ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	POLICÍA NACIONAL
CERTIFICACIÓN DE LA NECESIDAD	

En mi calidad de Delegado de la Coordinación SIIF de la Policía Nacional, manifiesto con la suscripción de esta certificación que consultado el archivo de contratos para la adquisición de novecientos cincuenta (950) dispositivos token para ser utilizados en el aplicativo SIIF Nación por los usuarios de las unidades policiales a nivel nacional, tres (3) dispositivos token para ser utilizados en Certificación Electrónica de Tiempos Laborados –CETIL y la Plataforma de Integración del Sistema de Información de la Protección Social – PISIS NEO y treinta (30) certificados digitales de persona jurídica, se constata la necesidad de realizar la contratación de estos teniendo en cuenta que la vigencia de los mismos es de un (01) año, por lo que se requiere sean renovados a partir del mes de agosto de 2025, para dar continuidad a las labores del ingreso de la información financiera y de facturación electrónica, de la Institución en el aplicativo SIIF Nación del Ministerio de Hacienda y Crédito Público, así mismo, mediante comunicación oficial No. GS-2025-015690-DITAH del 26 de febrero de 2025, la Dirección de Talento Humano manifiesta la necesidad de certificados digitales token, en atención al reconocimiento de viáticos dentro del país a través del SIIF-NACIÓN, considerando las pruebas piloto que se llevarán a cabo para la implementación del procedimiento "Reconocimiento de viáticos"

Firma,

Capitán **ERIKA GISELLE URREA VILLADA**
Delegado Coordinador SIIF Nación

HOJA

EN

BLANCO

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 Nacional.		
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 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 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	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 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	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 (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. 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 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. 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 (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	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 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 MÍNIMAS	CUMPLE	NO CUMPLE
1	Los certificados emitidos deben estar de acuerdo al estándar X.509 V3.		
2	El certificado digital debe utilizar algoritmo de firma: SHA256		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
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. 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 (6) días calendario		

No.	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	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 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.		
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. 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 (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 MINIMAS	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 • 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	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 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 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 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

EXPERIENCIA DEL PROPONENTE	CUMPLE	NO CUMPLE
Con el fin de garantizar la calidad y el cumplimiento en la ejecución de la aceptación de oferta, el oferente deberá anexar máximo tres (3) certificaciones de contratos (una certificación por contrato) celebrados con entidades públicas y/o privadas, cuyo objeto sea igual o similar al objeto de la presente contratación, la sumatoria de la cuantía de las certificaciones deberá ser mayor o igual al a 12,96 SMMLV, estas certificaciones deberán contener la siguiente información: • Fecha de suscripción del contrato. • Dirección y número telefónico del contratante. • Nombre o razón social del contratante. • Nombre o razón social del contratista. • Valor del contrato. • Objeto del contrato. • Fecha de la certificación o contrato. • Manifestación clara que el contratista cumplió a cabalidad con el objeto del contrato. Si el contrato corresponde a uno ejecutado bajo la modalidad de consorcio o unión temporal, el valor a tener en cuenta como experiencia, será igual al valor total facturado del contrato multiplicado por el porcentaje de participación de cada uno de los integrantes. Para lo cual deberá anexar copia del documento consorcial o unión temporal donde se pueda certificar el porcentaje de participación.		
REQUISITO AMBIENTAL	**CUMPLE**	**NO CUMPLE**
• 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	**CUMPLE**	**NO CUMPLE**
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.		

COMPROMISO ANTICORRUPCIÓN	CUMPLE	NO CUMPLE
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		
SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO	**CUMPLE**	**NO CUMPLE**
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.		

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

ETAPA PRECONTRACTUAL

La policía nacional prescinde de la exigencia de la garantía de seriedad de la oferta de conformidad con lo señalado en el artículo 7° de la Ley 1150 de 2007 que indica que *"(…) las garantías no serán obligatorias en los contratos de empréstito, en los contratos interadministrativos, en los de seguros* ***y en los contratos cuyo valor sea inferior al 10% de la menor cuantía*** *a que se refiere esta ley, caso en el cual corresponderá a la entidad determinar la necesidad de exigida (…)".* **(negrilla fuera de texto)**

Lo anterior, teniendo en cuenta la cuantía de la contratación, la naturaleza del objeto del contrato, la ejecución de los contratos antes celebrados por esta dirección con objeto igual o similar, en los que no se presentaron incumplimientos, no se considera necesario la solicitud de garantía de seriedad, tomando en consideración que las obligaciones y los riesgos analizados en el presente proceso se pueden avalar por el contratista a través de una garantía única de cumplimiento, expedida por una compañía de seguros legalmente autorizada en Colombia.

ETAPA CONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA Y VIGENCIA
GARANTÍA ÚNICA	RIESGO JURÍDICO	INCUMPLIMIENTO DEL CONTRATO	VEINTE POR CIENTO (20%) DEL VALOR DEL CONTRATO	CONTRATISTA	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.	PROPENDE POR EL CUMPLIMIENTO DEL OBJETO CONTRACTUAL EN ARAS DE VELAR POR LOS FINES ESENCIALES DEL ESTADO EVITANDO UN DETRIMENTO PATRIMONIAL PARA LA ADMINISTRACIÓN.
GARANTÍA ÚNICA	RIESGO OPERATIVO	CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES	CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO.	CONTRATISTA	VIGENTE A PARTIR DE LA RECEPCIÓN DE LOS BIENES Y DOCE (12) MESES MAS.	CUBRE A LA ENTIDAD ESTATAL DE LOS PERJUICIOS IMPUTABLES AL CONTRATISTA POR LA DEFICIENTE CALIDAD DE LOS BIENES QUE SURJAN DURANTE Y CON POSTERIORIDAD A LA EJECUCIÓN DEL MISMO, EVITANDO UN DETRIMENTO PATRIMONIAL PARA LA ADMINISTRACIÓN.

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA Y VIGENCIA
GARANTÍA ÚNICA	RIESGO OPERATIVO	CALIDAD DEL SERVICIO	CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO.	CONTRATISTA	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 MAS.	CUBRE A LA ENTIDAD ESTATAL DE LOS PERJUICIOS IMPUTABLES AL CONTRATISTA POR LA DEFICIENTE CALIDAD DEL SERVICIO QUE SURJAN DURANTE Y CON POSTERIORIDAD A LA EJECUCIÓN DEL MISMO, EVITANDO UN DETRIMENTO PATRIMONIAL PARA LA ADMINISTRACIÓN.
GARANTÍA ÚNICA	RIESGO JURÍDICO	NO PAGO DE SALARIOS, PRESTACIONES E INDEMNIZACIONES LABORALES	CINCO POR CIENTO (5%) DEL VALOR TOTAL DEL CONTRATO	CONTRATISTA	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.	AMPARA A LA ENTIDAD DE LOS PERJUICIOS QUE SE LE OCASIONEN COMO CONSECUENCIA DEL INCUMPLIMIENTO DE LAS OBLIGACIONES LABORALES A QUE ESTÉ OBLIGADO EL CONTRATISTA, DERIVADAS DE LA CONTRATACIÓN DEL PERSONAL UTILIZADO PARA LA EJECUCIÓN DEL CONTRATO.

CLAÚSULAS SANCIONATORIAS

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA Y VIGENCIA
MULTA	RIESGO JURÍDICO	LA NO CONSTITUCIÓN DENTRO DEL TÉRMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS DE LA PÓLIZA DE GARANTÍA ÚNICA Y/O ALGUNO DE LOS REQUISITOS DE LEGALIZACIÓN.	MULTA CUYO VALOR SE LIQUIDARÁ CON BASE EN EL CERO PUNTO DOS POR CIENTO (0.2%) DEL VALOR DEL CONTRATO.	CONTRATISTA	LA MULTA SE APLICARÁ POR CADA DÍA DE RETARDO Y HASTA POR DIEZ (10) DÍAS CALENDARIO	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.
MULTA	RIESGO JURÍDICO	INCUMPLIMIENTO PARCIAL	MULTAS CUYO VALOR SE LIQUIDARÁ CON BASE EN EL CERO PUNTO CINCO POR CIENTO (0.5%) DEL VALOR DEJADO DE CUMPLIR O ENTREGAR.	CONTRATISTA	LA MULTA SE APLICARÁ POR CADA DÍA DE RETARDO Y HASTA POR QUINCE (15) DÍAS CALENDARIO	AMPARA EL INCUMPLIMIENTO PARCIAL O TOTAL DEL CONTRATO POR PARTE DEL CONTRATISTA, SE BUSCA EL PAGO PARCIAL Y/O DEFINITIVO DE LOS PERJUICIOS QUE SE CAUSEN A LA ENTIDAD.
CLÁUSULA PENAL PECUNIARIA	RIESGO JURÍDICO	INCUMPLIMIENTO PARCIAL O TOTAL DE LAS OBLIGACIONES DERIVADAS DEL CONTRATO, INCLUYENDO LA DEL PLAZO Y/O DECLARATORIA DE CADUCIDAD.	VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO CUANDO SE TRATE DE INCUMPLIMIENTO TOTAL DEL CONTRATO O CADUCIDAD DEL MISMO, O PROPORCIONAL AL INCUMPLIMIENTO PARCIAL DEL CONTRATO, SIN QUE EN TODO CASO SUPERE EL PORCENTAJE SEÑALADO.	CONTRATISTA	A PARTIR DE LA SUSCRIPCIÓN DEL CONTRATO Y DE LAS PRÓRROGAS SI LAS HUBIESE POR UN TÉRMINO IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y HASTA LA LIQUIDACIÓN DEL MISMO.	AMPARA EL INCUMPLIMIENTO PARCIAL O TOTAL DEL CONTRATO POR PARTE DEL CONTRATISTA, SE BUSCA EL PAGO PARCIAL Y/O DEFINITIVO DE LOS PERJUICIOS QUE SE CAUSEN A LA ENTIDAD.

OTROS RIESGOS DERIVADOS DEL PROCESO DE CONTRATACIÓN

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DEL RIESGO	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA Y VIGENCIA
GARANTÍA TÉCNICA	RIESGO OPERATIVO	CALIDAD DE LOS BIENES	VALOR DESPERFECTOS Y/O COMPONENTES DE LOS ELEMENTOS	CONTRATISTA	VIGENTE POR UN TÉRMINO DE DOS (02) AÑOS DE ACUERDO A LA ESPECIFICACIÓN TÉCNICA CONTADOS A PARTIR RECIBIDO A SATISFACCIÓN DE LOS ELEMENTOS	AMPARA EL RIESGO DEL DAÑO OCASIONADO POR FALLAS DE CALIDAD DE LOS MATERIALES O FALLAS EN LA FABRICACIÓN TALES COMO: DEFECTOS EN LOS ACABADOS, DISEÑO ETC.

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

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS

ANÁLISIS DE RIESGO Y FORMA DE MITIGARLO

POLICÍA NACIONAL

No.	1	2	3	4	5
Clase	ESPECÍFICO	ESPECÍFICO	ESPECÍFICO	ESPECÍFICO	ESPECÍFICO
Fuente	INTERNO	EXTERNO	EXTERNO	EXTERNO	EXTERNO
Etapa	SELLECCIÓN	EJECUCIÓN	EJECUCIÓN	EJECUCIÓN	EJECUCIÓN
Tipo	OPERACIONAL	OPERACIONAL	OPERACIONAL	OPERACIONAL	OPERACIONAL
Descripción	RIESGOS ASOCIADOS AL NO CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS EN LA INVITACIÓN	QUE NO SE CUMPLA EL PLAN DE DISTRIBUCIÓN PROYECTADO POR LA INSTITUCIÓN	QUE LOS ELEMENTOS PRESENTEN FALLAS DE CALIDAD DURANTE SU USO.	NO ENTREGA DE LOS ELEMENTOS CONTRATADOS EN EL PLAZO DE EJECUCIÓN ESTIPULADO	QUE EL CONTRATISTA NO CUMPLA CON LA RESERVA Y CONFIDENCIALIDAD DE LA INFORMACIÓN.
Consecuencia de la Ocurrencia del Evento	DECLARATORIA DESIERTO DEL PRESENTE PROCESO	QUE NO SE CUMPLA CON EL PLAZO DE ENTREGA DE LOS BIENES CON LAS CONDICIONES TÉCNICAS REQUERIDAS EN EL	NO CONTAR CON LOS BIENES NECESARIOS PARA ENTREGAR A LAS UNIDADES POLICIALES.	NO SE SATISFACE LA NECESIDAD INSTITUCIONAL REFERENTE A LA ENTREGA DE LOS ELEMENTOS CONTRATADOS	NO CUMPLIMIENTO CON LA NECESIDAD
Probabilidad	2	1	1	3	1
Impacto	4	4	4	5	4
Calificación Total	6	5	5	8	5
Prioridad	ALTO	MEDIO	MEDIO	ALTO	MEDIO
¿A quién se le asigna el riesgo?	CONTRATISTA	CONTRATISTA	CONTRATISTA	CONTRATISTA	CONTRATISTA
Tratamiento controles a ser implementados	REDUCIR LA PROBABILIDAD DEL OFERENTE EN SU OCURRENCIA/ EL CONTRATISTA DEBERÁ EN LA OFERTA SEÑALAR Y ANEXAR LOS DOCUMENTOS QUE CUMPLE CON LA TOTALIDAD DE LOS REQUISITOS EXIGIDOS POR LA ENTIDAD.	REDUCIR LA PROBABILIDAD DE OCURRENCIA / DESDE LA PRESENTACIÓN DE LA OFERTA EL CONTRATISTA DEBERÁ GARANTIZAR QUE CUMPLE CON LA ENTREGA DE LOS BIENES EN EL PLAZO DE EJECUCIÓN REQUERIDO POR LA ENTIDAD.	REDUCIR LA PROBABILIDAD DE OCURRENCIA/ UNA VEZ SE EVIDENCIE LA DEFICIENCIA EN LA CALIDAD DE LOS ELEMENTOS EL CONTRATISTA DEBERÁ GARANTIZAR SU REEMPLAZO CONFORME A LO ESTABLECIDO EN LA GARANTÍA TÉCNICA, EN UN PERIODO NO MAYOR A 30 DÍAS.	REDUCIR LA PROBABILIDAD DE OCURRENCIA/ EL CONTRATISTA DEBERÁ GARANTIZAR QUE LOS ELEMENTOS SERÁN ENTREGADOS EN EL PLAZO DE EJECUCIÓN ESTABLECIDO EN EL CONTRATO	REDUCIR LA PROBABILIDAD DE OCURRENCIA/ EL CONTRATISTA DEBERÁ CONTEMPLAR EN SU OFRECIMIENTO ECONÓMICO LOS COSTOS ADICIONALES INCURRIDOS, DE ACUERDO A LOS REQUISITOS DE RECEPCIÓN DE LOS BIENES CONTEMPLADOS EN LAS ESPECIFICACIONES TÉCNICAS MÍNIMAS.
Impacto después del tratamiento: Probabilidad	1	1	1	1	1
Impacto después del tratamiento: Impacto	1	3	3	4	3
Impacto después del tratamiento: Calificación	2	4	4	5	4
Impacto después del tratamiento: Calificación total	BAJO	BAJO	BAJO	MEDIO	BAJO
Afecta la ejecución del contrato	NO	SI	NO	SI	NO
¿Afecta el equilibrio económico del contrato?	NO	SI	NO	SI	NO
Persona responsable por implementar el tratamiento	ESTRUCCTURADOR DEL PROCESO	SUPERVISOR	SUPERVISOR	SUPERVISOR	CONTRATISTA
Fecha estimada en que se inicia el tratamiento	PRESENTACIÓN DE LA OFERTA	APROBACIÓN GARANTÍA ÚNICA	APROBACIÓN GARANTÍA ÚNICA	APROBACIÓN GARANTÍA ÚNICA	PRESENTACIÓN DE LA OFERTA
Fecha estimada en que se complementa el tratamiento	ADJUDICACIÓN DE LA ACEPTACIÓN DE LA OFERTA	TERMINACIÓN DE LA ACEPTACIÓN DE LA OFERTA	TERMINACIÓN DEL CONTRATO Y PERIODO DE LA ACEPTACIÓN DE LA OFERTA	TERMINACIÓN DE LA ACEPTACIÓN DE LA OFERTA	TERMINACIÓN DE LA ACEPTACIÓN DE LA OFERTA
Monitoreo y Revisión: ¿Cómo se realiza el monitoreo?	COMUNICACIÓN OFICIAL AL ORDENADOR DEL GASTO	INFORME DE SUPERVISIÓN	INFORME NOVEDAD	INFORME DE SUPERVISIÓN	COMUNICACIÓN OFICIAL AL ORDENADOR DEL GASTO
Monitoreo y Revisión: Periodicidad ¿Cuándo?	ETAPA PRECONTRACTUAL	PERMANENTE	PERMANENTE	PERMANENTE	PERMANENTE

No.	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la Ocurrencia del Evento	Probabilidad	Impacto	Calificación Total	Prioridad	¿A quién se le asigna el riesgo?	Tratamiento controles a ser implementados	Impacto después del tratamiento				Afecta la ejecución del contrato	¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se complementa el tratamiento	Monitoreo y Revisión	
													Probabilidad	Impacto	Calificación	Calificación total						¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
6	GENERAL	EXTERNO	EJECUCIÓN	OPERACIONAL	RIESGO DERIVADO A FLUCTUACIÓN DE LA TASA DE CAMBIO	INCREMENTO DE PRECIOS EN LA MATERIA PRIMA E INSUMOS	2	3	5	MEDIO	CONTRATISTA	ACEPTAR EL RIESGO/ EL CONTRATISTA DEBERÁ PREVER QUE SE PUEDAN PRESENTAR LOS INCREMENTOS DE LA MATERIA PRIMA E INSUMOS POR CONCEPTO DEL DIFERENCIAL CAMBIARIO.	2	3	5	MEDIO	SI	SI	CONTRATISTA	PRESENTACIÓN DE LA OFERTA	TERMINACIÓN DE LA ACEPTACIÓN DE LA OFERTA	OFERTA ECONÓMICA	PERMANENTE

NOTA: con la presentación de la oferta, el oferente acepta y aprueba los riesgos propuestos por la Policía Nacional, así como el análisis realizado por la Entidad para su mitigación y gestión, de igual forma corresponde al estructurador del proceso, analizar los riesgos a los cuales se expone la entidad y el oferente frente a la ejecución del contrato, por cuanto cada proyecto es único en los factores ambientales, económicos, políticos, sociales, tecnológicos, entre otros.

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