Anexo 2 – Anexo Técnico
Fichas Técnicas y Especificaciones del Acuerdo Marco De Productos y Servicios Electrónicos y Digitales De Confianza

INTRODUCCIÓN

El presente documento tiene como principal insumo las fichas técnicas y especificaciones que se encuentren vinculadas al futuro Acuerdo Marco De Productos y Servicios Electrónicos y Digitales De Confianza para dar claridad de los interesados, posibles proveedores y las entidades compradoras se realizan las siguientes precisiones para el adecuado entendimiento del presente Anexo.

Se precisa que parte de los Derechos y Deberes de los Contratistas establecidos en el Artículo 5 de la Ley 80 de 1993, *"2º. **Colaborarán con las entidades contratantes en lo que sea necesario para que el objeto contratado se cumpla y que éste sea de la mejor calidad**; acatarán las órdenes que durante el desarrollo del contrato ellas les impartan y, **de manera general, obrarán con lealtad y buena fe en las distintas etapas contractuales**, evitando las dilaciones y entrabamientos que pudieran presentarse."* (negrilla y subraya fuera de texto), por tal motivo, deberán colaborar con las Entidades Compradoras bajo su calidad de Contratistas/Proveedores para que se cumpla el objeto contratado y sea de la mejor calidad, en ese orden de ideas, deberán informar a la Entidad cuando algún aspecto o requerimiento no se cumpla o no sea aplicable a su naturaleza y destinación.

CONTENIDO

1. ALCANCE DEL ACUERDO MARCO 3
2. CONDICIONES TRANSVERSALES DEL ACUERDO 3
2.1 Cobertura, zonas de entrega y prestación del servicio del Acuerdo Marco 3
2.2 Soporte técnico 4
2.3 Posventa adicional 4
3. LOTE 1. PRODUCTOS Y SERVICIOS ELECTRÓNICOS Y DIGITALES DE CONFIANZA 5
3.1 Condiciones transversales Lote 1 5
3.1.1 Tiempos de entrega 5
3.1.1.1 *Tiempos de entrega para los certificados de firma por medio de token físico* 5
3.1.1.2 Tiempos de entrega para los certificados de firma por medio de token virtual. 5
3.1.1.3 Tiempos de entrega para los servicios asociados a Lote 1 5
3.1.2 Vigencia de los certificados de firma 6
3.1.3 Reposición de los certificados de firma 6
3.1.4 Modalidades de adquisición y pago de los certificados de firma y servicios 7
3.1.5 Confidencialidad de la información 7
3.1.6 Protocolo de entrega de los productos y servicios 8
3.1.7 Capacitación o transferencia de conocimiento 9
3.1.8 Normatividad aplicable 9
3.1.9 Gestión Ambiental 10
3.2 Catálogo de Productos y servicios electrónicos y digitales de Confianza Lote 1 10
3.2.1 Certificados de Firma Electrónica Acreditado 11
3.2.2 Certificados digitales de persona natural Acreditado 12

3.2.3 Certificados digitales de profesional titulado Acreditado 14
3.2.4 Certificados digitales de persona jurídica acreditado 16
3.2.5 Certificados digitales de Representación legal Acreditado 18
3.2.6 Certificados digitales de Pertenencia a Empresa Acreditado 20
3.2.7 Certificados Digitales de Función Pública Acreditado 22
3.2.8 Archivo y conservación de documentos digitales 23
3.2.9 Software como Servicio de gestión de Firmas 25
3.2.10 Servicio de API de integración 29
3.2.11 Envío y recepción del mensaje de datos y de documentos electrónicos transferibles, a través de correo electrónico acreditado 30
3.2.12 Estampado Cronológico Acreditado 32
3.2.13 Lista de confianza de Adobe - Adobe Approved Trust List, AATL 33
3.2.14 Operador homologado por parte de la Administración de SIIF Nación 34
4. LOTE 2. CERTIFICADOS DIGITALES DE SITIO SEGURO 35
4.1 Condiciones transversales Lote 2 ..... *35*
4.1.1 Tiempos de entrega 35
4.1.2 Vigencia de los Certificados 35
4.2 Catálogo de Productos *35*
4.2.1 Certificado digital de sitio web SSL DV Validación Dominio 35
4.2.2 Certificado digital de sitio web SSL OV Validación Organización 37
4.2.3 Certificado digital de sitio web SSL EV Validación Extendida 39
5. SERVICIOS ADICIONALES TRANSVERSALES 41
5.1 Horas de implementación 41
5.2 Capacitación 41
5.3 Soporte Técnico 43
5.4 Soporte Técnico Proactivo 44
5.5 Soporte Técnico Reactivo 46

1. Alcance del Acuerdo Marco

El Acuerdo Marco permite a las Entidades la adquisición de (i) servicios de confianza digital definidos en el anexo técnico- Lote 1, servicio de gestión o flujos de firmas en modalidad SaaS - Software como Servicio y servicios complementarios definidos en el anexo técnico-Lote1 y (ii) certificados de sitio seguro y servicios complementarios definidos en el Anexo técnico- Lote 2.

2. Condiciones transversales del Acuerdo

Las siguientes son condiciones transversales de ejecución para las Órdenes de Compra suscritas al amparo del Acuerdo Marco.

2.1 Cobertura, zonas de entrega y prestación del servicio del Acuerdo Marco

El Acuerdo Marco, contempla una cobertura Nacional, es decir el 100% del territorio colombiano, y define las siguientes zonas para entrega de los productos y prestación del servicio en los casos que aplique[1].

Zona	Unidades del territorio nacional
Zona 1 (Distritos Especiales y Municipios de categoría 1)	Bogotá D.C., Cali, Medellín, Barranquilla Y Cartagena De Indias.
	Pasto, Armenia, Bucaramanga, Ibagué, Rionegro, Itagüí, Envigado, Mosquera, Chía, Floridablanca, Yumbo, Tunja, Manizales, Valledupar, Montería, Neiva, Santa Marta, Villavicencio, Cúcuta, Pereira, Buenaventura, Palmira, Sabaneta, Soacha, Barrancabermeja, Funza, Bello
Zona 2 (Municipios intermedios, categoría 2, 3 y 4)	Popayán, Girón, Cota, Tocancipá, Cajicá, Madrid, Soledad, La Estrella, Sincelejo, Yopal, Buga, Tuluá, Piedecuesta, Sogamoso, Jamundí, Dosquebradas, Fusagasugá, Zipaquirá.
	Acacias, Girardota, Copacabana, Guarne, Caldas, Candelaria, Malambo, Puerto Gaitan, Facatativá, Puerto Colombia. Florencia, Retiro, Girardot, Duitama, Apartado, Carmen De Viboral, Sopo, La Ceja, Tenjo.
	Riohacha, Arauca, Los Patios, Aguachica, Ricaurte, Maicao, Segovia, Uribia, Cartago, Manaure, Puerto Lopez, Villa Del Rosario, Coveñas, Quibdó, Remedios, Tumaco, Turbaco, Turbo, Marinilla, Pitalito, Ipiales, Espinal, Cumaribo, Barbosa.
Zona 3 (Municipios básicos, categoría 5, 6 y el resto del país.	Cogua, Lebrija, Granada, Paipa, Magangué, Anapoima, Albania, Sibaté, El Cerrito, Castilla La Nueva, Caucasia, Miranda, Sonsón, Villamaría, Chiquinquirá, San Gil, Santa Rosa De Cabal, La Mesa, Ciénaga, La Jagua Ibirico, Leticia, Aguazul, Tauramena, Bugalagrande, Calarcá, Villa Rica, Melgar, Sahagún, Providencia, Puerto Boyacá, Chinchiná, La Calera, La Dorada, Nobsa, Zarzal, Galapa, Santander De Quilichao, Ocaña, Guachené.
	Municipios de la Categoría 6 y el resto del País.

[1] Contaduría General de la Nación: https://www.contaduria.gov.co/categorizacion-de-departamentos-distritos-y-municipios

2.2 Soporte técnico

El Proveedor debe disponer de una mesa de servicio principal y único punto centralizado de contacto con las Entidades Compradoras a fin de resolver incidentes y peticiones de los usuarios que tengan relación con los productos y servicios prestados.
La mesa de servicio debe resolver incidentes y peticiones de los usuarios que tengan relación con los productos y servicios prestados, dejando un registro en el Software de Gestión de incidentes / Servicios de TI y realizar un seguimiento de los incidentes presentados dando una solución óptima en un determinado tiempo.
El Proveedor debe brindar soporte para evaluar y solucionar fallas e interrupciones que se presenten en la prestación del servicio contratado.
El proveedor debe contar con personal de soporte con suficientes conocimientos en los servicios contratados.
Debe disponer del servicio en el horario de 5x8 (5 días a la semana, 8 horas al día) de lunes a viernes.
El proveedor debe brindar soporte remoto a nivel nacional y disponer de diversos canales de atención como:

i. Línea telefónica nacional para las Entidades Compradoras (teléfono fijo PBX, 018000 o celular).
ii. Canal de atención web, entiéndase como un canal de atención dispuesto en la página web del Proveedor (por ejemplo: Clic to call o web to Call o chat o generación de tickets, etc)
iii. Correo electrónico
iv. Teléfono de al menos dos (2) personas de contacto, (nombre, cargo y teléfonos de contacto fijo o celular).

2.3 Posventa adicional

Las Entidades Compradora que así lo consideren pertinente, que lo requieran o que deseen acceder a la atención postventa, deberá revisar el informe final de evaluación del Proceso Licitatorio que genero el Acuerdo Marco a fin de determinar si el Proveedor adjudicatario de la Orden de Compra fue acreedor del puntaje por este criterio, y podrá acceder a este criterio sin ningún costo adicional.

La atención postventa será de diez (10) horas de un (1) profesional con conocimientos a fines a los productos y servicios electrónicos y digitales de confianza a fin de:

i. Establecer estrategias que permitan mejorar la experiencia de los productos y servicios adquiridos por la entidad comprada y/o contemplados en el Acuerdo Marco, para ser implementados en nuevos proyectos.
ii. El profesional será asignado de manera remota, sin embargo, debe estar disponible para cuando la entidad compradora solicite la atención postventa.
iii. El profesional estará a cargo del supervisor de la orden de compra. Las actividades que el supervisor le asigne deberán ser relacionadas con la orden de compra y limitadas a su ámbito de acción.
iv. Si al proponente se le adjudican varias órdenes de compra al mismo tiempo, deberá disponer del personal requerido bajo las condiciones establecidas para cada orden de compra.

3. LOTE 1. Productos y servicios electrónicos y digitales de Confianza

3.1 Condiciones transversales Lote 1

3.1.1 Tiempos de entrega

A continuación, se definen los tiempos de entrega de los Certificados de firma, los cuales comenzarán a contar a partir del cumplimiento de los requisitos definidos por el Proveedor para la emisión del certificado de firma de cada suscriptor..

3.1.1.1 *Tiempos de entrega para los certificados de firma por medio de token físico*.

PRODUCTO	Rango Cantidades	ZONA 1	ZONA 2	ZONA 3
Certificados de firma digital – token físico	1-100	5 días hábiles	6 días hábiles	12 días hábiles
	101-500	6 días hábiles	8 días hábiles	13 días hábiles
	501-999	8 días hábiles	10 días hábiles	14 días hábiles
	Más de 1.000	12 días hábiles	14 días hábiles	18 días hábiles

3.1.1.2 Tiempos de entrega para los certificados de firma por medio de token virtual.

PRODUCTO	Rango Cantidades	ZONA 1	ZONA 2	ZONA 3
Certificados de firma digital – token virtual	1-100	2 días hábiles	3 días hábiles	4 días hábiles
	101-500	3 días hábiles	4 días hábiles	5 días hábiles
	501-999	4 días hábiles	5 días hábiles	6 días hábiles
	Más de 1.000	5 días hábiles	6 días hábiles	7 días hábiles

La Entidad Compradora, debe brindar los datos de contacto del suscriptor de la firma para que el Proveedor realice la gestión pertinente, y debe brindar el acompañamiento al Proveedor para contactar al suscriptor dentro de los términos establecidos, so pena, de ampliar automáticamente el tiempo de entrega al doble del inicialmente establecido.

La Entidad Compradora debe coordinador con el Proveedor y si es el caso el suscriptor del certificado, los horarios en los que se recibe el certificado de firma, para que el Proveedor coordine con la empresa de mensajería si es el caso y la entrega se dé dentro de los tiempos establecidos, en caso contrario los tiempos se podrán ampliar hasta en un 50% al inicialmente definido.

Para los servicios de firma electrónica, estampado cronológico y archivo y conservación de documentos, el tiempo de implementación del servicio es el mismo que el establecido en el cuadro de los certificados de firma digital en token virtual.

3.1.1.3 Tiempos de entrega para los servicios asociados a Lote 1

A continuación, se definen los tiempos de entrega de los Servicios asociados al Lote 1.

PRODUCTO	ZONA 1	ZONA 2	ZONA 3
Servicios asociados al Lote 1	10 días hábiles	15 días hábiles	20 días hábiles

3.1.2 Vigencia de los certificados de firma

A continuación, se define la vigencia de los certificados de firma que habilita la opción para que las Entidades Compradoras puedan adquirir los certificados

PRODUCTO	VIGENCIA
Certificados de Firma	1 AÑO
	2 AÑOS

La vigencia de los certificados inicia a partir de su emisión.

3.1.3 Reposición de los certificados de firma

La reposición se debe realizar de acuerdo con los siguientes parámetros de cantidades adquiridas por la Entidad Compradora en cada Orden de Compra suscrita

CANTIDAD	VIGENCIA	REPOSICION
Entre 1- 10 certificados de firma	**1 AÑO**	**Una reposición**
Entre 11 – 40 Certificados de Firma	1 AÑO	10% de los certificados adquiridos
Más de 41 certificados de firma	1 AÑO	15% de los certificados adquiridos
Entre 1- 10 certificados de firma	**2 AÑOS**	**Una reposición**
Entre 11 – 40 Certificados de Firma	2 AÑOS	15% de los certificados adquiridos
Más de 41 certificados de firma	2 AÑOS	20% de los certificados adquiridos

Entiéndase la cantidad, como la suma total de certificados de firma adquiridos por la Entidad Compradora en cada Orden de Compra, indistintamente el tipo de certificado. El número de reposición se realizará conforme al número entero de la fracción según el cálculo porcentual.
La reposición no genera costo adicional a la Entidad Compradora.
La reposición puede ser por cualquier tipo de certificado de firma vinculados a la Orden de Compra, sin embargo, en ningún caso podrá reponerse un tipo de certificado por otro, es decir, a manera de ejemplo no se podrá solicitar la reposición de un certificado de persona natural por uno de persona jurídica. De igual manera la reposición aplica sobre la misma modalidad, es decir, la reposición de un token físico se debe reponer con un token físico.
La reposición para certificados con vigencia de 1 año podrá ser efectiva por la Entidad Compradora hasta 3 meses antes de su vencimiento.
La reposición para certificados con vigencia de 2 años podrá ser efectiva por la Entidad Compradora hasta 6 meses antes de su vencimiento.
El Proveedor se compromete a realizar la reposición de los certificados de firma por Orden de Compra suscrita en caso de presentarse las siguientes situaciones:

- Se debe hacer reposición por daño de token físico, entiéndase daño como avería, ruptura, deterioro, desperfecto del token físico o daño lógico NO atribuible al suscriptor y que no pueda ser reparado.
- Se debe hacer reposición por olvido de clave del token virtual, siempre y cuando no pueda llevarse a cabo la recuperación de clave con la metodología dispuesta para tal fin, cuando aplique y el Proveedor lo tenga definido en sus procedimientos.
- Se debe hacer reposición por retiro definitivo o parcial del suscriptor del cargo, siempre y cuando se mantengan las mismas funciones y el cargo.
- Se debe hacer reposición por retiro definitivo o parcial del suscriptor de la Entidad Compradora, siempre y cuando se mantengan las mismas funciones y el cargo.

NOTA: La reposición de los certificados de firma, se contempla por cualquiera de las situaciones descritas anteriormente que pueden llegar a presentarse durante la ejecución de la Orden de Compra y serán acumuladas en cada orden de Compra y hasta agotar el porcentaje de reposición definido. Ejemplo, si una Entidad adquiere 23 certificados de firma de diferente tipo, tiene la opción de reponer hasta 2 certificados durante toda la ejecución de la Orden de Compra, una vez agotada esta cantidad la Entidad debe proceder a la adquisición de los certificados que requiera reponer.

3.1.4 Modalidades de adquisición y pago de los certificados de firma y servicios

La Entidad Compradora con cada Orden de Compra suscrita, adquiere un cupo de certificados de firma por cada tipo de certificado requerido dentro de la Orden de Compra, la Entidad Compradora tiene dos opciones de pago

Opción 1. Pago total del cupo adquirido por productos y servicios, la Entidad Compradora realizará el pago total del cupo adquirido y consumirá por demanda los productos y servicios requeridos en la medida de sus necesidades. (Bolsa de recursos)

Opción 2. Pago por demanda de productos y servicios, la Entidad Compradora realizará el pago mensual por los productos y servicios consumidos en el respectivo periodo de conformidad con la estimación de consumo.

La vigencia de la Orden de Compra será determinada por la Entidad Compradora de acuerdo con su proceso interno de planeación, no obstante, la vigencia de los certificados de firma puede exceder el plazo de la Orden de Compra.

3.1.5 Confidencialidad de la información

EL Proveedor debe, con cada Orden de Compra suscrita con cada Entidad Compradora, garantizar la confidencialidad de la información que con ocasión de la ejecución de la Orden sea de su conocimiento.
Dar estricta aplicación a la Ley de Protección de Datos Personales vigente y expedida por las autoridades pertinentes.
La confidencialidad de la información se debe garantizar hasta incluso después de finalizada la ejecución de la Orden de Compra y vigencia de los certificados de firma entregados.

El proveedor debe adoptar las medidas necesarias que impidan la divulgación, sustracción, alteración y uso indebido de la información que con ocasión de la ejecución de la Orden sea de su conocimiento.
Para dar cumplimiento a esta condición, las partes deben suscribir un compromiso de confidencialidad e integridad de la información con las premisas que las partes consideren. En ningún caso, este compromiso implica costos adicionales para las partes.

3.1.6 Protocolo de entrega de los productos y servicios

A continuación, se sugiere el siguiente protocolo de entrega e implementación de los servicios, que puede ser modificado y replanteado por las partes si consideran pertinente para dar celeridad al proceso.
El protocolo describe y sugiere las actividades y procedimientos generales mínimos para la entrega, verificación y pruebas de operación de los productos adquiridos o servicios contratados.
Las actividades contempladas en el protocolo de entrega no significan costos adicionales para la Entidad Compradora.
Una vez ha sido emitida la Orden de Compra y se han llevado a cabo las actividades de perfeccionamiento de esta, el Proveedor tiene hasta 3 días hábiles para comunicarse con la Entidad Compradora y dar inicio al protocolo de entrega.
Si la Entidad Compradora no responde a los intentos de comunicación del Proveedor durante los 3 días hábiles siguientes del perfeccionamiento de la Orden, el Proveedor debe evidenciar los intentos fallidos de comunicación con la Entidad y debe notificar inmediatamente a Colombia Compra Eficiente.
La evidencia de los intentos fallidos de comunicación corresponde a correos enviados por el Proveedor que no han recibido respuesta por parte de la Entidad Compradora.
La Entidad Compradora y el Proveedor deben pactar el cronograma de entrega, prueba y operación de los productos adquiridos y servicios contratados, quedando a partir de este momento la fecha de inicio de ejecución de la Orden de Compra.
El cronograma debe respetar los tiempos de entrega, las obligaciones del Acuerdo y los ANS del Acuerdo Marco cuando apliquen.
Una vez el cronograma ha sido aprobado, las modificaciones deben ser discutidas, acordadas por las dos partes y debe quedar por escrito y firmado tanto por la Entidad Compradora como por el Proveedor, las modificaciones al cronograma se restringen a situaciones fortuitas, de fuerza mayor o de mutuo acuerdo.
El lugar y horario en el cual el Proveedor realizará la entrega es el lugar definido por la Entidad Compradora en la Orden de Compra y esta información debe ser incluida en el cronograma, siendo el horario definido por la Entidad, dentro de la jornada laboral, en días y horas hábiles, salvo que las partes lleguen a un acuerdo diferente.
La entrega y prueba de operación de los productos será en la ubicación descrita por la Entidad Compradora en la solicitud de cotización que incluye la distribución de los mismos cómo lo definió la Entidad, siempre y cuando se encuentre dentro de la zona en la que fue cotizado el producto o servicio.
El Proveedor debe entregar la documentación técnica y de operación de los productos y servicios cuando aplique. El proveedor debe entregar la documentación necesaria como manuales de usuario donde se especifique de forma clara la forma de uso, ejemplos, preguntas frecuentes, incidencias habituales y su solución.

El Proveedor se obliga a:

- ✓ Contar con personal idóneo para realizar las actividades de entrega y prueba de operación de los productos y servicios definidos en la Orden de Compra.
- ✓ Asignar y comunicar a la Entidad Compradora los datos de la persona que estará coordinando el proceso de entrega y prueba de operación de los productos y servicios definidos en la Orden de Compra.

- ✓ Debe cubrir los costos logísticos asociados a su personal durante el desarrollo de las actividades que integran el protocolo de entrega y prueba de operación de los productos y servicios definidos en la Orden de Compra.
- ✓ Suministrar la información requerida y/o acordada para llevar a cabo el proceso de entrega y prueba de operación de los productos y servicios definidos en la Orden de Compra.

La Entidad Compradora se obliga a:

- ✓ Allegar los documentos a la Entidad de Certificación Digital requeridos para la expedición de los certificados de firma. Estos documentos son: Copia de documento de identidad, acta de posesión o decreto de nombramiento con fecha (para funcionarios), estudios académicos (cuando aplique), documento de solicitud diligenciado, aceptación términos y condiciones de uso. Debe allegar los documentos requeridos por el Proveedor de acuerdo con su declaración de prácticas de certificación y de acuerdo con lo que requiera el ciclo de vida del tipo de certificado adquirido.
- ✓ Informar al Proveedor la ubicación exacta donde se van a realizar la entrega y prueba de operación de los productos y servicios definidos en la Orden de Compra.
- ✓ La Entidad Compradora debe brindar acompañamiento permanente en el desarrollo de las pruebas a manera de supervisión.
- ✓ La entidad debe cumplir con la Declaración de Prácticas de Certificación de acuerdo con lo establecido en el Decreto 033 de 2014, así como los demás deberes de los suscriptores establecidos en la Ley 527 de 1999 y las demás en esta materia y que las modifiquen.

3.1.7 Capacitación o transferencia de conocimiento

El Proveedor debe realizar la transferencia de conocimiento al personal que la entidad compradora disponga para el uso de los productos o servicios adquiridos y realizar la sensibilización pertinente sobre la importancia de los servicios de confianza.
El proveedor debe realizar la transferencia de conocimiento a la entidad compradora por medio de una capacitación virtual de máximo 2 horas por cada servicio de confianza contratado.
El proveedor debe disponer de los medios necesarios para su realización y entregará a la entidad compradora la evidencia de dicha transferencia de conocimiento.
La fecha y hora debe ser acordada por las partes y debe plasmarse en el cronograma suscrito al inicio de la ejecución de la Orden de compra.
La capacitación o transferencia de conocimiento debe ser convocada por la Entidad Compradora a los funcionarios que designe.
Para los servicios de Archivo y Conservación de Documentos Digitales, Software como Servicio de Generación de Firmas, Servicio de API de Integración y el Envío y recepción del mensaje de datos y de documentos electrónicos transferibles, a través de correo electrónico certificado, la transferencia de conocimiento contempla 8 horas de capacitación a usuarios técnicos y funcionales de la Entidad Compradora, en 1 o varias sesiones según acuerden las partes.

3.1.8 Normatividad aplicable

Los certificados de firma deben cumplir con los requisitos exigidos en la siguiente normatividad y demás normas que los complementen o modifiquen

- ✓ Ley 527 de 1999
- ✓ Decreto Ley 019 de 2012

- ✓ Decreto 1074 del 2015
- ✓ Decreto 333 de 2014

Para todos los tipos de certificados de firma, los Proveedores deben dar aplicación y cumplimiento a los Criterios específicos para la Acreditación de Entidades de Certificación Digital CEA-x en su última versión y vigente al momento de la adjudicación del Acuerdo Maco, Órdenes de Compra suscritas y/o posteriores versiones publicadas y definidas por el Organismo Nacional de Acreditación de Colombia ONAC durante toda la vigencia del Acuerdo..

3.1.9 Gestión Ambiental

Los certificados emitidos en la modalidad de token físico deberán ser reutilizados por el Proveedor siempre y cuando sea procedente, es decir, (i) haya sido expedido por él mismo Proveedor, (ii) sea para el mismo tipo de certificado y (iii) el nuevo certificado sea para el mismo suscriptor, para lo cual la Entidad debe permitir la reutilización de los token físico y hacerlo exigible cuando se cumplan las condiciones ya descritas.

3.2 Catálogo de Productos y servicios electrónicos y digitales de Confianza Lote 1

A continuación, se listan los diferentes tipos de productos de certificados de firma y servicios asociados, que dependiendo el nivel de riesgo y el fin último para lo cual requiere el certificado de firma, la Entidad Compradora determine el que se ajusta a sus necesidades.
Se agrupan partiendo de las condiciones que deben acreditarse para cada producto.

SEGMENTO	CODIGO Y NOMBRE DEL SERVICIO
SEGMENTO 1	AMSEDC-CD-02 Certificados digitales de persona natural acreditado
	AMSEDC-CD-03 Certificados digitales de profesional titulado Acreditado
	AMSEDC-CD-04 Certificados digitales de persona jurídica acreditado
	AMSEDC-CD-05 Certificados digitales de Representación legal acreditado
	AMSEDC-CD-06 Certificados digitales de Pertenencia a Empresa acreditado
	AMSEDC-CD-07 Certificados digitales de función pública acreditado
	AMSEDC-CD-10 Servicio de API de integración
	AMSEDC-CD-12 Estampado cronológico acreditado
	AMSEDC-ESP-01 Lista de confianza de Adobe - Adobe Approved Trust List, AATL
	AMSEDC-ESP-02 Operador homologado por parte de la Administración de SIIF Nación
	AMSEDC-SAT Servicios Adicionales transversales
SEGMENTO 2	AMSEDC-CD-01 Certificado de firma electrónica acreditado
	AMSEDC-CD-12 Estampado cronológico acreditado
	AMSEDC-SAT Servicios Adicionales transversales
SEGMENTO 3	AMSEDC-CD-08 Archivo y conservación de documentos digitales
	AMSEDC-CD-12 Estampado cronológico acreditado
	AMSEDC-SAT Servicios Adicionales transversales
SEGMENTO 4	AMSEDC-CD-9 Software como Servicio de gestión de Firmas
	Productos y servicios de Segmento 1

	AMSEDC-SAT Servicios Adicionales transversales
SEGMENTO 5	AMSEDC-CD-11 Envío y recepción del mensaje de datos y de documentos electrónicos transferibles, a través de correo electrónico certificado
	AMSEDC-SAT Servicios Adicionales transversales
Especificación	Ser miembro de la lista de confianza de Adobe - Adobe Approved Trust List, AATL
Especificación	Ser operador homologado por parte de la Administración de SIIF Nación del Ministerio de Hacienda y Crédito Público

3.2.1 Certificados de Firma Electrónica Acreditado

Definición	La firma electrónica certificada permite vincular y verificar la identidad del suscriptor y generar un documento firmado con validez jurídica así como de integridad y autenticidad.
Código y Nombre	AMSEDC-CD-01 Certificados de Firma Electrónica Acreditado
Unidad de facturación	Plataforma tecnológica mes Transacción
Descripción técnica	Este servicio permite el proceso de generación de firma electrónica certificada, bajo los lineamientos del Organismo de Acreditación ONAC, y permite verificar la identidad de personas, y puede ser utilizada para firmar cualquier tipo de documento. El proveedor informará el procedimiento para la utilización de la firma electrónica certificada para la firma de los documentos El Proveedor informará a la Entidad Compradora el procedimiento de vinculación y verificación de la identidad de la persona. El proveedor informará el procedimiento para la obtención de la firma del suscriptor. El proveedor debe utilizar sistemas confiables para el almacenamiento de los certificados de firma y debe garantizar la seguridad de los mismos. El proveedor entregará la documentación técnica y legal correspondiente a los servicios contratados. El costo de la transacción incluye los costos asociados a la firma electrónica como tal. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio.

<table>
<tr><td></td><td>El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo.

El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad.

El Proveedor debe garantizar que el servicio se preste bajo el modelo de Seguridad HSM (Hardware Security Module)

Los certificados deben cumplir con los requisitos exigidos en la normatividad vigente y las demás normas que los complementen o modifiquen.

Dentro del formato de documentos a firmas por parte de las Entidades, se contemplan *.PDF, archivos generados por Microsoft Office y Open Office.</td></tr>
<tr><td>Modalidad</td><td>Virtual</td></tr>
<tr><td>Certificación</td><td>Certificado de Acreditación aprobado vigente por ONAC</td></tr>
<tr><td>Soporte</td><td>Se debe brindar el soporte técnico para la implementación y aplicación del certificado de firma durante la vigencia de La Orden de Compra.

El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento.

<table><tr><td rowspan="2">Token Virtual</td><td>Prioridad 1: Perdida total del servicio
Efectividad de resolución <= 4 horas hábiles</td></tr><tr><td>Prioridad 2: Perdida parcial del servicio
Efectividad de resolución <= 8 horas hábiles</td></tr></table>El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos.</td></tr>
<tr><td>Capacitación</td><td>El proveedor debe realizar la transferencia de conocimiento a la entidad compradora por medio de una capacitación virtual de máximo 2 horas por cada servicio de confianza contratado.</td></tr>
</table>

3.2.2 Certificados digitales de persona natural Acreditado

Definición	La firma digital de Persona Natural acreditado valida la identidad del suscriptor, y tiene validez jurídica o legal.
Código y Nombre	AMSEDC-CD-02 Certificados digitales de persona natural Acreditado

Unidad de facturación	Certificado
Descripción técnica	Este servicio permite la generación de firma digital acreditada, es decir, certificada por el Organismo Nacional de Acreditación en Colombia ONAC, y permite verificar la identidad de personas, y puede ser utilizada para firmar cualquier tipo de documento. El proveedor informará el procedimiento para la utilización de los certificados. El proveedor debe utilizar sistemas confiables para el almacenamiento de los certificados y debe garantizar la seguridad de los mismos. Se debe informar a la Entidad Compradora el procedimiento de vinculación y verificación de la identidad de la persona. El proveedor entregará la documentación técnica y legal correspondiente a los servicios contratados. Los tokens pueden ser utilizados en cualquier dispositivo móvil (celular, Tablet, portátil, etc.) así como en los diferentes sistemas operativos de estos aparatos electrónicos. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo. . Los certificados deben cumplir con los requisitos exigidos en la normatividad vigente y las demás normas que los complementen o modifiquen. El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad. El Proveedor debe garantizar que el servicio se preste bajo el modelo de Seguridad HSM (Hardware Security Module)
Modalidad	Token físico

	Token virtual
Zonas	Zona 1 Zona 2 Zona 3
Certificación	Certificado de Acreditación aprobado vigente por ONAC
Garantía	Si el dispositivo (TOKEN) entregado por el proveedor no funciona de manera correcta, este será reemplazado sin costo alguno, teniendo en cuenta los criterios de reposición del presente Anexo Técnico.
Soporte	El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado. El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento. Token Virtual: Prioridad 1: Perdida total del servicio — Efectividad de resolución <= 4 horas hábiles Token Virtual: Prioridad 2: Perdida parcial del servicio — Efectividad de resolución <= 8 horas hábiles Token Físico: Prioridad 1: Perdida total del servicio — Efectividad de resolución <= 8 horas hábiles Token Físico: Prioridad 2: Perdida parcial del servicio — Efectividad de resolución <= 16 horas hábiles
Capacitación	El proveedor debe realizar la transferencia de conocimiento a la entidad compradora por medio de una capacitación virtual de máximo 2 horas por cada servicio de confianza contratado.

3.2.3 Certificados digitales de profesional titulado Acreditado

Definición	La firma digital de Profesional titulado acredita la identidad del suscriptor con el título profesional obtenido
Código y Nombre	AMSEDC-CD-03 Certificados digitales de profesional titulado Acreditado
Unidad de facturación	Certificado
Descripción técnica	El certificado de profesional titulado le permite acreditar su identidad y su título profesional, certificado de firma certificado por el Organismo Nacional de Acreditación ONAC. Se debe informar a la Entidad Compradora el procedimiento de vinculación y verificación de la identidad de la persona y el titulo obtenido.

	El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo. El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad. El Proveedor debe garantizar que el servicio se preste bajo el modelo de Seguridad de Hardware HSM.
Modalidad	Token físico Token virtual
Zonas	Zona 1 Zona 2 Zona 3
Certificación	Certificado de Acreditación aprobado vigente por ONAC
Garantía	Si el dispositivo (TOKEN) entregado por el proveedor no funciona de manera correcta, este será reemplazado sin costo alguno, teniendo en cuenta los criterios de reposición del presente Anexo Técnico.
Soporte	El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado. El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento. Token Virtual: Prioridad 1: Perdida total del servicio — Efectividad de resolución <= 4 horas hábiles Token Virtual: Prioridad 2: Perdida parcial del servicio — Efectividad de resolución <= 8 horas hábiles

	Token Físico	Prioridad 1: Perdida total del servicio Efectividad de resolución <= 8 horas hábiles
		Prioridad 2: Perdida parcial del servicio Efectividad de resolución <= 16 horas hábiles
Capacitación	El proveedor debe realizar la transferencia de conocimiento a la entidad compradora por medio de una capacitación virtual de máximo 2 horas por cada servicio de confianza contratado.	

3.2.4 Certificados digitales de persona jurídica acreditado

Definición	Certificado de persona jurídica es la credencial electrónica que se emite a la persona jurídica para ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente
Código y Nombre	AMSEDC-CD-04 Certificados digitales de persona jurídica acreditado
Unidad de facturación	Certificado
Descripción técnica	Los certificados de Persona Jurídica son emitidos a entidades, acreditan la identidad del titular y su condición como Persona Jurídica en la firma de documentos electrónicos garantizando la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El proveedor debe utilizar sistemas confiables para el almacenamiento de los certificados de firma y debe garantizar la seguridad de los mismos. Se firman digitalmente documentos electrónicos con la misma validez y eficacia jurídica que posee la firma manuscrita. Se expide a las personas jurídicas para su uso en sus relaciones con aquellas administraciones públicas, entidades y organismos públicos, vinculados o dependientes de las mismas. El proveedor entregará la documentación técnica y legal correspondiente a los servicios contratados. El proveedor entregará los Certificados de persona jurídica con un mecanismo para la identificación y autenticación, para los usuarios o suscriptores correspondientes, así como la validación de la vigencia de los mismos mediante el protocolo establecido. Los tokens pueden ser utilizados en cualquier dispositivo móvil (celular, Tablet, portátil, etc.) así como en los diferentes sistemas operativos de estos aparatos electrónicos. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y

<table>
<tr><td></td><td>liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio.

El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo.

El Proveedor debe garantizar que el servicio es compatible con el estándar PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados.</td></tr>
<tr><td>Certificación</td><td>Certificado de Acreditación aprobado vigente por ONAC</td></tr>
<tr><td>Modalidad</td><td>Token físico
Token virtual</td></tr>
<tr><td>Garantía</td><td>Si el dispositivo (TOKEN) entregado por el proveedor no funciona de manera correcta, este será reemplazado sin costo alguno, este será reemplazado sin costo alguno, teniendo en cuenta los criterios de reposición enmarcados en el presente Anexo Técnico.</td></tr>
<tr><td>Soporte</td><td>El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado.

El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos.

El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento.

<table>
<tr><td rowspan="2">Token Virtual</td><td>Prioridad 1: Perdida total del servicio
Efectividad de resolución <= 4 horas hábiles</td></tr>
<tr><td>Prioridad 2: Perdida parcial del servicio
Efectividad de resolución <= 8 horas hábiles</td></tr>
<tr><td rowspan="2">Token Físico</td><td>Prioridad 1: Perdida total del servicio
Efectividad de resolución <= 8 horas hábiles</td></tr>
<tr><td>Prioridad 2: Perdida parcial del servicio
Efectividad de resolución <= 16 horas hábiles</td></tr>
</table>
</td></tr>
</table>

Capacitación	El proveedor debe realizar la transferencia de conocimiento a la entidad compradora por medio de una capacitación virtual de máximo 2 horas por cada servicio de confianza contratado.

3.2.5 Certificados digitales de Representación legal Acreditado

Definición	Certificado digital de representante legal, acredita la identidad de una persona natural vinculándola como representante legal de una persona jurídica.
Código y Nombre	AMSEDC-CD-05 Certificados digitales de Representación legal Acreditado
Unidad de facturación	Certificado
Descripción técnica	Los certificados de Representante Legal son emitidos a personas Físicas, acreditan la identidad del titular y su condición de representante legal de una entidad o persona jurídica en la firma de documentos electrónicos. El proveedor utilizara sistemas confiables para el almacenamiento de los certificados para mantener la seguridad de los mismos. El proveedor garantizará la autenticidad del emisor de la comunicación, el no repudio del origen y la integridad del contenido. El poseedor de un certificado de representante legal actúa en nombre de la entidad o persona jurídica que representa. En una comunicación electrónica el suscriptor puede acreditar válidamente su identidad ante otra persona demostrando la posesión de la llave privada asociada con la respectiva llave pública contenida en el certificado. Existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor puesto que el resumen del documento es cifrado con la llave privada del emisor. Los datos del sistema relativos al ciclo de vida de los certificados se conservan de forma digital durante el periodo que establezca. Los certificados de Representante legal deben tener plena identificación del suscriptor con un nombre significativo. Los certificados deben tenar una llave privada junto con el algoritmo de firma. Los tokens pueden ser utilizados en cualquier dispositivo móvil (celular, Tablet, portátil, etc.) así como en los diferentes sistemas operativos de estos aparatos electrónicos.

	El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo. El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad.
Certificación	Certificado de Acreditación aprobado vigente por ONAC
Modalidad	Token físico Token virtual
Zonas	Zona 1 Zona 2 Zona 3
Garantía	Si el dispositivo (TOKEN) entregado por el proveedor no funciona de manera correcta, este será reemplazado sin costo alguno, teniendo en cuenta los criterios de reposición enmarcados en el presente Anexo Técnico.
Soporte	El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado. Se debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento.

Token Virtual	Prioridad 1: Perdida total del servicio Efectividad de resolución <= 4 horas hábiles
	Prioridad 2: Perdida parcial del servicio Efectividad de resolución <= 8 horas hábiles
Token Físico	Prioridad 1: Perdida total del servicio Efectividad de resolución <= 8 horas hábiles

		Prioridad 2: Perdida parcial del servicio Efectividad de resolución <= 16 horas hábiles
Capacitación	El proveedor debe realizar la transferencia de conocimiento a la entidad compradora por medio de una capacitación virtual de máximo 2 horas por cada servicio de confianza contratado.	

3.2.6 Certificados digitales de Pertenencia a Empresa Acreditado

Definición	Los certificados digitales de Pertenencia a Empresa Certificada, acredita la identidad del suscriptor y su condición de pertenencia a una empresa o persona jurídica y le permite firmar documentos de manera digital en la calidad que acredita su certificado.
Código y Nombre	AMSEDC-CD-06 Certificados digitales de Pertenencia a Empresa Acreditado
Unidad de facturación	Certificado
Descripción técnica	La firma digital de Pertenencia a Empresa Certificada sirve exclusivamente para que una persona natural acredite su condición de miembro de la empresa o persona jurídica y su uso se restringe para realizar todo tipo de trámites como miembro de dicha organización a la cual se encuentra vinculado como son firmar mensajes de datos y/o documentos relacionados con las funciones propias de su cargo dentro de la organizaciónEl proveedor debe utilizar sistemas confiables para el almacenamiento de los certificados de firma y debe garantizar la seguridad de los mismos. El proveedor informará el procedimiento para la utilización de los certificados digitales para la firma de los documentos. Se debe informar a la Entidad Compradora el procedimiento de vinculación y verificación de la identidad de la persona. El proveedor entregará la documentación técnica y legal correspondiente a los servicios contratados. Este servicio de firma digital acreditada puede ser utilizada para firmar cualquier tipo de documento. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de

<table>
<tr><td></td><td>transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo.

Los certificados deben cumplir con los requisitos exigidos en la normatividad vigente y las demás normas que los complementen o modifiquen.

El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad.

El Proveedor debe garantizar que el servicio se preste bajo el modelo de Seguridad de Hardware HSM.</td></tr>
<tr><td>Modalidad</td><td>Token físico
Token virtual</td></tr>
<tr><td>Certificación</td><td>Certificado de Acreditación aprobado vigente por ONAC</td></tr>
<tr><td>Garantía</td><td>Si el dispositivo (TOKEN) entregado por el proveedor no funciona de manera correcta, este será reemplazado sin costo alguno, teniendo en cuenta los criterios de reposición enmarcados en el ítem 3.1.3 del presente Anexo Técnico.</td></tr>
<tr><td>Soporte</td><td>El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado.

El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento.

<table>
<tr><td rowspan="2">Token Virtual</td><td>Prioridad 1: Perdida total del servicio
Efectividad de resolución <= 4 horas hábiles</td></tr>
<tr><td>Prioridad 2: Perdida parcial del servicio
Efectividad de resolución <= 8 horas hábiles</td></tr>
<tr><td rowspan="2">Token Físico</td><td>Prioridad 1: Perdida total del servicio
Efectividad de resolución <= 8 horas hábiles</td></tr>
<tr><td>Prioridad 2: Perdida parcial del servicio
Efectividad de resolución <= 16 horas hábiles</td></tr>
</table>

El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos.</td></tr>
<tr><td>Capacitación</td><td>El servicio del Certificado Digital de Persona Natural contempla 2 horas de capacitación al usuario suscriptor, en una o dos sesiones de acuerdo con la necesidad de la Entidad Compradora.</td></tr>
</table>

3.2.7 Certificados Digitales de Función Pública Acreditado

Definición	La firma digital de Función Pública sirve exclusivamente para que una persona natural acredite su calidad de Funcionario Público de una Entidad Compradora en particular del Estado y su uso se restringe para realizar todo tipo de trámites como funcionario Público de la Entidad Compradora a la cual se encuentra vinculado como son firmar mensajes de datos y/o documentos relacionados con las funciones propias de su cargo dentro de la Entidad Compradora Pública a la cual se encuentra vinculado.
Código y Nombre	AMSEDC-CD-07Certificados Digitales de Función Pública Acreditado
Unidad de facturación	Certificado
Descripción técnica	Este servicio de firma digital acreditada garantiza la connotación de función pública. Este servicio de firma digital acreditada puede ser usado en el Sistema Integrado de Información Financiera SIIF Nación Este servicio de firma digital acreditada puede ser utilizada para firmar cualquier tipo de documento. Se debe informar el procedimiento para firmar documentos El proveedor informará el procedimiento para la utilización de los certificados digitales para la firma de los documentos. Los certificados deben cumplir con los requisitos exigidos en la normatividad vigente y las demás normas que los complementen o modifiquen. El proveedor entregará la documentación técnica y legal correspondiente a los servicios contratados. Los tokens pueden ser utilizados en cualquier dispositivo móvil (celular, Tablet, portátil, etc.) así como en los diferentes sistemas operativos de estos aparatos electrónicos. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de

	la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo. El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad. El servicio contempla el apoyo técnico y funcional en la implementación del certificado de firma hasta su entrada en operación. Se deben llevar a cabo diferentes pruebas de escrito que permitan validar la correcta funcionalidad del certificado de firma entregado.
Modalidad	Token físico o Token virtual
Certificación	Certificado de Acreditación aprobado vigente por ONAC Certificado de operador homologado por parte de la Administración de SIIF Nación del Ministerio de Hacienda y Crédito Público
Garantía	Si el dispositivo (TOKEN) entregado por el proveedor no funciona de manera correcta, este será reemplazado sin costo alguno, teniendo en cuenta los criterios de reposición enmarcados en el ítem 3.1.3 del presente Anexo Técnico.
Soporte	El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado. El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento. Token Virtual: Prioridad 1: Perdida total del servicio Efectividad de resolución <= 4 horas hábiles Token Virtual: Prioridad 2: Perdida parcial del servicio Efectividad de resolución <= 8 horas hábiles Token Físico: Prioridad 1: Perdida total del servicio Efectividad de resolución <= 8 horas hábiles Token Físico: Prioridad 2: Perdida parcial del servicio Efectividad de resolución <= 16 horas hábiles
Capacitación	El servicio del Certificado Digital de Persona Natural contempla 2 horas de capacitación al usuario suscriptor, en una o dos sesiones de acuerdo con la necesidad de la Entidad Compradora.

3.2.8 Archivo y conservación de documentos digitales

Definición	Es un conjunto organizado de datos o de información que permite gestionar y almacenar documentos creados en formato digital a través de una plataforma electrónica asegurando la organización y seguridad de la información.
Código y Nombre	AMSEDC-CD-08 Archivo y conservación de documentos digitales
Unidad de facturación	Tamaño del archivo (1 megabyte) por mes
Descripción técnica	La Entidad Compradora debe realizar un análisis de requisitos y/o necesidades para definir la solución y el alcance del servicio a contratar para lo cual la Entidad Compradora durante el evento RFQ debe indicar el objetivo y alcance del requerimiento del servicio de modo tal que los Proveedores tengan conocimiento del propósito. El servicio contempla: El cargue de documentos Verificación de los documentos (vigencia y firma) Actualización de documentos Eliminación de documentos Devolución de documentos que no cumplan con las condiciones técnicas para su archivo y conservación Los documentos para su archivo y conservación deben contar con digital firma y estampa cronológica con el fin de generar validez jurídica. La Entidad Compradora debe determinar el tipo de información que va a almacenar (texto, imágenes y video) etc. El proveedor debe mantener la información centralizada, disponible y de fácil acceso. El proveedor debe mantener la información disponible en la nube con los protocolos de seguridad definidos. El proveedor debe realizar backups periódicos para evitar perdida de información. El proveedor y la Entidad Compradora deben determinar el tipo de acceso, clasificación de usuarios (consulta, modificación, etc.) y determinar qué información es clasificada, como su nivel de importancia y sensibilidad. El proveedor y la Entidad Compradora deben definir el listado de series (tablas de retención documental) con sus correspondientes tipos documentales. La Entidad Compradora puede hacer el uso de servicio para archivos físicos previa digitalización del mismo.

Modalidad	Virtual
Certificación	Certificado de Acreditación aprobado vigente por ONAC
Soporte	El proveedor debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado. El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. La entidad compradora definirá junto con el proveedor la criticidad de los incidentes que se puedan presentar y de igual manera definir los tiempos de atención a dichos incidentes.
Capacitación	El servicio contempla 8 horas de capacitación a usuarios técnicos y funcionales de la Entidad Compradora, en 1 o varias sesiones según acuerden las partes.

3.2.9 Software como Servicio de gestión de Firmas

Definición	Software como servicio de gestión de Firmas, es una plataforma centralizada de gestión de firmas y control de flujos de firmado que permite a las Entidades compradoras la generación de firmas digitales en la Entidad
Código y Nombre	AMSEDC-CD-09 Software como Servicio de gestión de Firmas
Unidad de facturación	Licencia SaaS mes / Licencia On Premises mes Transacción
Descripción técnica	Servicio que permite a las Entidades Compradoras hacer uso de este software, y generar documentos firmados por más de un suscriptor con firma digital y generar así flujos y gestión de firmas de documentos. Los certificados de firma podrán ser usados de manera independiente por el suscriptor. Se podrá hacer uso del certificado de firma del suscriptor siempre y cuando se encuentren en la modalidad virtual. El Software debe permitir las siguientes funcionalidades: - Generar flujos de trabajo para obtener las firmas de un documento - Definir o asignar roles para los diferentes suscriptores que pueden firmar un documento - Custodiar y administrar los certificados de firma, en token virtual o físico de acuerdo con los lineamientos determinados por ONAC que serán gestionados para la prestación del servicio.

	- El servicio prestado debe poderse acceder vía internet La Entidad Compradora debe tener en cuenta que debe disponer de los certificados de firma que utilizará en el software, caso contrario en el cual podrá adquirirlos a través del mismos Acuerdo y dentro de la misma Orden de Compra con la contratación del Software. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El proveedor debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 10 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, el Proveedor cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo. El proveedor garantizará el funcionamiento del software y permitirá el uso del mismo desde cualquier sitio El proveedor debe garantizar la seguridad y acceso del Software y no permitir accesos no autorizados. El Software debe permitir la validación de los certificados de firma utilizados por cada suscriptor para firmar los documentos. Permitir Actualizaciones de software, de acuerdo con las políticas de seguridad de la Entidad y del fabricante del software contratado. Permitir la actualización del software o acceso a la plataforma por parte de la Entidad Compradora por el tiempo elegido por la misma, sin que esto genere costo adicional para la Entidad Compradora, es decir, el proveedor deberá contemplar la realización de las actualizaciones durante el periodo contratado por la Entidad. La solución debe proporcionar una API integral para la automatización de procesos y la integración con las aplicaciones, en caso de requerirse, pero en todo caso si llegase a ser necesario el uso de la API de Integración, esta deber ser proporcionada por el Proveedor y debe ser incluida dentro del valor de la licencia del Software. Así las cosas, debe el Proveedor costear la API dentro del valor de la licencia.

	Contar con una consola de administración centralizada en la nube y con acceso remoto a la misma. - Debe permitir el control de acceso de los diferentes suscriptores con usuario y clave o cualquier otro mecanismo que brinde la seguridad de acceso a suscriptores autorizados - Debe tener el rol de administrador del Software para parametrizar y asignar roles a los diferentes suscriptores - Debe permitir acceso desde equipos de cómputo, portátiles, tabletas y smartphones con acceso a internet El proveedor debe realizar acompañamiento durante la instalación, configuración y/o puesta en funcionamiento del software contratado por la Entidad Compradora. (definir horas mínimas) El Proveedor debe realizar las tareas necesarias para garantizar la instalación, el funcionamiento y adaptar los productos adquiridos en la orden de compra de acuerdo con los parámetros definidos por la Entidad Compradora. El Software debe permitir su implementación en Nube Privada, es decir en el datacenter de la Entidad Compradora si esta así lo requiere, para lo cual la Entidad Compradora debe indicar tal requerimiento durante el evento RFQ. Si la Entidad no manifiesta tal intención el servicio se presta en modalidad SaaS en las condiciones fijadas por el Proveedor del servicio. El servicio contempla la activación y configuración de la plataforma y la parametrización según acuerdo entre las partes y actividades fijadas en el cronograma de actividades suscrito al inicio de la Orden de Compra. La implementación se contempla hasta el inicio de las funcionalidades del software y cuando la Entidad evidencie que puede iniciar flujos de trabajo y firmas con el software. El proveedor bajo el modelo de adquisición tipo SaaS, tendrá la responsabilidad de gestionar el acceso y mantener la estructura de datos, la conectividad y los servidores necesarios para el funcionamiento del servicio contratado por la entidad Compradora. El proveedor debe suministrar la última versión del software que se encuentre liberada en el mercado al momento de la entrega e incluir los medios de instalación (si aplica), manuales y guías. El Proveedor debe manifestar que acepta que la Entidad Compradora y Colombia Compra Eficiente o sus delegados verifiquen el licenciamiento del software utilizado.

	Así mismo, el proveedor deberá suministrar todo el software orientado al segmento empresarial y/o de negocios, no personal. La capacitación puede ser en modalidad presencial o virtual previo acuerdo entre las partes. El Proveedor debe preparar el material necesario para llevar a cabo la capacitación. El Servicio contempla soporte y mantenimiento durante toda la vigencia de la Orden de Compra. El servicio que se va a contratar debe contemplar los componentes indicados en la unidad de facturación según las necesidades de la Entidad Compradora en cantidades, y el servicio se paga mensualmente durante su vigencia con la activación de la plataforma. El Proveedor y el personal designado para realizar las labores en la Entidad Compradora debe garantizar la confidencialidad de la información Institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución de las actividades El servicio debe estar disponible 7x24, es decir 7 días a la semana 24 horas al día.
Modalidad	SaaS – Software como Servicio
Certificación	N/A
Capacitación	El servicio contempla 8 horas de capacitación a usuarios técnicos y funcionales de la Entidad Compradora, en 1 o máximo 4 sesiones virtuales según acuerden las partes.
Acuerdos de Nivel de Servicio	
DISPONIBILIDAD (D) D>=99,7% RTO incidente: 43 min Medición mensual	$d = \frac{Número\ de\ minutos\ de\ disponibilidad\ real\ de\ los\ Servicios\ EDC\ contratados}{Número\ de\ minutos\ contratados} * 100\%$ Número de minutos contratados corresponde a la cantidad de minutos en el horario de operación del servicio durante cada mes. $99{,}7\% \leq d < \mathrm{D}\%$ 3% de descuento $99.5\% \leq d < 99.7\%$ 5% de descuento $d < 99.5\%$ 7% de descuento Donde: D es la disponibilidad mínima exigida para cada nivel de servicio d es la disponibilidad real en cada mes

3.2.10 Servicio de API de integración

Definición	El servicio contempla la entrega y apoyo en la implementación de la API Application Programming Interface en español Interfaz de programación de aplicaciones de acuerdo con lo requerido por la Entidad Compradora
Código y Nombre	AMSEDC-CD-10 Servicio de API de integración
Unidad de facturación	Licencia mes
Descripción técnica	El servicio de API de integración busca que las Entidades puedan implementar e integrar en sus aplicaciones las diversas funcionalidades provistas a través de la API. La API instalada debe ser compatible con los certificados emitidos de cualquier entidad de Certificación Digital. La API debe permitir la integración de los diferentes certificados de firma vigentes con que cuente la Entidad Compradora al momento de contratación de este servicio o los contratados a través del presente Acuerdo Marco y con la misma Orden de Compra de contratación de la API. La Entidad Compradora durante el evento RFQ debe indicar el objetivo y alcance del requerimiento funcional de contratar la API, de modo tal que los Proveedores tengan conocimiento del propósito. La API de integración debe permitir funcionalidades como: ✓ Firmar documentos con los diversos certificados de firma disponibles en el presente documento y con que cuente la Entidad, indistintamente del proveedor de certificación digital ✓ Firmar documentos generados por las aplicaciones de las Entidades. ✓ Incluir y permitir estampas cronológicas, la Entidad Compradora debe dimensionar dentro de su necesidad las estampas requeridas durante el tiempo de contratación del servicio e incluirlas en el evento de cotización para que sean costeadas por el Proveedor. El servicio contempla el uso de los certificados de firma del mismo operador adjudicatario en el presente servicio, de modo tal que la Entidad Compradora debe incluir los certificados de firma a usar en las aplicaciones dentro de la contratación del servicio. El servicio debe estar disponible 7x24, es decir 7 días a la semana 24 horas al día.
Modalidad	SaaS Software como Servicio
Capacitación	El servicio contempla 8 horas de capacitación a usuarios técnicos y funcionales de la Entidad Compradora, en 1 o varias sesiones según acuerden las partes.
Acuerdos de Nivel de Servicio	

DISPONIBILIDAD (D) D>=99,7% RTO incidente: 43 min Medición mensual	$d = \frac{Número\ de\ minutos\ de\ disponibilidad\ real\ de\ los\ Servicios\ EDC\ contratados}{Número\ de\ minutos\ contratados} * 100\%$ Número de minutos contratados corresponde a la cantidad de minutos en el horario de operación del servicio durante cada mes. $99{,}7\% \leq d < \mathrm{D}\%$ 3% de descuento $99.5\% \leq d < 99.7\%$ 5% de descuento $d < 99.5\%$ 7% de descuento Donde: D es la disponibilidad mínima exigida para cada nivel de servicio d es la disponibilidad real en cada mes

3.2.11 Envío y recepción del mensaje de datos y de documentos electrónicos transferibles, a través de correo electrónico acreditado

Definición	El correo electrónico certificado es una comunicación que se realiza a través de un correo electrónico en donde existe una certificación del envío y de recepción, así como la fecha y hora de la comunicación. Este servicio permite obtener un acuse de recibo con la marca de tiempo en el documento.
Código y Nombre	AMSEDC-CD-11 Envío y recepción del mensaje de datos y de documentos electrónicos transferibles, a través de correo electrónico Acreditado
Unidad de facturación	Correo
Descripción técnica	El Correo electrónico Certificado otorga plena validez jurídica y probatoria a las notificaciones electrónicas certificadas emitidas a través del correo electrónico definido por la Entidad Compradora. La unidad de facturación se contempla como correo electrónico certificado enviado y recibido por cada destinatario definido. Es decir, un correo con 5 destinatarios implica facturación total de 5 correos electrónicos certificados. Se contempla el tamaño de correo electrónico en 1 Megabyte incluidos los adjuntos. El servicio de notificación electrónica certificada provee un registro del envío y de recepción de la información para cada destinatario. El proveedor informará a la Entidad Compradora el tamaño máximo que se puede adjuntar al correo electrónico que el sistema permita el envío de los correos sin inconvenientes.

	El proveedor debe suministrar a la Entidad Compradora el acompañamiento frente al proceso de configuración y puesta en operación del servicio Correo Electrónico Certificado. El proveedor debe contar con los elementos tecnológicos, económicos, y recurso de personal calificado requeridos para ofrecer los servicios de certificación de correo electrónico. El proveedor debe proteger los datos de la entidad compradora del servicio. El proveedor debe garantizar que se pueda determinar la fecha y hora del envío del correo electrónico certificado, la fecha y la hora de la llegada del mensaje al destinatario y la fecha y la hora de la apertura del mensaje. El proveedor debe garantizar la notificación de apertura del correo electrónico por parte del receptor, siempre y cuando el receptor abra el correo. El proveedor debe utilizar sistemas seguros y confiables para almacenar la información de las transacciones realizadas, durante la vigencia de la Orden de Compra. El servicio contempla por tanto el almacenamiento de las transacciones que se generen de acuse durante la vigencia de la Orden de Compra, y entregará periódicamente Backup a la Entidad de dichas transacciones. El Proveedor mantendrá hasta por 3 meses después de finalizada la ejecución de la Orden de Compra la información generada de cada transacción. Las partes podrán acordar otro tipo de mecanismo de almacenamiento en la infraestructura de la Entidad para suplir este requisito, previo acuerdo. El proveedor pondrá en conocimiento a la Entidad Compradora del servicio de Acuse de Recibo de los correos emitidos. El proveedor debe certificar la razón la razón por la cual no llegó el mensaje al destinatario. El proveedor debe permitir la integridad y la confidencialidad de los mensajes de correo electrónico certificado. Contar con la infraestructura tecnológica y de seguridad necesaria para la utilización adecuada de los correos electrónicos certificados.
Modalidad	SaaS Software como servicio
Certificación	Certificado de Acreditación aprobado vigente por ONAC

Soporte	El proveedor debe brindar el soporte técnico para la implementación y aplicación del certificado de firma durante la vigencia del certificado o de la Orden de Compra. La entidad compradora definirá junto con el proveedor la criticidad de los incidentes que se puedan presentar y de igual manera definir los tiempos de atención a dichos incidentes El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos.
Capacitación	El servicio contempla 4 horas de capacitación a usuarios técnicos y funcionales de la Entidad Compradora, en 1 o máximo 4 sesiones según acuerden las partes.

3.2.12 Estampado Cronológico Acreditado

Definición	El estampado cronológico es la asignación de la fecha y hora actual por parte de una entidad prestadora de servicios de certificación que asegura la exactitud e integridad de la marca de tiempo a una forma digital ya sea un documento, video, o audio.
Código y Nombre	AMSEDC-CD-12 Estampado Cronológico Acreditado
Unidad de facturación	Estampa
Descripción técnica	Garantizar que el servicio se provee con la hora legal colombiana del Instituto Nacional de Metrología (organismo que mantiene, coordina y difunde la hora legal de la República de Colombia) Hora definida como hora, minuto y segundo (hh: mm: ss) con la hora legal colombiana Fecha definida en día, mes y año (dd: mm: aaaa) de acuerdo con el calendario El Proveedor debe brindar el acompañamiento técnico de implementación y puesta en operación del servicio y en el valor de cada estampa debe incluir los costos asociados para su operación. El Proveedor no debe permitir hacer uso de la fecha y hora de sistemas de información o servidores de las Entidades o terceros. La plataforma tecnológica debe certificar que técnicamente que la serie de datos, documentos, videos o audios ha existido y no ha sido modificada. El proveedor garantizará que no se efectúe alteración de la información, asegura la integridad de los documentos y transacciones

	Brindar seguridad técnica y validez jurídica, que permita la trazabilidad de un mensaje de datos durante su ciclo. La Entidad Compradora adquiere un cupo limitado de estampas que puede usar durante la vigencia de la Orden de Compra. La asistencia para la instalación, configuración y atención de incidentes referentes al servicio adquirido no tendrá costo por parte del proveedor.
Certificación	Certificado de Acreditación aprobado vigente por ONAC
Soporte	El proveedor debe brindar el soporte técnico para la implementación y aplicación de la estampa durante la vigencia de la Orden de Compra. El proveedor debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. La entidad compradora definirá junto con el proveedor la criticidad de los incidentes que se puedan presentar y de igual manera definir los tiempos de atención a dichos incidentes.
Capacitación	El servicio de la firma contempla 2 horas de capacitación a los funcionarios definidos por la Entidad Compradora, en una o dos sesiones de acuerdo con la necesidad de la Entidad Compradora.

3.2.13 Lista de confianza de Adobe - Adobe Approved Trust List, AATL

Definición	Ser miembro de la lista de confianza de Adobe - Adobe Approved Trust List, AATL
Unidad de facturación	Porcentaje ATTL, paga una única vez
Código y Nombre	AMSEDC-ESP-01
Descripción	El Proveedor debe ser miembro de la lista de confianza de Adobe - Adobe Approved Trust List directamente o a través de una de las entidades emisoras de certificados (CA) que hace parte de la lista. En todo caso, el Proveedor debe garantizar que con los certificados de firma adquiridos por la Entidad Compradora acreditados por la ONAC se puede llevar a cabo la validación de ser parte de la lista de confianza. Se contempla esta especificación técnica a fin de que la entidad durante la operación secundaria, si lo requiere, seleccione que el Proveedor de los certificados sea miembro de la lista de confianza de Adobe - Adobe Approved Trust List, AATL, para lo cual se debe entregar el certificado emitido por Adobe o link de consulta donde se evidencia que el Proveedor hace parte de la lista de confianza de Adobe - Adobe Approved Trust List.

	Se contempla el pago una única vez por Orden de Compra suscrita por la entidad que incluya esta especificación dentro de los ítems a adquirir. El valor corresponde al porcentaje final ofertado de este ítem sobre el valor total final de los certificados adquiridos por la Entidad Compradora en la Orden de Compra. Este requerimiento puede ser tercerizado por los Proveedores que actualmente no son miembros de la Lista de confianza y en todo caso deben garantizar que los certificados entregados a la entidad son proveídos por un miembro de la lista de confianza. Esta especificación técnica aplica para el segmento 1 y 4

3.2.14 Operador homologado por parte de la Administración de SIIF Nación

Definición	Ser operador homologado por parte de la Administración de SIIF Nación del Ministerio de Hacienda y Crédito Público
Unidad de facturación	Porcentaje SIIF Nación – Pago una única vez por certificado
Código y Nombre	AMSEDC-ESP-02
Descripción	El Proveedor debe ser operador homologado por parte de la Administración de SIIF Nación del Ministerio de Hacienda y Crédito Público, para la cantidad de certificados de función pública adquiridos por la Entidad Compradora dentro de la Orden de Compra. Se contempla esta especificación técnica a fin de que la entidad durante la operación secundaria, si lo requiere, seleccione que el Proveedor de los certificados de función pública sea un operador homologado ante la administración de SIIF Nación y que la Entidad lo pueda verificar, para lo cual el Proveedor debe presentar el certificado emitido por la Administración de SIIF Nación del Ministerio de Hacienda que lo acredita como tal. Este requerimiento puede ser tercerizado por los Proveedores que actualmente no son Operadores homologados por la administración de SIIF Nación. Se contempla el pago una única vez por Orden de Compra suscrita por la entidad que incluya esta especificación dentro de los ítems a adquirir. El valor corresponde al porcentaje final ofertado de este ítem sobre el valor total final de los certificados de función pública en cualquier modalidad que la Entidad requiere para usar ante SIIF Nación. Esta especificación técnica aplica para el segmento 1 y 4

4. LOTE 2. Certificados Digitales de Sitio Seguro

4.1 Condiciones transversales Lote 2

4.1.1 Tiempos de entrega

A continuación, se definen los tiempos de entrega de los Certificados de Sitio Seguro

PRODUCTO	RANGO CANTIDADES	TODAS LAS ZONAS
Certificados de Sitio Seguro	1-50	5 días hábiles
	50-100	8 días hábiles
	101-499	12 días hábiles
	Más de 400	15 días hábiles

4.1.2 Vigencia de los Certificados

PRODUCTO	Vigencia
Certificados de Sitio Seguro	1 AÑO
	2 AÑOS

Para los certificados adquiridos con una vigencia de dos años, y en los casos indicados expresamente por el Proveedor por temas procedimentales, la Entidad Compradora deberá informar la vigencia inicial contratada y continuidad por un año más y el proveedor deberá tramitarlo oportunamente ante el emisor del certificado sin costo adicional para la Entidad.

4.2 Catálogo de Productos

4.2.1 Certificado digital de sitio web SSL DV Validación Dominio

Definición	Los certificados SSL DV validan el dominio y son totalmente automatizados, por lo que ofrecen seguridad en inicios de sesión, correos web, visitantes de su blog, entre otros. Estos certificados activan el candado del navegador y el protocolo https para proteger a los visitantes que ingresen a un sitio web.
Código y nombre	AMSEDC-SSL-01 Certificado digital de sitio web SSL DV Validación Dominio
Unidad de facturación	Certificado
Descripción técnica	El certificado SSL DV proporciona el nivel más básico de seguridad. Permite la validación del dominio garantizando que el dominio sea seguro. La adquisición de los certificados contempla la implementación y activación de los mismos hasta su entrada en operación.

	El proveedor debe proteger información confidencial que se genere de la adquisición de los certificados. El Certificado debe proteger la información que se intercambia entre los extremos, proporcionando la confidencialidad en los datos. El proveedor debe validar el portal o sistema de información para así mitigar el riesgo de suplantación de servicios tecnológicos de la Entidad Compradora. El proveedor debe entregar los certificados, de acuerdo con las características y especificaciones técnicas contratadas. El proveedor debe cargar en la plataforma de administración de manera virtual o vía correo electrónico, según se tenga definido por el fabricante del certificado, los certificados adquiridos por la Entidad Compradora de acuerdo con las fechas de vigencia. El proveedor debe garantizar la asistencia técnica de los certificados de sitio seguro SSL DV, una vez activados y durante su vigencia de la Orden de Compra o del certificado. El proveedor debe garantizar la compatibilidad universal con navegadores. El proveedor debe entregar a la Entidad Compradora la documentación técnica de la solución, manuales de manejo y operación y el respectivo soporte técnico El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) vigentes soportado por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para el tipo de certificado. El proveedor debe entregar a la Entidad Compradora la documentación técnica de la solución, manuales de manejo y operación y el respectivo soporte técnico.
Modalidad	Virtual
Soporte	Se debe brindar el soporte técnico para la implementación del certificado SSL DV durante la vigencia del certificado. Se debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. El Proveedor deberá dar solución a los incidentes reportados por la entidad compradora de acuerdo con la prioridad de los incidentes que se puedan

	presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento. Certificado SSL: Prioridad 1: Perdida total del servicio. Efectividad de resolución <= 4 horas hábiles Prioridad 2: Perdida parcial del servicio. Efectividad de resolución <= 8 horas hábiles
Capacitación	Realizar entrenamiento a dos (2) personas designadas por la Entidad, que incluya el protocolo de solicitud y la implementación de los certificados SSL de sitio seguro.

4.2.2 Certificado digital de sitio web SSL OV Validación Organización

Definición	Es un tipo de certificado que permite identificar el vínculo entre el dominio y la organización registrante del dominio, es decir, permite identificar que una URL sea real y confiable bajo un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.
Código y nombre	AMSEDC-SSL-02 Certificado digital de sitio web SSL OV Validación Organización
Unidad de facturación	Certificado
Descripción técnica	El certificado SSL OV proporciona el nivel medio de seguridad. La Entidad Compradora deben definir las características y el tipo de certificado SSL OV que va a ser contratado y la cantidad de los mismos. Si la Entidad Compradora requiere subdominios adicionales debe incluir la cantidad de certificados adicionales equivalente a la misma cantidad de subdominios a proteger, compatibilidad con dominios alternativos SAN, debe especificar la cantidad total de subdominios a proteger y debe indicar la cantidad de SAN a agregar. Los certificados Web SSL OV deben tener un cifrado desde 56bits hasta 256 Bits Los certificados Web SSL OV deben ser Compatibles con algoritmos de cifrado RSA El proveedor debe garantizar la compatibilidad universal con navegadores. Se contempla el certificado SSL Wilcard con un número ilimitado de subdominios con un solo certificado. Activación de candado de seguridad en el navegador.

	Seguridad activa con protocolo https. La adquisición de los certificados contempla la implementación y activación de los mismos hasta su entrada en operación. El proveedor debe cargar en la plataforma de administración de manera virtual, los certificados adquiridos por la Entidad Compradora de acuerdo con las fechas de vigencia, en los casos que aplique. El proveedor debe colocar y dejar en producción los certificados adquiridos por la Entidad Compradora utilizando una herramienta de navegación segura en internet, lo anterior con volúmenes superiores a 50 certificados. El proveedor debe administrar los certificados y gestionarlos directamente en la plataforma web con una herramienta de navegación segura que permita la activación. Actualización, operación y monitoreo de estos en tiempo real, en los casos que aplique. El proveedor debe garantizar la confidencialidad de la información de la Entidad Compradora en cuanto a los certificados, los datos contenidos en el fichero y la protección de los datos de los usuarios cuanto estos hagan uso del sitio web. El proveedor informará cualquier novedad al supervisor de la Orden de Compra que afecte la ejecución de la misma. La Entidad Compradora puede obtener el certificado SSL OV a manera de cupo y usarlo cuando efectivamente lo requiera. El proveedor debe volver a generar un certificado (reemitir) en caso de que se presente una migración de servidores o daño de hardware. El Proveedor debe garantizar que el servicio soporta la Autenticación comercial completa, verificación de la identidad comercial y la propiedad del dominio. El Proveedor debe garantizar que el servicio soporta Servicio MPKI (Managed Public Key Infrastructure) para la emisión y administración de certificados de Seguridad. Esto aplica en caso de adquirirse más de 100 certificados. El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) vigentes soportado por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio. El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards)

	El proveedor debe entregar a la Entidad Compradora la documentación técnica de la solución, manuales de manejo y operación y el respectivo soporte técnico.
Funcionalidad adicional con costo	Escaneo diario de malware para el portal web asegurado
Modalidad	Virtual
Tipo	Certificado SSL OV Certificado SSL - OV - Subdominio SAN Certificado SSL - OV - Wilcard
Soporte	Se debe brindar el soporte técnico para la implementación del certificado SSL OV durante la vigencia del certificado. Se debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos. Certificado SSL: Prioridad 1: Perdida total del servicio Efectividad de resolución <= 4 horas hábiles Prioridad 2: Perdida parcial del servicio Efectividad de resolución <= 8 horas hábiles
Capacitación	Realizar entrenamiento a dos (2) personas designadas por la Entidad, que incluya el protocolo de solicitud y la implementación de los certificados SSL de sitio seguro

4.2.3 Certificado digital de sitio web SSL EV Validación Extendida

Definición	Certificado de sitio WEB SSL EV- Extended Validation en español validación extendida que brinda el nivel más alto de seguridad
Código y nombre	AMSEDC-SSL-03 Certificado digital de sitio web SSL EV Validación Extendida
Unidad de Facturación	Certificado
Descripción técnica	El certificado SSL EV proporciona el nivel más alto de seguridad. Certificado SSL de Validación de Dominio y Organización EV Refleja la identidad de la organización Activación de candado de seguridad en el navegador Seguridad activa con protocolo https Refleja el emisor del certificado SSL El proveedor debe garantizar la compatibilidad universal con navegadores. Los certificados Web SSL OV deben tener un cifrado desde 56bits hasta 256 Bits

<table>
<tr><td></td><td>Los certificados Web SSL OV deben ser Compatibles con algoritmos de cifrado RSA

Si la Entidad Compradora requiere subdominios adicionales debe incluir la cantidad de certificados adicionales equivalente a la misma cantidad de subdominios a proteger, Compatibilidad con dominios alternativos SAN, debe especificar la cantidad total de subdominios a proteger y debe indicar la cantidad de SAN a agregar.

Activación de barra verde (URL)

Debe poder mostrar el nombre de la autoridad de certificación que la emitió el certificado.

El Proveedor debe garantizar que el servicio soporta la Autenticación comercial completa, verificación de la identidad comercial y la propiedad del dominio.

El Proveedor debe garantizar que el servicio soporta Servicio MPKI (Managed Public Key Infrastructure) para la emisión y administración de certificados de Seguridad. Esto aplica en caso de adquirirse más de 100 certificados.

El Proveedor debe garantizar que el servicio es compatible con el sistema operativo Windows 10 y superiores y IOS (MAC) vigentes soportado por el fabricante. Para el sistema operativo IOS (MAC) el proveedor debe realizar las configuraciones que se requieran para la prestación del servicio.

El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para el tipo de certificado.

El proveedor debe entregar a la Entidad Compradora la documentación técnica de la solución, manuales de manejo y operación y el respectivo soporte técnico</td></tr>
<tr><td>Modalidad</td><td>Virtual</td></tr>
<tr><td>Tipo</td><td>Certificado SSL EV
Certificado SSL EV - Subdominio SAN</td></tr>
<tr><td>Soporte</td><td>Se debe brindar el soporte técnico para la implementación del certificado SSL OV durante la vigencia del certificado.

Se debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos.

<table>
<tr><td rowspan="2">Certificado SSL</td><td>Prioridad 1: Perdida total del servicio
Efectividad de resolución <= 4 horas hábiles</td></tr>
<tr><td>Prioridad 2: Perdida parcial del servicio
Efectividad de resolución <= 8 horas hábiles</td></tr>
</table>
</td></tr>
<tr><td>Capacitación</td><td></td></tr>
</table>

	Realizar entrenamiento a dos (2) personas designadas por la Entidad, que incluya el protocolo de solicitud y la implementación de los certificados SSL de sitio seguro.

5. Servicios Adicionales Transversales

El objetivo de los servicios adicionales es satisfacer con las necesidades que la Entidad Compradora pudiese llegar a tener con la adquisición de los productos y servicios contratados. Aplica para lotes 1 y 2

5.1 Horas de implementación

Definición	Servicio de hora hombre para implementación e integración de servicios de Confianza Digital
Código y Nombre	AMSEDC-SAT-1 Hora de implementación
Unidad de facturación	Hora
Descripción técnica	Servicios de horas de implementación de profesionales con formación, experiencia en implementación de proyectos asociados a los productos y servicios definidos según el Lote. La Entidad Compradora adquiere las horas de implementación como servicios, en modalidad de cupo y agota en la medida de sus necesidades, puede contemplar el pago total del cupo adquirido y agotar durante la vigencia de la Orden de Compra o pagar mensualmente en la medida de su consumo.
Modalidad	Virtual Presencial
Zona	Presencial Zona 1 Presencial Zona 2 Presencial Zona 3
Formación	Título profesional universitario en Ingenierías y afines
Experiencia	Mínima de un (1) año en labores relacionadas con la implementación y desarrollo de proyectos asociados a servicios electrónicos y digitales de confianza

5.2 Capacitación

Definición	Servicio de capacitación especifica relacionada con los Servicios de Confianza Digital adquiridos.
Código y Nombre	AMSEDC-SAT-2 Sesión capacitación
Unidad de facturación	Sesión
Descripción técnica	La capacitación estará dirigida a usuarios, técnicos o administradores de los servicios contratados.

	La Entidad Compradora definirá junto con el proveedor la fecha, la hora y el lugar de la capacitación. El Proveedor puede prestar este servicio de forma remota o en sitio. La entidad Compradora definirá la temática o temas requeridos para la capacitación. La persona destinada por el proveedor debe contar con todas las herramientas necesarias de hardware y software requeridas para la correcta prestación de la capacitación contratada. El personal destinado por el proveedor debe tener el conocimiento específico, habilidades y experiencia relacionados con el tema contratado para la capacitación. El Proveedor debe proporcionar el material de capacitación de acuerdo con el tema definido con la Entidad Compradora. El proveedor realizará evaluaciones de la capacitación a los usuarios, técnicos o administradores una vez finalizada, con el objetivo de verificar la adquisición del conocimiento y entregar los resultados de las mismas. La modalidad de la capacitación puede ser remota o en sitio. En caso de ser remota, la Entidad Compradora determinará la vía de comunicación para para que el proveedor realice las actividades, entre las que se encuentran: Teams, Zoom, Streamyard, Meet, AWS Chime, u otro definido previamente por la Entidad. El personal dispuesto por el proveedor deberá estar vinculado a través de contrato laboral, prestación de servicios o por obra o labor contratada La entidad compradora junto con el proveedor definirá el número de usuarios que desea capacitar, dentro de las siguientes opciones: ➢ Una sesión de capacitación de 4 horas para un grupo de hasta20 usuarios técnicos o administradores definidos por la entidad ➢ Una sesión de capacitación de 4 horas para un grupo de 11 a 20 personas técnicos o administradores definidos por la entidad ➢ Una sesión de capacitación de 4 horas para un grupo de 1 a 10 usuarios finales definidos por la entidad ➢ Una sesión de capacitación de 4 horas para un grupo de 11 a 20 usuarios finales definidos por la entidad
Modalidad	Virtual Presencial
Zona	Presencial Zona 1 Presencial Zona 2 Presencial Zona 3

Formación	Título profesional universitario en Ingenierías y afines
Experiencia	Con experiencia mínima de dos (2) años en los temas de los productos y servicios definidos en el Acuerdo
Habilidades y destrezas	Excelentes relaciones personales y habilidad para el trabajo en equipo. Manejo avanzado de herramientas ofimáticas Capacidad de análisis y organización de datos Buena redacción, ortografía y capacidad de transmisión de ideas por escrito y oral Capacidad para transmitir información en ambientes pedagógicos

5.3 Soporte Técnico

Definición	El soporte técnico es un servicio por medio del cual se proporciona asistencia a los usuarios para que estos realicen un uso adecuado de los productos o servicios contratados.
Código y Nombre	AMSEDC- SAT-3 Soporte Técnico
Unidad de facturación	Hora
Descripción técnica	El Proveedor debe atender incidentes y consultas relacionadas con los Productos adquiridos por la Entidad Compradora. Los requerimientos deben ser formulados por los administradores de la plataforma o la mesa de ayuda de la Entidad Compradora. Las actividades de soporte técnico deben orientarse a solución de problemas, reconfiguración de las aplicaciones y a mantener la disponibilidad de los Productos adquiridos. El soporte puede ser prestado de manera remota o en sitio. En caso de que el soporte remoto no sea suficiente y adecuado para solucionar el problema, el Proveedor deberá desplazarse hasta las instalaciones de la Entidad Compradora para resolverlo. El Proveedor pondrá a disposición en las instalaciones de la Entidad Compradora el personal requerido en el horario y los perfiles solicitados, para prestar el servicio de soporte técnico. El Proveedor realizará la verificación de la configuración, activación y acceso a los servicios y /o productos contratados. El Proveedor realizará la reinstalación, desinstalación y reconfiguración de Productos. La Entidad Compradora debe solicitar el servicio al Proveedor, a través de los canales que establezca la Entidad Compradora de común acuerdo con el Proveedor.

	Los incidentes deben ser cerrados de común acuerdo entre la Entidad Compradora y el Proveedor siempre y cuando el problema sea resuelto satisfactoriamente. El consumo de las horas contratadas en la Orden de Compra se hará efectivo una vez se registre el incidente en la mesa de ayuda o el mecanismo que la Entidad Compradora de común acuerdo con el Proveedor. El Proveedor debe escalar el incidente con el fabricante oportunamente en caso de ser requerido. Este servicio aplica para cualquiera de los Productos adquiridos a través del Acuerdo Marco de Precios o con los que cuente la Entidad Compradora. El personal que ejecute el soporte técnico debe contar con un equipo de cómputo y todas las herramientas adicionales de hardware y software requeridas para la prestación optima del servicio. La Entidad Compradora debe establecer con el Proveedor la programación de los eventos de soporte programado. El Proveedor debe responder a las solicitudes de soporte de la Entidad de acuerdo con los tiempos definidos en el ANS. Una vez se realice el soporte técnico, el proveedor debe entregar un reporte técnico donde se indiquen las actividades realizadas, los procedimientos, recomendaciones y las actividades pendientes en caso tal.
Modalidad	Remoto En sitio
Zonas de prestación del servicio	En sitio Zona 1 En sitio Zona 2 En sitio Zona 3
Formación	Técnicos o tecnólogos de carreras profesionales en Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ingeniería de Sistemas, Ingeniería Informática o afines. Título profesional en Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ingeniería de Sistemas, Ingeniería Informática o afines; Con tarjeta profesional para el ejercicio de la profesión cuando así se requiera.
Experiencia	Debe poseer experiencia mínima de dos (2) años relacionada con los productos y servicios contratados por la Entidad Compradora y para la cual se prestará el servicio contratado.

5.4 Soporte Técnico Proactivo

Definición	El soporte técnico proactivo es un monitoreo continuo de tu red y equipos, para detectar posibles anomalías en el sistema desde el principio, utilizando para esto herramientas de monitoreo avanzadas.
Código y Nombre	AMSEDC- SAT-4 Soporte Técnico Proactivo
Unidad de facturación	Hora
Descripción técnica	Las actividades de soporte técnico proactivo están orientadas a la prevención de problemas o riesgos con el fin de mantener la disponibilidad de los productos adquiridos. El Proveedor debe llevar a cabo las actividades preventivas acordadas o solicitadas por la Entidad Compradora con el fin de evitar la interrupción del servicio y garantizar la operación correcta y permanente de los Productos. El soporte puede ser prestado de manera remota o en sitio. En caso de que el soporte remoto no sea suficiente y adecuado para solucionar el problema, el Proveedor deberá desplazarse hasta las instalaciones de la Entidad Compradora para resolverlo. El Proveedor pondrá a disposición en las instalaciones de la Entidad Compradora el personal requerido en el horario y los perfiles solicitados, para prestar el servicio de soporte técnico. El Proveedor realizará la verificación de la configuración, activación y acceso a los servicios y /o productos contratados. El Proveedor realizará la reinstalación, desinstalación y reconfiguración de Productos. La Entidad Compradora debe solicitar el servicio al Proveedor, a través de los canales que establezca la Entidad Compradora de común acuerdo con el Proveedor. El proveedor realizará el mantenimiento especifico a los productos adquiridos por la Entidad Compradora Los incidentes deben ser cerrados de común acuerdo entre la Entidad Compradora y el Proveedor siempre y cuando el problema sea resuelto satisfactoriamente. El proveedor dará soporte y realizará la actualización a los usuarios de la Entidad Compradora de los Productos adquiridos. El proveedor realizará la actualización de los Productos, Sistemas Operativos y Licencias de Productos, con sus respectivos parches de seguridad, para evitar pérdidas de información por posibles ataques informáticos.

	El consumo de las horas contratadas en la Orden de Compra se hará efectivo una vez se registre la solicitud en la mesa de ayuda o mediante el mecanismo que la Entidad Compradora acuerden con el Proveedor. Este servicio aplica para cualquiera de los Productos adquiridos a través del Acuerdo Marco de Precios o con los que cuente la Entidad Compradora. La Entidad Compradora debe establecer con el Proveedor la programación de los eventos de soporte programado. El Proveedor debe responder a las solicitudes de soporte de la Entidad de acuerdo con los tiempos definidos en el ANS. Una vez se realice el soporte técnico, el proveedor debe entregar un reporte técnico donde se indiquen las actividades realizadas, los procedimientos, recomendaciones y las actividades pendientes en caso tal.
Modalidad	Remoto En sitio
Zonas de prestación del servicio	En sitio Zona 1 En sitio Zona 2 En sitio Zona 3
Formación	Técnicos o tecnólogos de carreras profesionales en Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ingeniería de Sistemas, Ingeniería Informática o afines. Título profesional en Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ingeniería de Sistemas, Ingeniería Informática o afines; Con tarjeta profesional para el ejercicio de la profesión cuando así se requiera.
Experiencia	Debe poseer experiencia mínima de dos (2) años relacionada con los productos y servicios contratados por la Entidad Compradora y para la cual se prestará el servicio contratado.

5.5 Soporte Técnico Reactivo

Definición	El soporte técnico reactivo brinda soluciones a servicios de tanto hardware como software, que necesiten mantenimiento.
Código y Nombre	AMSEDC- SAT-5 Soporte Técnico Reactivo
Unidad de facturación	Hora
Descripción técnica	Las actividades de soporte técnico proactivo están orientadas a la prevención de problemas o riesgos con el fin de mantener la disponibilidad de los productos adquiridos. El Proveedor debe llevar a cabo las actividades preventivas acordadas o solicitadas por la Entidad Compradora con el fin de evitar la interrupción del servicio y garantizar la operación correcta y permanente de los Productos.

	El soporte puede ser prestado de manera remota o en sitio. En caso de que el soporte remoto no sea suficiente y adecuado para solucionar el problema, el Proveedor deberá desplazarse hasta las instalaciones de la Entidad Compradora para resolverlo. El Proveedor pondrá a disposición en las instalaciones de la Entidad Compradora el personal requerido en el horario y los perfiles solicitados, para prestar el servicio de soporte técnico. El Proveedor realizará la verificación de la configuración, activación y acceso a los servicios y /o productos contratados. El Proveedor realizará la reinstalación, desinstalación y reconfiguración de Productos. La Entidad Compradora debe solicitar el servicio al Proveedor, a través de los canales que establezca la Entidad Compradora de común acuerdo con el Proveedor. Los incidentes deben ser cerrados de común acuerdo entre la Entidad Compradora y el Proveedor siempre y cuando el problema sea resuelto satisfactoriamente. El proveedor realizará el mantenimiento especifico a los productos adquiridos por la Entidad Compradora El proveedor dará soporte y realizará la actualización a los usuarios de la Entidad Compradora de los Productos adquiridos. El proveedor realizará la actualización de los Productos, Sistemas Operativos y Licencias de Productos, con sus respectivos parches de seguridad, para evitar pérdidas de información por posibles ataques informáticos. El consumo de las horas contratadas en la Orden de Compra se hará efectivo una vez se registre la solicitud en la mesa de ayuda o mediante el mecanismo que la Entidad Compradora acuerden con el Proveedor. El proveedor realizará tareas de respaldo que permitan recuperar la información cuando ocurra un daño crítico del sistema operativo y configuraciones del servicio. Este servicio aplica para cualquiera de los Productos adquiridos a través del Acuerdo Marco de Precios o con los que cuente la Entidad Compradora. La Entidad Compradora debe establecer con el Proveedor la programación de los eventos de soporte programado. El Proveedor debe responder a las

	solicitudes de soporte de la Entidad de acuerdo con los tiempos definidos en el ANS. Una vez se realice el soporte técnico, el proveedor debe entregar un reporte técnico donde se indiquen las actividades realizadas, los procedimientos, recomendaciones y las actividades pendientes en caso tal
Modalidad	Remoto En sitio
Zonas de prestación del servicio	En sitio Zona 1 En sitio Zona 2 En sitio Zona 3
Formación	Técnicos o tecnólogos de carreras profesionales en Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ingeniería de Sistemas, Ingeniería Informática o afines. Título profesional en: Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Telemática, Ingeniería de Sistemas, Ingeniería Informática o afines; Con tarjeta profesional para el ejercicio de la profesión cuando así se requiera.
Experiencia	Debe poseer experiencia mínima de dos (2) años relacionada con la herramienta contratada por la Entidad Compradora y para la cual se prestará el servicio contratado.

CONTROL DE CAMBIOS DE DOCUMENTO			Versión vigente del documento:		01
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	04/08/2022	Creación de formato	Karlo Fernández Cala Gestor	Grupo Gestores SN	Catalina Pimienta Gómez Subdirector de Negocios

Nota: El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento que describe ficha técnica del presente documento.