POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 4.

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
V 4.0	29/11/2025	José Manuel Urrego	Actualización	Gerencia	Gerencia

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 que todo el personal que ingresa a la Compañía ya sea como empleado o tercero, suscriba el Acuerdo de Confidencialidad de la Información, con el fin de proteger la propiedad intelectual, la confidencialidad de la información de los clientes y de la Compañía, así como el uso adecuado de los recursos informáticos. Así mismo, deberá garantizar la firma del formato de aceptación del Código de Ética.

Los jefes de área deberán asegurar la suscripción del **Acuerdo de Confidencialidad** cuando el contrato de servicio esté relacionado con el acceso, uso o administración de los recursos informáticos o de la información de la Compañía, de acuerdo con el alcance de las funciones asignadas.

La obligación de confidencialidad aplica a toda la información, independientemente de su formato o medio de almacenamiento, incluyendo información física, digital, electrónica y aquella almacenada, procesada o transmitida a través de servicios en la nube o plataformas tecnológicas autorizadas por la Compañía.

El área de Tecnologías de la Información (TI) será responsable de implementar, administrar y controlar los mecanismos técnicos necesarios para proteger la confidencialidad de la información, incluyendo la gestión de accesos, perfiles de usuario, controles de seguridad y la revocación de permisos cuando aplique.

10.2 Política de Usuarios y Contraseñas

La Compañía cuenta con una política de usuarios y contraseñas administrada por el **área de Tecnologías de la Información (TI)**, con el fin de ejercer control de acceso sobre la red de datos, los sistemas de información, los servicios tecnológicos y las plataformas en la nube, restringiendo el ingreso no autorizado a los recursos informáticos.

En caso de pérdida u olvido de la contraseña, el usuario deberá notificar al área de TI para realizar el restablecimiento correspondiente, asegurando que únicamente el usuario tenga conocimiento de la contraseña asignada. En caso de sospecha de compromiso de la contraseña o acceso no autorizado, el usuario deberá notificar de manera inmediata al área de TI y reportar el incidente de seguridad a través de los medios definidos por CSI, tales como correo electrónico corporativo, WhatsApp u otros canales autorizados.

Las claves o contraseñas deberán cumplir, como mínimo, con las siguientes condiciones:

- Poseer un nivel adecuado de complejidad y no corresponder a palabras comunes que puedan encontrarse en diccionarios, ni contener información personal del usuario, datos familiares, fechas especiales, ni referencias asociadas a la Compañía.
- No utilizar contraseñas personales o utilizadas en servicios externos dentro del entorno laboral.
- Contar con un mínimo de ocho (8) caracteres alfanuméricos.
- Cambiarse obligatoriamente en el primer ingreso del usuario al sistema.
- Cambiarse periódicamente cada noventa (90) días, o cuando así lo establezca el área de TI según el nivel de riesgo.
- Cambiarse de manera inmediata cuando exista sospecha de compromiso, anomalías en la cuenta o indicios de acceso no autorizado.
- No estar conformadas únicamente por caracteres numéricos o alfabéticos, ni por caracteres idénticos consecutivos.
- Cumplir con al menos tres (3) de los siguientes cuatro (4) criterios:
  - Letras en mayúscula
  - Letras en minúscula
  - Dígitos numéricos (0 a 9)
  - Caracteres especiales (ejemplo: ¡, $, %, &)
- No ser visibles en pantalla al momento de ser ingresadas, ni ser compartidas, reveladas o divulgadas a terceros, incluyendo al personal del área de TI.
- No ser registradas en papel, archivos digitales o dispositivos físicos, salvo que se utilicen mecanismos de almacenamiento seguro previamente aprobados por el área de TI.

10.3 Gestión de Incidentes de Seguridad de la Información

Con el fin de asegurar los principios de **Confidencialidad, Integridad y Disponibilidad** de la información, CSI cuenta con un **procedimiento formal de gestión de incidentes de seguridad de la información** y un **grupo de respuesta a incidentes**, los cuales permiten la notificación, registro, análisis, contención, resolución, evaluación y seguimiento de los eventos que puedan afectar la seguridad de la información, tanto física como lógica.

Todo incidente real o sospechoso de seguridad de la información deberá ser reportado de manera inmediata al **área de Tecnologías de la Información (TI)** a través de los canales definidos por la Compañía, tales como correo electrónico corporativo, WhatsApp u otros medios autorizados. La omisión o retraso en el reporte de un incidente será considerada incumplimiento de la presente política.

El área de TI será responsable de coordinar la atención del incidente, definir las acciones de contención y mitigación, generar las recomendaciones correspondientes y establecer los planes de acción necesarios, de acuerdo con el nivel de impacto y riesgo identificado.
Cuando un incidente de seguridad de la información sea clasificado como un posible delito informático, ya sea originado por usuarios internos, externos o terceros, la Compañía podrá adelantar las acciones legales correspondientes ante las autoridades competentes, incluyendo la **Unidad de Delitos Informáticos de la Policía Nacional**.

La gestión detallada de los incidentes de seguridad de la información se regirá por lo establecido en la **Política de Gestión de Incidentes de Seguridad de la Información**, la cual forma parte integral del Sistema de Gestión de Seguridad de la Información de CSI.

10.4 Control Solicitud Recursos Informáticos y Accesos

Dentro del proceso de Seguridad de la Información, CSI dispone de un **procedimiento formal de control de accesos**, el cual regula la solicitud, asignación, modificación, suspensión y retiro de accesos lógicos y físicos a los recursos informáticos, sistemas de información, servicios tecnológicos y plataformas en la nube de la Compañía.

La gestión de los accesos será administrada por el **área de Tecnologías de la Información (TI)** o por el responsable designado de cada sistema de información, previa autorización del jefe inmediato o del responsable del proceso, de acuerdo con el principio de **mínimo privilegio** y la necesidad del rol.

El área de TI tendrá la facultad de **activar, modificar, restringir, suspender o revocar de manera inmediata** los accesos cuando se presenten cambios en las funciones del usuario, finalización del vínculo laboral o contractual, detección de riesgos de seguridad, incidentes de seguridad de la información o incumplimiento de la presente política.
Todo acceso otorgado deberá ser registrado y controlado, y estará sujeto a revisión periódica con el fin de asegurar su vigencia, pertinencia y alineación con las funciones asignadas.

10.5 Uso Adecuado de Recursos Informáticos

La Compañía, mediante la socialización de la presente política con empleados y terceros, propende por asegurar y controlar el uso adecuado de los recursos informáticos puestos a disposición para el desarrollo de las funciones laborales.
Como regla general, todos los recursos informáticos, incluyendo equipos de cómputo, redes, correo electrónico corporativo, acceso a Internet, sistemas de información, plataformas tecnológicas y servicios en la nube, están destinados **exclusivamente para uso interno y/o para actividades relacionadas con el negocio**, y no para uso personal.

No está permitido utilizar los recursos informáticos para:

- El almacenamiento, descarga o reproducción de música, videos, películas u otros contenidos de carácter personal o ajenos a las funciones laborales.
- La ejecución de juegos, aplicaciones recreativas o software no relacionado con el objeto del negocio.
- Realizar modificaciones en la configuración estándar de los equipos, sistemas operativos o dispositivos de cómputo.
- Instalar software, aplicaciones, extensiones o herramientas sin la debida autorización del **área de Tecnologías de la Información (TI)**.
- Utilizar los recursos tecnológicos para difamar, tergiversar o afectar la imagen de CSI, sus filiales, empleados, proveedores, clientes, competidores o accionistas.
- Obtener beneficios personales, económicos o realizar actividades ajenas al negocio durante la jornada laboral.

- Almacenar, procesar o transmitir información corporativa en plataformas, servicios externos o herramientas no autorizadas por la Compañía.

El área de TI podrá implementar mecanismos de **monitoreo, control, restricción o bloqueo** sobre el uso de los recursos informáticos cuando sea necesario para proteger la seguridad de la información, garantizar la continuidad del servicio o dar cumplimiento a la presente política.

El uso indebido de los recursos informáticos podrá ser considerado un incumplimiento de la política de seguridad de la información y, de ser aplicable, un incidente de seguridad.
Para mayor detalle, se deberá consultar el **Código de Ética de la Compañía**.

10.6 Computación Móvil (PC Portátil)

La computación móvil comprende el uso de equipos portátiles suministrados por la Compañía para el desarrollo de actividades laborales, ya sea en las instalaciones de CSI, en el hogar, en modalidad de teletrabajo, en sitios públicos o durante desplazamientos. Además de lo establecido en el numeral 10.7, se deberán cumplir las siguientes disposiciones:

Normas generales para el uso de computación móvil

- El sitio seleccionado para realizar actividades de computación móvil deberá garantizar condiciones adecuadas de **seguridad física y operativa**, procurando un ambiente de trabajo limpio, seguro y estable.
- Evitar condiciones de humedad, frío o calor extremos que puedan afectar el funcionamiento de los equipos.
- Mantener los equipos alejados de ambientes con alta concentración de polvo, partículas o exposición a líquidos.
- Evitar la exposición directa a los rayos del sol.
- No consumir alimentos ni bebidas cerca de los equipos portátiles.
- No colocar los equipos directamente sobre el cuerpo, ya que se puede obstruir la ventilación y generar daños.
- Asegurar que el equipo sea ubicado sobre superficies firmes y estables, evitando vibraciones o movimientos.
- Durante desplazamientos, los equipos portátiles no deberán transportarse en áreas de equipaje ni permanecer visibles dentro de vehículos. En caso de transporte en vehículo particular, deberán guardarse en la cajuela.
- Los equipos portátiles no deberán permanecer encendidos durante su transporte, independientemente de la distancia a recorrer.

Dispositivos y periféricos

- Salvo los equipos expresamente autorizados (equipo directivo), no está permitida la instalación o conexión de dispositivos adicionales o periféricos a los equipos suministrados por la Compañía sin autorización del **área de Tecnologías de la Información (TI)**.

- Dentro de estas restricciones se incluyen, entre otros:
  - Escáneres
  - Joysticks
  - Unidades de DVD o R/W
  - Discos externos u otros dispositivos de almacenamiento

Seguridad de la información y responsabilidad del usuario

- Los equipos portátiles deberán ser utilizados exclusivamente para actividades relacionadas con el negocio, y no deberán ser prestados ni compartidos con terceros, familiares o personas ajenas a la Compañía.
- El usuario es responsable de la custodia del equipo y de la información contenida en él, incluso fuera de las instalaciones de CSI.
- En caso de pérdida, robo, daño o sospecha de acceso no autorizado al equipo o a la información, el usuario deberá notificar de manera inmediata al área de TI, para la aplicación de las medidas de seguridad correspondientes, incluyendo el bloqueo de accesos y la revocación de credenciales.

10.7 Control Bloqueo Automático Estaciones de Trabajo

Con el fin de ofrecer mayor seguridad, control de acceso y confidencialidad de la información en las estaciones de trabajo, CSI dispone de un **control de bloqueo automático de pantalla**, el cual se activará cuando el equipo se encuentre inactivo durante un período máximo de **tres (3) minutos**.

Esta medida busca proteger la información en los momentos en que el puesto de trabajo queda desatendido, evitando accesos no autorizados. No obstante, los usuarios deberán **bloquear manualmente la estación de trabajo** cada vez que se ausenten de su puesto, aun por períodos cortos de tiempo.

Esta disposición aplica tanto para estaciones de trabajo ubicadas en las instalaciones de CSI como para equipos portátiles utilizados en modalidad de **teletrabajo, trabajo remoto o computación móvil**.

Los equipos que contengan o procesen información crítica, sensible o relevante para la Compañía no deberán dejarse desatendidos. En la medida de lo posible, deberán ser asegurados físicamente o almacenados en lugares seguros, con el fin de prevenir el acceso no autorizado, la pérdida o el robo de la información.

Cuando sea necesario ausentarse del puesto de trabajo, el usuario deberá bloquear la estación de trabajo utilizando los mecanismos definidos por el sistema operativo, tales como la

combinación de teclas **Windows + L**. En caso de no hacerlo, el bloqueo automático se activará conforme a la configuración establecida.

El **área de Tecnologías de la Información (TI)** será responsable de configurar, administrar y hacer cumplir los controles de bloqueo automático en las estaciones de trabajo, de acuerdo con los lineamientos de seguridad de la información de la Compañía.

10.8 Control de Dispositivos de Almacenamiento Digital

La política de restricción en el uso de dispositivos de almacenamiento digital, tales como **USB, CD, DVD, discos externos u otros medios removibles**, se establece de acuerdo con la clasificación de la información y su nivel de confidencialidad.

Por tal motivo, **no se permite el uso, conexión o activación de dispositivos de almacenamiento removible** en los equipos de la Compañía dentro de las instalaciones de CSI, salvo para los cargos expresamente autorizados por la Compañía (por ejemplo, cargos directivos) o aquellos casos debidamente justificados y aprobados por el **área de Tecnologías de la Información (TI)**.

El uso excepcional de estos dispositivos deberá estar limitado al alcance autorizado, y podrá ser monitoreado, controlado o restringido por el área de TI, de acuerdo con los riesgos identificados y los lineamientos de seguridad de la información.

10.9 Firewall y Antivirus Local

Las estaciones de trabajo, equipos portátiles y servidores de la Compañía cuentan con soluciones de **seguridad informática**, que incluyen funcionalidades de antimalware, firewall personal, control de dispositivos y bloqueo de sitios con mala reputación, con el fin de proteger los recursos informáticos y la información corporativa.

Ningún usuario está autorizado a **desactivar, modificar, interferir o alterar** el funcionamiento del antivirus, firewall u otros mecanismos de seguridad instalados en los equipos de la Compañía, ya que estas acciones exponen los recursos informáticos a amenazas, vulnerabilidades y riesgos de seguridad de la información.

En caso de detectarse un virus, alerta de seguridad, comportamiento anómalo del equipo o cualquier situación sospechosa relacionada con la seguridad informática, el usuario deberá **reportar de manera inmediata el incidente al área de Tecnologías de la Información (TI)** a través de los canales definidos por la Compañía, para su evaluación, contención y tratamiento conforme al procedimiento de gestión de incidentes de seguridad de la información.

El área de TI será responsable de la administración, actualización, monitoreo y configuración de las soluciones de seguridad instaladas, así como de la aplicación de las medidas correctivas necesarias para mitigar los riesgos identificados.

10.10 Control de Acceso de Terceros a la Plataforma Tecnológica

El acceso a la plataforma tecnológica de la Compañía por parte de terceros se encuentra **restringido** y únicamente será permitido cuando exista una necesidad operativa debidamente justificada, como fallas técnicas, soporte especializado, mantenimiento, cambios tecnológicos o requerimientos del negocio.

Todo requerimiento de acceso deberá ser solicitado y evaluado por el **área de Tecnologías de la Información (TI)**, quien analizará los riesgos asociados y autorizará el acceso únicamente cuando se cumplan, como mínimo, los siguientes requisitos:

- Existencia de un **Contrato de Servicios** vigente con el tercero o un acuerdo formal de soporte.
- Suscripción del **Acuerdo de Confidencialidad** por parte del tercero, debidamente firmado por su representante legal.
- Descripción clara y justificada del requerimiento de acceso, ya sea por necesidad interna de la Compañía o por solicitud del tercero.
- Definición del **tiempo o período de conexión**, el cual deberá ser limitado y previamente establecido.
- Identificación del **recurso tecnológico** al cual se requiere acceso (servidor, estación de trabajo, aplicación, plataforma en la nube, equipos de red o de seguridad).
- En caso de acceso a servidores o estaciones, definición de la **ruta, sistema o módulo específico** al cual el tercero tendrá permisos.
- Identificación del **usuario o cuenta de acceso** que será utilizada por el tercero.
- Definición de los **privilegios o permisos de seguridad** otorgados, aplicando el principio de **mínimo privilegio** (lectura, escritura, modificación, creación u otros estrictamente necesarios).
- Identificación de la información **crítica, sensible o confidencial** a la que el tercero podría tener acceso durante la prestación del servicio.

El área de TI será responsable de la **creación, control, monitoreo y revocación** de los accesos otorgados a terceros, y podrá suspender o cancelar dichos accesos de manera inmediata en caso de finalización del servicio, detección de riesgos, incumplimiento de la presente política o ante la ocurrencia de un incidente de seguridad de la información.

10.11 Clasificación de la Información

El uso adecuado de la información y la protección frente a accesos no autorizados es responsabilidad de todos los empleados y terceros que interactúan con la información de la Compañía. Considerando los principios de **confidencialidad, integridad y disponibilidad**, CSI ha adoptado un esquema de **clasificación de la información**, el cual deberá ser aplicado en todos los procesos, sistemas de información, plataformas tecnológicas y servicios en la nube utilizados por la Compañía.

Toda la información administrada por CSI será clasificada de acuerdo con su nivel de confidencialidad en las siguientes categorías:

a) Dato personal:
Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

b) Dato público:
Información calificada como pública según los mandatos de la ley o de la Constitución Política, así como aquella que no sea semiprivada, privada o sensible. Incluye, entre otros, datos relacionados con el estado civil, profesión u oficio, calidad de comerciante o servidor público, y aquella que pueda obtenerse sin reserva alguna a través de registros, documentos públicos, gacetas o boletines oficiales.

c) Dato privado:
Información que por su naturaleza íntima o reservada solo es relevante para el titular y cuyo acceso se encuentra restringido.

d) Dato sensible:
Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como datos que revelen el origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales o de derechos humanos, así como datos relativos a la salud, la vida sexual y datos biométricos.

La clasificación de la información deberá ser considerada para la definición de controles de acceso, mecanismos de protección, almacenamiento, transmisión, custodia y eliminación de la información, los cuales serán administrados y supervisados por el área de Tecnologías de la Información (TI), en coordinación con los responsables de cada proceso.

El acceso, uso y tratamiento de la información deberá realizarse conforme a su clasificación y a la normativa legal vigente. El incumplimiento de estas disposiciones podrá ser considerado un incidente de seguridad de la información.

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

Con el fin de preservar los principios de **Confidencialidad, Integridad y Disponibilidad** de la información, CSI dispone de mecanismos de control y seguridad para la **transferencia, procesamiento, almacenamiento, custodia y destrucción** de la información de clientes y de la Compañía, independientemente de su formato o medio.

La información deberá ser transferida y almacenada únicamente a través de **medios, sistemas y plataformas tecnológicas autorizadas**, aplicando los controles de seguridad definidos por la Compañía y de acuerdo con su clasificación de la información.

Para garantizar la confidencialidad de los datos de clientes y de la información sensible, se aplicarán **procedimientos de eliminación y borrado seguro**, tanto en medios físicos como

digitales, incluyendo sistemas, equipos de cómputo, plataformas en la nube y dispositivos de almacenamiento.

Las llaves criptográficas, contraseñas, credenciales de acceso o claves secretas que no se encuentren en uso deberán ser **revocadas o eliminadas** conforme a los procedimientos establecidos, con el fin de prevenir accesos no autorizados.

El **área de Tecnologías de la Información (TI)** será responsable de definir, implementar y supervisar los controles técnicos asociados a la transferencia, custodia y destrucción de la información, así como de verificar su correcta aplicación conforme a la presente política y la normativa vigente.

10.13 Destrucción Segura de la Información

Una vez la información del cliente o del negocio, clasificada como confidencial o sensible, haya cumplido su ciclo de vida o deje de ser requerida para las operaciones de la Compañía, deberá ser eliminada de forma segura, irreversible y controlada de los servidores, estaciones de trabajo, plataformas en la nube, sistemas de información, respaldos y demás dispositivos de almacenamiento y comunicaciones que hagan parte de la infraestructura tecnológica de CSI.

La destrucción de la información se realizará mediante mecanismos y herramientas de borrado seguro, que garanticen la imposibilidad de recuperación de los datos, conforme a buenas prácticas, estándares reconocidos y procedimientos definidos por el área de Tecnologías de la Información (TI).

El área de TI será responsable de autorizar, ejecutar y verificar los procesos de destrucción segura de la información, dejando evidencia cuando aplique, y asegurando que dichas actividades se realicen de acuerdo con la clasificación de la información, la normativa legal vigente y las políticas internas de la Compañía.

10.14 Retención de Información en Vapster 2 / VapsterSolutions

El CSI utiliza la plataforma **Vapster 2** (también conocida como **VapsterSolutions**) como herramienta tecnológica para la gestión de procesos de poligrafía y estudios de confiabilidad. En cumplimiento de los principios de disponibilidad, integridad y confidencialidad de la información, se establecen los siguientes lineamientos de retención:

Retención de información histórica:

- Los clientes podrán consultar y descargar el histórico completo de los procesos gestionados en la plataforma sin limitación de tiempo, garantizando así el acceso permanente a la información de sus estudios.

Retención de pruebas de poligrafía y material audiovisual:

- Las pruebas de poligrafía y los videos asociados a los procesos se mantendrán almacenados en la plataforma por un periodo de **un (1) año** a partir de la fecha de realización del estudio.

- Transcurrido este periodo, los archivos audiovisuales y registros poligráficos podrán ser eliminados de manera segura conforme a lo establecido en el numeral 10.13 de la presente política.

- La eliminación de estos archivos no afecta el acceso al histórico de información y a los reportes finales de los estudios, los cuales permanecen disponibles sin restricción temporal.

Seguridad y confidencialidad:

- Toda la información almacenada en Vapster 2 / VapsterSolutions estará protegida bajo los controles de seguridad, confidencialidad y acceso establecidos en la presente Política de Seguridad de la Información.
- El acceso a la información de cada cliente estará restringido mediante controles de autenticación y será gestionado de acuerdo con el principio de mínimo privilegio.

10.15 Software y Licenciamiento Legal

El software utilizado por CSI para el desarrollo de su objeto social es legal, autorizado y licenciado, y no presenta restricciones para su uso conforme a los términos establecidos por sus fabricantes o titulares de derechos.

La Compañía dará estricto cumplimiento a la normativa vigente en materia de propiedad intelectual y derechos de autor, por lo cual cualquier incumplimiento por parte de empleados, contratistas o terceros podrá dar lugar a sanciones disciplinarias, administrativas o legales, de acuerdo con la normatividad aplicable. Así mismo, CSI reconoce que las autoridades competentes podrán verificar el cumplimiento de estas disposiciones.

El software licenciado para CSI o propiedad de la Compañía solo podrá ser instalado en los equipos corporativos, y exclusivamente por personal autorizado del área de Tecnologías de la Información (TI).

No está permitido instalar, copiar, distribuir o utilizar software que no cuente con licencia válida para la Compañía. En el caso de software de prueba, software libre o herramientas temporales, su uso deberá contar con la autorización previa del responsable de TI, quien evaluará los riesgos de seguridad, legales y operativos asociados.

El área de TI será responsable de la gestión, control, inventario y verificación del licenciamiento de software, así como de asegurar que su uso se encuentre alineado con las políticas internas y la legislación vigente.

10.16 Uso de Inteligencia Artificial (IA) en Procesos de la Compañía

CSI reconoce el uso de herramientas de Inteligencia Artificial (IA) como un apoyo para la optimización de procesos operativos, administrativos y tecnológicos. No obstante, su utilización deberá realizarse de manera responsable, controlada y alineada con los principios de seguridad de la información, confidencialidad, ética y cumplimiento normativo.

El uso de herramientas de IA por parte de empleados, contratistas o terceros deberá cumplir con las siguientes disposiciones generales:

- La información ingresada o procesada mediante herramientas de IA no deberá incluir datos confidenciales, sensibles o información de clientes, salvo autorización expresa y evaluación previa del área de Tecnologías de la Información (TI).
- No está permitido el uso de herramientas de IA que comprometan la propiedad intelectual, la confidencialidad de la información o los intereses de la Compañía.
- Los resultados generados por herramientas de IA no sustituyen el criterio humano, por lo que su uso será de carácter asistido, siendo responsabilidad del usuario la validación, verificación y uso adecuado de la información obtenida.
- El uso de IA deberá respetar la normativa legal vigente, las políticas internas de CSI y los principios éticos definidos por la Compañía.
- Cualquier implementación, integración o uso institucional de herramientas de IA deberá contar con la aprobación previa del área de TI, quien evaluará los riesgos tecnológicos, de seguridad y de información asociados.

CSI desarrollará y actualizará de manera progresiva una Política específica de Uso de Inteligencia Artificial, en la cual se definirán los lineamientos, responsabilidades, controles y buenas prácticas aplicables.

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.
- Suscripción 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