1. OBJETIVO

Establecer los lineamientos internos de Seguridad de la Información para la Cámara de Comercio de Ibagué con el fin de asegurar los activos de información en todas sus formas y medios, contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de tal modo que se garantice la confidencialidad, la integridad y la disponibilidad de la información.

2. ALCANCE

La política aplica en todas las sedes de la Cámara de Comercio de Ibagué, es decir, a todo el personal, tanto interno como externo; así como a las personas que directa o indirectamente, prestan sus servicios profesionales dentro de la misma; igualmente a toda la información creada, obtenida, procesada, almacenada o intercambiada dentro y desde la entidad.

Este documento se aplica a todas las fases del ciclo de vida de la información: La generación, la distribución, el almacenamiento, el procesamiento, el transporte, la consulta y la destrucción de la información, al igual que los sistemas que la procesan.

3. DEFINICIONES Y ABREVIATURAS

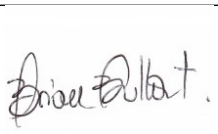
Integridad de la Información: Se refiere a la exactitud y fiabilidad de los datos.

Nivel de acceso: Grupos de derechos establecidos por un administrador de un sistema de información de acuerdo con el perfil del usuario.

Drive: Servicio de alojamiento de archivos en la nube.

Nube: Red de servidores remotos conectados a internet para almacenar recursos informáticos.

Streaming: Tipo de tecnología multimedia que envía contenidos de video y audio a un dispositivo conectado a internet.

			INTRANET / SGC / PROCESO / GERENCIAL / POLITICAS
CARLOS FERNANDO NIÑO ARTEAGA	**JOHN JAIRO DUSSAN RAMOS**	**BRIAN BAZIN BULLA TOVAR**	
ELABORÓ	**REVISÓ**	**APROBÓ**	**UBICACIÓN DEL DOCUMENTO**

Data Center: Centro de datos que tiene como función almacenar y distribuir información a través de servidores y equipos de comunicación.

Hacking: Conjunto de técnicas a través de las cuales se accede a un sistema informático vulnerando las medidas de seguridad establecidas originalmente.

4. RESPONSABILIDADES

Presidente Ejecutivo:

Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.

Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.

Impulsar entre los funcionarios de la CCI la divulgación de la Política de Seguridad de la Información.

Exigir el cumplimiento de la Política de Seguridad de la Información.

Considerar los riesgos de seguridad de la información en la toma de decisiones.

Equipo Humano de Tecnología:

Crear mecanismos a nivel TIC que restringa y controlen lo enmarcado en este documento.

Velar que los funcionarios en el desarrollo de sus actividades cumplan con los lineamientos establecidos en la presente política.

Atender todos los incidentes detectados o reportados relacionados con la seguridad de la información.

Funcionarios:

Comunicar al área de Tecnología cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información.

Informar al área de Tecnología cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente política.

5. DESARROLLO

Asignación de niveles de acceso

Se establecen los siguientes lineamientos para la creación, modificación y eliminación de los accesos a los sistemas de información, a la red y cuentas de correo electrónico, protegiendo la información de la organización:

Es responsabilidad de Talento Humano, reportar al área de Tecnología la relación de nuevos funcionarios contratados, para la asignación de usuarios según la necesidad, de igual manera cuando finalice el vínculo laboral.

El director de cada unidad deberá solicitar al área de Tecnología la asignación de usuario y acceso a los sistemas de información de acuerdo con el cargo del funcionario.

Cada usuario creado en los diferentes sistemas de información es generado de acuerdo con el cargo y los privilegios según las funciones asignadas.

Una vez es confirmado el retiro del funcionario, los accesos deben ser bloqueados en un tiempo no mayor a 20 minutos, por parte de Tecnología.

Uso de Internet

El uso de internet deberá ser únicamente para el cumplimiento de las labores asignadas y no podrá ser utilizado con fines diferentes, de igual manera se espera que su utilización se realice bajo los principios éticos establecidos por la entidad.

El acceso a internet será asignado de acuerdo con el cargo del funcionario.

No se permite el acceso a sitios web pornográficos, contenido multimedia, juegos, apuestas, armas, drogas, hacking y/o similares.

El acceso a páginas, streaming o cualquier contenido multimedia especializado debe ser solicitado previamente por el funcionario justificando las razones de acceso con el desarrollo de sus funciones.

Las redes sociales están restringidas de acuerdo con el perfil del funcionario.

No es permitido realizar descargas de programas, aplicativos y/o similares sin la autorización previa del equipo humano de Tecnología.

No es permitido el uso de conexiones a internet por medio de modem, mi-fi y/o celulares desde las instalaciones de la entidad, por lo cual siempre deben salir a este servicio a través de la red interna.

La entidad se reserva el derecho de auditar las acciones ejecutadas en la red por cualquier funcionario y sus resultados debe ser reportados al director de la unidad respectiva.

Todos los incidentes de seguridad relacionados con el acceso y uso de internet deben ser reportados al equipo humano de Tecnología, por medio de la plataforma de tickets o al correo electrónico.

Uso de Drive

Según comunicación interna (08 de febrero de 2019) de la presidencia, toda la información generada como producto de las labores en la entidad, debe reposar en el Google Drive que pertenece a la cuenta de correo electrónico del funcionario. No es permitido almacenar información institucional fuera de este almacenamiento en la nube.

Uso de correo electrónico

Los funcionarios deben usar el correo electrónico corporativo asignado para enviar o recibir comunicaciones de acuerdo con sus funciones y responsabilidades. Por lo anterior, queda

prohibido el uso del correo personal para cualquier tema institucional. De igual manera, el correo de la entidad no debe ser utilizado para guardar información de índole personal.

La asignación de correo electrónico se realizará de acuerdo con solicitud del director de unidad.

Las cuentas de correos serán creadas con el nombre del cargo, según consideración previa del director.

La CCI es la propietaria de los datos transmitidos o almacenados en las cuentas de correo electrónico.

Uso web

El sitio web de la entidad hace parte de los medios de comunicación masiva institucional. La página: www.ccibague.org tiene como función fundamental informar a todos los empresarios y a los usuarios externos, a nivel local, nacional e internacional durante las 24 horas del día sobre lo referente a la actualidad empresarial, a través de noticias, eventos, formación empresarial, convocatorias y diferentes formatos de interés general. Además, realizar trámites de forma virtual a través del sitio.

De igual manera, información relacionada con las dependencias, sedes, datos de contacto, PQRSF, etc.

Administradores: La administración está a cargo del área de Tecnología y Comunicaciones.

Tecnología: Es el administrador general y cuenta con todos los privilegios para realizar cualquier cambio sobre el sitio web.

Comunicaciones: Cuenta con los permisos para realizar cambios en las secciones de: Noticias, eventos, programas y capacitaciones.

Impedimentos y permisos: El área de Tecnología y Comunicaciones se reservan el derecho de impedir publicaciones que atenten contra la reputación y el bueno nombre de la Cámara de Comercio de Ibagué de manera directa o indirecta.

Publicación de contenidos: Las solicitudes se podrán realizar a través de la plataforma de tickets o vía correo electrónico. Una vez que la solicitud haya sido atendida y publicada en el sitio web, se notificará por el cierre del ticket o por correo electrónico al solicitante.

Protección de Virus

Proteger los recursos de la organización contra la intrusión de virus y de otros programas maliciosos, garantizando la seguridad de los datos y los recursos de la organización:

Es responsabilidad del área de Tecnología definir y actualizar el antivirus de toda la organización.

Es responsabilidad del área de Tecnología diseñar e implementar un plan para el manejo de incidentes de seguridad que cubra los incidentes de virus.

Es responsabilidad del área de Tecnología supervisar la eficacia de los sistemas de protección antivirus, así como llevar un registro detallado de incidentes.

Uso de dispositivos móviles

La entidad establece las directrices y uso de manejo de dispositivos móviles (Teléfonos inteligentes, tabletas), entre otros, suministrados por la CCI.

Los usuarios no están autorizados a cambiar la configuración

No es permitido utilizar el celular institucional para enviar comunicaciones con contenido ilegal, al igual que descarga de juegos, aplicaciones no autorizadas e imágenes que no corresponden a la organización.

Es responsabilidad de cada funcionario, velar por el buen uso y cuidado del dispositivo móvil asignado.

Uso de impresoras y del servicio de impresión

Asegurar la operación correcta y segura de las impresoras.

Los documentos que se impriman en las impresoras de la CCI deben ser de carácter institucional.

Es responsabilidad del usuario (Una vez recibida la capacitación) conocer el adecuado manejo de los equipos de impresión para no afectar su correcto funcionamiento.

Ningún funcionario debe realizar labores de reparación o mantenimiento de las impresoras.

En caso de presentar alguna falla, debe reportarse a través de la plataforma de tickets al área de Tecnología.

Seguridad Física y del Entorno

Los espacios físicos donde se ubiquen los centros de datos o de cableado deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medida preventivas de manera que pueda evitarse o mitigar el impacto de incidentes de seguridad (Accesos no autorizados, robo o sabotaje) y accidentes ambientales (Incendios, inundaciones, cortes de suministro eléctrico, etc.).

En las instalaciones del centro de datos o de los centros de cableado, no está permitido:

Fumar dentro del Data Center.

Introducir alimentos o bebidas al Data Center.

Mover, desconectar y/o conectar algún equipo sin autorización.

Modificar la configuración de algún equipo sin autorización.

Cada gabinete contiene una llave de ingreso, la cual debe reposar en la oficina de Tecnología.

Mesas limpias

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

Bloquear la sesión de los equipos cuando el funcionario deje el puesto de forma automatizada mediante la configuración del bloqueo de pantalla.

Mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.