POLITICAS DE OPERACIÓN Y SEGURIDAD DE LOS RECURSOS INFORMATICOS

Octubre de 2013

CAMARA DE COMERCIO DE BARRANQUILLA

Este documento establece las Políticas Generales a contemplar en el uso de los recursos y servicios de Tecnología de Información y Comunicaciones de la Cámara de Comercio de Barranquilla, para asegurar la integridad y disponibilidad de la infraestructura tecnológica y la confidencialidad e integridad de la información que opera a través de ella.

Elaboró (Nombre y Cargo): Marco Albarracin Reinoso - Ingeniero de Infraestructura de TI	Revisó(Nombre y Cargo): Augusto Melendez Ferrigno – Director de Operaciones, Tecnología e Innovación	Aprobó (Nombre y Cargo): Augusto Melendez Ferrigno – Director de Operaciones, Tecnología e Innovación

Contenido

POLITICAS DE OPERACIÓN Y SEGURIDAD DE LOS RECURSOS INFORMATICOS

CAMARA DE COMERCIO DE BARRANQUILLA

PRESENTACIÓN

En la Dirección de Operaciones, Tecnología e Innovación de la Cámara de Comercio de Barranquilla (la CAMARA), y con el respaldo de la Presidencia Ejecutiva, trabajamos incansablemente para garantizar la protección de la información y de todos los elementos que facilitan su gestión laboral, asegurando la preservación de su *Confidencialidad, Integralidad y Disponibilidad,* contando para ello con:

- La participación y compromiso de todo nuestro equipo de trabajo
- La vinculación de proveedores especializados
- La adopción de las mejores prácticas en seguridad informática
- El desarrollo de planes de inversión en tecnología relacionada

La CAMARA provee a cada uno de sus funcionarios, un conjunto de herramientas informáticas, de hardware y software, para el desempeño de sus actividades laborales, así como el acceso a la información requerida. Constituyéndose cada uno de los equipos de cómputo, en parte fundamental del desarrollo eficiente de las actividades de todas y cada una de las direcciones y jefaturas que conforman la Entidad; por lo que es de vital importancia establecer y velar por el cumplimiento de las medidas o políticas necesarias para garantizar el uso adecuado de los mismos; así como de la información almacenada en ellos.

En el marco de estas medidas o políticas, es necesario destacar los servicios que se utilizan mediante la red Institucional, entre los que se encuentran:

- Internet
- Correo electrónico
- Sistema de Información del Registro Público
- Sistema de Información del ERP
- Sistema de Información de Gestión Humana
- Consulta y Actualización de bases de datos de otros sistemas de información con que pueda contar la Entidad, entre otros.

Un conjunto sólido de políticas informáticas es un componente vital de un sistema de colaboración. Sin importar cuántas barreras físicas o lógicas se empleen, la falta de lineamientos claros para la interacción entre seres humanos y sistemas, pueden hacer que las medidas de seguridad sean minadas rápidamente.

En la medida que crezca el uso de los nuevos servicios de comunicación y transferencia electrónica de información, la capacitación adecuada de los empleados y el cumplimiento de las políticas definidas, son la mejor manera de combatir y disminuir las amenazas en la seguridad de recursos informáticos.

Todos los empleados tienen la responsabilidad de asignar el tiempo y los recursos suficientes para la incorporación de las políticas y directrices que se dispongan para alcanzar y mantener los niveles de seguridad esperados. Así mismo, deben acatar esta intención, todos los terceros en los que se deposite la confianza para que le presten sus servicios a la CAMARA o que actúen en su nombre.

DISPOSICIONES GENERALES

1. Alcance de las Políticas de Operación. Las políticas de operación para el uso de los recursos informáticos son aplicables a todo el personal de la CAMARA, incluyendo a los prestadores de servicios profesionales bajo el régimen de honorarios, contratistas, personal contratado temporalmente, bien sea de manera directa o por bolsa de empleo, o todo aquel que tenga acceso bajo cualquier forma de remuneración o sin ella o en calidad de préstamo, a los equipos, dispositivos y herramientas de la CAMARA, y tendrán la responsabilidad de respetar y hacer respetar la privacidad y confidencialidad de la información y hacer un uso legítimo de ésta.

2. La Dirección de Operaciones, Tecnología e Innovación será la responsable definir y hacer seguimiento el cumplimento de las políticas informáticas, y de manera conjunta con la Jefatura de Gestión Humana, difundirá y mantendrá informados a todos los empleados de cualquier modificación o cambio en estas.

3. El empleado de la CAMARA deberá utilizar únicamente el equipo y programas de cómputo autorizados por la Dirección de Operaciones, Tecnología e Innovación, con la finalidad de garantizar la compatibilidad, estandarización e integridad de los recursos informáticos.

4. Queda prohibido instalar en los equipos de cómputo de la CAMARA cualquier tipo de software, reservándose de manera exclusiva esta función a la Dirección Operaciones, Tecnología e Innovación; es total responsabilidad del empleado cumplir con esta disposición, quien asumirá solidariamente la responsabilidad de dicha instalación de programas, con o sin licencia.

5. En adición a todas las políticas de la CAMARA, los empleados deben respetar y hacer respetar las legislaciones establecidas, la Ley y reglamento de Propiedad Industrial y las condiciones de licenciamiento del software institucional; así como todo lo establecido por la Ley Estatutaria 1581 De 2012, Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.

EQUIPOS DE CÓMPUTO (HARDWARE)

1. El proceso de asignación y uso de los equipos de cómputo, periféricos (mouse, teclado, parlantes, memorias), software y consumibles en materia informática, deberán contar con el visto bueno de la Dirección de Operaciones, Tecnología e Innovación.

   Queda prohibido a los empleados adquirir o arrendar bajo cualquier modalidad equipos de cómputo, en función de los proyectos y actividades desarrolladas, sin el visto bueno de la Dirección de Operaciones, Tecnología e Innovación.

2. Los equipos de cómputo instalados en las diferentes áreas de la CAMARA, como computadores de escritorio, computadores portátiles, servidores, impresoras, unidades de almacenamiento, ratones, switchs y cualquier otro dispositivo, sólo podrá ser utilizado por el personal de la CAMARA, para lo cual la Dirección de Operaciones, Tecnología e Innovación deberá contar con el inventario de resguardo por empleado. Para esto, cada empleado de la Entidad firmará un acta de entrega y custodia de los distintos dispositivos a su cargo.

3. Queda prohibido al personal, usar el equipo y servicios de información para fines distintos a aquellos a los que están destinados, y de acuerdo a las funciones institucionales encomendadas.

4. El empleado deberá realizar un uso adecuado del equipo de cómputo y los programas de software. Queda prohibido abrir físicamente el equipo, así como golpearlos y, en general, causar daños por negligencia o de manera intencional, ante lo cual podrá ser sancionado.

5. Los computadores portátiles asignados a los empleados deberán estar asegurados, con su respectiva guaya, el tiempo que se encuentren dentro de las instalaciones de la CAMARA y no estén en uso. Es responsabilidad del empleado, mantener asegurado los equipos portátiles a su respectiva guaya al final de cada jornada laboral. La clave de seguridad de las guayas es confidencial, y es responsabilidad del empleado mantener en secreto dicha clave de seguridad y no debe divulgarla bajo ninguna circunstancia a terceros, sean funcionarios de la CAMARA o no.

6. El equipo de cómputo debe estar siempre conectado a corriente regulada que se identifica con un tomacorriente de color anaranjado, anexo al puesto de trabajo. El empleado debe velar por esta conexión en forma permanente.

7. A cada equipo de cómputo conectado a la red se le asignara una *dirección IP dinámica*, por parte del Área de Operaciones, Tecnología e Innovación. Esta información no puede ser modificada por personal distinto al Área de Operaciones, Tecnología e Innovación.

8. Cada empleado será responsable del correcto uso de sus equipos, si se detecta alguna falla o mal funcionamiento del equipo, ésta deberá ser reportada inmediatamente a Soporte Técnico de Tecnología para la corrección del problema.

   Si la labor de reparación es menor, el empleado responsable del equipo asignado deberá estar presente en dicha reparación, lo anterior con el objeto de digitar su clave de manera discreta.

   Si el mantenimiento es de carácter superior, que amerite el retiro del equipo, y si resulta necesario obtener la calve de usuario para corregir el problema presentado, se levantará un acta en la cual el funcionario entrega la clave al encargado de la revisión, dicha constancia deberá reportarse a la Dirección de Operaciones, Tecnología e Innovación; de tal forma que cuando se entregue el

equipo después del mantenimiento, el empleado responsable asigne una nueva clave. La negligencia en este reporte acarrea sanciones por parte de la CAMARA.

9. Queda prohibida la salida de las instalaciones de la CAMARA de cualquier equipo de cómputo, periféricos y similares, sin la autorización y correcta ejecución del procedimiento que para tal efecto existe.

10. Queda prohibido el uso de equipos de cómputo personales en las instalaciones de la CAMARA. Y en relación a esto, queda prohibido tener información de la CAMARA en equipos personales.

PROGRAMAS DE CÓMPUTO (SOFTWARE)

1. Las herramientas de cómputo, como programas o paquetes utilizados en las actividades de la CAMARA, serán suministrados exclusivamente por el área de Operaciones, Tecnología e Innovación, la cual llevará el control del inventario de licencias de software por equipo.

2. La persona a la que se le asigne un equipo de cómputo, también será la responsable del resguardo del software instalado en ese equipo. Cualquier modificación o instalación de software, que no se encuentre en dicho resguardo y que no haya sido autorizado previamente por la Dirección de Operaciones, Tecnología e Innovación, será responsabilidad de la persona que tenga a su cargo el equipo.

3. Se prohíbe la instalación y empleo de cualquier software no autorizado o instalado por el área de Operaciones, Tecnología e Innovación. Incluyendo software de libre licencia o gratuita.

4. Aquella área que requiera de programas de cómputo en particular, deberá informar o solicitar a la Dirección de Operaciones, Tecnología e Innovación, la cual evaluará la procedencia de la compra de la licencia o autorización de uso, así como el control de su instalación y registro, los mismo aplicará para el caso de los programas con licencias libres (shareware y freeware), así como los desarrollos específicos que apoyen la realización de actividades institucionales.

5. El área de Operaciones, Tecnología e Innovación será la única que contará con los originales y/o copias de respaldo de los programas de cómputo institucionales. Los empleados de la CAMARA no podrán hacer copias personales de los instaladores del software de la Entidad.

6. En caso de falla del software, los empleados deberán tomar nota de los mensajes de error o de las fallas en general, y reportar de inmediato tal situación al área de Soporte Técnico para su atención y solución.

7. Queda prohibido borrar o alterar archivos pertenecientes a los programas de los aplicativos, paquetes de suites de oficina, sistemas operativos y archivos de configuración del equipo.

8. Cada empleado deberá realizar los respaldos de la información contenida en su equipo periódicamente, para ello, el área de Operaciones, Tecnología e Innovación podrá apoyar, previa solicitud.

INFORMACIÓN

1. La información sólo deberá ser accedida por quienes la necesiten para el cumplimiento de sus funciones y debe ser protegida, aplicando todos los controles definidos en este documento y otros mecanismos que se consideren necesarios para evitar que sea expuesta a personas no autorizadas.
2. No se podrá fotocopiar, copiar, microfilmar, digitalizar o de otra manera reproducir la información de la CAMARA o de sus clientes, para fines diferentes a las actividades propias del negocio, en todo caso previa autorización del jefe inmediato.
3. Cuidados en el puesto de trabajo: La información confidencial o restringida debe tratarse como tal, por tanto, no debe dejarse expuesta o permanecer en lugares donde pueda ser accedida por personal no autorizado. Para su almacenamiento debe utilizarse un lugar seguro, cerrado o bloqueado dependiendo del formato (físico o electrónico). No debe divulgarse a personas no autorizadas, no debe entregarse por vía telefónica o electrónica (e-mail, chat, etc.) si no se cuenta con un mecanismo de verificación de la identidad del destinatario.

CORREO ELECTRÓNICO

La CAMARA cuenta con la plataforma de correos Microsoft Outlook. El servicio se otorga mediante la asignación de una dirección de correo electrónico institucional la cual se podrá acceder mediante un nombre de usuario y una contraseña asociada. Este servicio tiene como función ofrecer una herramienta de comunicación digital para la transferencia de información y documentos entre los empleados de LA CAMARA y el entorno, en función a las actividades que realiza en la Institución.

1. La CAMARA ha asignado a sus empleados, que así lo requieran para el desempeño de sus funciones, una dirección de correo electrónico institucional que contiene la identidad del dominio "camarabaq.org.co". Las cuentas de correo electrónico institucional deben ser solicitadas por los jefes de área a la Dirección de Operaciones, Tecnología e Innovación.
2. Se podrán otorgar cuentas de correo individuales o genéricas, según las necesidades del empleado.
3. Esta dirección de correo electrónico deberá ser utilizada exclusivamente para asuntos de la CAMARA, en forma responsable. Por tanto, no está autorizado el uso de las direcciones electrónicas que incluyan el dominio "camarabaq.org.co", para recibir y enviar mensajes personales, más aún cuando estos incluyan archivos de gran tamaño (fotos, videos, programas, música, etc.) y que también generan el ingreso de correo basura o no deseado (spam), que además congestionan el servidor de correo y demandan una gran cantidad de recursos de cómputo.
4. El empleado deberá notificar de manera inmediata si detecta el uso indebido o no autorizado de su cuenta de correo por terceras personas.
5. El empleado será responsable de revisar y depurar su buzón de correo periódicamente, a fin de evitar que el mismo se sature.
6. El empleado no enviará información de la CAMARA a su correo personal.
7. El empleado no hará réplica del correo de la CAMARA a su correo personal y viceversa.

ACCESO A INTERNET

La CAMARA provee a los empleados, que así lo necesiten para su trabajo cotidiano, un acceso a Internet de alta velocidad.

1. El uso y manejo que debe dársele a este acceso, es única y exclusivamente para apoyar los trabajos que se le han asignado al empleado.
2. Aunque se encuentra debidamente controlado el acceso a internet por lo servidores de la CAMARA, queda absolutamente prohibido:
    a. Acceder a sitios de sexo, pornografía, farándula, noticias de entretenimiento, tanto escritas como a través de audio (emisoras de radio y TV) o cualquier otro sitio nocivo y de servicios que no sean de utilidad para la Institución, y que degraden la calidad y agilidad de la red de los servicios de Internet.
    b. Instalar y utilizar Messenger, Skype, ICQ o cualquier otro tipo de software que permita realizar chats o intercambio de información cifrada.
    c. Descargar archivos de música y/o de vídeo en cualquier formato.
    d. Descargar e instalar juegos y demás software (freeware o shareware) no adquirido por la CCB.
    e. Acceder a correos electrónicos personales a través de los equipos de cómputo de la CAMARA.

Para garantizar el estricto acatamiento a esta directriz, el Área de Operaciones, Tecnología e Innovación realizará permanentemente monitoreos aleatorios sobre los mensajes de correo enviados y recibidos por todos los empleados, de los sitios web que visitó y el ancho de banda usado por cada PC y determinar el acceso a emisoras de radio. Estos monitoreos generarán reportes para el Departamento de Gestión Humana, dependencia que tomará las medidas pertinentes.

ANTIVIRUS

Este servicio tendrá como finalidad proteger los servidores de la CAMARA de ataques de virus y de mensajería no deseada. Es por esto que la CAMARA ha instalado en todos los equipos de cómputo o terminales de trabajo un software de antivirus, el cual se actualiza automáticamente.

1. Como medida preventiva los empleados deberán abstenerse de abrir o enviar archivos extraños y posiblemente dañinos que sean recibidos en su buzón electrónico. En caso de sospecha deberán notificar al área de Operaciones, Tecnología e Innovación, para su atención, prevención, corrección y registro.

2. Estará alerta de los correos electrónicos que reciba y desconfiará de aquellos correos de procedencia desconocida, o de un conocido con un 'Asunto' poco habitual en él, se debe comprobar su procedencia real antes de abrirlo.

3. No contestará mensajes spam (publicidad no deseada), ya que al hacerlo reconfirmará su dirección de correo. De igual modo, no distribuirá cartas en cadena, ya que esto puede causar diversos efectos como la sobrecarga de la red, del servidor de correo y además la molestia de los empleados al inundarle su buzón con muchos correos no deseados.

4. Queda prohibido la desinstalación y/o desactivación del software antivirus en cualquier PC o terminal de trabajo de la institución.

ASIGNACIÓN Y RESGUARDO DE CLAVES DE ACCESO PARA PROGRAMAS DE CÓMPUTO (SOFTWARE) INTERNOS

Responsabilidades de los empleados

Las funciones y obligaciones de cada uno de los empleados con acceso a los datos y a los sistemas de información, son claramente definidas por su jefe inmediato. En la inducción inicial se le dará a conocer las normas de seguridad establecidas y las consecuencias de su incumplimiento mediante un documento que debe ser firmado y conservado en su Hoja de Vida.

- El sistema mantendrá una bitácora o historial de cada una de las acciones y/o transacciones que realizó cada empleado, por lo que cada empleado es directamente responsable de las actividades hechas con su clave, tales como: ingresos, modificaciones y retiros en los datos, envíos de correos electrónicos, cualquier posible virus y por consiguiente cualquier pérdida o daño de información hechos con su clave personal.
- El administrador del sistema tendrá derecho de acceder y examinar los archivos de los empleados, en los casos de que exista cualquier sospecha de violación a cualquiera de las presentes políticas, infección de virus, o de la existencia de materiales nocivos para la CAMARA, previa autorización o solicitud del titular del área examinada.

Asignación de usuarios y claves

Los jefes de área serán los autorizados para solicitar a Tecnología, vía correo electrónico, la apertura y asignación de los nuevos usuarios de los sistemas de información y otros servicios como Internet, cuentas de correo institucional, Office y demás herramientas informáticas. La solicitud debe ir dirigida al Director de Operaciones, Tecnología e Innovación, a la Jefe de Informática y al Ingeniero de Infraestructura TI, indicando los privilegios y opciones de manejo que tendrá a su cargo el nuevo empleado y el nivel de responsabilidad sobre la información (consultar, actualizar, modificar, agregar o suprimir). El área de Operaciones, Tecnología e Innovación se encargará de que exista una relación actualizada de empleados que tengan acceso autorizado a los sistemas de información y establecer la seguridad y encriptación de las claves o contraseñas.

Vacaciones, traslados y retiros de empleados

El departamento de Gestión Humana informará a Operaciones, Tecnología e Innovación cada vez que un funcionario cumpla con los siguientes casos:

- Vacaciones y licencias: El área de Tecnología desactivará el empleado y clave del empleado hasta que se reintegre a sus labores. El jefe inmediato informará a Tecnología, vía correo electrónico, la reactivación del empleado.
- Traslados: Tecnología desactivará las opciones con las que venía trabajando y le creará las de su nuevo cargo.
- Retiros: Tecnología desactivará en forma definitiva el empleado del empleado que es retirado la CCB.

Manejo de usuarios y claves

Para propender al manejo adecuado y seguro del usuario/clave deben seguirse los siguientes lineamientos:

- El usuario del equipo de cómputo, deberá establecer una contraseña personal o clave de acceso al equipo, con la finalidad de evitar el uso del mismo por parte de terceros; así como de asegurar la confidencialidad de la información. Por lo tanto, la clave asignada a cada computador es confidencial, y es responsabilidad del empleado mantener en secreto dicha clave de acceso y no debe divulgarla bajo ninguna circunstancia a terceros, sean funcionarios de la CAMARA o no. En este mismo sentido, los empleados de la CAMARA se abstendrán de utilizar la clave secreta de acceso al sistema de otro funcionario, con o sin su consentimiento.
- El ingreso y la utilización de la(s) clave(s) de acceso al sistema es (son) de uso exclusivo de su titular y no podrá(n) ser divulgada(s) a otros empleados y/o a terceros. Cualquier acción u omisión frente a la custodia y guarda de las mismas, recaerá sobre la persona responsable de aquella.
- El empleado deberá cambiar su contraseña, siguiendo las políticas de contraseña robusta establecidas por la administración del servicio, es decir que no deberán colocar como contraseña palabras asociadas a su vida personal (ej: nombre de hijo, esposo, mascota, fecha de nacimiento, número de teléfono, cédula de identidad, etc.), ya que éstas son fáciles de averiguar o adivinar. Tampoco se deberán escribir las contraseñas en cualquier lugar donde alguna persona pueda visualizarla fácilmente, lo recomendable es memorizarla pero en caso de que no se pueda, entonces anotarla y resguardarla de modo seguro.
- El empleado deberá cumplir las normas y políticas de control y seguridad de los sistemas informáticos de la CAMARA.
- Cualquier incumplimiento o violación de estas obligaciones acarreará sanciones laborales tales como llamados de atención, suspensiones e inclusive la terminación del contrato de trabajo con justa causa de acuerdo con lo consagrado en el Código Sustantivo de Trabajo.
- Las claves de los empleados se cambiarán con una periodicidad de 30 días y se almacenarán de forma ininteligible en los sistemas de información. El no cambiar las claves de acceso aumenta la posibilidad que persona no autorizadas las conozcan.
- La clave debe tener una longitud mínima de ocho caracteres (números, letras, caracteres como, * / & _ - “).
- No repetir las claves que se han utilizado en los últimos 12 meses, en caso de hacerlo el sistema mostrar un mensaje de advertencia.
- A los 5 intentos fallidos de autenticación la cuenta de usuario se deshabilitara automáticamente y solo el área de TI podrá habilitarla.
- Se tendrán 5 oportunidades para el cambio de la contraseña, una vez el sistema lo solicite. No cumplido el cambio en estas 5 peticiones, la cuenta y acceso a la red será inhabilitado.
- Cambiar la clave en caso de sospecha de que sea conocida por otras personas.

- Cada empleado podrá cambiar la contraseña de su cuenta las veces que desee, según lo crea conveniente.
- Los empleados se harán responsables de recordar la contraseña de su cuenta, si en algún momento el empleado la olvida o se le bloquea, tendrá que informar por escrito a la Dirección de Operaciones, Tecnología e Innovación con visto bueno del jefe de área y solicitar una nueva clave. Es responsabilidad del empleado cambiar inmediatamente le sea posible, la clave suministrada por el Área de Operaciones, Tecnología e Innovación.

EXCEPCIONES A LA POLÍTICA

Todas las excepciones a las presentes políticas deberán ser autorizadas por la Dirección de Operaciones, Tecnología e Innovación, previa solicitud por escrito del Director del Área.