1 CONDICIONES GENERALES

La Cámara de Comercio de Sincelejo se ha comprometido con la implementación de buenas prácticas de Seguridad de la Información, de obligatorio cumplimiento para todos los empleados y aliados de la organización que realizan actividades dentro del alcance.

Con este documento se pretende establecer los lineamientos para asegurar el uso efectivo de las comunicaciones y asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información.

2 DEFINICIONES

Confidencialidad	Característica que indica que el activo de información solo sea accedido por el personal, procesos, sistemas o entidades que se encuentran autorizadas.
Tercero	Proveedores de TI relacionados con el CORE del negocio y que prestan servicios a los procesos dentro del alcance de seguridad de la información..
Información	Todo aquel conjunto de datos organizados en poder de la organización que poseen valor para la misma

3 ALCANCE DE LA POLÍTICA

La presente política debe ser cumplida por los directivos, colaboradores y terceros que desempeñen actividades dentro del alcance y buenas prácticas de seguridad de la información (SI).

DESCRIPCIÓN DE LA POLÍTICA

A13.1 GESTIÓN DE LA SEGURIDAD DE LA RED

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.(ISO27001)

A13.1.1 Controles de red

Los controles de red y seguridad deben ser administrados por los colaboradores del área de tecnología o con ayuda de un tercero siempre bajo supervisión del responsable dentro cualquier cambio a los controles de red deben siempre seguir los procedimientos y políticas establecidas en la gestión de seguridad de la información.

Para las redes disponibles para el público y redes inalámbricas, se deben conservar los siguientes controles para mantener las conexiones (disponibilidad) y la privacidad (confidencialidad) y la integridad de los datos:

- Segmentos de red o VLAN diferentes a los de las estaciones de trabajo o data center
- Redes Wifi con filtrado web y contraseñas seguras WPA2
- Límite de conexiones a las redes.

La red eléctrica y de datos, debe estar adecuadamente protegida, con el fin de prevenir impactos potenciales que puedan causar la pérdida de disponibilidad de la información y los servicios.

MONITOREO Y REGISTRO

Se debe realizar monitoreo y registro de las actividades en la red con el fin de utilizarlo tanto para establecer medidas correctivas y si es necesario disciplinarias como para establecer medidas preventivas cuando se requiera.

CONTROL DE ACCESO

Se deben establecer medidas de autenticación segura a la red uso de contraseñas seguras WPA2 y adicional utilizar políticas de navegación por usuario del dominio según su rol y funciones del cargo.

Adicional siempre que los sistemas de información lo permitan se debe hacer uso de otras herramientas de autenticación en los sistemas como lo son doble factor de autenticación, telefonía móvil SMS, token, preguntas de seguridad y demás.

El acceso remoto a la red interna debe ser a través de una VPN.

CONTROL DE PRIVILEGIOS

Se debe restringir el acceso a los sistemas y a las conexiones de red según los privilegios asignados de acuerdo al rol y funciones del cargo.

A.13.1.2 Seguridad en los servicios de red

El área de Tecnología debe asegurar la disponibilidad del servicio de internet y dispositivos de red involucrados en la prestación de los servicios del alcance de las buenas prácticas de seguridad de la información, con el objeto de prevenir interrupciones que puedan causar impactos significativos en la continuidad de las operaciones.

Adicionalmente el área de tecnología tiene la responsabilidad sobre la gestión de todos los equipos de red de la organización (switch, router, UTM, servidores, etc).

13.1.3 Segmentación de las redes

La red LAN de estaciones de trabajo de los colaboradores debe ser independiente a la red Wifi de invitados, a la red de Voz Ip y la red de video para evitar acceso no autorizado a la información.

A13.2 TRANSFERENCIA DE INFORMACIÓN

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

A13.2.1 Políticas y procedimientos de transferencia de información

- La información transferida a otras entidades debe contar con los controles técnicos y físicos para evitar la interceptación, copiado, modificación, y destrucción no autorizada.

- Los colaboradores no deben emitir copias, divulgar, emplear indebidamente, o reproducir por cualquier medio, datos o información contenida en los aplicativos, bases de datos y sistemas de información a los cuales se le haya otorgado acceso, con fines diferentes al cumplimiento de sus funciones o labores contratadas.

- Se debe contar con mecanismos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.

- La información digital que sea transferida por entidades externas o terceros, debe ser revisada previamente con el fin de detectar posible malware o código malicioso.

- Se deberá utilizar métodos de criptografía para la información de carácter confidencial que deba ser transferida para proteger la confidencialidad, la integridad y la autenticidad de la información.

- El personal no debe tener conversaciones confidenciales en lugares públicos, o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión, entre otros.

- Es responsabilidad del personal, las partes externas y cualquier otro usuario no comprometer a la Cámara de Comercio, por ejemplo, por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.

A13.2.2 Acuerdos sobre transferencia de información

- Los procesos o áreas que requieran realizar transferencias de información a partes externas, deberán establecer los lineamientos para proteger, controlar y notificar la transmisión, despacho y recibo de la información, así mismo deberá establecer cláusulas de confidencialidad entre La Cámara de Comercio y las partes externas.
- Los datos e información creados, almacenados y recibidos, serán propiedad de La Cámara de Comercio, en este sentido, para transferir cualquier tipo de información clasificada o reservada se debe contar con autorización escrita del jefe inmediato.
- Copia, sustracción, eliminación, modificación, daño intencional o utilización de la información para fines distintos a las labores

institucionales, serán sancionadas de acuerdo con las normas y legislación vigentes, inclusive cuando se haya dado con posterioridad a la finalización del contrato.

A13.2.3 Mensajería electrónica

- El uso del correo electrónico debe contar con controles apropiados para mantener la confidencialidad, Integridad y disponibilidad de la información.
- Se debe contar con controles para la protección ante acceso no autorizado (mensajes encriptados etc.)
- Está prohibido el envío o transferencia de información confidencial de la Cámara de Comercio o sus clientes a través de redes sociales, servicios de mensajería instantánea y/o correo electrónico en texto plano.
- El correo corporativo es única y exclusivamente asignado para fines totalmente laborales y no debe darle uso diferente de este recurso entregado.
- No está permitido opinar en foros, o redes sociales a nombre de La Cámara de Comercio

A13.2.4 Acuerdos de confidencialidad o de no divulgación.

- Los requisitos de protección y no divulgación de la información se deben especificar en el documento ***"Acuerdos de confidencialidad"***. En el caso de los terceros estos requerimientos se deben establecer de forma contractual.
- Desde el proceso de Gestión del talento humano al momento de la contratación de un colaborador deberá hacer firmar los acuerdos de confidencialidad y no divulgación para ser incorporados como parte integral de los contratos laborales para proteger la información e informar a los firmantes acerca de su responsabilidad y acciones para evitar divulgar información no autorizada.
- Los acuerdos de confidencialidad y no divulgación de información son aplicables a todos los empleados y contratistas quienes deberán aceptar y firmar los acuerdos de la Cámara de Comercio.
- Los acuerdos de confidencialidad y de no divulgación deben cumplir todas las leyes y reglamentaciones aplicables.

- Los requisitos para los acuerdos de confidencialidad y de no divulgación se deben revisar periódicamente, y cuando ocurran cambios que influyan en éstos.
- Los acuerdos de confidencialidad y de deber de secreto hay que tenerlos firmados por escrito antes de iniciar una transferencia de información.