requiere que todos los empleados que tengan acceso a sus recursos tecnológicos dispongan de un Usuario y una Clave de carácter privado, personal e intransferible.

- La asignación del Usuario y Clave debe estar acorde a las funciones, responsabilidades y actividades del usuario.

- Todos los empleados tienen la obligación de proteger sus datos de autenticación.

- El acceso a la infraestructura tecnológica de la Cámara para personal externo debe ser autorizado por la Presidencia Ejecutiva, la cual deberá notificarlo al Jefe Departamento TIC, quien lo habilitará.

- Está prohibido que los empleados utilicen la infraestructura tecnológica de la Cámara para obtener acceso no autorizado a la información o a otros sistemas de información de la Cámara.

- Todos los empleados deberán utilizar el Usuario y Clave provistos por el Departamento TIC antes de poder usar la infraestructura tecnológica de la Cámara.

- Los empleados no deben proporcionar información a personal externo de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Cámara, a menos que se tenga la autorización de la Presidencia Ejecutiva.

- Cada empleado que acceda a la infraestructura tecnológica de la Cámara debe contar con un Identificador de Usuario (UserID) único y personalizado, por lo cual no está permitido el uso de un mismo UserID por varios empleados.

- Cualquier cambio en los roles y responsabilidades de los empleados que modifique sus privilegios de acceso a la infraestructura tecnológica de la Cámara deberá ser notificado al Jefe Departamento TIC con el visto bueno de su Jefe Inmediato.

- La asignación de la Clave debe ser realizada en forma individual, por lo que el uso de claves compartidas está prohibido.

- Cuando un empleado olvide, bloquee o extravíe su Clave deberá informarlo al Departamento TIC para que se le proporcione una nueva Clave y una vez que la reciba deberá cambiarla en el momento en que acceda nuevamente a la infraestructura tecnológica.

- Está prohibido que las Claves se encuentren de forma legible en cualquier medio impreso y dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.

- Sin importar las circunstancias, las Claves nunca se deben compartir o revelar.

  Hacer esto responsabiliza al empleado que prestó su Clave de todas las acciones que se realicen con la misma.

- La Clave tendrá una vigencia de 45 días. Finalizando este periodo el empleado recibe una solicitud electrónica de cambio de contraseña.

  Si el empleado llegara a sospechar que su Clave ha sido descubierta deberá modificarla inmediatamente.

- Los empleados no deben almacenar las claves en ningún programa o sistema que proporcione esta facilidad.

- Las claves no deben ser guardadas en archivos que puedan ser leídos, computadores sin control de acceso o en lugares donde personal no autorizado tenga acceso.

- Los empleados deben elegir una Clave que sea difícil de adivinar y que no contenga información relativa a la vida personal.

  Por ejemplo, no debe contener el número de la cédula, la fecha de nacimiento, número de teléfono, nombre de familiares (esposa, esposo, hijo), nombre de la mascota, etc.

Algunos consejos para la creación de claves o passwords

- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos.
- Combinar varias palabras. Combinar palabras con signos de puntuación o números, caracteres mayúsculas y minúsculas.
- Transformar una palabra común utilizando un método específico y personal.
- Crear acrónimos
- Deliberadamente utilizar mal una palabra o escribirla mal ortográficamente.
- No deben ser idénticos o similares a claves o passwords que hayan sido usados previamente.
- No utilice la misma clave para los diferentes sistemas o puntos de acceso al que esté autorizado.
- Cuando la información requiera ser compartida los empleados deben hacerlo utilizando e-mails, bases de datos, y directorios públicos ubicados en la red con controles de acceso y otros medios de intercambio de información.
- Las claves en ningún momento deben ser compartidas o divulgadas.
- Si se advierte que un empleado está utilizando los datos de autenticación (Usuario y Clave) de otro empleado, es su responsabilidad avisar de este evento a su Jefe Inmediato y al Jefe Departamento TIC.

6.6 Política de cifrado

La entidad cuenta con controles criptográficos para la protección de la información siendo necesario emplearlos en el establecimiento de canales de comunicación, protección de los activos con información confidencial y sensible.

Estos mecanismos serán usados para mantener la confidencialidad y la integridad de la información.

Por lo anterior las llaves o componentes criptográficos deberán ser protegidos por los dueños o administradores en todo su ciclo de vida. Más detalle se encuentra en el **Documento Política de Cifrado.**

6.7 Política de Seguridad Física y Entorno

Las instalaciones de Cámara de Comercio Aburrá Sur deben ser protegidas de amenazas tanto internas como externas, en especial aquellas zonas que se consideran restringidas y que resguardan equipos de procesamiento de información o documentación confidencial y/o sensible, con alcance de perímetro de seguridad, control de acceso, seguridad en oficinas y puestos de trabajo, protección contra amenazas internas y externas, y seguridad en todas las áreas que se considere que manejen información.

Así mismo es responsabilidad de todas las áreas de la entidad proteger físicamente los activos a su cargo tanto aquellos que son usados al interior de la entidad como aquellos que por su perfil o labor requieran salir de las oficinas.

Como parte fundamental de esta Política es de obligatorio cumplimiento que los funcionarios protejan adecuadamente los equipos desatendidos y que se mantenga y cumpla la **Política de Escritorio y Pantalla Limpia** en cada uno de los puestos de trabajo y equipos que sean asignados durante la relación contractual.

6.7.1 Áreas seguras

El acceso al centro de cómputo, servidores y áreas de trabajo que contengan información sensible o crítica, como la contenida en los servidores, debe estar restringido y solamente el personal autorizado podrá acceder a estos lugares.

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

Cualquier persona que tenga acceso a las instalaciones de la Cámara deberá registrar al momento de su entrada el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la misma, el cual podrán retirar el mismo día.

Para lo anterior deberá diligenciarse el documento denominado **Formato Registro de Visitantes** dispuesta en los puestos de información de nuestras Sedes.

Los sistemas, equipos de red y dispositivos USB deben asegurarse físicamente cuando se encuentren en oficinas o lugares abiertos.

Tanto los equipos de red, servidores y otros sistemas multiusuario deben estar ubicados en lugares con control de acceso.

En el **Procedimiento Gestión de Seguridad Física**, se detalla los controles y las medidas para controlar el acceso a las instalaciones de la Cámara de Comercio Aburrá Sur.

6.7.2 Seguridad de los equipos

Los computadores portátiles deben estar asegurados por un cable, ubicados en gabinetes cerrados o asegurados cuando se encuentren en lugares no vigilados.

Deberá configurarse el computador de tal manera que durante un tiempo de inactividad éste sea bloqueado automáticamente y se requiera para el reinicio de actividades el ingreso de una clave, el tiempo de inactividad se ha establecido en 5 minutos.

Queda prohibido que el usuario abra o desarme los equipos de cómputo. Únicamente el personal autorizado por el Departamento TIC podrá llevar a cabo los servicios y reparaciones al equipo de cómputo.

Los empleados deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los empleados y el Departamento TIC, deberán asegurarse de respaldar la información que consideren relevante y borrarla cuando el equipo de cómputo sea enviado a reparación, evitando así la pérdida involuntaria de información, derivada del proceso de reparación.

El empleado que tenga bajo su custodia algún equipo de cómputo será responsable de su uso y conservación.

En consecuencia, responderá con su propio patrimonio por la pérdida, daño o deterioro que ocurra a los equipos cuando el hecho acontezca por negligencia o culpa del trabajador.

El resguardo para los portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

El empleado deberá dar aviso inmediato de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo a la Dirección Administrativa y Financiera y activar el Procedimiento Gestión de Activos Tecnológicos, en el subproceso 5.1.4 Robo o Pérdida de activos

Se debe mantener el *Escritorio Limpio*" para garantizar la restricción a documentos, es decir, el escritorio o puesto de trabajo deberá estar lo menos saturado posible de objetos, documentos e información.

Lo anterior permitirá brindar la menor información posible a usuarios que nos son los propietarios del puesto de trabajo.

Siempre que no se esté utilizando el computador debe cerrarse la sesión de trabajo para evitar que un empleado no autorizado acceda al sistema.

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

Las computadoras personales, las computadoras portátiles, módems, y cualquier activo de tecnología de información de la entidad sólo podrá ser retirado de las instalaciones con la autorización de salida de la Dirección Administrativa y Financiera y se debe activar el **Procedimiento Gestión de Activos Tecnológicos**, y diligenciar el **Formato Movimiento de Activos**

La Dirección Administrativa y Financiera será la encargada de generar el resguardo y recabar la firma del empleado como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Departamento TIC.

El movimiento o retiro de equipos por traslado, reemplazo o baja debe ser ejecutado conforme al **Procedimiento Gestión de Activos Tecnológicos.**

El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones de la Cámara.

Será responsabilidad del empleado solicitar al Departamento TIC la asesoría necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Es responsabilidad de los empleados almacenar su información únicamente en la partición de disco duro identificada como “Mis Documentos” o similares, ya que es exclusivamente desde ahí donde se generan las copias automáticas de seguridad.

Se debe mantener el computador en un entorno limpio y sin humedad.

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

Mientras se opera el equipo de cómputo no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la CPU.

El empleado que tenga bajo su resguardo dispositivos especiales es responsable del buen uso que se les dé.

La ejecución de los mantenimientos de los activos tecnológicos se deje ejecutar según lo descrito en el Procedimiento Gestión de Mantenimientos.

6.8 Política de seguridad en las operaciones tecnológicas

Los sistemas tecnológicos propios o de terceros que manejan información de Cámara de Comercio Aburrá Sur deben ser protegidos de riesgos como software malicioso, aprovechamiento de vulnerabilidades, pérdida de información, cambios no controlados o falta de registros de auditoría entre otros.

Para garantizar lo anterior cada área de la entidad o proveedor en conjunto con el Departamento TIC, deberá velar por la confidencialidad, integridad y disponibilidad en éstos, realizando registro y seguimiento.

De acuerdo con la designación del personal por parte del Comité de Seguridad de la Información se deben realizar auditorías periódicas para verificar la correcta aplicación de controles y estándares técnicos definidos, asegurando en el tiempo las medidas de Hardening para las estaciones de trabajo, hardware y software de la compañía.

6.8.1 Responsabilidades y procedimientos de operación

Se deben establecer los procedimientos adecuados para la correcta operación, para ello se disponen de diferentes procedimientos de acuerdo con las funciones a desempeñar, los cuales pueden ser solicitados con el Jefe de Área.

Los procedimientos deben estar en constante actualización para garantizar la correcta operación.

Los cambios en los recursos tecnológicos dispuestos por la Cámara de Comercio Aburrá Sur para llevar a cabo las diferentes actividades deben estar soportados de acuerdo al **Procedimiento Gestión de Cambios de Infraestructura.**

El procedimiento para el manejo de cambios se aplicará siempre que se lleve a cabo una modificación importante en los recursos tecnológicos.

Esta Política aplica para todos los elementos que forman parte de la plataforma tecnológica dispuesta por la Cámara.

6.8.2 Protección contra código malicioso

Los empleados no deberán cancelar los procesos automáticos de actualización de las definiciones de virus.

Todos los sistemas deben ser analizados por un antivirus.

Un Scan debe ser ejecutado antes de abrir un archivo nuevo y después de ejecutar un software nuevo. El antivirus instalado en el computador deberá garantizar este proceso de manera automática.

Para prevenir infecciones por virus informático los empleados de la Cámara no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el Departamento TIC.

Los empleados de la Cámara deben verificar que la información y los medios de almacenamiento, considerando que al menos unidades USB, CD's, cintas y cartuchos, estén libres de cualquier tipo de software malicioso o virus, para lo cual deben ejecutar el software antivirus autorizado por el Departamento TIC.

Todos los archivos de computadora que sean proporcionados por personal externo o interno en relación con programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, deben ser verificados por el empleado de que estén libres de virus utilizando el antivirus autorizado antes de ejecutarse.

Ningún empleado de la Cámara debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir códigos de computadora diseñados para auto replicarse, dañar, o, en otros casos, impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software.

Mucho menos pueden proceder a probarlos en cualquiera de los ambientes o plataformas de la Cámara. El incumplimiento de este estándar será considerado una falta grave.

Ningún empleado o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Jefe Departamento TIC.

Cualquier empleado que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Departamento TIC para la detección y erradicación del virus.

Cada empleado que tenga bajo su resguardo algún equipo de computador portátil asignado por la Cámara y que dicho activo no esté conectado permanentemente a la red institucional, será responsable de solicitar periódicamente al Departamento TIC las actualizaciones de las definiciones de virus.

Los empleados no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Cámara en: Antivirus, Outlook, Office, Navegadores u otros programas.

Todos los medios removibles y otros medios de almacenamiento electrónico sobre un computador infectado no deberán ser utilizados sobre otro computador hasta que el virus haya sido removido de manera exitosa.

El computador infectado deberá ser retirado de la operación para su revisión oportuna y efectiva.

Debido a que algunos virus son extremadamente complejos ningún empleado de la Cámara debe intentar erradicarlos de las computadoras.

El Departamento TIC será el encargado o responsable de llevar a cabo las acciones para la remoción del virus y garantizar la pérdida mínima de información, minimizar los daños y el tiempo fuera de servicio del computador infectado.

6.8.3 Copias de seguridad

La información de los computadores debe ser periódicamente respaldada en dispositivos destinados para tal fin, para lo cual la Cámara de Comercio cuenta con un **Procedimiento Copias de Respaldo,** en el cual se disponen de las instrucciones necesarias para realizar el respaldo de la información.

El Departamento TIC es el responsable de respaldar la información contenida en los servidores de la Cámara.

El Departamento TIC brindará apoyo y asistencia técnica para la instalación de software o hardware de Backup.

6.8.4 Registro de actividad y supervisión

El Jefe Departamento TIC, previa autorización de la Presidencia Ejecutiva, se reservará el derecho de supervisar, monitorear e inspeccionar en cualquier momento los sistemas de información utilizados por los empleados.

Las inspecciones pueden llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado.

Los Sistemas de Información sujetos a dicha inspección incluyen los registros de la actividad de los empleados: Archivos, log, correos electrónicos institucionales y los soportes físicos de la información auditada pueden ser sujetos de la misma inspección en cualquier momento.

Lo anterior, sin perjuicio del respeto a la intimidad personal y a la inviolabilidad de la correspondencia y demás formas de comunicación privada en los términos del mandato constitucional.

La Cámara dispone de un software para el control de la navegación en Internet, el cual restringe el acceso a las categorías que universalmente las instituciones bloquean como, por ejemplo, sitios de contenido pornográfico, consumo de ancho de banda, contenidos racistas, violencia, ocio, etc.

Dicho software genera periódicamente los informes de los resultados (logs) de la navegación, los cuales son enviados a los jefes de Área y al Coordinador de Control Interno.

De necesitarse el acceso a una página bloqueada deberá ser autorizado por el jefe de Área con el concepto del Jefe Departamento TIC.

Esto se deberá hacer a través de un ticket en donde se especifique la URL y el porqué del requerimiento.

Los empleados de la Cámara con acceso a Internet, al acceder al servicio están aceptando que:

1. Serán sujetos de monitoreo de las actividades que realizan en Internet.

2. Existe la prohibición de acceso a páginas no autorizadas.

3. Se prohíbe la transmisión de archivos reservados o confidenciales no autorizados.

4. Se prohíbe la descarga de software sin la autorización del Departamento TIC.

5. La utilización de Internet es para el desempeño de su función en la Cámara y no para propósitos personales.

La Cámara se reserva el derecho de retirar cualquier material lesivo para los intereses de la institución o que contenga información ilegal.

Se deberá mantener sincronizado los relojes de todos los sistemas de procesamiento de información.

6.8.5 Control de Software en explotación

El desarrollo de software a cargo de terceros deberá tener los niveles de garantía del servicio, permitiendo la estabilidad del Sistema.

Esto será requerido cuando un Sistema pasa del ambiente de pruebas a producción, y se deberá garantizar que los procesos sean ejecutados como se espera y que el Sistema sea estable.

Para respaldar lo anterior el proveedor de desarrollo de software debe brindar dichas garantías y la salida a producción no debe afectar el buen funcionamiento de las operaciones.

6.8.6 Gestión de la vulnerabilidad técnica

La Cámara de Comercio Aburrá Sur debe estar al tanto de los cambios que surjan de los softwares instalados.

Esto se refiere a actualizaciones de versiones, parches críticos, renovación de contratos de soporte, y todo ello es para minimizar las vulnerabilidades.

El Departamento TIC debe tener control del vencimiento de licencias de soporte o uso de los diferentes software o recursos tecnológicos, en especial de los encargados de Backup, firewall, certificados de seguridad, al igual que de las demás renovaciones para el vital funcionamiento, y estar al día con todas actualizaciones vigentes,

Lo anterior es con el fin de estar protegido, ofrecer servicio sin interrupciones y brindar seguridad al tener las últimas actualizaciones ofrecidas por el fabricante.

En el procedimiento Gestión de Activos Tecnológicos, se hace alusión al documento Control de Licenciamiento, en el cual se define la vigencia, proveedor y demás características relevantes para tener definidos los puntos críticos en el licenciamiento de software.

Los cambios realizados en los sistemas se deben realizar en un ambiente controlado de pruebas, para detener fallas y posibles interrupciones del servicio, con el fin de subsanar dichas alteraciones y poder dar salida a producción sin causar tropiezos.

Únicamente se autoriza la instalación de software que se encuentre soportado con su respectiva licencia y aprobado por el Departamento TIC.

No se permite descargar, instalar o utilizar programas de software no autorizadas.

Esta práctica, podría introducir serias vulnerabilidades de seguridad en las redes, sistemas e información de la Cámara, además de afectar el funcionamiento de su computador.

Los paquetes de software que permiten que el equipo sea manejado "a control remoto (por ejemplo, PCanywhere) y "Hacking tools" (por ejemplo, Sniffers de red y crackers de contraseñas) están explícitamente prohibidos en la Cámara, a menos que hayan sido expresamente autorizados previamente por la Presidencia Ejecutiva y aprobados por el jefe del Departamento TIC.

Solo está permitido el uso de programas de Control Remoto desde el Departamento de Sistemas hacia los computadores pertenecientes a la Cámara de Comercio Aburrá Sur y con el fin de brindar soporte a los usuarios.

Respecto a las licencias de software, la mayoría del software, a menos que esté específicamente identificado como "freeware" o "software de dominio público", sólo puede ser instalado y / o utilizarse si ha sido validado por el Departamento TIC.

Los paquetes de shareware o de prueba deben ser eliminados una vez haya expirado el período de prueba.

Algunos programas de software son sólo para uso libre de los particulares, mientras que el uso comercial o empresarial requiere un pago de licencia.

El Departamento de TIC determinará la conveniencia o no de la instalación de un determinado software en un computador.

Los empleados que requieran la instalación de software que no sea propiedad de la Cámara deberán justificar su uso y solicitar su autorización al Jefe del Departamento TIC, indicando el equipo de cómputo donde se instalará el software, el propósito y el período de tiempo que permanecerá dicha instalación, además de respaldar el mencionado software con la respectiva licencia de legalidad.

Las licencias deben ser custodiadas y controladas por el Departamento de TIC. 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.

Se considera una falta grave que los empleados instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Cámara, que no esté autorizado por el Jefe del área respectiva y el Jefe del Departamento TIC.

6.8.7 Consideraciones de las Auditorias de los Sistemas de Información

El Comité se Seguridad de la Información debe delegar con anticipación el personal encargado de la realización de las Auditorias al Sistema de Gestión de Seguridad de la Información, con el fin de definir los requisitos y actividades que involucran las verificaciones a los diferentes sistemas operacionales, y así evitar interrupciones en el servicio.

6.9 Política de Seguridad en las Comunicaciones

Las comunicaciones requeridas o asociadas al cumplimiento de la misión de Cámara de Comercio de Aburrá Sur se deben realizar por medio de los dispositivos dispuestos por la entidad y en el marco de las funciones laborales de cada área.

Es por ello que la información que viaja a través de las redes es protegida por medio de mecanismos que controlan, limitan, cifran o monitorean la información a través de éstas.

Así mismo cualquier conexión con terceros deberá realizarse usando protocolos seguros y contar con acuerdos de confidencialidad para su uso.

Se deben garantizar los parámetros requeridos para una conexión segura con los servicios de red, restringiendo el acceso a los servicios o aplicaciones de red cuando sea necesario.

Igualmente se debe garantizar en los dispositivos de firewall de las sedes y sucursales, que tengan las mismas configuraciones de seguridad del firewall principal.

6.9.1 Gestión de la Seguridad en las Redes

Los empleados no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Cámara sin la autorización del Jefe Departamento TIC.

Todos los computadores que contengan información sensible o crítica deben estar conectados a la red institucional, y disponer de controles de acceso aprobados por el Departamento TIC.

Será considerado como un ataque a la Seguridad de la Información y una falta grave contra la Cámara cualquier actividad no autorizada por el Departamento TIC en la que los empleados realicen la exploración de los recursos informáticos en la red de la Cámara, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el Jefe Departamento TIC.

La Cámara de Comercio debe segmentar la red de acuerdo a los grupos de servicios y usuarios para de esa manera separar y evitar la difusión de Broadcast y no permitir el acceso a nivel de red de personas no autorizadas a los grupos que no les corresponde.

Todos los cambios a la red interna deben ser realizados por el Departamento TIC.

Este procedimiento reduce el riesgo de divulgación no autorizada y que los cambios realizados sean hechos de manera pertinente y con el conocimiento y aprobación del Jefe Departamento TIC.

Este proceso aplica no sólo al personal de la Cámara, sino también a los proveedores de servicios o personal externo.

En cuanto a las redes de video vigilancia, se debe garantizar su aseguramiento tecnológico (Hardening, análisis de vulnerabilidades, firewall, segmento separado de red).

Todo lo anterior basado en acuerdos de confidencialidad y transferencia para la protección y no divulgación de la información.

6.9.2 Intercambio de información con partes externas

Se dispone de un procedimiento que en detalle define como se realiza el paso a paso para el intercambio de información con terceros, este documento lo encuentra como Procedimiento Transferencia de información con terceros.

Los empleados no deben establecer conexiones a redes externas sin la aprobación del Jefe Departamento TIC.

La Cámara ofrece un correo electrónico y servicios de mensajería electrónica para facilitar la ejecución de sus actividades.

El intercambio de correos debe utilizar los buzones institucionales. Está prohibido tramitar información institucional a través de e-mails privados o de uso personal (Yahoo, Gmail, Hotmail, etc.).

La firma al pie de página de los emails establecida para los emails deberá informar: El nombre del Colaborador, el cargo, el nombre de la institución, el teléfono y extensión.

El tamaño y tipo de fuente utilizada para la misma se deberá ajustar al Manual de Imagen institucional.

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.

Los empleados no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.

Si fuera necesario leer el correo de alguien más (mientras un empleado se encuentre fuera o de vacaciones) el jefe de la respectiva área determinará a qué buzón deben ser redireccionados sus correos en su ausencia. Esta solicitud se debe realizar a través de ticket.

Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos que reciba a través del correo institucional como información de propiedad de la Cámara.

La asignación de una cuenta de correo electrónico de un dominio no institucional externo deberá solicitarse a través de un ticket al Departamento TIC, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Jefe Inmediato.

Está prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

La Cámara de Comercio Aburrá Sur debe establecer los acuerdos de confidencialidad en las relaciones contractuales con terceros y con el personal interno.

6.10 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

Se deben tener en cuenta requerimientos de seguridad durante todo el ciclo de vida de los sistemas de información que adquiera o diseñe la entidad. Esto incluye la compra, el desarrollo, el mantenimiento y la dada de baja.

Deben considerarse elementos como análisis de riesgos de seguridad, protección de información en tránsito, lineamientos de desarrollo seguro, ambientes y datos de prueba, pruebas de seguridad, revisión de código, gestión de usuarios, entre otros.

Para mayor información debe consultarse el **Procedimiento Desarrollo y Mantenimiento de los Sistemas.**

En los procesos de desarrollo y soporte de sistemas se deben tener en cuenta el control de cambios, revisión técnica, restricciones, ambientes, desarrollo externo, y todas las pruebas y seguridad necesarias antes de la salida a producción.

Así mismo, la información confidencial personal cliente debe estar protegida en los ambientes no productivos de la organización.

6.10.1 Requisitos de seguridad de los sistemas de información

El desarrollo o mantenimiento de software por parte del personal interno o externo debe tener la aprobación del Jefe Departamento TIC, y de ser aprobado, debe ceñirse a las políticas, estándares, procedimientos y convenciones establecidas por el Departamento TIC.

Las convenciones o políticas incluyen pruebas, entrenamiento y documentación, para más información consultar el Procedimiento Desarrollo y Mantenimiento de Sistemas.

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

Además de ello se deben registrar los eventos de seguridad como intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

Las conexiones hacia internet para el consumo de algún servicio ofrecido por tercero, debe ser protegida para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

6.10.2 Seguridad en los procesos de desarrollo y soporte

La Cámara de Comercio debe controlar estrictamente los ambientes de desarrollo y soporte

Se debe garantiza para todo Sistema de información en desarrollo de un ambiente de desarrollo y un 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.

Luego de ello, se debe crear un plan de trabajo para la migración del ambiente de pruebas a la nueva versión, para mayor información consulte el Procedimiento Gestión de Cambios.

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.

Se debe hacer seguimiento a las actividades propuestas para el nuevo desarrollo y garantizar que el Área involucrada esté al tanto de su ejecución, por lo cual, se deben exigir informes de avances del proyecto.

Se deben realizar pruebas de los requisitos funcionales pruebas de aceptación y pruebas de seguridad durante el desarrollo.

6.10.3. Datos de prueba

Para el ambiente de Desarrollo se deben garantizar que los datos utilizados no sean divulgados hacia terceros y se les debe proteger su integridad, disponibilidad.

6.11 Política de Seguridad en la Relación con Proveedores

Los proveedores de la Cámara de Comercio Aburrá Sur deben dar cumplimiento a las Políticas de Seguridad definidas por la entidad y por la normatividad vigente en el ámbito del servicio prestado y la cadena de suministro.

Para esto se deben establecer mecanismos de seguridad para la gestión, seguimiento y revisión de los servicios contratados, que permitan proteger la información de la entidad a la que tienen acceso los proveedores manteniendo la confidencialidad y la integridad de la misma.

Lo anterior debe quedar establecido en el marco contractual y exigencias definidas entre las partes en el **Procedimiento Selección, Evaluación y Reevaluación de Proveedores**.

6.11.1 Seguridad de la información en las relaciones con proveedores

La Cámara de Comercio Aburrá Sur deberá firmar Acuerdos de Confidencialidad con sus Proveedores estipulando con claridad que la información suministrada no podrá ser trasferida a terceros, ni alterada, ni podrá usarse para beneficio propio.

Estos Acuerdos de Confidencialidad deben ser tan robustos de acuerdo con la prestación del servicio.

Se deben tener definidos los Riesgos de Seguridad de la Información asociados al servicio ofrecido por el proveedor.

Para el caso de los proveedores que requieran acceder remotamente para extraer información o solo para visualizar.

Se debe garantizar el acceso seguro, evitando la fuga o alteración de la información, y realizar inventarios y auditoria de las conexiones y accesos que estén habilitados a los proveedores.

Lo anterior, con el fin controlar y evitar conexiones innecesarias o habilitadas a proveedores que en el momento no estén prestando servicio.

6.11.2 Gestión de la Prestación del Servicio por Suministradores

Se debe realizar supervisión y revisión a la ejecución de las actividades de los proveedores, a través de informes de seguimiento o de acuerdo a lo estipulado contractualmente si es el caso.

6.12 Política de Gestión de Incidentes de Seguridad

Cualquier incumplimiento a las Políticas de Seguridad o de la normatividad aplicable a la entidad es constituido como un Incidente de Seguridad y es considerado como una falta a los lineamientos que podrá ser sancionada a discreción de Cámara de Comercio de Aburrá Sur.

Todos los terceros, funcionarios y especialmente los administradores y áreas de control deben realizar el reporte de las debilidades, eventos e incidentes de seguridad de la información que hayan sido identificados, para que cada caso sea priorizado y gestionado siguiendo lo definido en el **Procedimiento de Gestión de Incidentes de Seguridad** de la Información de la compañía.

En la gestión de incidentes se determinan responsabilidades y procedimientos que incluyen el reporte, análisis, evaluación, respuesta, recolección de evidencias, lecciones aprendidas y mejora continua frente a los incidentes presentados y tratados.

6.12.1 Gestión de Incidentes de Seguridad de la Información y Mejoras

Cualquier incidente generado durante la utilización u operación de información de la Cámara de Comercio Aburrá Sur debe ser reportado a través de un ticket.

Los empleados de la Cámara con acceso a Internet tienen que reportar todos los Incidentes de Seguridad de la Información al personal encargado, inmediatamente después de su identificación.

En el procedimiento Gestión de Incidente de Seguridad de la Información, están las definiciones, priorización de los eventos y descripción de las actividades a ejecutar para la gestión de incidentes.

Se debe garantizar la generación de reportes de los incidentes que se han detectado.

Siempre se deberá utilizar el conocimiento del resultado del análisis y la resolución de Incidentes de Seguridad de la Información, con el fin de disminuir la probabilidad de ocurrencia de los mismos.

6.13 Política de seguridad de la Información en Continuidad del Negocio

La Cámara de Comercio Aburrá Sur, a través de todas sus áreas, debe contar con los Planes de Contingencia y Continuidad del Negocio que consideren para la ejecución y el cumplimiento de las Políticas de Seguridad de la entidad y las regulaciones aplicables.

De esta manera se debe garantizar la Seguridad de la Información en ambientes tanto productivos como de contingencia, durante el tiempo de permanencia, incluyendo el retorno a la normalidad.

Todos los aspectos anteriores se deben adelantar con base en la planificación, implementación y revisión del Plan de Continuidad, el cual debe incluir aspectos de redundancia a nivel operativo y tecnológico. Dicha descripción está definida en el **Manual DRP** de la compañía.

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 deben crear planes de respuesta a emergencias, 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.

6.14 Política de Cumplimiento

Todas las áreas y terceros de Cámara de Comercio de Aburrá Sur deben cumplir con las presentes políticas y con las obligaciones legales, estatutarias, de reglamentación o contractuales que apliquen a la entidad en cuanto a la Seguridad de la Información.

De esta manera las áreas de control internas o contratadas por la entidad podrán verificar en cualquier momento o de manera periódica el cumplimiento de normatividad o regulaciones aplicables en términos operacionales, funcionales, y técnicos.

6.14.1 Cumplimiento de los Requisitos Legales y Contractuales

La política de cumplimiento incluye derechos de propiedad intelectual, protección de registros, privacidad y protección de información de datos personales, y controles criptográficos, que se deben proteger mediante el cumplimiento de los respectivos controles.

Para ello se dispone de la Matriz de Cumplimiento, donde se encuentra toda la normativa que rige nuestra entidad.

Está prohibido por las leyes de derechos de autor y por la Cámara realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Cámara.

Los sistemas desarrollados por el personal interno o externo que controle el Departamento TIC son propiedad intelectual de la Cámara.

La Cámara tiene propiedad y derechos exclusivos sobre las patentes, derechos de autor, invenciones, programas o cualquier otra propiedad intelectual desarrollada por sus empleados en la plataforma tecnológica de la entidad.

Para lo concerniente a la Protección de Datos y Privacidad de la Información Personal, la Cámara dispone del documento, **Manual de Políticas y Procedimientos de Protección de Datos Personales**

6.14.2 Revisiones de la seguridad de la información

El Departamento TIC y el Coordinador de Control Interno de la Cámara realizarán periódicamente Auditorías de Seguridad para garantizar el cumplimiento de las políticas aplicables, los procedimientos y la legislación.

El Comité de Seguridad de la Información tiene como una de sus funciones proponer y revisar el cumplimiento de las normas y políticas de seguridad que garanticen acciones preventivas y correctivas para la salvaguarda de los equipos e instalaciones de cómputo, así como de los bancos de datos de información automatizada en general.

El Departamento TIC y el Coordinador de Control Interno realizarán acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad de la Información de acuerdo con lo establecido en su Plan Anual de Trabajo.

Todos los empleados deben cumplir con las Políticas de Seguridad de la Información y sus documentos relacionados.

Los empleados que por negligencia violen estas normas serán objeto de sanciones disciplinarias o despido. Ver procedimiento de Gestión del Recursos Humanos.

El Departamento TIC y el Coordinador de Control Interno podrán implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, con el fin de revisar la actividad de los procesos que ejecuta y la estructura de los archivos que se procesan.

Todas las Políticas de Seguridad de la Información deben cumplir con la legislación aplicable, como las leyes de protección de datos, acceso a la información, protección de información personal y documentos electrónicos.

Las violaciones sospechosas de la Política de Seguridad de la Información (penetración del sistema, infección de virus) que podrían comprometer la integridad de los sistemas de información deben ser reportadas oportunamente al Jefe Inmediato y al Departamento TIC.

La violación comprobada o el incumplimiento de la Política de Seguridad de la Información suponen graves consecuencias para los infractores y medidas disciplinarias que varían de acuerdo con la severidad de la violación y puede ocasionar el despido del infractor.

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.

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 ésta para su respectiva divulgación.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización.

El desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

7. ACTUALIZACION Y MANTENIMIENTO

Esta Política de Seguridad de la Información deberá seguir un proceso de actualización y mantenimiento periódico, mínimo una (1) vez cada año, sujeto a los cambios organizacionales relevantes: Crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, cambio en los procesos, productos, estructura organizacional, entre otros.

El documento que contiene la Política de Seguridad de la Información deber ser difundido a todo el personal involucrado en la definición de estas políticas.

8. 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 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 (1) 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 deberán 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.

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 (2) personas deberán tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de la Cámara de Comercio.

Personal competente en el área de Sistemas para dar pronta solución a problemas.

Con el fin de garantizar la continuidad de los sistemas de información, la Cámara de Comercio deberá 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 deberá procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

9. REVISIÓN DE LA GERENCIA

La alta dirección de la Cámara de Comercio Aburrá Sur revisará el SGSI a intervalos planificados, como mínimo cada año, y cuando se produzcan cambios significativos para asegurar su conveniencia, adecuación y eficacia.

Como insumo para la revisión de la gerencia al SGSI, se tendrán en cuenta los siguientes aspectos:

a) El estado de acciones de las revisiones previas de la gerencia.

b) Cambios relevantes externos e internos que puedan afectar el SGSI

c) Información sobre el desempeño del SGSI, incluyendo tendencias en:

1. No conformidad y acciones correctivas

2. Resultados de la evaluación de medición y monitoreo

3. Resultados de auditorias

d) Oportunidades para el mejoramiento continuo

Igualmente, las revisiones por la dirección deben considerar el desempeño de la organización, incluyendo:

- Actualización de los resultados de acciones de revisiones previas por la gerencia.
- Las necesidades de cambios del SGSI, incluyendo la política y los objetivos.
- Oportunidades de mejoramiento
- Resultados de auditorías y revisiones del SGSI
- Técnicas, productos o procedimientos, los cuales puedan ser utilizados por la organización para el mejoramiento del desempeño y efectividad del SGSI.
- El estado de las acciones correctivas
- Resultados de ejercicios y pruebas
- Riesgos y problemas que no hayan sido adecuadamente direccionados en los análisis de riesgos previos.
- Cualquier cambio interno o externo que pueda afectar el alcance del SGSI.

- Adecuación de la política
- Recomendaciones de mejoramiento
- Lecciones aprendidas y acciones surgidas de incidentes de interrupción, y
- Nuevas buenas prácticas y guías.

10. MEJORAMIENTO CONTINUO

La Cámara de Comercio Aburrá Sur está comprometida en mejorar continuamente su Sistema de Gestión de Seguridad de la Información a través de los siguientes mecanismos:

a. Resultados de las pruebas de vulnerabilidades realizadas
b. Resultados de auditorías
c. Resultados de las revisiones por la gerencia.
d. Revisiones de la documentación
e. Acciones correctivas y preventivas
f. Lecciones aprendidas de interrupciones de los procesos del negocio
g. Capacitación, entrenamiento y sensibilización.

11. CAPACITACIÓN Y SENSIBILIZACIÓN

La Cámara de Comercio Aburrá Sur ha determinado unos principios y lineamientos frente a la capacitación y sensibilización de la política de seguridad de información:

1. Realizar la inducción en los aspectos de seguridad de la información a nuevos funcionarios, incluidas las Políticas de Seguridad de la Información.

2. Realizar capacitación y sensibilización frente a las políticas de seguridad de la información de manera periódica y por lo menos una vez al año para todos los funcionarios.

Los procesos de capacitación y sensibilización incluyen diferentes mecanismos y medios como correo electrónico, periódico semanal, charlas, boletines, fondos de escritorio, entro otros mecanismos de divulgación.

Todos los aspectos de capacitación y sensibilización incluyen adicional a la Política de Seguridad de la Información aspectos de continuidad, su conocimiento y gestión.

12. AUDITORÍAS INTERNAS

Las auditorías internas hacen parte del proceso de mantenimiento y revisión del SGSI.

Es proceso asegura que La Cámara de Comercio Aburrá Sur tenga un programa efectivo de Continuidad de Negocio y tiene las siguientes funciones:

- Establecer la conformidad de los requerimientos de la Cámara de Comercio Aburrá Sur en relación con el SGSI y los requerimientos del estándar ISO 27001:2013

- Asegurar que el SGSI es efectivamente implementado y mantenido.

La auditoría debe ser ejecutada por personal idóneo y competente que sea designado formalmente por la organización para asegurar la aplicabilidad y eficacia del SGSI.

A partir de las evidencias recogidas, luego de realizada la auditoría, debe hacerse seguimiento a los cambios o planes de acción resultantes, mediante control de cambios y actualización.

Para dar cumplimiento a lo anterior se deberán seguir los pasos del **Procedimiento Auditoría Interna de Calidad, SST, SGSI.**

13. CONTROL DE CAMBIOS

ELABORO	REVISO	APROBO
CARGO JEFE DEPARTAMENTO TIC	CARGO JEFE DEPARTAMENTO TIC	CARGO PRESIDENTE EJECUTIVO
NOMBRE ALVARO L. GUERRA Z.	NOMBRE ALVARO L. GUERRA Z.	NOMBRE LILLYAM MESA ARANGO
FIRMA Alvaro Leon Guerra Z.	FIRMA Alvaro Leon Guerra Z.	FIRMA
FECHA – 2019/04/03	FECHA – 2019/04/03	FECHA 2019/04/03