1. ALCANCE

La política de seguridad de la información se aplica a toda información obtenida, creada, manipulada o administrada por la Cámara de Comercio del Cauca, dentro de sus Recursos de Información y los procesos core de la Entidad. Adicionalmente, esta política se aplica a toda la información que surge por las funciones, procesos y procedimientos generada por los Recursos de Información de la Cámara de Comercio del Cauca, durante el tiempo de transferencia hacia un agente externo de la organización o durante su propia disposición y destrucción. Esta política se aplica igualmente a todo el personal de la Cámara de Comercio del Cauca y a todos los usuarios externos autorizados a acceder a los recursos de Información de la organización.

2. DEFINICIONES

Información: Toda información, independientemente de su forma, que es creada, almacenada o procesada por los recursos de información, redes de comunicaciones y datos o medios de almacenamiento

Recursos de Información (RI): Todo equipo de cómputo, impresiones, recursos en línea, medios de almacenamiento magnético y todas las actividades relacionadas con sistemas de cómputo, incluyendo cualquier dispositivo capaz de recibir e-mails, navegación en la web, o con capacidad de recepción, almacenamiento, manejo, o transmisión electrónica de datos, por ejemplo y no limitado a: servidores, computadores personales, computadores portátiles, computadores de mano, asistentes personales portátiles (PDA), smart phone, sistemas de procesamiento distribuido, redes de datos, recursos de telecomunicación, teléfonos, equipos de fax e impresoras. Adicionalmente, son considerados como Recursos de información: los procedimientos, los equipos, instalaciones físicas, software, y data que sean diseñados, producidos, operados y mantenidos para crear, recolectar, grabar, procesar, almacenar, recuperar, desplegar y transmitir información.

3. DESARROLLO

3.1. APLICACIÓN DE LAS POLÍTICA

La Cámara de Comercio del Cauca protegerá todos los Recursos de Información de la organización de acuerdo con las políticas definidas.

Específicamente, la organización aplicará políticas, procedimientos, buenas prácticas, estándares y guías para proteger las funciones de los RI de datos internos, errores de programación, mal manejo por individuos dentro o fuera de la Entidad. Esto con la finalidad de proteger a la organización de riesgos que comprometan la integridad de los

COPIA NO CONTROLADA

programas, violación de los derechos individuales a la privacidad y confiabilidad, violación del derecho penal o de potenciales daños a la seguridad pública.
Todos los programas de seguridad de los recursos de información asociados a la organización serán responsables y adaptables a los cambios tecnológicos que afecten los recursos de información.

3.2. VIOLACIONES

Cualquier evento que resulte en robo, pérdida o uso desautorizado, declaración no autorizada, modificaciones desautorizadas, destrucciones desautorizadas, o acceso a RI denegados, constituyen una violación de la seguridad y su confidencialidad. Estas violaciones pueden incluir, pero no limitarse, a las siguientes:

- Exponer a la organización a actuales o potenciales pérdidas monetarias comprometiendo la seguridad de los RI.
- Involucrar las declaraciones de información sensible o confidencial o el uso no autorizado de datos o recursos de la organización.
- Incluir el uso de los RI para beneficio personal, no ético, dañino o con propósitos ilícitos.

3.3. ROLES Y RESPONSABILIDADES

Área de Tecnología: área responsable de la gestión y administración de los recursos de información de la CAMARA DE COMERCIO DEL CAUCA. La designación del área de Tecnología está dirigida a establecer la responsabilidad de diseñar e implementar políticas para el manejo de los recursos de información, proveer una mejor coordinación de las actividades que involucren acceso, procesamiento y administración de la información dentro de la organización, y para asegurar una mejor orientación de tales actividades dentro y fuera de la misma. El área de tecnología tiene la autoridad y responsabilidad para implementar Políticas de seguridad, procedimientos, prácticas, estándares y guías para proteger los Recursos de Información de la empresa.

Propietario: Es el gerente, director o usuario responsable de las funciones que tienen que ver con el manejo y soporte de los recursos, las personas a los cuales se les responsabiliza de llevar a cabo los programas que utilizan los recursos de información. El propietario es responsable de establecer los controles que provean la seguridad. Dependiendo sea el caso, la propiedad puede ser compartida por gerentes o directores de diferentes áreas o departamentos.

Usuario: Tiene la responsabilidad de (1) usar los recursos sólo para los propósitos establecidos por el propietario y la organización, (2) cumplir con los controles establecidos por el propietario y la organización y (3) prevenir declaraciones de información

COPIA NO CONTROLADA

confidencial o sensible. El usuario es la persona que ha sido autorizada para leer, ingresar o actualizar información, por el propietario de la información.

4. POLÍTICAS ESTÁNDAR

a. Los controles de seguridad de los RI no deben ser obviados o inutilizados.

b. La conciencia de seguridad del personal debe ser continua, reforzada, actualizada y validada.

c. Todo el personal es responsable por el manejo y el uso de los RI y por los actos relacionados a la seguridad de los mismos. El personal es igualmente responsable de reportar cualquier sospecha o confirmación de violaciones o manejo inapropiado de las políticas de seguridad de la información.

d. Las contraseñas, números de identificación de personal (PIN), claves de seguridad (tarjeta inteligente de seguridad), y otros procedimientos y dispositivos de seguridad en los sistemas de información deben ser protegidos por el usuario. Toda violación de seguridad debe ser reportada al responsable o director encargado y/o al área de tecnología.

e. El acceso al cambio y el uso de los RI debe ser estrictamente seguro. La autorización para acceso a la información para cada usuario debe ser revisada regularmente, así como el cambio de status del trabajador como: transferencia, promoción, baja o culminación de sus actividades.

f. El uso de los RI debe ser oficialmente autorizado. No existe garantía de privacidad personal o acceso a herramientas como e-mail, navegación en internet, y otras herramientas de discusión electrónica. El uso de estas herramientas de comunicación electrónica puede ser monitoreado para realizar o esclarecer reclamos o procesos de investigación. Las direcciones o áreas que tienen a cargo el manejo de computadores, deben ser responsables de la adecuada utilización de los RI, el efectivo manejo del mismo, y de reportar su estado y manejo.

g. Cualquier información utilizada en un sistema de los RI, debe ser mantenida con confidencialidad y seguridad por el usuario. El hecho de que la información sea almacenada electrónicamente no cambia el requerimiento de mantener la información segura y confiable. Más bien, el tipo o clasificación de la información por sí misma es la base para determinar si la información debe guardarse en forma confidencial y segura. Adicionalmente, si esta información es almacenada en un papel o un formato electrónico, o si la información es copiada, impresa o trasmitida electrónicamente debe ser protegida como confidencial y segura.

h. Al término de la relación de trabajo con la Entidad, los usuarios deben entregar todos los bienes y RI asignados por la organización. Se deben aplicar todas las

COPIA NO CONTROLADA

políticas de seguridad de los RI y relacionadas con el evento de culminación de relaciones laborales hasta que la devolución sea realizada. Así mismo, esta política da por terminada toda relación.

i. El propietario debe comprometer al director del área de tecnología y recibir su visto bueno, a la elaboración de cualquier proyecto de adquisición de hardware, compra o desarrollo de software para la organización. Los costos de las adquisiciones, desarrollo y operación del hardware y aplicaciones, deben ser autorizados por la Presidencia. La Presidencia Ejecutiva y las áreas solicitantes deben actuar dentro de sus límites de aprobaciones de acuerdo con las políticas de autorización de compras de la organización.

j. La dirección o área que requiera o autorice una aplicación de computador, debe cumplir con los pasos apropiados para asegurar la integridad y seguridad de todos los programas y archivos de información creados u obtenidos por las aplicaciones de cómputo.

k. La red de RI es responsabilidad del área de tecnología y debe ser controlada por la misma. Las aprobaciones deben ser obtenidas del área de tecnología antes de conectar a la red un recurso que no cumpla con las guías o estándares de la red publicados. El área de tecnología se reserva el derecho de remover de la red cualquier recurso que no cumpla con los estándares o que no sean considerados como adecuadamente seguros.

l. La venta o alquiler de aplicaciones de cómputo o datos, incluyendo lista de e-mail y directorios telefónicos, a otras personas u organizaciones debe cumplir con todas las políticas y procedimientos legales y fiscales de la organización y las leyes nacionales existentes en particular, la Ley 1581 y 1276 de protección de datos personales.

m. La integridad del uso general de software, utilidades, sistemas operativos, redes y archivos de información, son responsabilidad de cada uno de las direcciones o áreas en que se encuentra dividida la Entidad. Los datos para pruebas y con propósitos de investigación deben ser autorizados por la Presidencia Ejecutiva.

n. Todos los cambios o modificaciones en los sistemas de RI, redes de datos, programas o datos deben ser aprobados por el área encargada, la cual es responsable de su integridad.

o. El Área de Tecnología en conjunto con la Presidencia Ejecutiva debe proveer los controles de acceso adecuados para monitorear los sistemas y proteger la información y programas de malos manejos de acuerdo con las necesidades definidas por los propietarios o usuarios. El acceso debe estar correctamente documentado, autorizado y controlado.

p. Todas las direcciones o áreas deben evaluar cuidadosamente los riesgos de cambios

COPIA NO CONTROLADA

desautorizados, declaraciones desautorizadas, o pérdida de los datos de los que son responsables, y asegurar a través del uso de sistemas de monitoreo, que la organización esté protegida contra daños u otros. El propietario de las aplicaciones y el área de tecnología deben contar con un back up apropiado y planes de contingencia para así contrarrestar desastres o riesgos de daños o perjuicios basados en los requerimientos de la organización.

q. Los sistemas de cómputo de los RI y equipos asociados, utilizados para los fines de la organización, y que son operados y administrados fuera del control de la Entidad, deben cumplir requerimientos contractuales y estar sujetos a monitoreo.

r. El acceso externo desde y hacia los RI debe cumplir las guías de seguridad apropiadas y publicadas por la organización.

s. Todo software comercial utilizado en los sistemas de cómputo debe contar con acuerdos de licencias de software, que describan los derechos de uso y las restricciones del producto. El personal debe cumplir con todas los acuerdos de licencias y no debe realizar copias ilegales del software. El área de tecnología se reserva el derecho de remover cualquier software sin licencia de los RI.

t. El área de tecnología se reserva el derecho de remover cualquier software o archivos de cualquier sistema de cómputo, no relacionado con el negocio o fines de la organización. Ejemplos de este software son: juegos, programas instant messengers o chat, pop e-mail, archivos de música, fotos, freeware y shareware.

u. Las adherencias a todas las otras políticas, prácticas estándar, procedimientos y guías utilizadas, como soporte de esta política de Seguridad de Información, es obligatoria.

5. REFERENCIAS

ISO 27001:2013 Estándar
Revisión de Estándares y Publicación de Recomendaciones.

COPIA NO CONTROLADA