INTRODUCCIÓN

La Cámara de Comercio de Palmira ha establecido un protocolo de seguridad informática que especifica los derechos y deberes de la organización y de los empleados, contratistas y demás miembros de la Comunidad Cameral sobre los servicios que presta en las áreas de tecnología y de telecomunicaciones.

Estas normas buscan orientar a los usuarios en el uso eficaz y correcto de los recursos y servicios informáticos que brinda la Cámara para el desempeño de sus funciones, sin desconocer el respeto de derechos como la intimidad y privacidad.

Departamento Administrativo
Tecnologías de la Información - TI

Esta guía no constituye un listado completo de los protocolos de seguridad informática de la Cámara de Comercio de Palmira, pero resalta algunos de los aspectos más importantes para la seguridad de la información.

CONTENIDO

1 OBJETIVOS DEL PROTOCOLO

Establecer unos principios, reglas y lineamientos que permitan a la Cámara de Comercio de Palmira controlar el uso de los activos (hardware y software) de la información minimizando el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, así como proteger su información para su procesamiento y administración.

2 ALCANCE

El Protocolo de seguridad informática de la Organización está dirigida a los empleados, contratistas, proveedores y demás miembros de la Comunidad Cameral, que tengan acceso o utilicen los recursos informáticos de propiedad de la Cámara de Comercio de Palmira o que los tengan bajo su custodia, y a terceros propietarios de equipos informáticos que sean conectados a las redes de la Cámara.

El propósito de la gestión de la seguridad de la información en la Cámara de Comercio de Palmira es velar por la integridad, disponibilidad, confidencialidad y confiabilidad de la información destinada a la realización de actividades propias del Registro Mercantil y el resto de áreas de la Cámara.

La Cámara dispondrá (de acuerdo con los lineamientos de eficiencia, eficacia, transparencia y optimización de recursos) los recursos y mecanismos apropiados para garantizar el cumplimiento de las normas sobre seguridad informática, así como para la implementación de prácticas globalmente reconocidas en seguridad de la información de acuerdo con estándares internacionales.

De igual manera, propiciará y desarrollará programas de formación y actualización continua en temas de seguridad informática a los miembros de la Comunidad Cameral, de acuerdo con los niveles de autoridad y responsabilidad, para formar su competencia en el manejo de los recursos informáticos.

La Dirección Administrativa es responsable de la definición, promulgación y revisión continua de las normas de seguridad informática que garanticen la confiabilidad, confidencialidad, integridad y disponibilidad de la información.

3 DESCRIPCIÓN

- Esta guía fue diseñada para brindar a los miembros de la Comunidad Cameral los lineamientos que permitan asegurar la información y los recursos tecnológicos de la Cámara.
- La Cámara como propietaria de los sistemas de recepción, transmisión, almacenamiento y procesamiento de información organizacional está en la obligación de garantizar su integridad, confidencialidad y disponibilidad, así como de atender los requerimientos de orden legal o regulatorio exigidos por los organismos de control, para lo cual se establecerán los mecanismos necesarios que le permitan responder adecuadamente.
- La Institución pondrá a disposición de organismos de control, previa presentación del requerimiento oficial firmado por el representante autorizado de la autoridad competente, la información solicitada de los usuarios, así como aquella que permita identificarlos.

4 RESPONSABILIDADES DE LOS USUARIOS CON LOS RECURSOS Y SERVICIOS DE TECNOLOGÍA

Cada usuario de los servicios de tecnología de la Cámara de Comercio de Palmira tiene las siguientes responsabilidades al igual deberán tener en cuenta el **PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN Y SOPORTE TÉCNICO GESTIÓN DE SOPORTE:** GESTIÓN DE TI donde el área de tecnología comparte a través de correo electrónico y/o WhatsApp:

- Usar de manera ágil, eficiente y racional los recursos tecnológicos asignados.
- No deshabilitar o evadir ningún control de seguridad de los sistemas o servicios informáticos de la Organización.
- No debe interferir en los procesos computacionales de la Cámara mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados. Así mismo y bajo ningún pretexto debe intentar burlar los esquemas de seguridad de los sistemas de la Camara de Comercio.
- Cumplir a cabalidad con los protocolos, estándares y normas de seguridad.
- Informar al Área de Tecnologías de Información acerca de irregularidades o problemas relacionados con los servicios, para que se puedan aplicar correctivos oportunamente.

5 MANEJO DE INFORMACIÓN Y CONFIGURACIÓN EN LOS COMPUTADORES PERSONALES

- Los computadores deben tener instalado un papel tapiz y protector de pantalla institucional con contraseña. Estas características no deben ser modificadas sin previa autorización del área de TI y Comunicaciones.
- Los usuarios son responsables de guardar en la carpeta de C:\trabajo toda la información susceptible para sus funciones laborales con el fin de que se le realice un backup automático a un directorio de red según la programación que tenga estipulada el área de Tecnologías. El tamaño máximo de la carpeta de "Trabajo" es de 5Gb, por lo tanto, es responsabilidad del usuario hacer constante depuración de la información, moviendo a otra ruta la información histórica (aquella que no se consulta ni modifica en la actualidad) y haciendo backup en un medio externo. El usuario puede solicitar al área administrativa los medios para almacenar la información (DVD, CD) o al área de TI en caso de que el tamaño de la información a respaldar sea de gran tamaño y requiera una unidad externa USB.
- La Cámara no garantiza ni provee espacio en los computadores corporativos ni en los servidores para que los usuarios copien información personal a ser respaldada, por lo tanto, dichos archivos tampoco pueden estar en la carpeta de C:\trabajo. Los usuarios son responsables del backup de su archivo personal, por lo tanto y pese a que pueden trabajar documentos sobre los computadores asignados para sus labores, no deben almacenar ningún tipo de información personal en estos, es decir que, una vez realizada la actividad específica, deberá retirar los archivos del equipo.

6 NOMBRES DE USUARIO Y CONTRASEÑAS

- Todos los colaboradores de la Cámara de Comercio deben tener un identificador para los servicios de red (ingreso al dominio) y para aquellos que aplique también un identificador para el ingreso a las aplicaciones (correo electrónico y sistemas de información).

- La solicitud de los identificadores para el caso de los servicios de red, Sistema Integrado de Información (SII) debe realizarse directamente al Área de Tecnologías, para el sistema de Gestión Documental (DOCXFLOW) deberá tramitar con el administrador del software en este caso el auxiliar de archivo y digitalización. El resto de aplicaciones deben tramitarse a través del área de Tecnología con una autorización del jefe de área responsable del aplicativo y el jefe inmediato del colaborador que requiere el acceso.
- **Los nombres de usuario y claves de acceso** a los sistemas de procesamiento de información y a los servicios de red que les sean otorgados a los colaboradores **son de carácter personal e intransferible**. Las personas no deben obtener claves u otros mecanismos de acceso de otros usuarios que puedan permitirles un ingreso indebido, es decir que no se deben compartir contraseñas entre compañeros de trabajo ni con personal externo a la entidad.
- En casos de ausentismo por cualquier motivo (calamidad, enfermedad o vacaciones), el colaborador deberá suministrar la clave de acceso al equipo de cómputo al jefe de área inmediato o al que designe el jefe. Para el caso del área de registros públicos deben suministrarse a los coordinadores jurídicos, teniendo en cuenta las rotaciones que se realizan y el sistema de pares que manejan.
- Las personas son responsables de todas las actividades llevadas a cabo con su nombre de usuario y sus claves personales.
- La contraseña debe ser conformada con un mínimo de ocho (8) caracteres, y se sugiere una combinación alfanumérica entre letras mayúsculas, minúsculas y/o caracteres especiales.
- Los usuarios deben asignar contraseñas que sean difíciles de adivinar, no se recomienda el uso de nombres propios, apodos, fechas de cumpleaños, ni palabras reservadas.
- Las contraseñas deberán ser cambiadas máximo cada 60 días.
- Las contraseñas no deberán escribirse en lugares visibles o de fácil acceso ni entregarse a otras personas.
- Deshabilitar los usuarios de los sistemas de información de un empleado que se le haya finalizado el contrato laboral por cualquier motivo.

7 SOFTWARE

- Cualquier requerimiento de licencias de software que deban ser consideradas como parte del equipo institucional y que podrían ser utilizadas por el usuario para el desarrollo de su actividad en la Cámara, deberá ser solicitado al área de Tecnología para que se evalúe la necesidad de compra de la licencia o en su defecto se analice un software gratuito que cumpla con las necesidades del usuario y condiciones de seguridad.
- Los usuarios no deben participar en la copia, distribución, transmisión o cualesquiera otras prácticas no autorizadas en las licencias de uso de software. Cualquier duda al respecto deberá ser consultada con el área de Tecnologías.
- En los equipos asignados a los colaboradores sólo se debe usar software legal autorizado y aprobado por la organización.
- El uso ilegal o no autorizado de software es una violación de los lineamientos de la Cámara de Comercio de Palmira y de las leyes colombianas, y podría implicar acciones correctivas, incluyendo la terminación del contrato y/o procesos legales.
- Toda instalación, desinstalación o traslado de software (incluyendo aquellos de dominio público o de distribución libre - shareware, freeware, etc.) desde y hacia el equipo institucional requiere autorización y coordinación previa del área de Tecnologías.
- Los usuarios no deben instalar o descargar software comercial de forma en que se violen las normas sobre licenciamiento y derechos de autor.

- Los usuarios no deben instalar, ejecutar y/o utilizar archivos, programas o herramientas de software o hardware que:
- Adivinen las contraseñas alojadas en las tablas de usuarios de equipos locales o remotos.
- Monitoreen la actividad de los sistemas informáticos de equipos locales o remotos, salvo aquellos que estén autorizados por la Institución para que el área de Tecnologías administre la funcionalidad y la seguridad de los recursos informáticos de la Organización.
- Rastreen vulnerabilidades en sistemas de cómputo (hardware o software), salvo aquellos que estén autorizados por la Institución para que el área de Tecnologías evalúe la seguridad de los recursos informáticos de la Cámara.
- Exploten alguna vulnerabilidad de un sistema informático para acceder así a privilegios que no han sido explícitamente otorgados por el administrador de la red o de un recurso informático en particular, salvo aquellos que estén autorizados por la Institución para que la el área de Tecnologías administre y evalúe la seguridad de los recursos informáticos de la Cámara.
- Tengan un carácter de juegos, música, videos, películas y/o pornográficos.
- El uso de herramientas que permitan el intercambio de información entre equipos, tales como Kazaa®, Emule®, Morpheus®, Gnutella®, y otros que puedan surgir para realizar dicha práctica, será autorizado para propósitos relacionados con las labores propias de cada empleado, por el director de área respectivo y controlado por el área de Tecnologías.
- Los equipos (computadores de escritorio, servidores, portátiles) cuentan con un adhesivo laminado (COA) que contiene la información del licenciamiento del sistema operativo en la CPU y que viene directamente del fabricante, este adhesivo ha sido protegido por el área de TI con papel contact, esto con el fin de conservar los datos allí registrados como único soporte admitido por las entidades de control sobre la legalidad del software que se está utilizando. Es deber del usuario mantener el adhesivo en óptimas condiciones o informar al área de TI de cualquier anomalía al respecto. **Nota:** los equipos modernos traen la información de licencia integrada en la Motherboard.
- Si el usuario cuenta con una licencia de software que no está a nombre de la Cámara, pero que desea instalar en el equipo institucional que se le ha asignado, deberá demostrar que es legal, que está a su nombre y que la licencia permite su instalación. En tal caso, el usuario deberá firmar un documento de responsabilidad de uso, previa coordinación con el área de TI y autorización del jefe de área respectivo.
- Dado el caso de que se haga necesario instalar una licencia de software en un equipo personal de un empleado, una vez que el empleado no requiera utilizar más el software instalado en su equipo personal, termine su relación con la Cámara, o cuando el área de Tecnologías así lo solicite, el usuario deberá llevar su equipo personal a las instalaciones del Departamento de Tecnologías para proceder a la desinstalación o verificación de la desinstalación del software.
- En el eventual caso de que en el proceso anterior quedara algún software sin desinstalar en el equipo personal del usuario al momento de la terminación de la relación con la Cámara, éste deberá inmediatamente proceder a desinstalarlo. De no ser así, el usuario asume las consecuencias y la responsabilidad de operar un software sin contar con la respectiva licencia.
- Cualquier software que no cumpla con lo estipulado anteriormente y que haya sido instalado en el equipo institucional asignado al empleado, será desinstalado y eliminado sin que ello derive ninguna responsabilidad para la Cámara.
- Al usar una licencia de software que ha sido instalada en el equipo institucional o en el equipo personal, el usuario reconoce los derechos de la Cámara anteriormente descritos y será consciente de ellos.

8 SEGURIDAD DE LOS EQUIPOS

- Durante la jornada laboral y en todo tiempo de uso, corresponde al usuario prestar la debida custodia y cuidado a los equipos de cómputo que le han sido asignados, así como impedir su sustracción, destrucción, ocultamiento o utilización indebida.
- No se permite facilitar el uso de un equipo a personas externas a la organización, de presentarse una eventualidad donde se haga necesario facilitar un equipo, el usuario deberá informar al área de TI para que ésta proporcione una solución segura al requerimiento. De igual manera el usuario será responsable de verificar la utilización del equipo por parte del externo y para esto deberá permanecer presente durante todo el tiempo que el cliente haga uso del computador.
- Los usuarios externos, proveedores, consultores y demás personal ajeno a la organización, deben reportar al guarda de turno en portería el ingreso y salida de equipos de cómputo personales y la Cámara de Comercio de Palmira no se hará responsable por el cuidado del mismo.
- Ningún equipo de cómputo puede ser expuesto a factores externos que comprometan su integridad, tales como humedad, humo y polución.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren equipos de cómputo.
- No está permitido desactivar el monitor del antivirus de los equipos.
- Sobre los equipos de cómputo no deben ubicarse elementos pesados, radios de comunicación o teléfonos celulares.
- Toda pérdida de equipos de cómputo ya sea de escritorio o portátil, o de alguno de sus componentes, debe ser informada de inmediato al área Administrativa, o al área de Tecnologías por el usuario que tenga a cargo el equipo.
- Los usuarios de la Institución deben apagar correctamente los equipos en las ausencias prolongadas y al final de la jornada laboral.
- En caso de que los usuarios ingresen a la entidad equipos de cómputo o de comunicaciones de propiedad personal, la Cámara de Comercio no se hará responsable por el daño, robo o pérdida de los mismos.
- Todo problema de orden técnico con los equipos debe ser reportado por los usuarios al área de Tecnologías a la mayor brevedad posible.
- Los usuarios solicitarán asesoramiento o servicios al área de Tecnologías a través del formato de ***Solicitud de Servicios Informáticos F4***, correos electrónicos u otros mecanismos automatizados, de manera que se genere un registro de los trabajos efectuados por los colaboradores del área de Tecnologías y de las solicitudes de los empleados.
- Los funcionarios del Área de Tecnologías son los únicos autorizados para realizar modificaciones a la configuración original de los equipos, así como para destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes o en su defecto indicarán qué empresa o persona (proveedor) podrá realizar dichas actividades.
- El Área de Tecnologías es la única dependencia autorizada para coordinar el traslado de los equipos de cómputo de un puesto a otro, o por fuera de la organización y es responsable del control individual de inventarios.

9 SEGURIDAD EN LOS EQUIPOS FUERA DE LAS INSTALACIONES

- Los usuarios no deben prestar los equipos portátiles a terceros cuando se encuentren por fuera de la organización y será responsabilidad cualquier daño físico o lógico que le ocurra al equipo durante el tiempo que permanezca bajo su custodia.

- Los usuarios no deben dejar los equipos de cómputo portátiles a simple vista y desatendidos ni dentro ni fuera de la organización.
- Cuando el usuario se desplace en automóvil con un equipo de propiedad de la entidad, se recomienda que lo transporte en el portaequipaje o debajo de los asientos.
- Aplica también para todos los equipos portátiles que se extraigan de la organización, los ítems consignados bajo el título de *Software* del presente documento.
- Aplica también para todos los equipos portátiles que se extraigan de la organización, los ítems consignados bajo el título de *Acuerdos de Confidencialidad* del presente documento.

10 CONTROL DE ENTRADA Y SALIDA DE EQUIPOS/DISPOSITIVOS TECNOLÓGICOS

- Para extraer un equipo/dispositivo tecnológico en aras de cumplir funciones laborales en espacios fuera de la organización y para el control de la propiedad perteneciente a los clientes o proveedores externos, se debe diligenciar el formato entrada y salida de equipos/dispositivos tecnológicos (F12-A2). Una copia del formato diligenciado debe entregarse en portería antes de retirar o ingresar (cuando el proveedor ingresa un equipo para dejarlo como soporte) el equipo/dispositivo tecnológico y deberá ir firmado por el Coordinador de TI o el Director Administrativo y en su ausencia por la persona que ellos designen como también debe ir firmado por el responsable.
- Para los empleados que tienen equipo portátil como su herramienta de trabajo y que deben salir continuamente de la entidad para desarrollar labores en sitios externos, no es obligatorio diligenciar el formato de entrada y salida (F12-A2) de equipos para no hacer tan dispendiosa la salida y evitar la impresión de mucho papel, teniendo en cuenta que durante la semana es constante la entrada y salida del mismo equipo y queda bajo absoluta responsabilidad del empleado el cuidado del equipo e información que contenga en él.
- Este formato será guardado en una carpeta física de hoja de vida del dispositivo ubicada en el área de TI y para el caso de ser un dispositivo de propiedad del proveedor externo se archivará en la carpeta del mismo proveedor.
- **Nota**: Cuando un dispositivo de propiedad del proveedor tenga ingreso o salida de la entidad y el mismo proveedor entrega algún documento (remisión u orden) que indique la referencia del dispositivo, no se hace obligatorio diligencia el formato de entrada y salida de equipos/dispositivos tecnológicos (F12-A2).

11 ACUERDOS DE CONFIDENCIALIDAD

- Cada usuario debe salvaguardar la información crítica o confidencial aún después de salir de la Cámara de Comercio de Palmira, cualquiera que haya sido el motivo de su salida (Retiro, aceptación de otro cargo, terminación voluntaria o no voluntaria del contrato laboral).
- Un usuario no debe revelar información obtenida en el desempeño de sus labores en la Institución sin primero recibir una autorización escrita de los directivos.
- Cada usuario deberá reportar cualquier incidente de hardware o software suscitado con los recursos y/o servicios informáticos de la organización al área de Tecnologías de la Información y dicha área será la única encargada de brindar la solución más adecuada para que el usuario (interno o externo) pueda llevar a cabo sus funciones.
- Cada usuario es responsable de reportar a su jefe inmediato y al área de Tecnologías, las siguientes situaciones:

- Si una persona se niega a proveer verificación de la autorización apropiada para obtener información que le ha sido solicitada.
- Información sensible no protegida o desatendida.
- Material sensible faltante o mal ubicado.
- Revelación no autorizada de información sensible.
- Si existe evidencia de que su escritorio, computador, archivo o área de trabajo han sido accedidos o alterados en su ausencia.
- Copias no autorizadas de información confidencial o crítica.
- Si observa que contraseñas o nombres de usuarios son conocidos por personas diferentes a sus dueños.
- Actividades sospechosas de personas diferentes al área o la Institución.
- Incidentes con virus informáticos.

- Los empleados deben tener en cuenta las siguientes recomendaciones en caso de encontrarse fuera de las instalaciones de la Cámara en representación de la misma:

  - Llevar únicamente los documentos y materiales que necesite.
  - Conservar copias de seguridad para disminuir el impacto por pérdida o robo de la información.
  - Estar alerta ante señales que indiquen que compañeros de viaje o recién conocidos muestren demasiado interés en sus asuntos de negocio.
  - Evitar hacer referencias a temas sensibles relacionados con el trabajo.
  - No acceder, leer, o exponer documentos o información en un lugar donde pudiera ser observado por personas no autorizadas.

12 CONDICIONES DE USO DE HERRAMIENTAS TECNOLÓGICAS

12.1 INTERNET CORPORATIVO

- La conectividad a Internet será otorgada para propósitos relacionados con las labores propias de cada empleado y será debidamente autorizada.
- Los usuarios no deben utilizar este servicio para realizar actividades ilegales, apuestas en línea, ni acceder o descargar material pornográfico, tampoco deben acceder a juegos, escuchar música, visualizar contenidos en línea o acceder a redes sociales; para acceder deben contar con previa autorización directa del director del área.
- Se prohíbe el uso de aplicaciones, programas y/o herramientas que saturen los canales de comunicación o Internet, tales como gestores de descarga de archivos multimedia (audio y/o videos), P2P, Torrent entre otros.
- Los usuarios no deben instalar o descargar software comercial de forma en que se violen las normas sobre licenciamiento y derechos de autor.
- El uso de Internet será monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, la Institución puede revisar el contenido de las comunicaciones y le será suspendido el servicio al usuario sin que ello derive ninguna responsabilidad para la Cámara.

12.2 INTERNET INALÁMBRICO

- Para la red inalámbrica se crean dos redes de acceso, una para personal corporativo (empleados) y otra para personal externo (invitados o visitantes), donde sus nombres de red (SSID) son CCP_CORPORATIVO e INVITADOS_CCP.

- La red inalámbrica será administrada por personal de TI para permitir su funcionalidad y buen uso, todo empleado que desee incluir un dispositivo (portátil o teléfono móvil) personal a la red CCP_CORPORATIVO debe solicitarlo al área de TI donde se registra el dispositivo para ser identificado en el servidor, esto como medida de control y así no permitir el acceso a dispositivos desconocidos.
- Los Dispositivos que se encuentren conectados a la red CCP_CORPORATIVO y no estén identificados o registrados serán bloqueados en la red por seguridad.
- Las redes inalámbricas deben ser protegidas por contraseña para prevenir el aprovechamiento de los alrededores.
- El acceso a la red inalámbrica desde los equipos portátiles y dispositivos móviles institucionales y personales por parte de los empleados deberá ser sólo con propósitos relacionados con las labores propias de su cargo.
- Ningún empleado ni usuario externo debe instalar dispositivos inalámbricos en los equipos de la Cámara de Comercio.

12.3 CORREO ELECTRÓNICO

- El sistema de correo electrónico de la Cámara debe ser usado únicamente para propósitos de trabajo, para tal efecto se desarrolló entre el Área de Tecnologías y el Área de Comunicaciones el Manual del buen uso del correo electrónico, el cual se encuentra enmarcado dentro del proceso de Gestión de Tecnologías de la Información bajo el nombre: ***"MT-A-2 Manual de uso del correo electrónico institucional"***.
- El Área Administrativa autorizará la revisión de los correos y archivos enviados por este medio sólo cuando considere que el equipamiento de la Institución es utilizado inadecuadamente o en caso de solicitud formal por autoridad competente en cumplimiento de requerimientos legales y regulatorios.
- El servicio de correo electrónico de la Institución no debe ser utilizado para enviar correo basura (SPAM).
- Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso apropiado del lenguaje.
- Los colaboradores, y demás miembros de la Comunidad Cameral no deben enviar mensajes personales u ofensivos, injuriosos, cadenas de mensajes, o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Organización.
- Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otro trabajador. En caso de ausencias o vacaciones, se debe recurrir a mecanismos alternos como redirección de mensajes.
- Al recibir un mensaje sospechoso, los usuarios deben informar al Área de Tecnologías para validar que esté libre de virus.
- Los empleados no están autorizados para utilizar versiones escaneadas de firmas hechas a mano sobre cualquier tipo de comunicación electrónica.

12.4 MENSAJERÍA ELECTRÓNICA INSTANTÁNEA

- La Cámara fomentará la utilización de un sistema de mensajería electrónica integrado a las herramientas de comunicaciones (teléfono - e-mail) que garantice las condiciones de seguridad mínimas requeridas para la protección de la información y de los medios institucionales. Actualmente la herramienta proporcionada es el aplicativo *"Utalk".*

13 PROTECCIÓN DE DOCUMENTOS

- La información enviada a través de equipos de comunicaciones de la Institución se considera privada, a menos de que en forma expresa se indique lo contrario. Para mayor información, revise el aparte de *Acuerdos de Confidencialidad* del presente documento.
- Todos los usuarios de los aplicativos o programas del computador deben cerrar las sesiones de trabajo si no están utilizando el equipo o no se encuentran en sus puestos de trabajo.
- Los usuarios son responsables de:

    - La información impresa y de los reportes físicos generados por ellos a través de los diferentes sistemas.

    - Sólo deben usar el número de copias o impresiones requeridas, además, deben verificar que en la fotocopiadora o impresora no quedan copias pendientes.

    - Asegurarse de tener el original antes de retirarse de la fotocopiadora.

    - Si la impresora no está funcionando, debe borrar el archivo de la cola de impresión.

    - Recoger inmediatamente todos los documentos recibidos vía fax para prevenir revelar información no autorizada.

    - No enviar documentos que contengan información confidencial vía fax.

    - No dejar documentos con información confidencial a la vista en el escritorio ni en las impresoras.

14 INGRESO AL CENTRO DE DATOS

El ingreso al Centro de Datos de la Cámara de Comercio de Palmira se reglamenta de la siguiente manera:

- Se permite únicamente el ingreso del personal de TI de la CCP.
- Si un usuario de otra área requiere ingresar, deberá solicitar autorización al área de TI y realizar el ingreso en su compañía.
- Los proveedores deben solicitar autorización para el ingreso al Centro de Datos y permanecer únicamente en el área dispuesta para su labor, de igual manera deberá permanecer bajo la inspección del personal de TI y remitirse únicamente a la labor para la cual fue contratado.
- Si un usuario observa alguna anomalía en el Centro de Datos, deberá reportarla inmediatamente al área de TI o al área Administrativa.

15 BUENAS PRÁCTICAS

- Para evitar el bloqueo o la lentitud del equipo, es recomendable no abrir de manera simultánea varias ventanas de un mismo programa, o mantenerlas innecesariamente abiertas.

- Velar por un escritorio limpio, es decir procurar por no mantener el escritorio del computador lleno de archivos y carpetas que pueden afectar el rendimiento del equipo.
- Los usuarios son responsables de crear las rutas de almacenamiento de información en sus computadores asignados, esto con el fin de organizar y posteriormente poder ubicar la información producto de sus labores, sin embargo deben adoptar la buena práctica de tener especial cuidado en que toda la cadena de caracteres que componen la ruta no exceda los 255 caracteres, ejemplo: en la siguiente ruta "*C:\trabajo\2013\FormaciónEmpresarios\Evento1.ppt*" se pueden contar 45 caracteres después de "C:\". Así mismo se deben analizar las rutas de los equipos antes de crear nuevos nombres de carpetas y archivos. Una recomendación es abreviar las palabras, acortar las frases y cuando sea viable concatenar las palabras para evitar los espacios entre éstas (los espacios cuentan como un carácter), ejemplo: *Formación Empresarios*, nótese que la primera letra de cada palabra usa la convención de mayúscula, lo cual facilita la lectura y entendimiento de la frase.

16 ANEXO

Documento anexo del acuerdo de confidencialidad y no divulgación de la información que permite a las partes implicadas seguir los lineamientos de la entidad protegiendo la información y garantizando la confidencialidad, privacidad y no divulgación de la misma.

	NOMBRE	CARGO
ELABORÓ	Oscar Eduardo Varela	Coordinador de Tecnologías de la Información
REVISÓ	Oscar Eduardo Varela	Coordinador de Tecnologías de la Información
APROBÓ	Oscar Eduardo Varela	Coordinador de Tecnologías de la Información

ANEXO
ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN

Con el objetivo de garantizar la confidencialidad, privacidad y no divulgación de los datos y la información de propiedad de la Cámara de Comercio de Palmira, se genera este documento de lineamientos de buenas prácticas en Seguridad y Privacidad, donde aplica para cada una de las partes implicadas como son: colaborador, pasantes, aprendices Sena, personal temporal, proveedores, contratistas, empresarios y demás partes que hagan uso de los recursos e información de la organización se acojan y/o adhieran a este acuerdo que garantiza el buen uso y seguridad a la información contando con las mejores prácticas; por esta razón se da por responsable a cada parte implicada a partir de la fecha del documento y su difusión.

El contenido del acuerdo es el que figura a continuación.

CLAÚSULAS

PRIMERA. LA PARTE IMPLICADA se obliga a no divulgar ni compartir a terceras partes, la Información, datos, credenciales de acceso, VPN y conexión de bases de datos, que reciba por parte de la CAMARA DE COMERCIO PALMIRA y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad. Para efectos del presente acuerdo de confidencialidad, “Información Confidencial” comprende toda la información divulgada por la CAMARA DE COMERCIO PALMIRA ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible e intangible entregada a LA PARTE IMPLICADA.
SEGUNDA. LA PARTE IMPLICADA se obliga a mantener de manera privada la “Información confidencial” que reciba de la CAMARA DE COMERCIO PALMIRA y no darla a terceros, diferente de su equipo de trabajo y asesores que tengan la necesidad de conocer dicha información para los propósitos autorizados, y quienes deberán estar de acuerdo en mantener de manera confidencial dicha información.
TERCERA. Es obligación de la PARTE IMPLICADA no divulgar la “Información confidencial”, incluyendo, mas no limitando, el informar a sus empleados que la manejen, que dicha información es confidencial y que no deberá ser divulgada a terceras partes.
CUARTA. LA PARTE IMPLICADA se obliga a utilizar la “Información confidencial” recibida, únicamente para los fines laborales durante el tiempo de su vínculo con la organización.
QUINTA. LA PARTE IMPLICADA se compromete a efectuar una adecuada custodia y reserva de la información y gestión -es decir tratamiento- de los datos suministrados por CAMARA DE COMERCIO PALMIRA al interior de las redes, Servidores y bases de datos (físicas y/o electrónicas) en donde se realice su recepción y tratamiento en general.
SEXTA. Para el caso del manejo de información que incluya datos personales, LA PARTE IMPLICADA dará estricto cumplimiento a las disposiciones constitucionales y legales sobre la protección del derecho fundamental de habeas data, en particular lo dispuesto en el artículo 15 de la Constitución Política y la ley 1581 de 2012.
SÉPTIMA. En caso de que LA PARTE IMPLICADA incumpla parcial o totalmente con las obligaciones establecidas del presente acuerdo de confidencialidad, éste será responsable de los daños y perjuicios que dicho incumplimiento llegase a ocasionar a la CÁMARA DE COMERCIO PALMIRA.
OCTAVA. La vigencia del presente acuerdo de confidencialidad será indefinida y permanecerá vigente mientras exista relación entre ambas partes, si durante la presente vigencia del acuerdo LA PARTE IMPLICADA incumple el acuerdo aquí plasmado, el mismo se hará acreedor a la Pena Convencional establecida en la Cláusula Séptima del presente acuerdo de confidencialidad.

Para constancia se firma por las partes el día __ del mes _____ del año ____

Elaborado por: **Aceptado por:**

Área de tecnología de la información
Cámara de Comercio de Palmira

Nombre y Firma