CONTRATO DE COMPRAVENTA PN DILOF No. 06-2-10169-25

Bogotá D.C., 30 ABR 2025

Señor
JUAN CARLOS YAÑEZ ARENAS
Representante Legal
THOMAS SIGNE SOLUCIONES TECNOLÓGICAS GLOBALES S.A.S.
Teléfonos: (601) 3693720
Correo Electrónico: notificacionesjudicialestgs@thomasgreg.com
Dirección: Avenida de las Américas No. 44-57, Bogotá D.C.

Asunto: aceptación de oferta proceso PN DILOF MIC 163 2025

La Subdirección Logística y Financiera de la Policía Nacional, informa que la propuesta presentada por usted el 23/04/2025 mediante la plataforma SECOP II, dentro del proceso de Mínima Cuantía **PN DILOF MIC 163 2025,** cuyo objeto es la **"ADQUISICIÓN DISPOSITIVOS TOKEN PARA FIRMA DIGITAL Y CERTIFICADOS DE PERSONA JURÍDICA**", ha sido aceptada así:

CONTRATANTE	POLICÍA NACIONAL – DIRECCIÓN LOGÍSTICA Y FINANCIERA
NIT	800.141.397–5
ORDENADOR DEL GASTO	Coronel EDWIN ORLANDO CORREA CORREA
CÉDULA DE CIUDADANÍA No.	79.999.736 expedida en Bogotá D.C.
CARGO	Subdirector Logístico y Financiero
DISPOSICIÓN DE NOMBRAMIENTO	Orden Interna de Personal No. 026 del 16/02/2024
RESOLUCIÓN DE DELEGACIÓN	Resolución Nro. 00364 del 12/02/2025
CONTRATISTA	NOMBRE: THOMAS SIGNE SOLUCIONES TECNOLOGICAS GLOBALES S.A.S. NIT: 900.962.071-5 REPRESENTANTE LEGAL: JUAN CARLOS YAÑEZ ARENAS C.C. No: 13.468.672 de Cúcuta CIUDAD DE NOTIFICACIÓN: Bogotá D.C. DIRECCIÓN: Avenida de las Américas No. 44-57, Bogotá D.C. TELÉFONOS: (604) 3693720 CORREOS: comercial@thomas-signe.co, juan.yanez@thomasgreg.com, rosmery.sanchez@thomas-signe.co, notificacionesjudicialestgs@thomasgreg.com
SUPERVISOR DE LA ACEPTACIÓN DE OFERTA	La supervisión de los ítems Nros. 1 y 3 estarán a cargo del Delegado Coordinador del Sistema integrado de Información Financiera – SIIF Nación ante el Ministerio de Hacienda y Crédito Público o quien haga sus veces, o quien con posterioridad designe la Subdirección Logística y Financiera, la supervisión del ítem Nro. 2, estará a cargo del sustanciador Grupo de Información y Consulta de la Secretaría General de la Policía Nacional o quien haga sus veces, o quien con posterioridad designe la Subdirección Logística y Financiera, quienes deberán dar estricto cumplimiento a lo establecido en la Ley 1474 del 12 de julio de 2011 "*Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública*", en su artículo 83 "*Supervisión e interventoría contractual*" y artículo 84 "*Facultades y deberes de los supervisores y los interventores*", además de las establecidas en la Resolución No. 00090 del 15 de enero de 2018.

<table>
<tr><td>FORMA DE PAGO</td><td>La Policía Nacional – Dirección Logística y Financiera cancelará el valor de la aceptación de la oferta de la siguiente forma:

Se realizará un sólo pago contra entrega de los dispositivos token criptográficos (CETIL y PISIS-NEO) y de la emisión de los dispositivos token servidor seguro (HSM) y de los certificados digitales persona jurídica, al Almacén Técnico 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, en moneda legal colombiana, dentro de los sesenta (60) días calendario, siguientes a la radicación de la factura y el recibido a satisfacción por parte del supervisor del contrato, se deberá anexar el formato planilla de recepción de la DIAN y la declaración de importación, junto con los demás documentos requeridos por la Dirección Logística y Financiera, de acuerdo al derecho a turno y a la disponibilidad del Plan Anual de Caja (PAC).

Si los documentos en referencia no se reciben dentro del plazo establecido o si recibidos son devueltos por inconsistencias tales como la falta de información o mal diligenciamiento de los mismos, la Policía Nacional Dirección Logística y Financiera, reprogramará el valor a cancelar una vez se hubieren subsanado las observaciones, se haya cumplido con el trámite documental dentro del plazo indicado y de acuerdo al derecho a turno y a la disponibilidad Plan Anual de Caja (PAC).

Nota: para efectuarse el pago el contratista deberá cumplir con lo establecido en la Resolución No. 165 del 01/11/2023, "Por la cual se desarrolla el sistema de facturación, los proveedores tecnológicos, se adopta la versión 1.9 del anexo técnico de factura electrónica de venta, se expide el anexo técnico 1.0 del documento equivalente electrónico, y se dictan otras disposiciones en materia del sistema de facturación" y los lineamientos y parámetros contemplados en las Circulares Externas 002 del 08/01/2016, mediante la cual se implementó el "PAGO A BENEFICIARIO FINAL A TRAVÉS DEL SIIF NACIÓN" y 042 del 26/12/2023, mediante la cual se implementó el "SISTEMA FACTURACIÓN ELECTRÓNICA DEL SIIF NACIÓN", expedidas por el Ministerio de Hacienda y Crédito Público, en caso de que aplique.
El pago se hará a la siguiente cuenta:

NOMBRE BENEFICIARIO: THOMAS SIGNE SOLUCIONES TECNOLÓGICAS GLOBALES S.A.S
IDENTIFICACIÓN: 900.962.071-5
TIPO DE CUENTA: CORRIENTE
CUENTA No: 095758504
ENTIDAD FINANCIERA: BANCO DE BOGOTÁ</td></tr>
<tr><td>APROPIACIÓN PRESUPUESTAL</td><td>La contratación se encuentra amparada con el Certificado de Disponibilidad Presupuestal No. 34525 del 22/03/2025, por valor de TREINTA Y SEIS MILLONES NOVECIENTOS DIECISIETE MIL NOVECIENTOS CUARENTA Y UN PESOS CON VEINTE CENTAVOS MONEDA LEGAL ($36.917.941,20), recurso 10.</td></tr>
<tr><td>VALOR</td><td>El valor del contrato es de VEINTINUEVE MILLONES QUINIENTOS SESENTA Y CINCO MIL PESOS MONEDA LEGAL ($29.565.000,00) EXENTO DE IVA, discriminado así:

<table>
<tr><th>ÍTEM</th><th>RUBRO Y DESAGREGACIÓN PRESUPUESTAL</th><th>UNIDAD</th><th>DESCRIPCIÓN</th><th>RECURSO</th><th>CANTIDAD</th><th>VALOR UNITARIO EXENTO DE IVA</th><th>VALOR TOTAL EXENTO DE IVA</th></tr>
<tr><td>1</td><td rowspan="3">MAQUINARIA DE OFICINA, CONTABILIDAD E INFORMÁTICA

A-02-02-01-004-005</td><td rowspan="3">DILOF 000A</td><td>Token Servidor Seguro (HSM) Para SIIF Nación</td><td rowspan="3">10</td><td>950</td><td>$ 30.000,00</td><td>$28.500.000,00</td></tr>
<tr><td>2</td><td>Token Criptográfico Para CETIL y PISIS NEO</td><td>3</td><td>$ 35.000,00</td><td>$105.000,00</td></tr>
<tr><td>3</td><td>Certificado Digital Persona Jurídica</td><td>30</td><td>$ 32.000,00</td><td>$960.000,00</td></tr>
<tr><td colspan="6">VALOR TOTAL</td><td colspan="2">$29.565.000,00</td></tr>
</table>
</td></tr>
</table>

	Nota: los elementos de acuerdo a su utilización, desde el componente técnico se encuentran catalogados por el Grupo Contaduría General de la Policía Nacional en el numeral 3 literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional, del artículo 188 de la Ley 1819 del 29/12/2016, el cual modificó el artículo 477 del Estatuto Tributario, son bienes que no causan el impuesto sobre las ventas. Mediante comunicación oficial electrónica No. GS-2025-004634-DILOF del 13 de febrero de 2025, el Grupo de Central de Cuentas de la Dirección Logística y Financiera, indica: *(..) "… están exentos del IVA, la ADQUISICIÓN DE DISPOSITIVOS TOKEN PARA FIRMA DIGITAL Y CERTIFICADOS DE PERSONA JURÍDICA".*
ESPECIFICACIONES TÉCNICAS	Las contempladas en el ANEXO No. 1 de la presente aceptación de oferta.
GARANTÍA ÚNICA Y SANCIONES	Dentro de los tres (3) días hábiles siguientes a la publicación de la aceptación de oferta, el CONTRATISTA deberá constituir, firmar y presentar a favor de la POLICÍA NACIONAL – DIRECCIÓN LOGÍSTICA Y FINANCIERA, la Garantía Única que cubra los siguientes amparos: **1. GARANTÍA ÚNICA:** **a). CUMPLIMIENTO DEL CONTRATO:** por el veinte por ciento (20%) del valor de la aceptación de la oferta, vigente a partir de la suscripción de la aceptación de la oferta y de las prórrogas si las hubiere, por un término igual al plazo de ejecución y seis (06) meses más. **b). CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES:** por el cincuenta por ciento (50%) del valor de la aceptación de la oferta, vigente a partir de la recepción de los bienes y doce (12) meses más. **b). CALIDAD DEL SERVICIO:** por el cincuenta por ciento (50%) del valor de la aceptación de la oferta, vigente a partir de la suscripción de la aceptación de la oferta y de las prórrogas si las hubiere, por un término igual al plazo de ejecución y doce (12) meses más. **c). PAGO DE SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES:** por el cinco (5%) del valor de la aceptación de la oferta, vigente a partir de la suscripción de la aceptación de la oferta y de las prórrogas si las hubiere, por un término igual al plazo de ejecución y tres (3) años más. **PARÁGRAFO:** en caso de constituirse póliza, debidamente firmada por el tomador, en la misma deberá constar expresamente que la entidad aseguradora renuncia al beneficio de excusión y que se ampara el cumplimiento del contrato, el pago de las multas y de la penal pecuniaria convenidas. **2. SANCIONES:** **a). MULTA POR LA MORA EN LA CONSTITUCIÓN DE LOS REQUISITOS DE EJECUCIÓN:** cuando el CONTRATISTA no constituya dentro del término y en la forma prevista en el contrato, o en alguno de sus modificatorios, la póliza de garantía única, la POLICÍA podrá mediante acto administrativo afectar al CONTRATISTA con multa, cuyo valor se liquidará con base en el cero punto dos por ciento (0.2%) del valor del contrato, por cada día de retardo y hasta por diez (10) días calendario. **b) MULTAS:** en caso de mora o incumplimiento parcial de alguna de las obligaciones derivadas del contrato por causas imputables al CONTRATISTA- salvo circunstancias de fuerza mayor o caso fortuito conforme a las definiciones del artículo 1 de la Ley 95 de 1890, las partes acuerdan que la POLICÍA, mediante acto administrativo, hará efectivas multas sucesivas, cuyo valor se liquidará con base en el cero punto cinco por ciento (0.5%) del valor dejado de cumplir o entregar, por cada día de retardo y hasta por quince (15) días calendario. Esta sanción se impondrá conforme a la ley y se reportará a la Cámara de Comercio competente de conformidad con lo previsto en el artículo 6 de la Ley 1150 de 2007, modificado por el artículo 221 del Decreto 19 de 2012. **c) PENAL PECUNIARIA:** de conformidad con lo previsto en los artículos 1592 y 1599 del Código Civil Colombiano y el

	artículo 17 de la Ley 1150 de 2007, en caso de declaratoria de caducidad o de incumplimiento total o parcial de las obligaciones derivadas del contrato **incluyendo la del plazo**, previo al desarrollo del debido proceso y en concordancia con el principio de proporcionalidad de que trata el artículo 867 del Código de Comercio, el CONTRATISTA pagará a la POLICÍA, a título de pena pecuniaria como tasación anticipada de perjuicios, una suma equivalente al veinte por ciento (20%) del valor del contrato cuando se trate de incumplimiento total del contrato y proporcional al incumplimiento parcial del contrato, sin que en todo caso supere el porcentaje ya señalado. Para efectos de calcular el monto del incumplimiento parcial relativo a la obligación del plazo de ejecución, se empleará la misma fórmula de estimación de valor contemplada en el literal b) de la presente cláusula. La imposición de esta pena pecuniaria se considerará como pago parcial y definitivo de los perjuicios que cause a la POLICÍA. No obstante, la POLICÍA se reserva el derecho de cobrar perjuicios adicionales por encima del monto de lo aquí pactado siempre que los mismos se acrediten. **PARÁGRAFO. - APLICACIÓN DEL VALOR DE LAS SANCIONES PECUNIARIAS:** una vez ejecutoriada la resolución por medio de la cual se hace efectiva alguna de las sanciones aquí estipuladas, el CONTRATISTA dispondrá de quince (15) días calendario para proceder de manera voluntaria para a su pago. Las multas no serán reintegrables aún en el supuesto que el CONTRATISTA dé posterior ejecución a la obligación incumplida. En caso de no pago voluntario las multas y/o sanciones impuestas se podrán tomar del saldo a favor del CONTRATISTA si lo hubiere, hacer efectiva la garantía si la hubiere o acudir al cobro coactivo.
PLAZO Y FORMA DE EJECUCIÓN	**PLAZO DE EJECUCIÓN** El plazo de ejecución de la aceptación de la oferta será a partir de la aprobación de la garantía única y la expedición del Registro Presupuestal de Compromiso, hasta el 15 de agosto del 2025, previa coordinación con los supervisores designados. **Nota:** Se deberá hacer entrega de la totalidad de los dispositivos token servidor seguro (HSM) para firma digital; los dispositivos token criptográfico para el uso del Sistema de Certificación Electrónica de Tiempos Laborados - CETIL y la Plataforma de Integración del Sistema de Información de la Protección Social - PISIS NEO, y certificados digitales persona jurídica. **FORMA DE EJECUCIÓN** La forma de ejecución del contrato se realizará de manera total, de conformidad con el anexo "ESPECIFICACIONES TÉCNICAS" y demás obligaciones, en coordinación permanente con el supervisor de la aceptación de oferta, dentro del plazo de ejecución. Una vez entregados los dispositivos token criptográfico, servidor seguro (HSM) y certificados de persona jurídica deberán ser emitidos y activados de acuerdo a las solicitudes de la Coordinación SIIF de la Policía Nacional y/o Supervisor de la aceptación de oferta, para ser enviados a cada funcionario a nivel país, hasta agotar la totalidad de los certificados de acuerdo a los requerimientos estipulados en el anexo "ESPECIFICACIONES TÉCNICAS". Posteriormente, cuando el supervisor envíe la solicitud con los documentos soporte requeridos para proceso de asignación, reasignación o desbloqueo según sea el caso, el contratista deberá entregar a los usuarios finales dentro de los seis (6) días calendario siguientes a la radicación de la solicitud, el dispositivo token criptográfico, servidor seguro (HSM) o certificados de persona jurídica con el respectivo documento de recibido a satisfacción, donde se identifique el nombre del funcionario que recibe, de acuerdo a las condiciones estipuladas en el anexo "ESPECIFICACIONES TÉCNICAS" del presente documento. Por otro lado, para el recibido a satisfacción y el ingreso a los inventarios de la Policía Nacional, una vez se realice la aprobación de la garantía única, el contratista emitirá certificación de entrega de los novecientos cincuenta (950) Token Servidor Seguro (HSM) Para SIIF Nación y de los treinta (30) certificados de persona jurídica.

LUGAR DE ENTREGA	Se deberá hacer entrega de la totalidad de los dispositivos token criptográfico, servidor seguro (HSM) y de los certificados de persona jurídica, en el Almacén Técnico 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.
MONEDA DEL CONTRATO	Pesos colombianos
VIGENCIA	La vigencia de la presente aceptación de oferta será de cuatro (4) meses adicionales al plazo de ejecución.

De acuerdo a lo anterior, el Jefe del Área de Contratación, recomienda al señor Subdirector Logístico y Financiero, aceptar la oferta presentada en el proceso de Mínima Cuantía **PN DILOF MIC 163 2025**, cuyo objeto es la **"ADQUISICIÓN DISPOSITIVOS TOKEN PARA FIRMA DIGITAL Y CERTIFICADOS DE PERSONA JURÍDICA",** por la firma THOMAS SIGNE SOLUCIONES TECNOLÓGICAS GLOBALES S.A.S., identificada con NIT: 900.962.071-5, en atención a que cumplió técnica, jurídica y económicamente, de acuerdo con los términos establecidos en la invitación que rigió el proceso y la oferta presentada.

Atentamente,

Teniente coronel **LUIS FERNANDO BURGOS MEJÍA**
Jefe Área de Contratación

Coronel **EDWIN ORLANDO CORREA CORREA**
Subdirector Logístico y Financiero de la Policía Nacional

Elaboró: CPS4. Andrea Galindo Muñoz/ DILOF - GUPRE
Revisó: CT. Yuly Katherine Beltrán Gutiérrez / DILOF - GUPRE
MY. José Ricardo Rodríguez Andrade / DILOF – ASJUR

Fecha de elaboración: 29/04/2025
Ubicación c:\\mis documentos\Informes 2025

Carrera 59 26-21 CAN
Teléfonos: 601 5159000 Ext 20183 - 20184
dilof.arcon-gupre14@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

ANEXO No. 1
ESPECIFICACIONES TÉCNICAS

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

No.	ESPECIFICACIONES TÉCNICAS
1	El contratista debe estar autorizado por el Organismo Nacional de Acreditación de Colombia – ONAC, para expedir certificados digitales de Función Pública.
2	El contratista debe estar autorizado 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 el contratista, 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 el contratista, quien 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 el contratista.
4	El contratista debe garantizar el ingreso a la sede electrónica del Ministerio de Hacienda Nacional.
5	El contratista 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 del contratista para que verifique personalmente la instalación en los equipos de la Policía Nacional.
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 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. El contratista debe proveer el soporte para el uso de los certificados digitales para la firma de archivos o documentos electrónicos.

No.	ESPECIFICACIONES TÉCNICAS
8	El contratista debe 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 el contratista deberá proveer una URL de acceso a este servicio. Cualquier cambio de alguno de estos datos debe ser informado previamente por el contratista 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.
9	El contratista 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 el contratista.
10	El contratista 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 el contratista.
11	El contratista debe 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	El contratista 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. El contratista debe disponer de un contacto de soporte directo con nivel central para resolver casos de tipo técnico y demás requerimientos que se presenten.
13	El contratista debe 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
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 almacenista técnico de la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional; 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	El contratista deberá enviar los certificados digitales token servidor seguro (HSM), a la dirección de correo electrónico que suministre el supervisor en los seis (6) 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	El contratista 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 (6 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. El costo del desbloqueo cuando sea superior a **dos (02)** veces, 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.
19	El contratista debe otorgar sin costo adicional, reasignaciones a la Policía Nacional, por la misma cantidad de dispositivos token servidor seguro (HSM) adquiridos en la presente 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 seis (06) días calendario, contados a partir de la radicación de los documentos. El contratista debe 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 (6 días calendario siguientes a la radicación de la solicitud)
21	El año de vigencia del certificado digital token servidor seguro (HSM) empezará a contar a partir de la fecha de su activación.
22	El contratista 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 contratista debe cumplir con las políticas de seguridad establecidas sin que sea necesario habilitar puertos, extensiones, accesos a paginas especificas 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.

CERTIFICADO DIGITALTOKEN 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
1	Los certificados emitidos deben estar de acuerdo al estándar X.509 V3.
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 estándar FIPS 140-2 level 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 o 10, 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. El costo del desbloqueo cuando sea superior a **dos (02)** veces, 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	El contratista debe entregar a los usuarios finales en la dirección que suministre el supervisor, mediante correo certificado en sobre de seguridad en los seis (6) 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	El contratista debe otorgar sin costo adicional, reasignaciones a la Policía Nacional por la misma cantidad total de certificados digitales tokens criptográficos adquiridos en la presente 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
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 Técnico 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. El contratista debe entregar a los usuarios finales en la dirección que suministre el supervisor, mediante correo certificado, en sobre de seguridad, en los seis (6) 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
1	El contratista debe 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 • 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 ó cambio de titular.
6	El contratista debe 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	El contratista debe entregar los certificados digitales, a la dirección de correo electrónico que suministre el supervisor en los seis (6) 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

No.	ESPECIFICACIONES TÉCNICAS
	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 contratista debe cumplir con las políticas de seguridad establecidas sin que sea necesario habilitar puertos, extensiones, accesos a paginas especificas 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

REQUISITO AMBIENTAL

- El contratista deberá alinearse al Sistema de Gestión Ambiental de la Policía Nacional conforme a la norma ISO 14001:2015, con el propósito de promover la sostenibilidad ambiental en los procesos, productos y servicios de la institución, esto incluye la adherencia a la Política Ambiental.

- El contratista se compromete a promover la protección del medio ambiente y la conservación de los recursos naturales, mediante la implementación de medidas preventivas para la reducción de la contaminación, así como el cumplimiento de la legislación y normatividad ambiental vigente, asociadas a su actividad económica o productiva.

- El contratista deberá garantizar, en lo posible y sin comprometer la calidad del producto, que los materiales utilizados para los empaques y/o embalajes sean reciclables o provengan de fuentes sustentables (declaración del fabricante – especificaciones técnicas), de igual forma evitar el uso excesivo de los mismos, de acuerdo a los parámetros contemplados por las autoridades ambientales competentes.

- El contratista deberá garantizar que todo el material que se entregue a la Policía Nacional en forma digital, se realice en un medio reutilizable, los escritos deberán estar ajustados de acuerdo a la Directiva Presidencial 04 de 2012 "Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública" (Aplica a los contratos en donde se deben presentar informes"

- "*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*".

- El contratista deberá dar cumplimiento a la Política Ambiental del Sistema de Gestión Ambiental, cada vez que se realicen actividades dentro las instalaciones policiales e involucren el alcance del Sistema de Gestión Ambiental o alguno de los procesos: (Convivencia y Seguridad Ciudadana, Prevención, Logística y Abastecimiento, Administración de Recursos Financieros, Direccionamiento del Talento Humano, Direccionamiento Estratégico, Direccionamiento del SGI, Mejora Continua e Innovación, Direccionamiento Tecnológico, Integridad Policial, Comunicación Pública, Control Interno, Actuación Jurídica y Gestión Documental y Relaciones Internacionales), así como las actividades y servicios generados de otros procesos para la Selección e Incorporación.

ACUERDO DE CONFIDENCIALIDAD

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 contratista firmó un acuerdo de confidencialidad y no revelación de la información, para lo cual diligenció el formulario "ACUERDO DE CONFIDENCIALIDAD".

COMPROMISO ANTICORRUPCIÓN
Cumplir con el compromiso de anticorrupción durante la ejecución del contrato 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 contratista, sus empleados, representantes, asesores o de cualquier otra persona que actúe en su nombre, es causal suficiente para la terminación anticipada del contrato, para lo cual el contratista diligenció el formulario "COMPROMISO ANTICORRUPCIÓN".
SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO
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 el contratista diligenció el formulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO".



Capitán **ERIKA GISELLE URREA VILLADA**
Estructurador estudio previo