POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La virtualización de los servicios regístrales, la implementación del programa de gestión documental y la implementación de Sistema de Prevención de Fraudes (SIPREF), imponen la necesidad de adoptar estándares más elevados de seguridad de la información con el fin de minimizar los riesgos asociados a su custodia y administración.

Con el ánimo de mejorar la estrategia de Seguridad de la información de la Cámara de Comercio del Putumayo, 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 apropiado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

2. OBJETIVO

Definir los lineamientos que debe seguir la Cámara de Comercio del Putumayo para proteger de posibles riesgos de daño, pérdida y uso indebido de la información que reposa en la entidad formalizando el compromiso frente a la gestión de la seguridad de la información.

3. ALCANCE

La información proveniente de la función registral tiene la calidad de información pública, por lo tanto su custodia y administración requiere de la implementación de procedimientos y controles que eviten la manipulación indebida, sustracción no autorizada o adulteración de la misma. Así mismo, los expedientes deben ser conservados bajo estándares tecnológicos que al mismo tiempo respalden su integridad y disponibilidad. La implementación de SIPREF a su turno con la consulta de los datos biométricos a través de las bases de la Registraduría Nacional del Estado Civil ha exigido la adopción de la política de seguridad de la información para garantizar la inviolabilidad y el uso indebido de los datos biométricos de los usuarios.

La información proveniente de las demás funciones de la Cámara de Comercio del Putumayo, es administrada y conservada observando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información previamente clasificada, bajo autorización del titular de la misma para su tratamiento y de acuerdo a los lineamientos estipulados por gestión documental.

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de la Cámara de Comercio del Putumayo, y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios de los activos de información de la entidad deberán diligenciar un acuerdo de confidencialidad, que los

compromete con el cumplimiento de la política de seguridad aquí descrita. 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 del Putumayo: Se definen como los empleados de la Cámara de Comercio del Putumayo que son susceptibles de manipular sistemas de información.

- Contratistas: son aquellas personas que han suscrito un contrato de prestación de servicios con la Entidad.

- Entidades de Control Externos
  - ✓ Procuraduría
  - ✓ Unidad de pensiones y parafiscales
  - ✓ Archivo general de la nación
  - ✓ Contraloría General de la República
  - ✓ Superintendencia de Industria y Comercio

- Otras Entidades
  - ✓ DIAN
  - ✓ CONFECAMARAS
  - ✓ ASOCAMARAS

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Para la implementación de la estrategia de seguridad de la información, la Cámara de Comercio del Putumayo 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 del Putumayo.

Administradores: Usuarios a quienes la Cámara de Comercio del Putumayo 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.

Riesgo: 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.

Comité de Control Interno, Calidad y Riesgos: Equipo de trabajo conformado por el presidente ejecutivo, director jurídico y de registros públicos, director administrativo y financiero, directora de competitividad y productividad empresarial y coordinador de control interno calidad y riesgos; para el caso de ésta política, se podrá solicitar, en caso de ser necesario, la presencia del técnico de sistemas o los funcionarios que hagan sus veces y/o técnico en gestión documental.
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.

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.

Firewall: Software o hardware que protege los 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 ente y amenazar la seguridad de la información.

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

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

LAN: Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).

Licencia de Software: Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.

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

Propiedad Intelectual: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.

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

Política: Toda intención y directriz expresada formalmente por la dirección.

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.

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.

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 encriptación: Software que permite 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.

Tercera parte: Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

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

Usuarios de red y correo: Usuarios a los cuales La Cámara de Comercio del Putumayo 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 del Putumayo a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.

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

6. RESPONSABLE

6.1. COMPROMISO DE LA DIRECCIÓN

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

- Estableciendo objetivos y planes de seguridad de la información.
- Definiendo funciones y responsabilidades de la seguridad de la información.
- Comunicando a la Entidad la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidad de la mejora continua.
- Gestionando auditorías internas.

6.2. RECURSOS

La Cámara de Comercio del Putumayo, garantizará los recursos humanos, tecnológicos y financieros necesarios para la correcta aplicación de la política de seguridad de la información.

7. COMUNICACIÓN

Los miembros del Comité de Control Interno, Calidad y Riesgos, transmitirán la política a los usuarios de los activos de la información y las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

8. LINEAMIENTOS

8.1. SEGURIDAD DE LA INFORMACIÓN

La Cámara de Comercio del Putumayo 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 uso no adecuado de los activos de información puede poner en peligro la continuidad del servicio 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 integridad y disponibilidad de los activos de información de La Cámara de Comercio del Putumayo con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la entidad, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

8.2. CUMPLIMIENTO Y SANCIONES

8.2.1. Cumplimiento con la seguridad de la información

Todos los colaboradores de la entidad, 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 del Putumayo y al Comité de Control Interno, Calidad y Riesgos de la información.

8.2.2. Medidas disciplinarias por incumplimiento de la política de seguridad.

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

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

8.3. USO DE RECURSOS INFORMÁTICOS

8.3.1. Instrucciones para el uso de recursos informáticos.

El uso de cualquier sistema de información y demás recursos informáticos por parte del funcionario o usuario de los sistemas de la Cámara de Comercio del Putumayo, debe someterse a todas las instrucciones técnicas, que imparta el Comité de Control Interno, Calidad y Riesgos.

8.3.2. Uso personal de los recursos

Los recursos informáticos de La Cámara de Comercio del Putumayo, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la entidad. Cualquier otro uso está sujeto a previa autorización de la Presidencia ejecutiva.

8.3.3. Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos de La Cámara de Comercio del Putumayo, 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; además deberá tener en cuenta que la instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de cómputo o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por la Cámara de Comercio del Putumayo.

8.3.4. Uso del aplicativo entregado.

La Cámara de Comercio del Putumayo suscribe con los proveedores un contrato de compraventa o una orden de suministro para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que manejen información de uso restringido a La Cámara de Comercio del Putumayo. Adicional a esto, cada usuario, dependiendo de las actividades que realice sobre las aplicaciones, maneja un perfil limitado, de esta forma es controlado el acceso.

8.3.5. Responsabilidad del Usuario.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realice labores bajo su identidad y 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 del Putumayo.

8.3.6. Declaración de reserva de derechos.

La Cámara de Comercio del Putumayo, 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 del Putumayo se reserva el derecho y la autoridad de:

- Restringir o revocar los privilegios de cualquier usuario;
- Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados.
- Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Cámara de Comercio del Putumayo. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios.

8.3.7. Recursos compartidos.

Para el caso en que se compartan documentos en la red, se hace necesario tener una copia de seguridad en una dirección diferente a la carpeta compartida, que servirá como Backup, en caso de errores en la red o supresión de los documentos ya sea de manera voluntaria o involuntaria.

Se sugiere no compartir información calificada como reservada, clasificada o de interés particular y en caso de que sea necesario realizar esta acción, cifrarla por clave o por dominio.

8.3.8. Monitoreos.

Un usuario podrá ser monitoreado o supervisado en cualquier momento y sin previo aviso en el correcto uso de los recursos de la entidad.

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

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

8.3.10. Posibilidad de acceso no implica permiso de uso.

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

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

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

8.3.12. Manejo de sesiones en sistemas informáticos

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

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

Cualquier incidente de Seguridad debe reportarse por escrito al Comité de Control Interno, Calidad y Riesgos o al jefe del área, para que éste a su vez realice las acciones pertinentes de información y salvaguarda de la información.

8.3.14. Traslado de equipos.

Ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de La Cámara de Comercio del Putumayo sin previa autorización. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

8.3.15. Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con La Cámara de Comercio del Putumayo se debe diligenciar el documento de entrega de cargo. 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 asignado o el recurso tecnológico suministrado con carácter permanente o temporal, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el acta de

entrega de cargo (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos.

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

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

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

Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet.

8.3.18. Protección por Defecto de Copyright

Todos los colaboradores de La Cámara de Comercio del Putumayo 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 entidad.

8.3.19. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área de gestión tecnológica. 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.

8.3.20. Apagado de equipos.

Con fin de proteger la seguridad y distribuir bien los recursos de la entidad, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche, y en caso de que no se maneje información de carácter primordial, también se deberán apagar en horas de receso laboral.

8.3.21. Tiempo limitado de conexión en aplicaciones de alto riesgo

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

8.4. USO DE LAS CONTRASEÑAS

8.4.1. Identificación única por usuario.

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

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

8.4.2. 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.

8.4.3. Uso de diferentes contraseñas para diferentes recursos informáticos.

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

8.4.4. Cambios de contraseñas.

Todos los usuarios deben cambiar su contraseña por lo menos una vez al año.

8.4.5. Longitud mínima de contraseñas.

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

8.4.6. Las contraseñas creadas por usuarios no deben ser reutilizadas.

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente.

8.4.7. Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción del almacenamiento de contraseñas por parte del administrador, en caso de que lo requiera.

8.4.8. Sospechas de contraseña comprometida.

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

8.4.9. Bloqueo estación de trabajo.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 5 min.

8.5. USO DE LA INFORMACIÓN

8.5.1. Divulgación de la información.

La Cámara de Comercio del Putumayo 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 del Putumayo, es administrada y conservada observando las disposiciones propias del régimen de protección de datos personales, garantizando la privacidad de la información previamente clasificada, bajo autorización del titular de la misma para su tratamiento.

8.5.2. Registro de receptor de información privada.

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

8.5.3. Transferencia de la custodia de información de un funcionario saliente.

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

8.5.4. Clasificación de la Información

Se debe tener clasificada por parte de los encargados de área, la información que se maneje dentro de su dependencia, calificándola según los criterios de gestión documental estipuladas por la entidad y la ley de habeas data.

8.5.5. Eliminación Segura de la Información en Medios Informáticos

Todo medio informático reutilizable de terceros como equipos cedidos utilizados por La Cámara de Comercio del Putumayo, antes de su entrega se les realizará un proceso de borrado seguro de la información.

8.5.6. Eliminación segura de la información en medios físicos

Cualquier documento registral físico que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción aprobado por el comité de gestión documental y con base en los lineamientos estipulados por las tablas de retención y tablas de valoración documental aprobadas por la entidad.

8.6. USO DE INTERNET Y CORREO ELECTRÓNICO

8.6.1. Uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas.

8.6.2. Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal.

8.6.3. Preferencia por el uso del correo electrónico.

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

8.6.4. Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo diariamente y dar trámite dentro de los términos previstos.

8.6.5. Mensajes prohibidos.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, 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.

8.6.6. Acciones para frenar el SPAM.

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

8.6.7. Responsable del buzón.

Todo buzón de correo asignado debe tener una persona responsable de su administración, éste debe pertenecer al área de gestión tecnológica o comunicaciones de la Cámara de Comercio Putumayo.

8.6.8. Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet o de la red LAN pero exclusivamente para propósitos laborales, usando los mecanismos de seguridad apropiados o a través de las carpetas compartidas para este fin.

8.7. ASPECTOS GENERALES DE GESTION DE RIESGO

8.7.1. Evaluación y tratamiento del riesgo

La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo; los resultados de esta evaluación deben guiar y determinar la acción de gestión adecuada.

El alcance de la evaluación de riesgos puede abarcar a toda la entidad, a partes de la entidad, a un sistema individual de información o a componentes específicos del sistema.

8.7.2. Entrenamiento compartido para labores técnicas críticas.

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

8.7.3. 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 del Putumayo cuenta con personal técnico competente interno y externo que pueda detectar problemas y buscar la solución de una forma eficiente.

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

La Cámara de Comercio del Putumayo debe procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

8.8. PARA ADMINISTRADORES DE SISTEMAS

8.8.1. Soporte para usuarios con privilegios especiales.

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

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

Todos los privilegios sobre los recursos informáticos de La Cámara de Comercio del Putumayo otorgados a un usuario deben eliminarse en el momento que éste abandone la entidad, previa comunicación al área de sistemas.

8.8.3. Cuándo y cómo pueden asignar contraseñas los administradores

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

8.8.4. Límite de intentos consecutivos de ingreso al sistema.

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados:

a) ser temporalmente bloqueado.
b) Ser suspendido hasta nueva reactivación por parte del administrador.

Para los usuarios de sistemas de registros públicos se debe solicitar al área de gestión tecnológica para escalarlo al administrador del sistema.

8.8.5. Cambio de contraseñas por defecto.

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización.

8.8.6. Brindar acceso a personal externo.

El técnico en sistemas, velará porque individuos que no sean funcionarios, contratistas o consultores de La Cámara de Comercio del Putumayo no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación de la Presidencia ejecutiva o quien haga sus veces.

8.8.7. Dos usuarios requeridos para todos los administradores.

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

8.8.8. Privilegios por defecto de usuarios y necesidad de aprobación.

Sin autorización por parte de presidencia ejecutiva los administradores no deben otorgarle privilegios de administración a ningún usuario.

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

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas.

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

Para suministrar evidencia para investigación, seguimiento y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea.

La información a recolectar incluye configuración actual del sistema, copias de Backup y todos los archivos potencialmente involucrados.

8.8.11. Revisión regular de los registros del sistema.

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

8.8.12. Confidencialidad en la información relacionada con investigaciones internas.

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

8.8.13. Software de identificación de vulnerabilidades.

Para asegurar que el equipo técnico de La Cámara de Comercio del Putumayo ha tomado las medidas preventivas adecuadas, en las estaciones de trabajo se cuenta con un antivirus que a su vez cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS por sus siglas en inglés (Sistema de Detección de Intrusos), detección de virus y bloqueo de correo no deseado.

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

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

8.8.15. Mantenimiento de los Sistemas

Se debe realizar periódicamente el mantenimiento en antivirus y servidores de correo de La Cámara de Comercio del Putumayo.

8.8.16. Verificación física de equipos críticos

Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos (equipos que tienen configuraciones especiales).

8.8.17. Servicios de Red

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

8.9. BACKUP

8.9.1. Tipo de datos a los que se les debe hacer Backup y con qué frecuencia.

A toda la información de La Cámara de Comercio del Putumayo ubicada en los equipos de los directores de área, líder seccional, presidencia ejecutiva, asistente ejecutiva coordinación de control interno calidad y riesgos, equipos de la dirección administrativa, se le debe hacer un

Backup como mínimo una vez al mes o cuando por necesidad se requiera. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada. Esta tarea estará bajo la responsabilidad del área de gestión tecnológica.

8.10. USO DE FIREWALL

Al menos en la sede principal de la Cámara de Comercio del Putumayo se contará con un sistema de firewall para:

8.10.1. 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.

8.10.2. 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.

8.10.3. Filtrado de contenido activo en el Proxy.

El área de sistemas de la Cámara de Comercio, debe asegurar que, dentro de las configuraciones de Proxy, se filtre todo contenido activo como aplicaciones de java, adobe flash player, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información.

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

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

8.11. ACCESO FÍSICO

8.11.1. Orden de salida para equipos electrónicos.

Ningún equipo de cómputo podrá salir de las instalaciones de la sede principal de la Cámara de Comercio del Putumayo sin haberse registrado en el libro de salida de equipos, manejado por la dirección Administrativa y Financiera.

9. USO DE PORTATILES

9.1. Protección de la información

El antivirus siempre debe estar activo y actualizado

No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones de La Cámara de Comercio del Putumayo.

Cuando el equipo deba ser devuelto a La Cámara de Comercio del Putumayo para reparación, mantenimiento etc. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo.

De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas

10. ACTUALIZACIÓN, MANTENIMIENTO Y DIVULGACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

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

El Coordinador de control interno, calidad y riesgos o la persona designada por la presidencia, es responsable por su publicación y comunicación a todos los funcionarios. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

RELACION DE VERSIONES Y NATURALEZA DE CAMBIOS

Versión	Fecha	Acuerdo	Cambio
001	30/06/2016	250	Adopción de la política de seguridad de la información de la Cámara de Comercio del Putumayo

REVISION Y APROBACIÓN

Elaboración	**Revisión**	**Aprobación**
Control Interno, Calidad y Riesgos	Comité Control Interno, Calidad y Riesgos	Junta Directiva
DEIVY ARLEY DELGADO MELO	DECCY YANIRA IBARRA GONZÁLEZ	LUÍS EVELIO IBARRA CEBALLOS
Coordinador	Presidenta	Presidente
17/06/2016	21/06/2016	30/06/2016