POLÍTICAS DE SEGURIDAD Y CONFIDENCIALIDAD

DE LA INFORMACIÓN

CÁMARA DE COMERCIO DE SEVILLA

CAMARA DE COMERCIO DE SEVILLA

¡QUEREMOS LO NUESTRO!

Aprobada por la Junta Directiva, mediante acta N° 614

del 22 de septiembre de 2022.

1. INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de la CÁMARA DE COMERCIO DE SEVILLA, en adelante La Cámara de Comercio, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

2. OBJETIVO

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la Cámara de Comercio establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

El presente documento define los lineamientos que debe seguir la Cámara de Comercio con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

3. ALCANCE

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

- Colaboradores de Planta: se definen como colaboradores de planta aquellas personas que han suscrito un contrato laboral con la Entidad.

- Funcionarios de la Cámara de Comercio: Se definen como los empleados de la Cámara de Comercio que son susceptibles de manipular sistemas de información.
- Contratistas: se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:
  - Colaboradores en Misión;
  - Colaboradores por Outsourcing: son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos;
  - Personas naturales que prestan servicios independientes a la Entidad;
  - Proveedores de recursos informáticos.

- Entidades de Control
  - Procuraduría;
  - Revisoría Fiscal;
  - Contraloría General de la República;
  - Superintendencia de sociedades.

- Otras Entidades
  - DIAN.

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: 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. 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.
- 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]

---

[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

- 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.
- 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.
- Plan de contingencia: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de La Cámara de Comercio en casos de desastres y otros casos que impidan el funcionamiento normal.
- Política: Toda intención y directriz expresada formalmente por la dirección.
- Protector de pantalla: Programa que se activa a voluntad del usuario, o automáticamente después de un tiempo en el que no ha habido actividad.
- 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.
- Sesión: Conexión establecida por un usuario con un Sistema de Información.
- Sistema de control de acceso: Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.
- Sistema de detección de intrusos (IDS): Es un conjunto de hardware y software que ayuda en la detección de accesos o intentos de acceso no autorizados a los recursos informáticos de La Cámara de Comercio.
- Sistema de encripción: Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.
- Sistema multiusuario: Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.
- Sistema operativo: Software que controla los recursos físicos de un computador.
- Sistema sensible: Es aquel que administra información confidencial o de uso interno que no debe ser conocida por el público en general.
- Tercera parte: Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.
- 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.

6. RESPONSABLE

6.1. COMPROMISO DE LA DIRECCIÓN

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

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

6.2. GESTIÓN DE LOS RECURSOS

- Asegurar que las políticas de seguridad de la información brindan apoyo al cumplimiento de la misión y visión de La Cámara de Comercio.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales;
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados;
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.

7. PROCEDIMIENTO

- Comunicación de las políticas de seguridad:

El coordinador de sistemas, consciente 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.

7.1. POLÍTICA DE SEGURIDAD DE LA CÁMARA DE COMERCIO.

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

Los 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.

7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA

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

- Políticas de Cumplimiento y Sanciones
- Políticas de uso de recursos informáticos.
- Políticas de contraseñas.
- Políticas de uso de la información.
- Políticas del uso de Internet y correo electrónico.

- Política Sitio Web de La Cámara de Comercio
- Políticas Generales de la Presidencia.
- Políticas para Administradores de Sistemas.
- Políticas de Copias de respaldo (Backup).
- Políticas para Usuarios externos.
- Políticas de Acceso Físico.
- Política De Uso De Portátiles

7.3. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

7.3.1. Cumplimiento con la seguridad de la información

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de política de seguridad y confidencialidad de la información en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de La Cámara de Comercio, a través de la inclusión de esta obligación en el manual de funciones y las cláusulas contractuales.

7.3.2. 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.

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

7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

7.4.1. 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 coordinador de Sistemas. Subproceso Actualización, implementación e implantación de software y hardware y procedimientos de inducción y reinducción.

7.4.2. Uso personal de los recursos

Los recursos informáticos de La Cámara de Comercio, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad y estará catalogado como lo consagran las políticas de la Entidad.

7.4.3. Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos de La Cámara de Comercio, todo usuario debe firmar un **acuerdo de confidencialidad** de los sistemas de información antes de que le sea otorgado su Loguin de acceso a los sistemas de información y sus respectivos privilegios.

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.

7.4.4. Uso del aplicativo entregado.

La Cámara de Comercio ha suscrito con los fabricantes y proveedores un “CONVENIO” para los aplicativos que utiliza.

Cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil y unos permisos limitados, para cada sistema los cuales se encuentran relaciones en el documento **Perfiles de Usuarios.**

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

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien ésta 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 sistemas o a la propiedad de La Cámara de Comercio.

7.4.6. 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 coordinador de sistemas y/o autorizado por el presidente ejecutivo.

7.4.7. Todo monitoreo debe ser registrado y documentado.

El coordinador de sistemas es la persona encargada de realizar monitoreos en los equipos de la entidad las veces que crea necesario en el transcurso del año sin previo aviso.

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

7.4.9. 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.

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

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

vulnerabilidades, estas deben ser reportadas de inmediato al Coordinador de sistemas.

7.4.11. 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.

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

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del Coordinador de Sistemas.

7.4.13. Traslado de equipos debe estar autorizado.

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

El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado. Diligenciar el formato solicitud de **traslado de activos fijos.**

7.4.14. Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con La Cámara de Comercio se debe diligenciar el formato **acta 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 **acta de entrega de inventario**, con el que recibió; El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

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

Solamente a coordinadora de sistemas está autorizada para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

7.4.16. Protección por Defecto de Copyright

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

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

7.4.17. Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el responsable del proceso Gestión de Tecnología y Sistemas de Información. 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 Coordinador de Sistemas.

7.4.18. Apagado de equipos en la noche

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

7.4.19. 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 la aplicación deberá cerrar la sesión iniciada por el usuario.

7.4.20. Prohibición de uso de memorias USB

Esta totalmente prohibido conectar a los equipos de la entidad memorias USB, que sean de usuarios públicos, toda documentación debe ser enviada por correo electrónico, adicional las memorias internas de uso de los funcionarios no deben ser expuestas y conectadas en sitios públicos, y al ser conectada a los equipos deben ser siempre analizadas contra virus con el coordinador de sistemas. Para mayor seguridad los puertos de conexión USB se encuentran bloqueados, en caso de requerir alguna conexión informar al coordinador de sistemas

7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

7.5.1. 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.

7.5.2. 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.

7.5.3. Identificación única para cada usuario.

Cada usuario tendrá una identificación única al sistema 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 responsable del proceso Gestión de Tecnología y Sistemas de información, de La Cámara de Comercio.

7.5.4. Cambios periódicos de contraseñas.

Todos los usuarios deben ser automáticamente forzados (en los sistemas que lo permitan) o de forma manual a cambiar la contraseña de todos los sistemas de información.

7.5.5. Creación de las contraseñas.

Es recomendable que todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres, no debe ser generada idéntica o similar a una que se haya utilizado anteriormente y se recomienda que maneje un nivel de complejidad.

7.5.6. Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, notas, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas.

7.5.7. 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.

7.5.8. 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, a excepción del Coordinador de Sistemas.

7.5.9. 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. 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.

7.6. POLÍTICAS DE USO DE LA INFORMACIÓN

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

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

información, previamente clasificada, salvó autorización del titular de la misma para su divulgación.

7.6.2. Transferencia de datos solo a organizaciones con suficientes controles.

La Cámara de Comercio puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

7.6.3. Registro de las compañías que reciben información privada.

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

7.6.4. Eliminación Segura de la Información en Medios Informáticos

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

7.6.5. Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse la respectiva destrucción aprobado por el comité de archivo.

7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

7.7.1. Detección de intrusos.

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

7.7.2. Toda conexión externa debe estar protegida por el firewall.

Toda conexión de La Cámara de Comercio proveniente del exterior, sea Internet, redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización, este viene incluidos con el antivirus y modem proveedor de internet.

7.7.3. 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.

7.7.4. Prohibición de uso de Internet para propósitos personales.

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

7.7.5. Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto, podrá ser supervisada por el superior inmediato del empleado.

7.7.6. 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.

7.7.7. Uso de correo electrónico.

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

7.7.8. Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos 2 veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

7.7.9. Mensajes prohibidos.

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

7.7.10. Acciones para frenar el SPAM.

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al Coordinador de Sistemas.

7.7.11. Enviando software e información sensible a través de Internet.

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

7.7.12. Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet, pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

7.8. POLÍTICAS DE SITIOS WEB DE LA CÁMARA DE COMERCIO

7.8.1. 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.

7.8.2. Prohibición establecer conexiones a los sitios Web de La Cámara de Comercio

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de La Cámara de Comercio por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización de la Presidencia, dependiendo del caso.

Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Entidad en sitios diferentes a los institucionales.

Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados de La Cámara de Comercio o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con La Cámara de Comercio.

7.9. POLÍTICAS GENERALES DE LA PRESIDENCIA

7.9.1. Evaluación y tratamiento del riesgo

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

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

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

7.9.2. Restricción por acceso a Internet sobre recursos tecnológicos de uso interno a clientes externos.

No se otorgarán privilegios de acceso a Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios para ese usuario mediante una red pública con previa autorización de presidencia y Coordinador de sistemas.

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

Todos los computadores multiusuario, equipos de comunicaciones, otros equipos propiedad de la Entidad deben ubicarse dentro de un lugar asegurado bajo la responsabilidad del Coordinador de Sistemas, Además que no contengan información sensible.

7.9.4. 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 de La Cámara de Comercio.

7.9.5. Preparación de planes en casos de eventualidades, desastres y respuesta a emergencias.

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar un plan el cual permita dar una oportuna respuesta en caso de una eventualidad con el fin de que se pueda dar pronta solución y puedan estar operativos en tal caso. La contingencia de sistemas que se acuerdan con terceros deberá disponer de una infraestructura acorde a las necesidades de la Cámara de Comercio.

Para la recuperación de desastres de igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias de todo tipo.

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

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

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

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

7.10. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

7.10.1. Soporte para usuarios con privilegios especiales.

Todos los sistemas 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.

7.10.2. 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 otorgados a un usuario deben eliminarse en el momento que éste abandone la Entidad.

7.10.3. Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el funcionario debe cambiar su contraseña; todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización.

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

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en todos los sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

7.10.5. Brindar acceso a personal externo.

El Coordinador de Sistemas velará porque individuos que no sean empleados, contratistas o consultores de La Cámara de Comercio no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación por parte de la Presidencia

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de La Cámara de Comercio se requiere la firma de un acuerdo de confidencialidad.

7.10.6. Dos usuarios requeridos para el administrador.

Administradores de sistemas deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal en caso de requerirse necesario si desempeña otras funciones.

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

Sin autorización escrita por presidencia de la Cámara de comercio, los administradores no deben otorgarle privilegios de administración a ningún otro usuario.

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

Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

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

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

7.10.10. 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.

7.10.11. Información con múltiples niveles de clasificación en un mismo sistema.

Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

7.10.12. Software de identificación de vulnerabilidades.

Para asegurar que el equipo técnico de La Cámara de Comercio ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de

Cortafuegos y Antivirus en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades, detección de virus y bloqueo de correo no deseado.

7.10.13. En dónde usar controles de acceso para sistemas informáticos.

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

7.10.14. Mantenimiento preventivo en computadores, equipos y sistemas de comunicación.

Se debe realizar mantenimiento preventivo anualmente en todos los computadores y equipos electrónicos para que el riesgo de falla se mantenga en un nivel bajo, además se debe verificar en el estado físico de los equipos de cómputo.

7.11. POLÍTICAS DE COPIAS DE RESPALDO (BACKUP)

7.11.1. Tipo de datos a los que se les debe hacer backup.

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

7.11.2. Copias de información sensible.

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

7.11.3 Periodicidad copias de seguridad

Las copias de seguridad se realizarán de manera automática semanalmente y/o manual por cada funcionario cuando lo requiera necesario para cada equipo. Esto se debe a que gran parte de la información que se maneja en la Cámara de Comercio de Sevilla, se resguarda automáticamente en los sistemas de información.

7.12. POLÍTICAS PARA USUARIOS EXTERNOS

7.12.1. Términos y condiciones para clientes de Internet.

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

7.12.2. Acuerdos con terceros que manejan información o cualquier recurso informático de La Cámara de Comercio

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de La Cámara de Comercio por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a La Cámara de Comercio ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información.

7.12.3. Definición clara de las responsabilidades de seguridad informática de terceros.

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

7.13. POLÍTICAS DE ACCESO FÍSICO

7.13.1. Reporte de pérdida o robo de identificación.

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

7.13.2. Orden de salida para equipos electrónicos.

Ningún equipo electrónico podrá salir de las instalaciones de La Cámara de Comercio sin el diligenciamiento debido del formato de **solicitud de préstamo**.

7.13.3. Cuando se da una terminación laboral, los privilegios de acceso a la sede de La Cámara de Comercio deben ser revocados.

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de identificación de las instalaciones (carnés etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (funcionarios autorizados) correo electrónico al área de Sistemas (sistemas@camcciosevilla.org.co).

7.14. POLITICA DE USO DE PORTATILES

7.14.1. El antivirus siempre debe estar activo y actualizado

7.14.2. No se debe tener información sensible guardada.

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

7.14.4. No dejar el computador en lugares públicos o expuesto.

7.14.5. No prestar el computador portátil a familiares y/o amigos

7.14.6. Al momento de realizar entrega del computador este debe estar totalmente cargado.

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

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

La persona designada por la presidencia debe aprobar el documento, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

9. Oficial de Seguridad de la Información

Oficial de Seguridad de la Información (Coordinador de sistemas o persona designada para los temas de seguridad de la Entidad):

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de la compañía.

- Actualización y seguimiento periódico al mapa de riesgos de la compañía, validando el riesgo que corresponde al área de sistemas.
- Concientizar en seguridad de la información las áreas de la Cámara de Comercio de Sevilla.
- Evaluar en forma continua la efectividad de la seguridad de la información de la organización con el propósito de identificar oportunidades de mejoramiento y necesidades de capacitación.

VERIFICACION E IMPLEMENTACION DE ACCIONNES DE MEJORA.
Aplicar semestralmente las listas de chequeo:
Lista de Chequeo Seguridad de la Información
Realizar seguimiento a las acciones implementadas.

CONTROL DE CAMBIOS			
versión	Fecha de aprobación	Descripción del cambio	Responsable cambio
1			
2			
3			
4			
5	23/09/2022	Se actualiza la descripción de documento realizando ajustes según observaciones y recomendaciones dadas por la revisora fiscal, se socializa tanto a funcionarios como a la junta directiva la cual aprueba su actualización.	Catherine martinez osorio