Las especificaciones técnicas requeridas son de obligatorio cumplimiento (excluyentes), de no hacerlo la propuesta se considerará no apta técnicamente. Debe diligenciarse con las especificaciones técnicas ofertadas.

En una columna CUMPLE/NO CUMPLE, el comité técnico que la Policía Nacional designe, evaluará las especificaciones técnicas ofertadas por la firma.

El oferente deberá cumplir estrictamente con las especificaciones solicitadas atendiendo los factores descritos a continuación:

CERTIFICADO DIGITAL TOKEN SERVIDOR SEGURO (HSM) PARA EL SIIF NACIÓN DEL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1	La entidad de certificación digital abierta debe estar autorizada por el Organismo Nacional de Acreditación de Colombia – ONAC, para expedir certificados digitales de Función Pública.		
2	La entidad de certificación digital abierta debe estar autorizada por la Administración SIIF Nación para utilizar sus certificados digitales de función pública en el aplicativo SIIF Nación almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital, lo cual deberá demostrarlo mediante documento emitido por la Administración SIIF Nación del Ministerio de Hacienda y Crédito Público.		
3	Los certificados de función pública a utilizar en el SIIF Nación, deben estar almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital, la entidad de certificación digital debe proveer a sus suscriptores los controladores o driver para acceder al certificado digital del suscriptor. Este controlador o driver debe cumplir mínimo con: a) Integrarse con el terminador de VPN para acceso al SIIF Nación y con el componente cliente de firma digital del SIIF Nación. b) Implementar doble factor de autenticación del usuario para acceder al certificado digital almacenado en el servidor seguro (HSM) provisto por la entidad.		
4	La entidad de certificación abierta deberá garantizar el ingreso a la sede electrónica del Ministerio de Hacienda y Crédito Público.		
5	La entidad de certificación abierta debe proveer a sus suscriptores los controladores o drivers para el certificado digital token servidor seguro (HSM), en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación, de presentarse inconvenientes deberá proveer un técnico de la entidad para que verifique personalmente la instalación en los equipos de la Policía Nacional.		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
6	Los certificados digitales a utilizar en el aplicativo SIIF Nación para sus usuarios, son certificados de Función Pública con estándar X.509.V3, los certificados deben cumplir con los requisitos exigidos en el artículo 35 de la Ley 527 de 1999, teniendo en cuenta las siguientes características del certificado digital requeridos en el SIIF Nación: a) Nombre b) Correo electrónico c) Ciudad d) Entidad e) Cédula de ciudadanía f) NIT de la entidad usuaria g) Título o cargo del usuario. h) El certificado digital debe utilizar algoritmo de firma: SHA2RSA		
7	Los certificados digitales de función pública se deben poder utilizar en el SIIF Nación para: a) Autenticación, utilizando un terminador de VPN para acceso al SIIF Nación, el cual verifica la información del certificado y la autorización del SIIF Nación de la entidad de certificación. b) Firmar digitalmente transacciones. c) Firmar digitalmente archivos para ser utilizados en cargas masivas en el SIIF Nación. d) El aplicativo SIIF Nación no provee la herramienta para la firma de archivos. La entidad de certificación debe proveer el soporte para el uso de los certificados digitales para la firma de archivos o documentos electrónicos.		
8	La entidad de certificación digital abierta deberá proveer a la Administración SIIF Nación, para la validación del estado de revocación del certificado, la publicación de la CRL, adicionalmente el SIIF Nación utilizará el método de verificación del estado del certificado llamado OCSP, para la cual la entidad de certificación digital abierta deberá proveer una URL de acceso a este servicio. Cualquier cambio de alguno de estos datos debe ser informado previamente por la entidad de certificación abierta a la administración SIIF Nación. Una vez la Administración SIIF Nación informe que dichos cambios fueron aplicados, podrán ser utilizados en el aplicativo SIIF Nación.		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
9	La entidad de certificación digital abierta debe garantizar, la actualización de la CRL, siendo su responsabilidad que sea oportuna y que esté disponible para consulta durante 7 x 24 x 365 días. La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la actualización o disponibilidad de la CRL, dicha responsabilidad recae directamente sobre la entidad certificadora digital abierta.		
10	La entidad de certificación digital abierta debe garantizar la disponibilidad del servicio OCSP, siendo su responsabilidad que sea oportuno y que esté disponible para consulta durante 7 x 24 x 365 días. La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la disponibilidad del servicio OCSP, dicha responsabilidad recae directamente sobre la entidad de certificación digital abierta.		
11	La entidad de certificación abierta deberá disponer de la infraestructura de operación, servicio y soporte a sus usuarios, según los acuerdos de niveles de servicio que tenga con la entidad usuaria, en este caso (SIIF NACION del Ministerio de Hacienda y Crédito Público).		
12	La entidad de certificación digital debe dar a conocer y capacitar al coordinador SIIF de la entidad y usuarios del SIIF Nación sobre los procedimientos y trámites administrativos para el manejo del ciclo de vida del certificado digital token servidor seguro (HSM). De igual manera brindar el soporte para la solicitud, revocación, bloqueo, reasignación de los certificados digitales, procesos de instalación y uso de las funcionalidades de los dispositivos, el servicio de soporte y asistencia deberá estar disponible de lunes a viernes de 8:00 A.M a 6:00 P.M para lo cual deberá garantizar, el servicio de soporte técnico y asistencia necesaria a través de acceso telefónico, vía web, chat. La entidad de certificación abierta deberá disponer de un contacto de soporte directo con nivel central para resolver casos de tipo técnico y demás requerimientos que se presenten.		
13	La entidad de certificación digital abierta deberá notificar por lo menos con un mes de anticipación la fecha de vencimiento del certificado digital, así mismo ofrecer al coordinador SIIF Nación de la Policía Nacional las herramientas para la gestión (fechas de emisión, fechas de caducidad, cupo utilizado) para una oportuna gestión por parte de este de los certificados digitales token servidor seguro (HSM).		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
14	El contratista deberá otorgar una garantía técnica de los dispositivos token servidor seguro (HSM) por un término no inferior a dos (02) años contados a partir del recibido a satisfacción del bien por parte del supervisor de la aceptación de la oferta de la Policía Nacional una vez se surta todo el trámite administrativo correspondiente; teniendo en cuenta que estos se emiten a los usuarios de forma paulatina a medida que se vence la vigencia y hasta agotar existencias, para lo cual puede transcurrir más de un año desde el recibido a satisfacción de los dispositivos token por parte de la entidad. Una vez enviado el dispositivo token servidor seguro (HSM) al usuario final a partir de su activación y recibido a satisfacción por parte del mismo, tendrán una vigencia de un (1) año.		
15	La entidad de certificación digital deberá enviar los certificados digitales token servidor seguro (HSM), a la dirección de correo electrónico que suministre el supervisor en los tres (03) días calendario siguientes a la radicación de la solicitud, con el respectivo documento de recibido a satisfacción, donde se identifique fecha de emisión, para que sea firmado por el usuario y remitido a la coordinación SIIF, como garantía de recibido del mismo.		
16	La entidad de certificación digital deberá garantizar dentro del día hábil siguiente a la radicación de la solicitud, realizar el proceso de validación de identidad del usuario que recibe el certificado digital token servidor seguro (HSM), sin afectar los términos de emisión (03 días calendario siguientes a la radicación de la solicitud).		
17	En caso que la documentación radicada por el supervisor para la entrega del dispositivo al usuario final tenga algún error, deberá informarse de inmediato para ser subsanada, evitando dilatar los tiempos de entrega.		
18	Cada certificado de firma digital servidor seguro (HSM) tendrá derecho a ser desbloqueado **dos (02)** veces sin costo durante la vigencia del contrato. En la propuesta la entidad deberá informar el costo del desbloqueo cuando sean superior a las **dos (02)** veces, el cual no deberá tener incremento durante la vigencia de la aceptación de oferta y será asumido por el usuario del certificado digital, así mismo, se deberá garantizar que el desbloqueo se realice de forma remota.		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
19	La entidad certificadora abierta deberá otorgar sin costo adicional, reasignaciones a la Policía Nacional, por la misma cantidad de dispositivos token servidor seguro (HSM) adquiridos con la aceptación de oferta. Las reasignaciones por cambio de suscriptor pueden ser solicitadas durante la vigencia del dispositivo token sin tener en cuenta la cantidad, siempre y cuando no exceda la sumatoria del total de certificados digitales servidor seguro (HSM) adquiridos, y que cuente con sesenta (60) días calendario para su vencimiento.		
20	Cuando se solicite la revocación y reasignación del certificado digital token servidor seguro (HSM), el envío al usuario nuevo se debe realizar en un plazo máximo de tres (03) días calendario, contados a partir de la radicación de los documentos. La entidad de certificación digital deberá garantizar dentro del día hábil siguiente a la radicación de la solicitud, realizar el proceso de validación de identidad del usuario que recibe el certificado digital token, sin afectar los términos de emisión (03 días calendario siguientes a la radicación de la solicitud). Así mismo, una vez el usuario reciba el certificado digital deberá garantizar el soporte técnico de instalación y activación del mismo.		
21	El año de vigencia del certificado digital token servidor seguro (HSM) empezará a contar a partir de la fecha de su activación.		
22	La entidad de certificación digital debe proveer una plataforma que permita la carga masiva de solicitudes, teniendo en cuenta que en ocasiones se requiere realizar entre 10 a 100 solicitudes al tiempo.		
23	En cumplimiento al Sistema de Gestión de Seguridad de la Información, el oferente debe cumplir con las políticas de seguridad establecidas sin que sea necesario habilitar puertos, extensiones, accesos a páginas específicas no autorizadas por la Policía Nacional, que generen con ello riesgo o afectación a la Seguridad de la Información de la Policía Nacional o su infraestructura tecnológica y Políticas de dominio y acceso a la red.		

CERTIFICADO DIGITAL TOKEN CRIPTOGRÁFICO PARA EL SISTEMA DE CERTIFICACIÓN ELECTRÓNICA DE TIEMPOS LABORADOS – CETIL Y LA PLATAFORMA DE INTEGRACIÓN DEL SISTEMA DE INFORMACIÓN DE LA PROTECCIÓN SOCIAL – PISIS NEO

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1	Los certificados emitidos deben estar de acuerdo al estándar X.509 V3.		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2	El certificado digital debe utilizar algoritmo de firma: SHA256.		
3	Reconocidos por equipos clientes con sistema operativo Windows 7 o superior.		
4	Reconocimiento a través del puerto USB. (NO es compatible el token Virtual)		
5	Cumplir como mínimo el estándar FIPS 140-1, 140-2 nivel 3 o superior de aseguramiento criptográfico.		
6	Cumplir mínimo IKEY 1000.		
7	Soportar interfaz PKCS11.		
8	La firma se realiza a través de una librería Sclient, la cual debe ser instalada en la máquina del cliente, y es utilizada a través de código JavaScript.		
9	Se requiere que el navegador permita la ejecución de código JavaScript. No se requieren especificaciones adicionales a las del navegador y la utilidad Sclient.		
10	La utilidad Sclient debe ser compatible con Windows 7, 8, 10 o superior, las cuales deben contar con el .Net Framework 4.5 o superior.		
11	Para el proceso de firma no se requiere la apertura de puertos adicionales. La comunicación se realiza a través del puerto HTTS estándar (443).		
12	Cada certificado de firma digital tendrá derecho a ser desbloqueado **dos (02)** veces sin costo durante la vigencia del contrato. En la propuesta la entidad deberá informar el costo del desbloqueo cuando sean superior a las **dos (02)** veces, el cual no deberá tener incremento durante la vigencia de la aceptación de oferta y será asumido por el usuario del certificado digital, así mismo se deberá garantizar que el desbloqueo se realice de forma remota, es decir sin requerir token físico.		
13	La entidad de certificación digital deberá entregar a los usuarios finales en la dirección que suministre el supervisor, mediante correo certificado en sobre de seguridad en los seis (06) días calendario siguientes a la radicación de la solicitud, el dispositivo token criptográfico con el respectivo documento de recibido a satisfacción, donde se identifique el número de serial del token y nombre del funcionario que recibe, para que sea firmado por el usuario directo y remitido a la coordinación SIIF, como garantía de recibido del mismo		
14	La entidad certificadora abierta deberá otorgar sin costo adicional, reasignaciones a la Policía Nacional por la misma cantidad total de certificados digitales tokens criptográficos adquiridos con la aceptación de oferta, así mismo, si el certificado digital token criptográfico le quedan noventa (90) días calendario para su vencimiento podrá ser reasignado nuevamente.		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
15	El año de vigencia del certificado digital token criptográfico empezará a contar a partir de la fecha de su activación.		
16	El contratista deberá otorgar una garantía técnica de los dispositivos token por un término no inferior a dos (02) años contados a partir del recibido a satisfacción del bien por parte del supervisor; teniendo en cuenta que estos se entregan a los usuarios de forma paulatina a medida que se vence la vigencia y hasta agotar existencias, para lo cual puede transcurrir más de un año desde el recibido a satisfacción de los dispositivos token por parte de la entidad. Una vez entregado el dispositivo token al usuario final a partir de su activación y recibido a satisfacción por parte del mismo, tendrán una vigencia de un (1) año.		
17	Los certificados digitales serán entregados de forma total en el Almacén de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, ubicado en la Calle 64 G No. 92-29 Barrio Álamos, teléfono 5159000 ext. 20158, en horario de oficina de lunes a viernes. Posteriormente, el supervisor hará entrega de los dispositivos token a la empresa y realizará la solicitud y radicación de los documentos soporte requeridos por el contratista (*sin ningún otro trámite adicional que dilate la entrega*) en la plataforma que este suministre. La entidad de certificación digital deberá entregar a los usuarios finales en la dirección que suministre el supervisor, mediante correo certificado, en sobre de seguridad, en los seis (06) días calendario siguientes a la radicación de la solicitud, el dispositivo token con el respectivo documento de recibido a satisfacción, donde se identifique el número de serial del token y nombre del funcionario que recibe, para que sea firmado por el usuario directo y remitido a la coordinación SIIF, como garantía de recibido del mismo.		

CERTIFICADO DIGITAL PERSONA JURÍDICA

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1	La entidad certificadora abierta deberá demostrar la autorización de acreditación ante el Organismo Nacional de Acreditación de Colombia – ONAC (Ley 527 de 1999 art. 29-34 y el Decreto 333 de 2014) para expedir certificados digitales de Representación empresa entidad.		
2	El certificado de firma digital debe contener las siguientes características: • El certificado digital se emite mediante el formato PKCS#10. • Certificado X.509 V3		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	• Llave privada de 2048 bits con algoritmo de encripción SHA256 • Algoritmo de firma de certificado con HASH		
3	El certificado para emisor de factura electrónica acredita la identidad del suscriptor y su condición como facturador electrónico, y le permitirá al suscriptor firmar documentos digitalmente en la calidad que acredita su certificado.		
4	El año de vigencia del certificado digital empezará a contar a partir de la fecha de su activación.		
5	Cada certificado digital de persona jurídica tendrá derecho a cuatro (04) reasignaciones de forma gratuita, ya sea por bloqueo de claves o cambio de titular.		
6	La entidad de certificación abierta deberá brindar el soporte para el uso de los certificados digitales, para lo cual deberá garantizar, el servicio de soporte técnico y asistencia necesaria (como acceso telefónico vía web, chat) a las unidades policiales. En caso de que sea necesario el servicio de soporte técnico y asistencia de manera presencial, deberá contar con un funcionario con conocimiento en instalación de certificados digitales token, quien se deberá desplazar hasta las instalaciones de la Dirección General de la Policía Nacional que brinde asesoría.		
7	La entidad de certificación digital deberá entregar los certificados digitales, a la dirección de correo electrónico que suministre el supervisor en los tres (03) días calendario siguientes a la radicación de la solicitud, el certificado de persona jurídica con el respectivo documento de recibido a satisfacción, donde se identifique fecha de emisión, para que sea firmado por el usuario directo y remitido a la coordinación SIIF, como garantía de recibido del mismo.		
8	En cumplimiento al Sistema de Gestión de Seguridad de la Información, el oferente debe cumplir con las políticas de seguridad establecidas sin que sea necesario habilitar puertos, extensiones, accesos a páginas específicas no autorizadas por la Policía Nacional, que generen con ello riesgo o afectación a la Seguridad de la Información de la Policía Nacional o si infraestructura tecnológica y Políticas de dominio y acceso a la red.		

REQUISITOS GENERALES

No.	ACUERDO DE CONFIDENCIALIDAD	CUMPLE	NO CUMPLE
1	Las partes acuerdan que cualquier información intercambiada, facilitada, creada o hallada, entre ellas en el transcurso de la aceptación de la oferta, será mantenida en estricta confidencialidad y salvo orden de autoridad judicial competente podría ser revelada. Toda información intercambiada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso.		

	El oferente deberá firmar un acuerdo de confidencialidad y no revelación de la información para lo cual deberá diligenciar el FORMULARIO ACUERDO DE CONFIDENCIALIDAD.		
No.	**COMPROMISO ANTICORRUPCIÓN**	**CUMPLE**	**NO CUMPLE**
2	Cumplir con el compromiso de anticorrupción dentro del proceso manifestando que se encuentra dispuesto a suministrar la información propia que resulte necesaria para aportar transparencia al mismo y si se comprueba el incumplimiento del proponente, sus empleados, representantes, asesores o de cualquier otra persona que en el proceso de contratación actúe en su nombre, es causal suficiente para el rechazo de la oferta o para la terminación anticipada del contrato, si el incumplimiento ocurre con posterioridad a la adjudicación del mismo, para lo cual deberá diligenciar el FORMULARIO COMPROMISO ANTICORRUPCIÓN		
No.	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO**	**CUMPLE**	**NO CUMPLE**
3	Cumplir con la implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo, de acuerdo a lo establecido en el Decreto 1072 de 2015, Decreto Único Reglamentario del Sector Trabajo y demás normas que lo complementen, para lo cual deberán diligenciar el FORMULARIO SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO.		
No.	**REQUISITO AMBIENTAL**	**CUMPLE**	**NO CUMPLE**
4	El oferente deberá presentar el certificado de consulta del Registro Único de Infractores Ambientales (RUIA), expedido a través del enlace oficial del Ministerio de Ambiente: https://vital.minambiente.gov.co/SILPA_UT_PRE/RUIA/ConsultarSancion.aspx?Ubic=ext; En caso de presentarse como unión temporal o consorcio, deberá aportarse el certificado RUIA de cada uno de sus integrantes. Así mismo, este certificado deberá		
	ser presentado durante la ejecución del contrato cuando el supervisor lo requiera, con el fin de verificar la existencia o no de sanciones ambientales vigentes que puedan afectar la ejecución del objeto contractual.		
5	El oferente deberá verificar la necesidad de permisos, licencias, concesiones o autorizaciones ambientales de acuerdo a su actividad comercial y, de ser legalmente exigibles, obtenerlos y presentar el documento emitido por la autoridad ambiental competente. En caso de que no aplique por la naturaleza de su actividad comercial deberá declararlo de forma escrita el representante legal bajo la gravedad de juramento, asumiendo plenamente las consecuencias legales, ambientales y contractuales que se deriven del incumplimiento. Se deberán mantener vigentes durante toda la ejecución del contrato. Este requisito se debe entregar junto con la oferta.		
6	El contratista, deberá aplicar buenas prácticas ambientales y adoptar medidas de prevención, mitigación, corrección y control		

	de los impactos ambientales derivados de la ejecución contractual, garantizando el uso eficiente de los recursos naturales y la adecuada gestión de residuos.		
7	El contratista debe cumplir con la política ambiental: *"En la Policía Nacional nos comprometemos a contribuir con la protección del ambiente a través de la prevención de la contaminación, el cumplimiento de la legislación y las diferentes regulaciones ambientales y el control de los impactos ambientales adversos asociados a nuestras instalaciones, procesos y servicios; así como al mejoramiento continuo del desempeño ambiental de la Institución".*		
8	El contratista deberá garantizar que toda la información y documentación entregada a la Policía Nacional que se realicen en formato digital, utilizando medios reutilizables, y ajustándose a los lineamientos de la Directiva Presidencial 04 de 2012 sobre eficiencia administrativa y la Política de Cero Papel en la Administración Pública, (Aplica cuando el contrato contemple la presentación de informes o documentación extensa). En Caso de ser necesaria a la entrega de archivos físicos en papel garantizar su buen uso.		
9	El contratista debe acreditar, mediante los soportes documentales pertinentes, el cumplimiento de las obligaciones legales relacionadas con el pago de los aportes al Sistema de Seguridad Social Integral, prestaciones sociales y afiliación y pago a la Administradora de Riesgos Laborales ARL de sus trabajadores, en misión al objeto contractual. Nota: los anteriores requerimientos ambientales son establecidos mediante comunicación oficial GS-2026-015654-DILOF del 14/05/2026.		
No.	**EXPERIENCIA DEL PROPONENTE**	**CUMPLE**	**NO CUMPLE**
1	**PROPONENTE NACIONAL Y EXTRANJERO CON DOMICILIO O SUCURSAL EN COLOMBIA** El oferente que vaya a proveer los bienes o servicios objeto del presente proceso de selección, trátese de personal natural o jurídica, deberá anexar mínimo una (01) máximo tres (03) constancias (certificaciones o actas de liquidación) de contratos celebrados y ejecutados con entidades públicas o privadas, cuyo objeto sea igual o similar al objeto de la presente contratación "ADQUISICIÓN DISPOSITIVOS TOKEN PARA FIRMA DIGITAL Y CERTIFICADOS DE PERSONA JURÍDICA", la sumatoria de la cuantía de los contratos deberá ser mayor o igual a 9.97 SMMLV. Los documentos deberán contener como mínimo la siguiente información: 1. Nombre del contratista 2. Nombre del contratante		

	3. Objeto del contrato 4. Valor del contrato 5. Fecha de suscripción y fecha de inicio del contrato 6. Fecha de terminación del contrato 7. Personal de contacto para verificar la información: teléfono fijo o celular, correo electrónico institucional, logo (en caso de certificación). 8. Estado del contrato: ejecutado o liquidado. 9. Si es certificación, deberá estar suscrita por el funcionario competente para tal fin. 10. Manifestación clara y explícita donde se evidencie que el contratista cumplió a cabalidad con el objeto del contrato. 11. Porcentaje del valor del contrato que ejecutó como miembro de un consorcio, unión temporal u otra forma de asociación. **NOTA 1**: en cumplimiento del Decreto 1860 de 2021 el cual reglamentó parcialmente la Ley 2069 de 2020 "*Por medio de la cual se impulsa el emprendimiento en Colombia*" y el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, se toma como criterio diferencial para las MiPymes, el numeral 2. Número de contratos para la acreditación de la experiencia. Por tanto, deberán anexar mínimo una (01) máximo cuatro (04) constancias (certificaciones o actas de liquidación) que cumplan con lo antes relacionado. **NOTA 2:** no se aceptarán auto certificaciones. **NOTA 3**: no se tendrán en cuenta las certificaciones de contratos en ejecución. **NOTA 4**: no se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas. **NOTA 5**: cuando los documentos no indiquen su valor en SMMLV o si estos son de años anteriores a 2026, se hará la respectiva conversión de acuerdo al año en que terminó el contrato. La verificación será realizada por el comité evaluador técnico. **NOTA 6**: si los contratos acreditados fueron realizados bajo la modalidad de consorcio, unión temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del consorcio, unión temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del consorcio, unión temporal u otra forma de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes en la ejecución del contrato.		

	NOTA 7: en el caso de proponentes plurales, todos sus integrantes deben acreditar experiencia en contratos ejecutados con objeto igual o similar al del presente proceso de contratación. **NOTA 8**: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite. La Policía Nacional se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.		

Subteniente **TANIA JULIETH PRECIADO CAICEDO**
Estructurador estudio previo