CAMARA DE COMERCIO DE IPIALES Forjando el presente y futuro de nuestra región	**POLÍTICA DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN.**

CONTENIDO

CAMARA DE COMERCIO DE IPIALES Forjando el presente y futuro de nuestra región	**POLÍTICA DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN.**

INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de la CÁMARA DE COMERCIO DE IPIALES. 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.

Cada día nos enfrentamos a nuevas modalidades y técnicas de ataques informáticos que acceden, sin el consentimiento del propietario a todo activo de información, no obstante, es importante reconocer que también hay acciones preventivas y correctivas que contrarrestan este hecho; lo más importante es conocerlos y aplicarlos en el momento adecuado.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad informática y 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 informática y de la Información.

Estos lineamientos están escritos en forma de políticas.

1.2. OBJETIVOS ESPECÍFICOS

Promover el uso de las mejores prácticas de seguridad informática en el área de trabajo.

- Implementar los mecanismos de seguridad informática de modo que propicie la Confidencialidad, integridad y disponibilidad de la información.
- Guiar el comportamiento profesional y personal de los funcionarios de la Cámara de Comercio de Ipiales, en procura de minimizar los incidentes de seguridad internos.
- Implementar prácticas de seguridad que permitan la correcta custodia de los datos y equipos administrados por los líderes de cada departamento en la Cámara de Comercio de Ipiales.

2. ALCANCE

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la Cámara de Comercio, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad 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.
  - 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.

3. CONCEPTOS GENERALES

3.1. ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La información es un activo importante, tiene valor para la organización y por lo tanto requiere una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la empresa y maximizar el uso de los recursos informáticos.

La información en sus diversas formas, presentaciones y divulgaciones debería ser protegida adecuadamente a partir del momento que se crea, almacene y comparta.

La seguridad de la información se caracteriza aquí como la preservación de:

a) Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.
b) Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
c) Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

3.2. ¿PORQUÉ ES NECESARIA LA SEGURIDAD DE INFORMACIÓN?

La información, los procesos que la apoyan, los sistemas y redes son completamente indispensables. La disponibilidad, integridad y confidencialidad son esenciales para mantener su competitividad, rentabilidad y cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Para la Cámara de Comercio de Ipiles es importante implementar la seguridad de la información con el fin de mantener su integridad brindando un servicio confiable, a todos los clientes que requieren una solución acorde a sus necesidades.

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia de seguridad de la información, la Cámara de Comercio debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Cámaras de Comercio o entidades que las regulan y aglutinan.

5. DEFINICIONES

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

- ✓ Activo: Cualquier bien que tenga valor para la organización.
- ✓ Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de La Cámara de Comercio.
- ✓ Administradores: Usuarios a quienes la Cámara de Comercio ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la Cámara de Comercio.
- ✓ 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 del negocio y amenazar la seguridad de la información.

- ✓ Información confidencial (Reservada): Información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.
- ✓ Información confidencial (Confidencial): Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.
- ✓ Información privada (Uso interno): Información generada por La Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.
- ✓ Información pública: Es la información administrada por La Cámara de Comercio en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo, la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.
- ✓ LAN: Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio ó una oficina).
- ✓ Licencia de Software: Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación. 1
- ✓ Copyright: Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. 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. 2
- ✓ Open Source (Fuente Abierta): Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.
- ✓ Software Libre: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.

- ✓ Software pirata: Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
- ✓ Software de Dominio Público: Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- ✓ Freeware: Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- ✓ Shareware: Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico.
- ✓ 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, ó 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 ó 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.
- ✓ 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.

1 Tomado del diccionario Wikipedia. http://es.wikipedia.org/wiki/Licencia_de_software
2 Tomado de http://www.derautor.gov.co/htm/preguntas.htm#01

6. ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA

DIRECCION
Autoridad de nivel superior que integra el comité de seguridad. Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad en concordancia con las autoridades de nivel superior.

COORDINADOR DE SISTEMAS
Persona dotada de conciencia técnica, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control con la ayuda de la unidad de informática referente a los servicios prestados y niveles de seguridad aceptados para tales servicios.

UNIDAD DE SISTEMAS Entidad o Departamento dentro de la Corporación, que vela por todo lo relacionado con la utilización de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

RESPONSABLE DE ACTIVOS
Personal dentro de los diferentes departamentos administrativos de la Corporación, que velan por la seguridad y correcto funcionamiento de los activos informáticos, así como

de la información procesada en éstos, dentro de sus respectivas áreas o niveles de mando. (Líderes de Procesos)

7. RESPONSABLES

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

7.2. 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.

8. PROCEDIMIENTO

- ✓ Comunicación de las políticas de seguridad: Conscientes que los recursos de información son utilizados de manera permanente por los usuarios que acceden a diferentes servicios, definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.
- ✓ Aplicación de las políticas de seguridad: Las políticas de seguridad informática se orientan a reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

8.1. POLÍTICA DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN CÁMARA DE COMERCIO.

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

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

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

8.2. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

8.2.1. CUMPLIMIENTO CON LA SEGURIDAD DE LA INFORMACIÓN

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

8.2.2. 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.

8.3. POLÍTICA PARA VINCULACIÓN DE FUNCIONARIOS

La Cámara de Comercio de Ipiales, tiene a consideración los recursos humanos para el cumplimiento de sus objetivos. Con el fin de contar con el personal idóneo, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

8.3.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO RELACIONADAS CON LA VINCULACIÓN DE FUNCIONARIOS

- El área de Gestión Humana debe certificar que los funcionarios de la empresa firmen una Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad informática y de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.
- El funcionario provisto por terceras partes, deben garantizar el cumplimiento de la Cláusula de Confidencialidad y aceptación de las Políticas de Seguridad informática y de la Información.

8.4. POLÍTICA QUE CONTEMPLA LICENCIAS, DESVINCULACIÓN, ACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS

La Cámara de Comercio de Ipiales debe asegurar de forma controlada y segura la desvinculación o reasignación del personal para la ejecución de nuevas labores.

8.4.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA LA DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIOS DE LABORES DE LOS FUNCIONARIOS

El área de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la empresa llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

- El área de Talento Humano debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios al área Tecnológica.
- El área Tecnológica debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

8.5. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

8.5.1. INSTRUCCIONES PARA EL USO DE RECURSOS INFORMÁTICOS.

El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de la Cámara de Comercio, debe someterse a todas las instrucciones técnicas, que imparta el área de sistemas como veedor de la seguridad y correcto funcionamiento de los activos informáticos.

8.5.2. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA EL ACCESO Y SEGURIDAD DE LAS ÁREAS FÍSICAS DONDE SE ENCUENTREN RECURSOS INFORMÁTICOS

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios que pertenecen al Área Tecnológica. Los visitantes siempre deberán estar acompañados de un funcionario de dicha área durante su visita al centro de cómputo o a los centros de cableado.
- El área Tecnológica debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; como sensores de humo extractores de calor, un pararrayos.
- Los funcionarios deben portar el carné en un lugar visible mientras se encuentren en las instalaciones de la empresa; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Los funcionarios de la Cámara de Comercio de Ipiales y aquellos que tengan a cargo terceras partes no deben ingresar a ubicaciones a las cuales no tengan autorización.
- El área tecnológica debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo
- Ningún equipo electrónico podrá salir de las instalaciones de La Cámara de Comercio sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

8.6. POLÍTICA PARA LA RESPONSABILIDAD DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de la Cámara de Comercio de Ipiales realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

8.6.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA LA RESPONSABILIDAD DE ACCESO DE LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Cámara de Comercio de Ipiales deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes a menos que haya una justificación que lo amerite; dado el caso se realizará un análisis de esta causa con el superior directo, el área de Control Interno y el área Tecnológica.

8.7. POLÍTICA DEL USO 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.

8.7.1 INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DEL USO DE LOS RECURSOS

- Para el uso de los recursos tecnológicos de La Cámara de Comercio, todo usuario debe firmar un acuerdo de confidencialidad 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.
- El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.
- 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.
- 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.
- Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.
- Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.
- Notificación de sospecha de pérdida, divulgación o uso indebido de información.
- Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del área tecnológica.
- Traslado de equipos debe estar autorizado.
- Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de La Cámara de Comercio sin previa autorización. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de tecnología autorizado.
- Control de recursos informáticos entregados a los usuarios.

- Cuando un usuario inicie su relación laboral con La Cámara de Comercio se debe diligenciar el documento de 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.
- Solamente los funcionarios del área tecnológica están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.
- 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.
- Las licencias deben ser custodiadas y controladas por el área de tecnología. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por el jefe de cada área.
- 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.

8.8. POLITICA DE USO DEL CORREO ELECTRÓNICO

La Cámara de Comercio de Ipiales, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

8.8.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE USO DEL CORREO ELECTRÓNICO

- El área Tecnológica debe proporcionar las cuentas de correo electrónico.
- que pudiera ser transmitido a través de los mensajes.
- El área de Gestión Tecnológica debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la empresa, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya a menos que haya una justificación que lo amerite.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Cámara de Comercio de Ipiales. El correo institucional no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Cámara de Comercio de Ipiales y cada usuario, como responsable de su buzón, debe
- mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido la remisión de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la empresa.
- No se permite el envío de archivos que contengan extensiones ejecutables.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Cámara de Comercio de Ipiales y deben conservar en todos los casos el mensaje legal corporativo.
- 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.

8.9. POLÍTICA DE USO ADECUADO DE INTERNET

La Cámara de Comercio de Ipiales consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la empresa.

8.9.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE USO ADECUADO DE INTERNET

- El área Tecnológica debe proporcionar los recursos necesarios para la
- implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El área Tecnológica debe monitorear continuamente el canal o canales del
- servicio de Internet.
- El área Tecnológica debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- Los usuarios del servicio de Internet de la Cámara de Comercio de Ipiales deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este manual.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y El área de Gestión Tecnológica, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de la Cámara de Comercio de Ipiales, de sus clientes y/o de sus funcionarios, con terceros.
- 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

8.10. POLÍTICA SOBRE POLÍTICA EDITORIAL Y DE ACTUALIZACIÓN DE LA INFORMACIÓN EN LA PÁGINA WEB

La información publicada en la página web de la empresa debe ser actualizada permanentemente y además será objetiva, clara, imparcial, sin emisión de juicios de valor, veraz, institucional, accesible y confiable para la consulta tanto de los usuarios internos como externos de la empresa.

La información publicada en la página web de la empresa deberá mantener un formato y un estilo constante, con fuentes de información claramente definidas y confiables que serán presentadas en concordancia con la plataforma estratégica de la empresa y las políticas de comunicación y seguridad informática.

8.10.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO SOBRE POLÍTICA EDITORIAL Y DE ACTUALIZACIÓN DE LA INFORMACIÓN EN LA PÁGINA WEB

- La información publicada en la página web de la empresa será entregada por cada una de las dependencias responsables de los procesos generadores de la misma, con revisión y aprobación del jefe o líder del proceso.
- El administrador de la Página Web de la empresa será el responsable y compartirá las funciones de actualización de los datos y contenidos de las diversas secciones de la página, junto con el responsable de su edición. Dicha actualización se realizará simultáneamente al proceso de publicación, cuando sea necesaria o se presente alguna novedad.
- La Página Web de la empresa podrá contar con enlaces hacia otros sitios Web, cuando se considere que estos son útiles y de relevancia bien sea para comunidad en general o para el personal del sector cameral. Una vez que el usuario acceda a otro portal a través de un link almacenado en la página web de Cámara de Comercio de Ipiales, estará sujeto a la política de privacidad y a la política editorial del portal nuevo.
- Los derechos de propiedad intelectual de cualquier material presentado en la Página Web de la empresa, incluyendo textos, fotografías, otras imágenes, sonidos y otros, son de propiedad de sus autores, incluyendo a la Cámara de Comercio de Ipiales, así se reservan todos los derechos de propiedad intelectual sobre los contenidos de su autoría y sobre las que sean cedidas.

8.11. POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Cámara de Comercio de Ipiales a través de la Oficina de Control Interno, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la Cámara de Comercio de Ipiales, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la Cámara de Comercio de Ipiales, hayan suministrado datos personales. Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la Cámara de Comercio de Ipiales conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la empresa y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

8.11.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el

tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la empresa.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las empresas vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.
- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identificación de la empresa de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico, por correo certificado, entre otros.

8.12. PÓLITICA PARA USO DE TERMINALES MÓVILES

La Cámara de Comercio de Ipiales suministrará las condiciones para el manejo de los dispositivos móviles institucionales y personales que hagan uso de los servicios de la empresa.

8.12.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA USO DE DISPOSITIVOS MÓVILES

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

8.13. POLÍTICA PARA CONEXIONES REMOTAS

La Cámara de Comercio de Ipiales establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la empresa; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

8.13.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO PARA USO DE CONEXIONES REMOTAS

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Cámara de Comercio de Ipiales y deben acatar las condiciones de uso establecidas para dichas conexiones.
- El área Tecnológica debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Cámara de Comercio de Ipiales.
- El área Tecnológica debe implantar los métodos y controles de seguridad para establecer conexiones

8.14. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

La Cámara de Comercio de Ipiales velará porque la información de la empresa, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

8.14.1. CUMPLIMIENTO DE CONTROLES CRIPTOGRÁFICOS

- El área Tecnológica debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- El área Tecnológica debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

8.15. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

- La Cámara de Comercio de Ipiales proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

8.15.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

- El área de Tecnológica debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Cámara de Comercio de Ipiales y los servicios que se ejecutan en la misma.
- El área Tecnológica debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- El área Tecnológica debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- El área Tecnológica, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- El área de Tecnológica, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por El área Tecnológica; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área Tecnológica para tomar medidas de control pertinentes.

8.16. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La Cámara de Comercio de Ipiales autenticará la generación de copias de respaldo y almacenamiento de su información importante, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo del área Tecnológica, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

8.16.1. INSTRUCCIONES DE OBLIGATORIO CUMPLIMIENTO DE COPIAS DE RESPALDO DE LA INFORMACIÓN

- El área Tecnológica, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad, según procedimiento de copias de seguridad.
- El área Tecnológica debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- El área Tecnológica, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- El área Tecnológica debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- Es responsabilidad de los funcionarios de la Cámara de Comercio de Ipiales identificar la información crítica que debe ser respaldada y almacenada, para que el área de sistemas realice los Backups correspondientes.

8.17. POLÍTICAS DE USO DE LAS CONTRASEÑAS

8.17.1. CONFIDENCIALIDAD DE LAS CONTRASEÑAS.

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

8.17.2. IDENTIFICACIÓN ÚNICA PARA CADA USUARIO.

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

8.17.3. CAMBIOS PERIÓDICOS DE CONTRASEÑAS.

Se establece como política de seguridad de la entidad que todos los funcionarios que manejen usuarios y contraseñas en cualquier aplicativo, deben realizar cambio de contraseña por lo menos cada 30 días.

8.17.4. LONGITUD MÍNIMA DE CONTRASEÑAS.

Todas las contraseñas deben tener una longitud mínima de SEIS (6) caracteres se recomienda que tengan las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales.

8.17.5. ALMACENAMIENTO DE CONTRASEÑAS.

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

8.17.6. SOSPECHAS DE COMPROMISO DEBEN FORZAR CAMBIOS DE CONTRASEÑA.

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

8.17.7. REVELACIÓN DE CONTRASEÑAS PROHIBIDA.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.

8.17.8. 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.

8.18. POLÍTICAS DE USO DE FIREWALL

8.18.1. DETECCIÓN DE INTRUSOS.

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

8.18.2. TODA CONEXIÓN EXTERNA DEBE ESTAR PROTEGIDA POR EL FIREWALL.

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

8.18.3. TODA CONEXIÓN HACIA INTERNET DEBE PASAR POR EL FIREWALL.

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

8.18.4. FIREWALL DEBE CORRER SOBRE UN COMPUTADOR DEDICADO O APPLIANCE.

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

9. FUNCIONAMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS

La Empresa debe contar con un plan de contingencia que permita dar continuidad al funcionamiento de sus sistemas de información y a sus recursos informáticos, garantizando su disponibilidad en el evento de una emergencia o desastre como terremoto, erupción volcánica, terrorismo, inundación, robo etc. Este plan de contingencia deberá socializarse en toda la empresa, deberá actualizarse y probarse periódicamente para que se aplique en el evento en que se ponga en riesgo la continuidad de los sistemas de información o el funcionamiento de los recursos informáticos.

10. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN

Las Políticas de Seguridad informática y de la Información pretenden instaurar y consolidar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de la Cámara de Comercio de Ipiales. Por tal razón, es necesario que los desacatos a las Políticas Seguridad informática y de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad informática y de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo a las circunstancias.

11. 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 área tecnológica, siempre con el concurso de la Presidencia o de quién él delegue esta función.

Este documento se debe revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz. Una vez aprobado el documento ya sea por presidencia o quien el autorice, se procede a 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 informática y de seguridad de la información será mediante correo electrónico.

12. ANEXOS

ANEXO 1.

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

Firma: _____
Documento de identificación: _____
Empresa: _____
Área de La Cámara de Comercio: _____
_____
Vo. Bo. Recursos Humanos

ANEXO 2.

POLÍTICA DE ASUNTOS ESPECÍFICOS: IDENTIFICACIÓN BIOMÉTRICA

1. ALCANCE
El presente anexo al documento de política de seguridad informática y de la Información, reglamenta la protección y uso de los activos de información relacionados con la integración de los servicios de la Cámara de Comercio, Confecámaras y la Registraduría Nacional del estado civil, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la Entidad deberán diligenciar previamente un acuerdo de confidencialidad (Anexo 1),

que los compromete con el cumplimiento de las políticas de seguridad ya descritas. Los usuarios de los activos de se denominan así:
Funcionarios de La Cámara de Comercio: _____Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular el sistema de autenticación biométrica en línea.

2. PROCEDIMIENTO
Conscientes que los recursos de información son utilizados de manera permanente por los usuarios de la Cámara de Comercio que manipulan el servicio de identificación biométrica, definidos en este anexo, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

3. Medidas disciplinarias por incumplimiento de políticas de seguridad
Cualquier incumplimiento de una política de seguridad informática y 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.

4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

4.1 Instrucciones para el uso de recursos informáticos.

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

4.2 Uso personal de los recursos

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

4.3 Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos las Cámaras de Comercio, todo usuario debe firmar un acuerdo de confidencialidad (Anexo 1) y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware.

4.4 Traslado de equipos debe estar autorizado.

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones de la Cámaras de Comercio sin previa autorización. Así mismo, ningún equipo de cómputo asignado en el kit de identificación biométrica debe ser reubicado o trasladado de la instalación. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

5.1 Identificación única para cada usuario.
Cada usuario tendrá una identificación única en cada sistema al que tenga acceso (Usuario), acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.
Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. En caso del sistema de autenticación biométrica en línea, el acceso al sistema se realizará mediante un cotejo inicial entre el sistema biométrico y el sistema registral, los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de la Cámara de Comercio.