POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 3.

TABLA DE CONTENIDO

CONTROL DE VERSIONES

Versión	Fecha	Autor	Cambios	Revisado por	Aprobado por
V 1.0	29/05/2018	Andrés Santana	Creación	José Gil	José Gil
V 2.0	08/08/2022	Jaime Osorio Ruiz	Actualización	Javier Piedrahita	José Fernando Gil
V 3.0	23/03/2023	Jose Manuel Urrego	Actualización	Alexander Higuita	José Fernando Gil

1. Introducción

La Política de Seguridad de la Información, describe los principios, prácticas y directrices usadas en CSI. El propósito principal de nuestra política de seguridad es garantizar la confidencialidad, la integridad y la disponibilidad de la información, asegurando la continuidad del servicio ofrecido a nuestros clientes. Este documento está basado en los requerimientos y las recomendaciones definidas por la legislación nacional, requisitos y recomendaciones de seguridad y normas internacionales de buenas prácticas como ISO 27001:2013.
Todas las personas relacionadas con nuestra organización deben seguir las instrucciones de esta política de seguridad de la información. Estas personas son llamadas los usuarios y pueden ser empleados directos de CSI, consultores, contratistas, visitantes o cualquier persona que use nuestras instalaciones o sistemas de información.

2. Objetivo

Con el propósito de asegurar la confidencialidad, la integridad y disponibilidad de la información la presente política tiene como objetivo:

- Propender, asegurar y controlar el acceso físico y lógico sobre la información para que sólo las personas autorizadas puedan hacerlo según la clasificación de esta, asegurando que los métodos de proceso son exactos y completos, y esté disponible cuando se requiere para los autorizados.
- Administrar los procesos de seguridad física y lógica que intervienen en los procesos productivos del negocio.
- Definir y establecer los controles para el uso adecuado de los recursos físicos e informáticos, los cuales deben ser utilizados para las funciones e intereses del negocio.
- Establecer las medidas de control necesarias y razonables que permitan una adecuada gestión de la seguridad Física e Informática, así como el tratamiento de los riesgos asociados.
- Establecer seguimiento y monitoreo de los controles como auditoría, gestión de los planes de acción y mejoramiento de los procesos.

3. Alcance

La política de seguridad de la información de CSI, considera que la información es un activo que como otros activos importantes tiene valor y requiere una protección adecuada, la cual puede estar:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Trasmitida por correo o medios electrónicos
- Mostrada en filmes
- Hablada en conversación
- Alojada en la nube (Cloud)

Por esta razón debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparte o almacene.

4. Cumplimiento

La Política de Seguridad de la Información es de obligatorio cumplimiento por parte de todos los empleados y/o usuarios de los recursos físicos e informáticos.
El incumplimiento de la presente política por parte de los usuarios, cualquiera sea su vinculación con la compañía, será considerado como una violación grave de las obligaciones y prohibiciones que a éstos les asisten en relación con CSI., quien estará facultada para adoptar las medidas que estime conducentes y necesarias para sancionar dicho incumplimiento.

5. Responsabilidad

El incumplimiento de las políticas aquí descritas puede convertirse en una amenaza o vulnerabilidad para la compañía, exponiéndola a pérdidas financieras, de imagen y credibilidad ante sus clientes, accionistas y entes reguladores, por esto el cabal cumplimiento de estas hace parte de las responsabilidades de cada uno de los empleados y/o usuarios que interactúan con los recursos físicos e informáticos de la Compañía.
Los usuarios son responsables de familiarizarse y cumplir con las políticas de seguridad de la información, las inquietudes al respecto deben ser consultadas al rol encargado de TIC.

6. Actualización y Publicación

Este documento será revisado anualmente y modificado en la medida que se requiera y permanecerá publicado para su consulta para todos los empleados y terceros de CSI.

7. Área de Seguridad de la Información

Por lo valiosa que es la información que maneja CSI, asociada a nuestros clientes, productos, operaciones y corporativa; la compañía cuenta con un responsable de TIC asignado directamente por la Gerencia para asumir este rol.
La responsabilidad del rol del responsable de TIC es proteger y asegurar que la información tanto física como lógica preserve su confidencialidad, integridad, disponibilidad.

8. Misión Área Seguridad de la Información

Tiene la función de brindar los servicios de seguridad en la compañía a través de la planeación, coordinación y administración de los procesos de Seguridad Física e Informática, así como difundir la cultura de seguridad entre todos los miembros de la organización.

8.1 Objetivos Área Seguridad de la Información

- Definir la misión y la estrategia de la seguridad de la organización.
- Aplicar una metodología de análisis de riesgo.

- Definir la Política de seguridad de la información.
- Definir los procedimientos para aplicar la Política de Seguridad de la Información.
- Seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro de la misión establecida.
- Crear un grupo de respuesta a incidentes de seguridad de la información.
- Promover la aplicación de auditorías enfocadas a la seguridad.
- Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la organización.
- Crear un grupo de seguridad en la organización.

8.2 Responsabilidades Área Seguridad de la Información

- La administración y coordinación diaria del proceso de Seguridad de la información.
- Guiar al cuerpo directivo, a la administración y a los usuarios de la organización ante posibles incidentes de seguridad mediante un Plan de Respuesta a Incidentes.
- Proponer y coordinar un análisis de riesgos.
- Asegurar la adecuada selección de los mecanismos y herramientas de seguridad para fortalecer los controles de Seguridad Física e Informática.
- Implementación de procedimientos que permitan fortalecer la política de Seguridad de la Información.
- Mantener contacto con los Líderes de Seguridad de otras organizaciones.
- Promover la creación y actualización de las políticas de seguridad de la información.
- El desarrollo de un Plan de Seguridad.
- Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
- La elaboración de un Plan de Respuesta a Incidentes de Seguridad.
- Gestión de la Continuidad del Negocio.

9. Política de Seguridad de la Información

Para el logro de los objetivos de la presente política alineada con la estrategia de CSI, la Compañía ha establecido e implementado los siguientes controles y normas de seguridad, las cuales deben ser cumplidas por los empleados y demás funcionarios a la que va dirigida. Teniendo en cuenta lo anterior, la política se dará a conocer de manera oportuna a los empleados, contratistas, Outsourcing y proveedores con los que la compañía tenga vinculación para que sea aplicada.

Con la finalidad de dar cumplimiento a la política de seguridad de la información, se definen 3 pilares fundamentales los cuales rigen dispositivos/recursos y pasivos/activos que intervienen dentro CSI:

- Confidencialidad: Propiedad por la cual la información no esté disponible ni sea divulgada a individuos, organismos o procesos no autorizados.
- Integridad: Propiedad de proteger la precisión y la totalidad de los activos, información y métodos de procesos.
- Disponibilidad: asegurando a los usuarios autorizados el acceso a la información y a los recursos asociados al momento que se requiere.

9.1 Modelo de Gestión de Seguridad

La presente política se ha desarrollado teniendo en cuenta las buenas prácticas del sistema de gestión de seguridad de la información SGSI definida por la ISO27001:2012, donde el cual considera el siguiente plan de implementación:

1. Respaldo De La Dirección
2. Creación Del Proyecto
3. Identificación De Requerimientos
4. Alcance Y Objetivos De La Dirección
5. Metodología De Riesgos
6. Apreciación De Riesgos Y Plan De Tratamiento
7. Selección De Controles Del Anexo A
8. Plan De Implementación De Controles
9. Mecanismos De Medición De La Efectividad
10. Implementación Y Controles Y Procedimientos De Apoyo.
11. Capacitación Y Concienciación
12. Usar El SGSI
13. Supervisión Del SGSI
14. Auditorías Internas
15. Revisión Por La Alta Dirección
16. Procesos De Mejora Continua

El anexo A relacionado en el numeral 7 considera catorce (14) categorías, donde a su vez existen ciento catorce (114) puntos de control

ANEXO A

A5: Política de SI
A6: Organización de SI
A7: Seguridad de los Recursos Humanos
A8: Gestión de Recursos
A9: Controles de Acceso
A10: Criptografía
A11: Seguridad Física y Ambiental
A12: Seguridad Operacional (malware…)
A13: Seguridad de las Comunicaciones
A14: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
A15: Relación con los proveedores
A16: Gestión de Incidentes de SI
A17: Aspectos de SI de la gestión de continuidad del negocio.
A18: Cumplimiento

10. Controles Generales de Seguridad Corporativa

Estos controles están asociados con las prácticas que los empleados y terceros deben aceptar y responsabilizarse con su cumplimiento.

10.1 Protección de la Confidencialidad de la Información

CSI, en especial el área de Recursos Humanos deberá asegurar para todo el personal que ingresa a la compañía como nuevo empleado, la firma de las Actas de Confidencialidad de la información, que busca proteger la propiedad intelectual, la confidencialidad de la información de los clientes y de la compañía y el buen uso de los recursos informáticos para el estricto cumplimiento por parte de empleados o terceros. Así mismo la firma del formato de aceptación del código de ética.
Los jefes de área deberán hacer firmar el **ACUERDO DE CONFIDENCIALIDAD** cuando su contrato de servicio esté relacionado con el acceso, uso o administración de los recursos informáticos o de la información de la Compañía, según se delimite el alcance de sus funciones.

10.2 Política de Usuarios y Contraseñas

La compañía cuenta con la política de usuarios y contraseñas implementada en por el encargado de TIC para ejercer control de acceso sobre la red de datos y demás servicios, la cual restringe el ingreso no autorizado sobre los recursos informáticos. En caso de pérdida y olvido de contraseña, se debe notificar al encargado de TIC para realizar el cambio de esta asegurando que solo el usuario conozca la contraseña asignada. En caso de sospecha de que la contraseña fue comprometida, se debe notificar al responsable de TIC y reportar el incidente de seguridad a través de los medios que se dispongan en CSI ya sea correo electrónico, WhatsApp entre otros.

Las claves o contraseñas deben:

- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de la compañía, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Nunca utilice sus contraseñas personales en el entorno laboral.
- La contraseña debe tener mínimo ocho caracteres alfanuméricos.
- Cambiarse obligatoriamente la contraseña, la primera vez que el usuario ingrese al sistema.
- La contraseña debe cambiarse obligatoriamente cada 90 días, o cuando lo establezca el líder de TIC.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- La contraseña, no se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- La clave de acceso no debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo ¡,$,%,&)
- Las contraseñas de acceso, No ser reveladas a ninguna persona, incluyendo al líder de TIC.
- No registrar las contraseñas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

10.3 Gestión de Incidentes de Seguridad de la Información

Teniendo en cuenta el cumplimiento y aseguramiento de los criterios de Confidencialidad, Integridad y Disponibilidad de la información, CSI cuenta con un procedimiento de gestión de incidentes de seguridad y un grupo de respuesta de incidentes que permite notificar, registrar, resolver, valorar, evaluar, generar las recomendaciones y planes de acción a que haya lugar y monitorear los eventos que puedan afectar la seguridad de la información física y lógica.
Este procedimiento aplica para la gestión de todos los eventos e Incidentes de Seguridad de la Información relacionados con el tratamiento de datos personales al interior de la Empresa, iniciando desde el reporte hasta el cierre y finalización del incidente, comprendiendo las siguientes actividades:

- Reporte y registro del evento y/o incidente de seguridad de la información.
- Evaluación inicial del reporte.
- Análisis y evaluación del impacto.
- Aplicación de acciones de contención y acciones complementarias.
- Documentación de lecciones aprendidas.
- Notificación de cierre del evento y/o incidente.

Si el incidente de seguridad de la información se califica como delito ya sea por usuarios externos, empleados o terceros en general, la policía cuenta con la unidad de delitos informáticos y es con esta unidad que se puede iniciar un proceso de denuncia. https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

10.4 Control Solicitud Recursos Informáticos y Accesos

Dentro del proceso de Seguridad, se dispone de un procedimiento de control de accesos el cual permite el ingreso, cambios o retiros e inactivación de cuentas de usuario y accesos lógicos y físicos, los cuales son gestionados por el rol encargado de TIC o del responsable de administración del respectivo sistema de información.

10.5 Uso Adecuado de Recursos Informáticos

La compañía propende bajo la socialización de la presente política con los empleados y terceros, asegurar y controlar el uso adecuado de los mismos.
Como regla general, todos los recursos informáticos están disponibles exclusivamente para

uso interno y/o para asuntos relacionados con el negocio, no para uso personal.

No está permitido utilizar los recursos informáticos para:

- Almacenamiento o reproducción de música (en sus diferentes formatos), videos, películas, entre otros, de propiedad personal.
- Ejecución de juegos genéricos posiblemente incluidos dentro de los sistemas operativos, o que provengan de otras fuentes.
- Realizar cambios en la configuración estándar de los PC´s o dispositivos de computación.
- Instalar software o herramientas sin la debida autorización del responsable de TIC.
- Difamar, tergiversar o manifestar una impresión desfavorable de CSI, de sus filiales o los intereses de su negocio, empleados, proveedores, clientes, competidores o accionistas.
- Obtener ganancias o beneficios personales, o utilizados indebidamente durante el tiempo de trabajo.

Para mayor detalle, recomendamos leer el código de ética.

10.6 Computación Móvil (PC Portátil)

Normas para tener en cuenta para utilizar computación móvil según el sitio de trabajo, en el hogar, sitios públicos o vehículos. Además de tener en cuenta lo estipulado en el 10.7, considerar lo siguiente:

Normas generales para utilizar la computación móvil

- El sitio seleccionado para realizar actividades de computación móvil debe tener las siguientes características:
- Debe garantizarse un sitio de trabajo limpio y seguro.
- Evitar condiciones de humedad, frío o calor extremas que afecten los equipos.
- Debe estar alejado de sitios en los que exista gran concentración de partículas de polvo (arena, residuos de madera o rocas, etc.) o propensos a ser salpicados con cualquier tipo de líquido.
- No debe entrar en contacto directo con los rayos del sol.
- No consumir alimentos ni bebidas cerca de los equipos utilizados para computación móvil.
- No colocar los equipos portátiles sobre alguna parte del cuerpo para trabajar en ellos ya que esto bloquea la ventilación del equipo y puede generarle daños.
- Deberá siempre asegurar que el sitio en donde se colocan los equipos sea firme y estable, debe evitarse cualquier vibración o movimiento.
- Cuando se transporten equipos portátiles, no deberán ser almacenados en las áreas de equipaje. Debe procurarse al máximo que estos equipos permanezcan a la mano durante el período de viaje.
- Los equipos no deben permanecer encendidos cuando sean transportados, no importando la distancia que sea necesario moverlos. Debe evitarse dejar los equipos portátiles en vehículos, de tal manera que sean visibles desde el exterior, si se transportan

en vehículo particular, debe hacerse en la cajuela, no en las sillas.

- Excepto los equipos autorizados (Equipo directivo), los demás no deben ser instalados ningún tipo de dispositivos adicionales o periféricos a los equipos suministrados por la Compañía para actividades de computación móvil. Dentro de estas restricciones se incluyen:

    - Scanner
    - Joystick
    - Unidades de DVD o R/W.
    - Discos externos

En CSI

- Está prohibido el ingreso de equipos portátiles personales para ser operados dentro de las instalaciones de CSI, para conexión a la red, almacenamiento o procesamiento de información de propiedad de la compañía.
- Cuando se requiera el ingreso sólo de carácter especial, el responsable de TIC evaluará las condiciones y los riesgos.

En el hogar o en Teletrabajo

- Los equipos entregados por parte de CSI al empleado para actividades de computación móvil no deberán ser utilizados para nada diferente a trabajos relacionados con el negocio, esta restricción aplica para que no sean dispuestos a su grupo familiar o de amigos.
- El acceso general a Internet, para usos de recreación por parte de miembros de la familia o amigos del empleado, utilizando equipos para computación móvil a través de la red de CSI no está permitida. El empleado es responsable de asegurar que los miembros de la familia o amigos no violen ninguna de las políticas de seguridad informática de CSI, no realicen actividades ilegales y no usen el acceso para intereses de negocio ajenos a la Compañía.

En caso de Contingencia

- En caso de presentarse una evacuación en el lugar de trabajo siendo necesario dejar el equipo en estado desatendido, procure dejar bloqueada la estación.
- Mantener siempre copias de seguridad actualizadas de la información crítica del equipo utilizado para computación móvil. Estas copias deberán permanecer almacenadas en un sitio seguro.
- En caso de robo de equipos, deberá notificarse de inmediato al responsable de TIC para proceder a desactivar los usuarios y privilegios de ingreso a la red corporativa de la Compañía.

10.7 Control Bloqueo Automático Estaciones de Trabajo

Con el fin de ofrecer mayor seguridad, control de acceso y confidencialidad en las estaciones de trabajo (PC´s), se dispone del control de bloqueo automático de la pantalla, el cual se activará cuando el equipo se encuentre en estado inactivo durante 3 minutos. Esta medida busca mejorar la privacidad en los instantes en que dejamos desatendida la oficina o el puesto de trabajo y olvidamos bloquear el PC. Sin embargo, los usuarios por precaución deben bloquear manualmente el equipo en el momento de retirarte del puesto de trabajo.

Equipos que transporten información crítica, sensible o importante para la Compañía no deben dejarse desatendidos; en lo posible deben ser asegurados físicamente o utilizar lugares seguros de almacenamiento (casilleros). Esto evitará el robo de los equipos o de la información que ellos tengan almacenada. Cuando sea necesario dejar el equipo en estado desatendido, deben tenerse las siguientes precauciones:

- Si por algún motivo se debe ausentar del puesto de trabajo, es necesario bloquear la estación de trabajo mediante la siguiente combinación de teclas: Tecla Windows + L. En caso de no hacerlo, la suspensión automática de 3 minutos se activará.

10.8 Control de Dispositivos de Almacenamiento Digital

La política de restricción en el uso de dispositivos USB o CD-DVD se estructura de acuerdo con la clasificación de la información según su grado de confidencialidad, por tal motivo, dentro de las instalaciones de CSI no se permite el uso o activación de estos dispositivos, excepto los cargos autorizados (Cargos Directivos).

10.9 Firewall y Antivirus Local

Las estaciones de trabajo y servidores cuentan con Antivirus que ofrece antimalware, firewall personal, control de dispositivos y bloqueo de sitios por mala reputación.

Ningún usuario deberá intentar de ser posible, desactivar el programa de antivirus en su estación de trabajo (PC), el cual dejaría expuesto los recursos informáticos ante una amenaza o vulnerabilidad.

En caso de detectarse un virus o una situación sospechosa en el funcionamiento de los recursos informáticos, los usuarios deben reportar a su jefe directo el incidente para que sea evaluado, y si es del caso registrarlo en el sistema de gestión de incidentes de seguridad para dar el adecuado tratamiento.

10.10 Medios de Comunicación Seguros

CSI dispone de los siguientes medios de transferencia de información, los cuales deberán ser utilizados de acuerdo con los parámetros de seguridad y configuración definidos en común acuerdo con los clientes, asegurando la confidencialidad, integridad y disponibilidad en la transferencia de la información.
Transferencia de información mediante canales dedicados bajo túneles seguros (VPN 3DES-IPSec) con certificados de firma digital.

Transferencia de información mediante Internet Site to Site bajo túneles seguros (VPN 3DES-IPSec) con certificados de firma digital.

Transferencia de información mediante FTP's seguros SFTP con certificados de firma digital.

Adicionalmente se podrá transmitir información vía correo electrónico, siempre y cuando el cliente lo acepte.

10.11 Control de Acceso de Terceros a la Plataforma Tecnológica

El acceso a la plataforma tecnológica de la compañía por parte de terceros queda restringido, al menos que por una falla o cambio en la tecnología sea requerida. Cualquier requerimiento deberá ser elevado al responsable de TIC, quien evaluará cada caso exigiendo:

- La existencia del Contrato de Servicios establecido con el tercero o el servicio de soporte.
- La existencia del Acuerdo de Confidencialidad de proveedores firmado por su representante legal.
- Descripción y justificación del requerimiento, bien sea por una necesidad al interior de la compañía o por solicitud del tercero.
- Tiempo o periodicidad de conexión (período definido o estimado) en el cual se dejará activo este acceso.
- Nombre del recurso (servidor o estación) donde se encuentre la aplicación y/o equipos activos de red o seguridad del servicio.
- Si es un servidor o estación, detalle de la ruta específica donde el tercero debe tener permiso de acceso.
- Nombre del usuario requerido para el acceso.
- Privilegios o permisos de seguridad que deben ser otorgados al tercero sobre los recursos informáticos, considerando las siguientes características: lectura, escritura, modificación, creación u otra específica.
- Detalle de información crítica o confidencial dentro del servidor de pruebas, estación y/o equipos de red.

10.12 Clasificación de la Información

El buen uso de la información y el aseguramiento frente a accesos no autorizados de terceros es responsabilidad de todos. Considerando los criterios de confidencialidad, integridad y disponibilidad, CSI ha adoptado un esquema de clasificación de la información categorizada en cuatro grupos según su nivel de confidencialidad. Toda la información administrada por la compañía está clasificada en cuatro niveles:

a) **Dato público:** Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y aquel que no sea semiprivado, privado o sensible. Son

públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales.

b) **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

c) **Dato Semiprivado**: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio.

d) **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

10.13 Seguridad en la Transferencia, Custodia y Destrucción de la Información

Para preservar la confidencialidad, integridad y disponibilidad de la información, se dispone de mecanismos de control y seguridad en la transferencia, procesamiento, almacenamiento, custodia y destrucción de los datos de nuestros clientes.

Para garantizar que los datos de clientes guarden confidencialidad, se aplicarán procedimientos de borrado seguro, y las llaves o claves secretas no utilizadas serán eliminadas bajo los procedimientos respectivos.

10.14 Destrucción Segura de la Información

Una vez la información del cliente o del negocio considerada confidencial o secreta, no se requiera o haya llegado a su ciclo de vida de acuerdo con las condiciones de seguridad exigidas, se eliminará de manera segura de los servidores, PC, de los diferentes dispositivos de almacenamiento y comunicaciones que hagan parte de la plataforma informática de la compañía.

Para lograr un borrador definitivo se utilizarán herramientas de borrado seguro, la cual deberán cumplir el estándar de 7 pasos de sobreescritura.

10.15 Software y Licenciamiento Legal

El software utilizado por CSI para el desarrollo del objeto social es legal y no existe ninguna

restricción para su utilización.

La Compañía, conforme a las leyes, dará cumplimiento a las normas sobre propiedad intelectual y derechos de autor, razón por la cual quien las viole se hará acreedor a las respectivas sanciones penales o administrativas. Así mismo es claro que las autoridades colombianas podrán verificar el estado de cumplimiento de las normas sobre este tipo de derechos por parte de las Compañías para impedir que, a través de su violación se evadan tributos.

El software que es licenciado para CSI o propiedad de esta solo podrá ser instalado en los computadores de la Compañía y por personal del área de TIC.

No está permitido Instalar software que no esté licenciado para la Compañía. En caso de tratarse de software de prueba, es necesario la aprobación del responsable de TIC.

11. Seguridad en la Contratación del Personal

El proceso de selección y contratación deberá tener en cuenta los siguientes procedimientos que deben cumplir los empleados a contratar:

- Suscripción de Acuerdo de Confidencialidad.
- Socialización de Política de Seguridad CSI
- Suscripción de autorización de consulta a la central de riesgos y autorización para tratamiento de datos personales.
- Pruebas psicotécnicas según perfil, con énfasis en aspectos de confiabilidad, integridad y seguridad.
- Estudio de Confiabilidad
- Validación de referencias laborales y personales.
- Visitas domiciliarias inicial y de mantenimiento para cargos que lo requieren.
- Evaluación de antecedente penales