

# SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO AMABLE E.I.C.E.

## PLAN DE TRTAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



## INTRODUCCION

La Entidad ha reconocido la información como uno de los activos más importantes de la organización, haciendo necesaria la protección de la misma frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, de gestión pública, y de conformidad legal necesarios para alcanzar las metas con la formulación de la presente Política de Seguridad de la Información, AMABLE E.I.C.E , materializa la gestión responsable de información que proyecta garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos y metas trazadas en la administración pública.

## CONCEPTOS BÁSICOS

La Seguridad Informática refiere las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar suconfidencialidad, integridad y disponibilidad.

Se evidencian tres conceptos fundamentales que representan las acciones durante el proceso, el primero la amenaza, la vulnerabilidad y finalmente la contramedida.

Considerar aspectos de seguridad significa:

- Conocer e identificar el peligro
- Clasificarlo
- Protegerse de los impactos o daños de la mejor manera posible.

Esto significa que solamente cuando se conoce las amenazas,



agresores y sus intenciones dañinas (directas o indirectas) se pueden tomar medidas de protección adecuadas, para que no se vulneren los recursos valiosos.

“La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo”

La gestión del riesgo, partiendo desde la seguridad informática se divide en cuatro fases:

- **Análisis:** Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
- **Clasificación:** Determina si los riesgos encontrados y los riesgos restantes son aceptables.
- **Reducción:** Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.
- **Control:** Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

El proceso se basa en la política de seguridad, las cuales describen las normas y reglas institucionales, que forman el marco operativo en la entidad, logrando así:

- Fomentar las capacidades institucionales, reduciendo la vulnerabilidad confinando las amenazas reduciendo así el riesgo.
- Guiar u orientar un funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Tomar medidas correctivas a las conductas o prácticas que hacen un sistema vulnerable.
- Sincronizar la coherencia entre las acciones pensar, decir y hacer.

La seguridad informática se enfatiza en propender a acceder a datos y recursos del sistema garantizando mecanismos de autenticación y

control, para que los usuarios que accedan a estos recursos sólo posean los derechos que se les han configurado.

Estos sistemas de control de seguridad pueden causar inconvenientes a los usuarios. A medida del que la red crece las reglas de seguridad se vuelven cada vez más complicadas por lo que deben estudiarse monos que eviten que los usuarios desarrollen usos necesarios y así poder utilizar los sistemas de información de una forma segura.

Por esta razón, para asegurar la información se debe definir una política de seguridad que se pueda implementar en concordancia a las siguientes etapas:

- Conocer las necesidades de seguridad y los riesgos informáticos, así como sus posibles consecuencias.
- Tomar acciones preventivas que proporcionen las reglas y los procedimientos que se deben implementar para afrontar los riesgos identificados en los diferentes departamentos o secretarías de la organización.
- Detectar y controlar las vulnerabilidades del sistema de información, y mantener alerta para evitar posibles falencias en el control de las mismas.
- Desarrollar acciones correctivas que se puedan utilizar en caso de detectar una amenaza.

#### PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- **Autenticidad:** Principio que garantiza veracidad en la autoría de la información . sin embargo, no garantiza la veracidad del contenido de la información. La autenticidad garantiza la veracidad del autor, de quien la produjo la información, sin importar si el contenido es verdadero o falso.
- **Confidencialidad:** Los activos de información solo



pueden ser accedidos y custodiados por usuarios que cuente con permisos para ello.

- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que cuenten con los permisos adecuados.

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad es un documento que denota el compromiso del Gerente de AMABLE E.I.C.E con la seguridad y privacidad de la información, la cual tiene como objetivo preservar, proteger y administrar de forma eficiente la información de AMABLE E.I.C.E junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad confiabilidad de la información.

### ALCANCE

Esta política de seguridad y privacidad de la información incluye terceros y a todo el personal de la Empresa independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

### OBJETIVOS

- Preservar, proteger y administrar de forma eficiente la información de Empresa AMABLE E.I.C.E junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.



- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información de AMABLE E.I.C.E, para asegurar la sostenibilidad de la misma y el nivel de eficacia.

## CONCEPTOS Y DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio:** Es el ambiente físico y virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o

privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados:** Dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3, literal h).

- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultura (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento do Datos:** Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).



- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 8).

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1286 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

- las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).



- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/EC 27000).
- **Seguridad de la Información:** Preservación de la confidencialidad, Integridad, y disponibilidad de la información en cualquier medio: impreso o digital.
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la Información que se encuentra en medios digitales.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento

de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

## RESPONSABILIDADES ASIGNADAS

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de AMABLE E.I.C.E, independiente del tipo de vinculación, el área o dependencia a la cual se encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El comité institucional de gestión del desempeño es el responsable de formular, analizar y proyectar el documento de la política de seguridad y

privacidad de la información para que el Gerente lo avale. Es compromiso del Comité determinar las estrategias de capacitación de las políticas de seguridad y privacidad de la información en AMABLE E.I.C.E.

El coordinador del Comité deberá coordinar las gestiones para promover la socialización, seguimiento y control de la política.

Los propietarios de la información son los responsables de la producción, documentación, clasificación, actualización y valorización de la misma de acuerdo con los cargos desempeñados, funciones, competencias y acuerdos de confidencialidad a que haya lugar.

El Director Administrativo es el responsable de brindar la inducción al personal acerca de las obligaciones de seguridad y privacidad de la información.

En consecuencia AMABLE E.I.C.E se compromete a cumplir a cabalidad y de forma permanente con los preceptos que a continuación se mencionan.

a) Garantizar al titular de forma indefinida y permanente el pleno y



efectivo respeto de sus derechos referidos a sus datos personales.

- b) Conservar la información bajo estrictas medidas de seguridad con el fin de impedir pérdida, consulta uso o acceso no permitido o fraudulento.
- c) Tramitar las consultas y reclamos interpuestos por los titulares de la información en los términos que para ello tiene fijado el artículo 14 de la Ley 1581 de 2012 en cuanto al tiempo de respuesta.
- d) Permitir el acceso a la información únicamente a las personas que con ocasión de sus labores como empleados deban tener dicho acceso.

## IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

La información cada área de AMABLE E.I.C.E debe actualizar el inventario de los activos de información a medida que se procese o produzcan unidades de datos.

## SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO

Cada funcionario y contratista de AMABLE E.I.C.E, independiente del tipo de vinculación laboral debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado.

El área de sistemas debe mantener actualizado un directorio completo y actualizado de los perfiles creados.

Desde la Dirección Administrativa se determina cuáles son los privilegios que tendrían los diferentes perfiles del personal, a su vez debe elaborar, mantener, actualizar, mejorar y difundir las responsabilidades Personales para la seguridad de la información de la Entidad. La responsabilidad de la preservación de documentos y cuidado de la información de personal que se retira o cambia de cargo, la asume el respectivo supervisor del contratista.

## ASUNTOS OPERACIONALES Y DE MANEJO

Para que la Política de seguridad y privacidad de la información sea práctica, AMABLE E.I.C.E debe utilizar las mejores prácticas y procedimientos para cumplir con las estrategias de preservación y cuidado de la información como la documentación de la generación y el control de cambios de las unidades de datos, estos deben ser establecidos e implementados en la Entidad para proveer una protección adecuada de los activos de la información.

## RESPONSABILIDADES DEL PERSONAL

Los servidores públicos y contratistas de AMABLE E.I.C.E deben suscribir un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de Tecnologías de la información y las reglas que autorizan el uso de la información generada en la Entidad. El Director Administrativo y el contratista de apoyo en sistemas de la entidad se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que proyecte la socialización y concientización individual y colectiva en temas de seguridad de la información en todo el personal.

El contratista de apoyo de la Entidad es el responsable de realizar los procedimientos para crear los respectivos perfiles y los privilegios de cada funcionario o contratista de acuerdo a los lineamientos en cuanto al uso de

los dispositivos de hardware y los elementos de software, además, deberá publicar en medios impresos y virtuales como intranet, correo electrónico, entre otros, información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de documentos, archivos, buenas prácticas, amenazas de seguridad, entre otros.

## RESPONSABILIDADES DE USUARIOS EXTERNOS

El personal de empresas externas deben estar autorizados por una persona designada por parte de AMABLE E.I.C.E para controlar y supervisar el uso adecuado de la información y procurar por la buena utilización de recursos tecnológicos.



Los procedimientos para el uso adecuado de los recursos tecnológicos y de la información deben ser diseñados e implementados por el contratista de sistemas. Los dueños de los activos de la información se encargaran de

orientar a los usuarios externos autorizados para que hagan adecuado uso de la información y componentes tecnológicos facilitados.

Todos los usuarios externos sin excepción deben aceptar por escrito los términos y condiciones de uso de la información y recursos Tics institucionales.

#### ADMINISTRACION DE LAS COMUNICACIONES Y OPERACIONES REPORTE Y REVISIÓN DE INCIDENTES DE SEGURIDAD

El contratista de sistemas de AMABLE E.I.C.E notificará al Gerente y a la Dirección Administrativa de la Entidad las novedades que se presenten a nivel de seguridad, claramente cuando amerite y se presenten situaciones específicas el mismo funcionario afectado realizará el reporte respectivo; describirá la solicitud y las actividades de solución.

Entre tanto, el contratista de sistemas realizará procedimientos específicos para la actualización de las bases de antivirus, el análisis y búsqueda de amenazas en los equipos de cómputo sin que esto suponga un impacto alto o una prolongada interrupción en el desarrollo normal de actividades de la Entidad.

#### PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING.

A nivel administrativo, físico y técnico se deben proteger todos los sistemas de información como control básico, todas las estaciones de trabajo de AMABLE E.I.C.E deben estar protegidas por software antivirus, cabe recordar que los usuarios de cada puesto de trabajo no están autorizados para deshabilitar las opciones de protección del antivirus en sus diferentes enfoques, tales como, antivirus para archivos, antivirus para la web, supervisor de software malicioso y buscador de objetos peligrosos.

## COPIAS DE SEGURIDAD

Toda información que sea valorada como activo de información corporativa debe ser respaldada con copias de seguridad (backups) con la periodicidad que determine el encargado del área de sistemas de la Entidad y almacenada en el disco externo en carpetas por área según corresponda. El área de sistemas debe proveer la herramienta para que los funcionarios y contratistas puedan consultar el registro de la información y las copias de seguridad.

## ADMINISTRACIÓN DE REDES DE ÁREA LOCAL.

La configuración de terminales de red, enrutadores, switches, firewall y los

sistemas de seguridad de red a que haya lugar; debe ser documentada, resguardada como copia de seguridad y mantenida por el contratista de sistemas de la Entidad.

## INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS

Las solicitudes de información por parte de entes externos a AMABLE E.I.C.E deben ser primero aprobadas por la Directora de Control interno y en calidad de enlace posteriormente solicitado a los responsables del manejo custodia de dichos activos de información.

Estas peticiones de información deben ser realizadas por un medio válido que permita el registro de la solicitud, donde pueda identificarse el remitente, el asunto y la fecha toda la información de la Entidad debe ser manejada de acuerdo a la legislación colombiana y según la normatividad vigente.

## INSTALACIÓN DE SOFTWARE

Todas las instalaciones de software que se realicen sobre los sistemas operativos previamente instalados en AMABLE E.I.C.E, deben ser autorizados por el Gerente y/o por el Director Administrativo bajo la supervisión del contratista de Sistemas.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. El contratista de Sistemas debe desinstalar cualquier



software ilegal, al igual debe mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

### CONTROL DE CLAVES Y NOMBRES DE USUARIO

Cada funcionario o Contratista se debe autenticar para iniciar sesión en su equipo de cómputo con una contraseña previamente asignada para garantizar que cada uno sea el responsable de la transformación y custodia de la información institucional allí generada, igualmente, las cuentas de usuario para acceder a los sistemas de información con que cuenta la Entidad deben ser únicas y creadas para la persona que tiene esas funciones designadas, ese rol tendrá ciertos privilegios dentro de cada software según corresponda.

### SEGUIMIENTO

El contratista de Sistemas hará seguimiento sobre el Uso que se haga de los recursos de tecnologías de la información en AMABLE E.I.C.E por parte de algún funcionario autorizado, en caso de encontrarse alguna novedad lo reportará ante el Gerente y Director Administrativo. De igual manera se realizará la revisión a la presente política de seguridad y los objetivos planteados.

### CUMPLIMIENTO

Toda compra de hardware y adquisición y/o desarrollo de software en AMABLE E.I.C.E y todo uso y seguimiento de los recursos de Tecnologías de la información y las comunicaciones en la Entidad, debe estar sujeta a normas y estatutos internos así a la legislación nacional.

Esta política interna de seguridad y privacidad de la información deberá revisarse y actualizarse cada año o cuando se considere pertinente por cambios normativos o necesidades del servicio, riesgos de seguridad que así lo ameriten.

### POLÍTICAS DE PRIVACIDAD Y CONDICIONES DE USO

Se considera norma de confidencialidad y protección de datos toda



aquella información personal que el usuario ingresa libre y voluntariamente al Portal Web de AMABLE E.I.C.E [www.armeniaamable.gov.co](http://www.armeniaamable.gov.co), la entidad no se hace responsable por los daños y/o perjuicios ocasionados por el uso inapropiado de la información o datos derivados de la página web en aras del incumplimiento de la política de seguridad de la información y protección de datos personales.

El portal web de la entidad, adopta una política de confidencialidad y protección de datos, con el objetivo de salvaguardar la privacidad de la información personal de sus usuarios obtenida a través de su sitio Web y se reserva el derecho de modificar o actualizar las Normas de confidencialidad y Protección de Datos que se describen más adelante con el fin de adaptarse a nuevos requerimientos legislativos o técnicos que permitan brindar mejores servicios y contenidos informativos, por lo cual se sugiere consultar estas normas periódicamente.

La entidad desde su portal web [www.armeniaamable.gov.co](http://www.armeniaamable.gov.co) actúa de buena fe al publicar documentos elaborados con fuentes propias y procura garantizar la disponibilidad, veracidad y confidencialidad de los mismos. No obstante, no se hace responsable de la precisión y actualización de la información suministrada por entidades externas que sean difundidos en el sitio web La Entidad, se reserva el derecho a introducir modificaciones o interrumpir los servicios ofrecidos, sin previo aviso a sus usuarios.

---

**JAMES CASTAÑO HERRERO**

**Gerente**

Elaboró: Leonardo Sánchez Ariza - Contratista  
 Revisó: Gabriela Giraldo Contratista Profesional Líder Administrativa y Financiera.  
 Aprobó: Gerente – James Castaño Herrera – Comité institucional


