GOBERNACIÓN DE CASANARE
NIT: 892099216-6

ESPECIFICACIONES TÉCNICAS – ESTUDIO PREVIO No 2026-03201

OBJETO A CONTRATAR:

ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE CONTROL DE ACCESO E IDENTIFICACIÓN DEL PERSONAL AL CENTRO ADMINISTRATIVO DEPARTAMENTAL DE LA GOBERNACION DE CASANARE.

SECRETARIA GENERAL

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TIC

Yopal, Octubre 2026

GOBERNACIÓN DE
CASANARE
NIT: 892099216-6

INTRODUCCIÓN

En la actualidad, las entidades públicas enfrentan desafíos crecientes en materia de transformación digital, gestión segura de la información y continuidad operativa. La infraestructura tecnológica juega un papel fundamental para garantizar servicios ágiles, eficientes, seguros y con altos estándares de calidad. En este contexto, se hace indispensable contar con sistemas robustos de procesamiento, almacenamiento, conectividad y soporte.

El presente documento técnico tiene como finalidad describir la necesidad, justificar la intervención, presentar la metodología de ejecución, y definir los componentes técnicos requeridos para la implementación, instalación, configuración y puesta en funcionamiento de la infraestructura tecnológica para el control de acceso de funcionarios, contratistas y visitantes a la sede administrativa de la Gobernación de Casanare (CAD).

Lo anterior, con el fin de garantizar la seguridad física, regular, registrar y restringir el ingreso de personas; así como mejorar la operatividad, seguridad, disponibilidad y rendimiento de los servicios digitales institucionales, teniendo en cuenta que la infraestructura será de uso permanente.

En este sentido, se establecen las condiciones técnicas necesarias para asegurar la correcta integración entre los componentes de hardware y software que garanticen la seguridad física, entendiendo que ambos elementos son complementarios para la prestación eficiente del sistema de control de acceso en la red centralizada.

OBJETO:

ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE CONTROL DE ACCESO E IDENTIFICACIÓN DEL PERSONAL AL CENTRO ADMINISTRATIVO DEPARTAMENTAL DE LA GOBERNACION DE CASANARE.

Objetivos específicos

1. Suministrar los elementos y/o dispositivos tecnológicos necesarios para garantizar el correcto funcionamiento del sistema de control de acceso e identificación de personal, de acuerdo a lo estipulado en el documento complementario, denominado fichas técnicas y especificaciones técnicas.
2. Realizar el ingreso de todos los elementos y/o dispositivos tecnológicos (hardware y software) del sistema de control de acceso e identificación de personal, según los procedimientos y directrices establecidas por almacén Departamental
3. Realizar la instalación, configuración y puesta en funcionamiento del sistema de control de acceso e identificación de personal (funcionarios, contratistas y visitantes; e Integrar la nueva infraestructura con los sistemas tecnológicos existentes en la Entidad, asegurando su interoperabilidad.
4. Configurar los tipos de control de acceso según método de autenticación para funcionarios, contratistas y visitantes.
5. Capacitar al personal designado por la Dirección TIC en la instalación, administración y operación de la nueva infraestructura tecnológica implementada.

6. Presentar un (1) documento o informe técnico que detalle las actividades realizadas (Instalación, configuración, puesta en funcionamiento, pruebas funcionales) con sus respectivas evidencias.

ESPECIFICACIONES TÉCNICAS

1. INFRAESTRUCTURA DE CONTROL DE ACCESO E IDENTIFICACIÓN

Proceso integral para la actualización y optimización de la infraestructura tecnológica para el control de acceso; con el propósito de mejorar la eficiencia, el rendimiento, la seguridad y la escalabilidad, que permita a la entidad adaptarse a nuevas tecnologías. Se debe determinar e identificar cada uno de los componentes y elementos necesarios para la instalación de la nueva tecnología de la entidad, contemplando, el suministro, instalación, pruebas técnicas y puesta en funcionamiento; que garantice:

- Prevenir accesos no autorizados
- Registrar entradas y salidas
- Gestionar el flujo de personas
- Cumplir normativas de seguridad

Se debe realizar la instalación, configuración, y pruebas funcionales de los elementos y/o dispositivos tecnológicos y eléctricos para habilitar el registro e ingreso de usuarios. intervención piso, paredes, instalación de red eléctrica y de datos, instalación de licenciamiento de software, instalación de rack, barreras abatibles, Terminales de reconocimiento facial, y demás elementos de tecnología, garantizando la interacción entre todos los dispositivos. (incluye mano de obra)

- **Intervención de piso y paredes:** incluye materiales para realizar obras complementarias y necesarias para la adecuación de la infraestructura física de la entidad, que garantice el óptimo funcionamiento e instalación de los dispositivos para el control de acceso.

- **Red eléctrica y de datos:** incluye materiales, herramientas y servicios requeridos para la identificación ordenada de cableado estructurado, red datos y eléctrico, etc. Instalación, Configuración y Pruebas Funcionales en Sitio.

- **Instalación de licenciamiento:** configuración, instalación, pruebas técnicas y puesta en funcionamiento de las licencias de software requeridas para los equipos y dispositivos tecnológicos.

- **Instalación de Hardware en Sitio:** Proceso integral para la configuración, instalación, pruebas técnicas y puesta en funcionamiento. Este servicio incluye:

  - ✓ Gabinete - Rack
  - ✓ Switch
  - ✓ UPS
  - ✓ barreras abatibles
  - ✓ Terminales de reconocimiento facial
  - ✓ Estación de registro de tarjetas
  - ✓ Equipo de lectura de código de barras

- ✓ Tarjetas inteligentes
- ✓ y demás elementos de tecnología

2. Recurso humano

- **Un (1) profesional** en Ingeniería de Sistemas, Electrónica o afines, con experiencia mínima de cinco (5) años. El ingeniero aporta una visión integral en planeación, supervisión y toma de decisiones técnicas que permiten asegurar la operatividad técnica y el cumplimiento de estándares de calidad y seguridad. De igual manera, es quien realiza la configuración de los mismos y el enlace con la infraestructura existente

- **Un (1) técnico** en sistemas, redes o electrónica, con experiencia mínima de dos (2) años. El técnico realiza la ejecución directa de la instalación de equipos aplicando los procedimientos específicos y asegurando la correcta implementación de los lineamientos establecidos por los estándares adoptados nacional e internacionalmente.

Ambos perfiles deberán garantizar la correcta instalación, configuración e integración de la infraestructura tecnológica.

3. Lugar y tiempo de ejecución

En la ciudad de Yopal - Casanare, en el Centro Administrativo Departamental (CAD) de la Gobernación de Casanare, el proyecto tiene como tiempo estimado de ejecución de un (1) mes.

4. Requerimientos Técnicos

- Todos los equipos deben ser nuevos, originales, sellados y cumplir con la ficha técnica.

- La solución implementada debe garantizar integración, estabilidad y seguridad de la infraestructura tecnológica institucional.

- Entregar junto a los elementos las *fichas técnicas del fabricante de los productos ofrecidos*; La ficha técnica es el documento que detalla las características, especificaciones, materiales, rendimiento y dimensiones del producto, asegurando que los bienes o servicios cumplen con la calidad, modernidad y [vigencia tecnológica] necesarias para la finalidad pública.

Nota: *presentar fichas técnicas para los ítems* ***(1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.11, 1.12,1.13, 1.14, 1.20).***

- El proveedor debe anexar el *Certificado de Distribuidor Autorizado de las marcas de los productos de hardware y software ofrecidos*, esto con el fin de prevenir la piratería de hardware y software a que está expuesta la distribución de tecnología en nuestro país, garantizando que los elementos que se pretenden adquirir hayan ingresado legalmente al país.

Nota: *presentar certificado de distribuidor autorizado para los ítems* ***(1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.8, 1.11, 1.12,1.13, 1.14, 1.20).***

- El oferente debe tener implementado el sistema de seguridad y salud en el trabajo garantizando sus estándares mínimos.

Los requerimientos fichas técnicas del fabricante de los productos ofrecidos, Certificado de Distribuidor Autorizado de las marcas de los productos de hardware y software ofrecidos, y SST, tienen fundamento legal y técnico de acuerdo a lo siguiente:

4.1 Fichas técnicas: Solicitar fichas técnicas de los elementos tecnológicos en una convocatoria pública es un paso crítico y obligatorio para garantizar la transparencia, objetividad y eficiencia en la contratación estatal. Estos documentos permiten verificar que lo ofrecido por los proponentes cumple estrictamente con los requerimientos técnicos mínimos establecidos.

Razones fundamentales para solicitar fichas técnicas:

- Garantizar la Calidad y el Cumplimiento Técnico: La ficha técnica es el documento que detalla las características, especificaciones, materiales, rendimiento y dimensiones del producto, asegurando que los bienes o servicios cumplen con la calidad, modernidad y vigencia tecnológica necesarias para la finalidad pública.

- Permitir la Evaluación Objetiva: Al obtener los datos precisos de cada producto, el comité evaluador puede comparar objetivamente las ofertas bajo los mismos parámetros, evitando subjetividades en la selección del proveedor.

- Verificación Precontractual y Contractual: Sirve para constatar que el bien ofertado se ajusta al estudio de sector y a las necesidades de la entidad antes de contratar (fase de selección) y para verificar que lo entregado coincida con lo ofertado (fase de ejecución).

- Transparencia y Evitar la Licitación Desierta: Permite a los proponentes demostrar la idoneidad técnica de sus productos, reduciendo la ambigüedad y asegurando que las ofertas sean claras y completas.

En resumen, la ficha técnica es esencial para evitar la adquisición de equipos obsoletos, de baja calidad o que no cubren la necesidad técnica de la entidad, garantizando que el gasto público sea eficiente.

4.2 Certificación como distribuidor autorizado:

Se justifica técnica y jurídicamente por qué la Entidad exige que el oferente acredite su condición de distribuidor autorizado, mediante certificación del fabricante, para los ítems:

1.1 TERMINAL DE RECONOCIMIENTO FACIAL
1.2 EQUIPO DE TRANSMISION DE FASCIMIL DE SEGURIDAD
1.3 SOFTWARE DE ACCESO - TERMINAL DE RECONOCIMIENTO FACIAL
1.4 EQUIPO DE LECTURA DE CODIGO DE BARRAS
1.5 IMPRESORAS DE INJECCION DE TINTA
1.6 COMPUTADORES DE ESCRITORIO
1.8 FUENTES ININTERRUMPLIBLES DE POTENCIA
1.11 SISTEMAS DE SEGURIDAD O DE CONTROL DE ACCESO – BARRERA ABATIBLE
1.12 TARJETAS INTELIGENTES
1.13 ENRUTADORES (ROUTERS) DE RED
1.14 SOFTWARE DE ACCESO – GESTIÓN Y MONITOREO
1.20 CABLES DE REDES

Los anteriores ítems hacen parte del proceso y se encuentran identificados en el documento anexo de fichas técnicas.

4.2.1 Fundamento jurídico

Requisitos habilitantes adicionales y autonomía de la Entidad

"Los requisitos habilitantes miden la aptitud del proponente para participar en el proceso y ejecutar el contrato. El numeral 1 del artículo 5 de la Ley 1150 de 2007 enuncia los que la ley contempla, pero la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE) ha precisado, en el Concepto C-659 del 7 de julio de 2025, que esa disposición limita la discrecionalidad de la Entidad sin impedirle exigir otros requisitos. El fundamento está en el principio de autonomía de la voluntad (Ley 80 de 1993, artículos 13, 32 y 40, y artículo 1602 del Código Civil), siempre que los requisitos sean adecuados y proporcionales a la naturaleza y al valor del contrato, y guarden relación directa con su objeto."

En el presente proceso, donde el factor de selección es el menor valor, la verificación de la idoneidad técnica del oferente se realiza en la etapa de habilitación y no mediante puntaje. Por eso los requisitos habilitantes técnicos cobran especial importancia.

La certificación del fabricante

Según el Concepto C-659 de 2025, la certificación del fabricante es el documento que determina si una empresa está oficialmente autorizada por un fabricante o proveedor para distribuir sus bienes o servicios. Permite validar la relación comercial con el productor y le otorga a la empresa ciertos derechos y responsabilidades.

El concepto señala que su exigencia no es desproporcionada cuando se busca:

- La garantía de calidad y origen del producto: calidad, idoneidad, seguridad y buen estado y funcionamiento (Ley 1480 de 2011, artículo 7).

- El cumplimiento de los requisitos y condiciones técnicas y de funcionamiento, que por lo general brinda el productor o fabricante.

- La verificación de que el bien fue obtenido de forma legal.

- La exigencia de garantía por bienes o productos defectuosos (Ley 1480 de 2011, artículo 5, numeral 17), sin perjuicio de garantías suplementarias y otras condiciones necesarias para cumplir el objeto y los fines del contrato.

Adicional a lo anterior, exigir el certificado garantiza que los elementos y/o dispositivos cumplan con:

- Ley 1762 de 2015 (Ley Anticontrabando): Esta ley establece instrumentos para prevenir, controlar y sancionar el contrabando, el lavado de activos y la evasión fiscal. Exigir el certificado garantiza que los productos tecnológicos no provengan de rutas informales que eluden controles aduaneros.

- Normas Aduaneras (Decreto 1165 de 2019): Todo producto importado debe contar con documentación legal que demuestre su nacionalización (declaración de importación). El certificado asegura que el proveedor cumple con este requisito técnico-aduanero.

Aunado a lo anterior, como el sistema a contratar controlará el ingreso de un flujo aproximado de 2.000 personas por día al Centro Administrativo Departamental (CAD), almacenará datos biométricos (rostros y huellas dactilares), considerados datos sensibles por la Ley 1581 de 2012, y operará de forma continua. En ese contexto, la certificación del fabricante persigue:

- **Calidad, origen y seguridad:** que los equipos sean originales, cumplan las certificaciones declaradas y ofrezcan la seguridad razonable exigible, especialmente en equipos eléctricos y de evacuación.

- **Cumplimiento técnico y de funcionamiento**: que cada equipo opere con el firmware, el SDK correspondientes y los protocolos del fabricante (OSDP, Wiegand, MIFARE, PoE), de modo que los componentes interoperen entre sí.

- **Obtención legal:** que los bienes y, en particular, las licencias de software provengan de un canal legítimo, en cumplimiento de las normas de derechos de autor (Ley 23 de 1982).

- **Garantía efectiva:** que la garantía de fábrica, el soporte, los repuestos y las actualizaciones puedan hacerse efectivos ante el fabricante durante la vigencia del contrato.

4.2.2 Condiciones de acreditación

El oferente deberá presentar certificación del fabricante o de su representante en Colombia que cumpla lo siguiente:

- Esté firmada por el representante legal o la persona designada por el fabricante o su representante en Colombia.

- Identifique al oferente, la marca y las referencias o líneas de producto cubiertas, con indicación de los ítems a que corresponden.

- Evidencie el vínculo comercial, su término de duración y las condiciones de la autorización, y se encuentre vigente a la fecha de presentación de la oferta.

- Incluya un dato de contacto (teléfono o correo electrónico) que permita a la Entidad verificar su autenticidad.

- No requiere estar dirigida a la Gobernación de Casanare ni expedirse para el presente proceso.

- Podrá subsanarse dentro del término que fije la Entidad, conforme a las reglas de subsanabilidad de los requisitos habilitantes.

4.2.3 Certificación de manera independiente

- **La autorización es por marca y/o línea de producto.** Si cada ítem corresponde a fabricantes y líneas distintas (terminales biométricas, software, barreras, periféricos, cómputo, UPS, redes). Ser distribuidor autorizado de una marca no acredita autorización sobre otra. Cuando los elementos y/o dispositivos son del mismo fabricante se acredita en una sola certificación.

- **Las garantías y el soporte dependen del canal de cada fabricante.** Los términos, el alcance y el procedimiento de garantía varían entre marcas, por lo que su verificación debe hacerse ítem por ítem.

- **El sistema es integrado e interoperable.** Las terminales faciales (1.1), la estación de registro (1.2), las barreras (1.11), las tarjetas (1.12) y el software (1.3 y 1.14) deben funcionar como un solo sistema. La certificación individual permite verificar que cada componente proviene del canal autorizado y cuenta con el SDK, el firmware y las licencias que garantizan esa integración.

- **Trazabilidad.** Seriales, licencias y firmware son propios de cada producto y verificables solo ante su fabricante.

4.2.4 Justificación técnica por ítem

1. **Sistema de identificación y control de acceso**

- **Ítem 1.1 – Terminal de reconocimiento facial (3 unidades).** La ficha exige algoritmo de aprendizaje profundo, capacidad de 3.000 rostros, 3.000 huellas y 3.000 tarjetas por equipo, sistema operativo Linux, compatibilidad con Push SDK, protocolo OSDP V2.1.7, salida Wiegand y alimentación PoE (IEEE 802.3at). Estas funciones dependen del firmware, del algoritmo y del SDK propietarios del fabricante. Como el equipo captura y almacena datos biométricos sensibles, la Entidad debe asegurar firmware legítimo, actualizaciones de seguridad y soporte oficial, que solo el canal autorizado puede garantizar. Además, debe integrarse con el software (ítems 1.3 y 1.14) y con las barreras (ítem 1.11).

- **Ítem 1.2 – Estación de registro de tarjetas (1 unidad).** Lectora y codificadora USB compatible con ISO 14443 A/B e ISO 7816, a 13,56 MHz y 125 kHz, con 2 ranuras SAM, cifrado de transmisión, biblioteca de interfaz y actualizaciones en línea. Se usará para registrar las 1.000 tarjetas del ítem 1.12 y manejar claves de seguridad. La biblioteca de interfaz, las actualizaciones y la gestión de las SAM provienen del fabricante; un equipo fuera del canal autorizado puede carecer de SDK, controladores o actualizaciones.

- **Ítem 1.11 – Barrera abatible (3 unidades).** Equipo electromecánico con motor sin escobillas (MCBF de al menos 3 millones de ciclos), 4 pares de sensores infrarrojos con función anti-tailgating, controlador de acceso y lectores integrados, capacidad de 20 a 60 personas por minuto y liberación de las hojas ante alarma de incendio. Esta última es una función de seguridad de vida que debe operar y mantenerse correctamente. Con un flujo aproximado de 2.000 personas por día, el soporte técnico, los repuestos y la garantía del fabricante son críticos, y el controlador integrado debe ser compatible con las terminales y el software.

- **Ítem 1.12 – Tarjetas inteligentes (1.000 unidades).** Tarjetas de proximidad duales MIFARE S50 (13,56 MHz) y EM (125 kHz), compatibles con ISO/IEC 14443A y 7816-5, con garantía de 2 años. La autenticidad del chip y la uniformidad del lote determinan la compatibilidad con las terminales y la estación de registro, y la seguridad del sistema. En el mercado circulan tarjetas clonadas y lotes heterogéneos; el certificado permite verificar la procedencia.

2. **Software y licenciamiento**

- **Ítem 1.3 – Software de acceso, terminal de reconocimiento facial (3 unidades).** Licencia vitalicia de control de acceso y asistencia (1 puerta, personas ilimitadas), con portal web, aplicación móvil (iOS y Android), aplicación para PC y conexión P2P.

- **Ítem 1.14 – Software de acceso, gestión y monitoreo (1 unidad).** Plataforma con licencia vitalicia que incluye sincronización con Active Directory, mapas interactivos, estrategias anti-passback y de múltiples puertas, códigos QR dinámicos, informes de ingreso, salida e incidentes, e integración con ERP, HRMS y nómina y con el software existente en la Administración Departamental.

En ambos ítems, las licencias, las claves de activación, las actualizaciones, los servicios de conexión y las interfaces de integración son del fabricante. La licencia solo es válida, actualizable y con soporte si proviene del canal autorizado. La certificación mitiga el riesgo de licencias ilegítimas (derechos de autor), de pérdida de actualizaciones y de fallas de integración con los sistemas existentes.

3. **Periféricos y cómputo**

- **Ítem 1.4 – Lector de códigos de barras 2D, QR y cédulas (1 unidad).** Escáner de imagen de área con certificaciones de compatibilidad electromagnética y seguridad, sellado IP52, resistencia a caídas, interfaces USB, RS-232 y emulación de teclado, herramientas de configuración, SDK y servicios del fabricante, y garantía de fábrica de 5 años. Esa garantía y esas herramientas solo las respalda el fabricante a través de su canal autorizado.

- **Ítem 1.5 – Impresora de etiquetas a color (1 unidad).** Tecnología de inyección de tinta con cabezal permanente y tinta pigmentada, ancho de impresión de 4 pulgadas, lenguaje ZPL II, gestión remota, interfaces Ethernet y USB, y garantía limitada de 1 año en centro de servicio. El certificado asegura el acceso al centro de servicio autorizado, a suministros originales y al respaldo de la garantía.

- **Ítem 1.6 – Computador todo en uno (1 unidad).** Procesador Intel Core i7 de 13.ª generación, 16 GB de memoria, SSD de 500 GB, Windows 11 Pro y Microsoft Office 2024 con licencia vitalicia. Es el puesto de administración del sistema. La certificación respalda la garantía del fabricante, la trazabilidad por serial y la legalidad del licenciamiento preinstalado.

4. **Infraestructura de red, energía y cableado**

- **Ítem 1.8 – UPS on-line de doble conversión de 3 kVA (1 unidad).** Control por DSP, 6 baterías VRLA/AGM de 12 V y 9 Ah, carcasa en ABS retardante de llama (UL94), software de monitoreo y certificación RETIE. Es un equipo eléctrico que respalda todo el sistema, con riesgo de daño e incendio si no cumple. El certificado asegura el origen, la certificación de producto, la garantía del equipo y de las baterías y el soporte técnico.

- **Ítem 1.13 – Switch administrable PoE de 8 puertos Gigabit (1 unidad).** Switch de capa 2 con 4 puertos PoE/PoE+ (hasta 30 W por puerto y presupuesto de 52 W), gestionado mediante la plataforma del fabricante y con certificaciones CE, FCC e IC. Alimenta las terminales faciales y es el núcleo de conectividad del sistema. El certificado respalda el firmware, la administración, la garantía y el cumplimiento de las certificaciones declaradas.

- **Ítem 1.20 – Cable de red Categoría 6A U/UTP (305 metros).** Cobre sólido calibre 23 AWG, 4 pares, 500 MHz, chaqueta LSZH, para 10GBASE-T y PoE/PoE+, bajo ANSI/TIA-568.2-D e ISO/IEC 11801 Clase EA. En el mercado circula cable que no cumple lo declarado (conductores de aluminio cobrizado o calibres menores), con fallas de desempeño y calentamiento en aplicaciones PoE. La certificación respalda la autenticidad de la categoría, el cumplimiento de las normas, la seguridad (LSZH) y la garantía del cableado.

4.2.5 Ítems en los que no se exige el certificado

No se exige certificación del fabricante para los ítems 1.7 (Gabinete Rack),1.9 y 1.10 (mobiliario), 1.15 a 1.19 y 1.21 (conectores, módulos, tomas, cables eléctricos y canaletas) ni para el servicio 2.1 (instalación). Su conformidad puede verificarse mediante la ficha técnica y las normas que ella cita (ANSI / EIA 310D, ANSI/TIA-568.2-D, NTC 1332 y UL), sin depender de firmware, licencias ni de una garantía de canal. Esta delimitación evidencia que la exigencia es proporcional y se limita a lo estrictamente necesario.

4.2.6 Proporcionalidad y libre concurrencia

La exigencia es proporcional al objeto y valor del contrato por las siguientes razones:

- Se refiere a la marca ofertada y no a una marca determinada. Cualquier oferente que sea distribuidor autorizado de la marca que ofrezca, o de marcas equivalentes, puede participar.

- Cada fabricante cuenta, por lo general, con varios distribuidores autorizados, por lo que no se restringe la pluralidad de oferentes.

- No se exige un certificado dirigido a la entidad ni expedido para el proceso, conforme al Concepto C-659 de 2025.

- Guarda relación directa con el objeto: un sistema de control de acceso de operación continua, con datos biométricos y componentes que deben interoperar.

4.3 Sistema de seguridad y salud en el trabajo: Decreto 1072 de 2015 (Artículo 2.2.4.6.4 y Artículo 2.2.4.6.28): Obliga a los empleadores y contratantes (incluidas las entidades públicas y privadas) a garantizar la implementación, mantenimiento y mejora continua del SG-SST, adoptando disposiciones para que sus contratistas y subcontratistas cumplan con las normas de seguridad y salud en el trabajo durante la ejecución del contrato.

JAVIER FONSECA ROSAS
DIRECTOR DIRECCIÓN TIC

Proyectó: Juan Fernando Gutiérrez P. – Cto 1508 – 2026

Revisó: Judy Elizabeth Lapeira Rojas – Profesional contratada SG