OBJETO

Contratar las suscripciones de seguridad en la nube para los servicios de trabajo colaborativo Microsoft Office 365 según las especificaciones técnicas definidas por la Entidad.

Proyectó	Aprobó
Frank Córdoba Profesional Especializado Oficina de sistemas	BARRERA PINO LUIS MARTIN Firmado digitalmente por BARRERA PINO LUIS MARTIN Ing. Luis Martin Barrera Pino Jefe Oficina de Sistemas

Bogotá D.C, octubre de 2023

El presente documento refleja el estudio adelantado por el Departamento Administrativo Nacional de Estadística –DANE, de manera previa a la ejecución del proceso de selección, que sirven de soporte para la compra por Instrumento de agregación de demanda.

1. NECESIDAD

1.1. Descripción de la Necesidad

A través del Decreto 1170 de 2015 se definieron los objetivos, funciones generales, dirección e integración del sector estadístico y se planteó como objetivo general para el Departamento Administrativo Nacional de Estadística – DANE, garantizar la producción, disponibilidad y calidad de la información estadística estratégica, y dirigir, planear, ejecutar, coordinar, regular y evaluar la producción y difusión de información oficial básica. Siendo de esta manera el DANE el ente rector de la producción de las estadísticas oficiales del país, para lo cual desarrolla investigaciones, encuestas, registros y demás operaciones estadísticas tendientes a la recolección de información, así como su posterior crítica, análisis, depuración, procesamiento y difusión de la misma, que cubren aspectos del entorno político, económico, social, poblacional, ambiental, tecnológico y cultural, para contribuir a la planeación estratégica del sector público y privado del país.

Además, el Departamento Administrativo Nacional de Estadística –DANE tiene como misión: "*Producir y difundir información estadística oficial, como bien público, con altos estándares de calidad y rigor técnico para la toma de decisiones a nivel nacional y territorial, que contribuyan a la consolidación de un Estado con justicia social, económica y ambiental.*" y como visión "*En 2026 el DANE se consolidará como un referente nacional e internacional en la producción de información estadística oficial a partir de la transformación digital, con principios éticos, procesos innovadores, altos estándares de calidad, con un enfoque colectivo e intersectorial para la visibilización de las inequidades sociales, económicas y ambientales del país.*"

Ahora bien, para el cumplimiento de estos propósitos, como se dispone en el artículo 9 del Decreto 262 de 2004, son funciones de la Oficina de Sistemas, entre otras, las siguientes: *"4. Coordinar el uso e implantación de los sistemas, tecnologías de Información y comunicaciones, para los procesos de producción, recolección, crítica, procesamiento y control de calidad de las investigaciones del Departamento."*, "*5. Apoyar las actividades de análisis, desarrollo e implantación de los sistemas de información necesarios para dar cumplimiento a los compromisos del Departamento"*, *"7. Seleccionar los recursos tecnológicos que se requieran para el desarrollo de las actividades relacionadas con los sistemas, tecnologías de información y comunicaciones del Departamento"*; así como *"8. Administrar y realizar los procesos de soporte informático y tecnológico que la gestión del Departamento demande"*.

Adicionalmente, para llevar a cabo la misionalidad de la Entidad, se definió en el Plan Estratégico de Tecnologías de Información (PETI) 2023 a 2026, en el cual se identifican los aspectos de seguridad que se deben cubrir de acuerdo con el modelo de gestión y gobierno de TI, en su capítulo 6 como parte de las estrategias: "*7. Fortalecimiento de los Servicios Tecnológicos y Migración Incremental a la nube"*, y en el análisis de madurez expuesto en el capítulo 4 se identificó la brecha en el dominio de Seguridad: *"El DANE se encuentra en el proceso de implementación del Modelo de Seguridad de la Información en la fase de planeación definiendo el inventario de activos de información de la Entidad para proseguir con la identificación, valoración y mitigación de los riesgos asociados a los activos aplicando la metodología de gestión del riesgo de Función Pública."*. Estos apalancan la Línea Estratégica *"Tecnología de la Información para la Gestión Institucional"*, cuyo objetivo estratégico se concentra en los Principios y estándares para rigor y pertinencia de la misionalidad del DANE.

En este contexto, la Oficina de Sistemas debe responder a las necesidades de la Entidad a nivel nacional, atendiendo a los requerimientos que soporten la información estadística, para apoyar su misión y visión. En el marco

del uso de las Tecnologías de información y las comunicaciones, la adopción por parte de las entidades de los nuevos servicios y prácticas de computación en la nube y herramientas colaborativas, conlleva también la necesidad de proteger y hacer seguimiento a las prácticas de cada uno de los usuarios que tienen acceso a estos servicios, asegurando la gestión y elaboración colaborativa de documentación, así como, definir estrategias de seguridad que adopten en el uso del medio ambiente en la nube, los retos para la seguridad de los servicios en la nube son cada vez más importantes y aunque la Entidad tome las medidas y haya definido las estrategias y políticas de seguridad para mantener su infraestructura protegida, la falta de educación e información sobre seguridad a los usuarios que acceden a los recursos de nube puede provocar situaciones en las que los usuarios incurren en errores como lo es el uso de contraseñas poco seguras, medios o recursos compartidos sin previsión de seguridad, compartir contraseñas y accesos, así como otras prácticas que se salen del posible control de la misma Entidad, pues al facilitar el acceso desde cualquier dispositivo estos ya no están bajo el dominio de la red segura ni de la observación del equipo de TI o de los encargados de seguridad. Por tanto, se requiere la adquisición de un conjunto de herramientas que permitan: primero, automatizar la seguridad nativa de la nube de Microsoft Office 365; segundo, optimizar la detección y agilizar las operaciones de seguridad en la nube; tercero, habilitar el desarrollo de operaciones de monitoreo de la seguridad para hacer frente a la evolución de las amenazas y finalmente tener la información de cumplimiento a las exigencias legales de protección de datos.

Los proveedores de nube pública son conscientes de esta situación y se han esforzado los últimos años haciendo énfasis en que la responsabilidad al nivel de seguridad es de responsabilidad compartida: la seguridad que el proveedor ofrece llega hasta un punto, que es básicamente proteger la infraestructura subyacente, y de ahí en adelante es la Entidad usuario la que debe proveer las estrategias, mecanismos y políticas para asegurar que las aplicaciones, los datos y la infraestructura virtual sean seguras y que estén protegidas. Debe por tanto la Entidad considerar la adopción de mecanismos adicionales que le permitan reducir los riesgos inherentes a la misma red pública, bien sea a través de proveedores como terceros expertos en seguridad o de los mismos recursos diseñados por el proveedor de la nube.

Dada la amplitud de posibilidades para acceder a los servicios en la nube y al interés que genera para grupos de ciber atacantes de impactar de alguna manera entidades públicas, financieras, académicas, de gobierno o de investigación, que pueden iniciar con el simple hecho de ganar u obtener notoriedad dentro de una sociedad de hackers, hasta la posibilidad de afectar el funcionamiento de todo un sistema político o financiero, para el caso de nuestra Entidad que es la que provee la información estadística oficial del estado colombiano sobre la cual se definen políticas económicas, sociales y de gobierno en general, se convierte esta necesidad en algo del deber ser de la institución, y esta situación debe ser acogida desde la dirección de la Entidad hasta el nivel de trabajadores auxiliares y de apoyo de las actividades no misionales de la organización, y para esto la Entidad intenta, primero, crear esta sensibilización en el tema, luego crear una política que apoye a la dirección en la toma de decisión sobre qué hacer en esta dirección, y con esto obtener el apoyo necesario tanto en lo económico como en lo organizacional, para adquirir las herramientas tecnológicas suficientes y los presupuestos que permitan mantener esta política en el tiempo, para implementar y sostener los servicios de seguridad de la información para el buen funcionamiento de la Entidad, reducir o suprimir en un gran porcentaje las amenazas y los riesgos inherentes y minimizar su impacto en la operación y cumplimiento de los objetivos misionales de la Entidad.

Los recursos y cargas de trabajo que se implementan en la infraestructura tecnológica de la Entidad, están expuestos a una gran variedad de ataques y amenazas de ciberseguridad: ingeniería social (robo de credenciales, suplantación de identidad, comportamientos retaliativos o con ánimo de venganza), ransomware, ataques de denegación de servicio, phishing, virus informáticos (troyanos, worms, botnets, rootkits, etc), filtración de información, los ciber atacantes pueden explotar estas vulnerabilidades para acometer sus tareas criminales y lograr sus objetivos, disponer de herramientas, sistemas y prácticas de seguridad en la nube que sean sólidos, estos

son parte importante para lograr los niveles de disponibilidad deseados tanto de las aplicaciones como de los datos, los cuales son vitales para la Entidad; proteger la información confidencial y garantizar el cumplimiento de las normas y exigencias en cuanto a la seguridad cibernética se refiere en el ordenamiento legal colombiano.

La Entidad debe evaluar y categorizar el tipo de información que se está moviendo a la nube, o que a través de servicios contratados para soportar algunos servicios no misionales y de apoyo como correo electrónico, herramientas colaborativas para conferencias mediadas por sistemas como Microsoft 365, generan un cierto tipo de tráfico que incluye información de la Entidad, de acuerdo con los resultados de esta actividad orientar sus esfuerzos para adoptar modelos y herramientas que ayuden en el objetivo de proveer seguridad a su operación, garantizar la disponibilidad, la confiabilidad, la autenticidad y el acceso a sus funcionarios y colaboradores a la información que se supone deben tener para el desarrollo y cumplimiento de sus funciones y sobre todo en la información de base que contribuye a la implementación del modelo de producción estadística con el fin de generar la estadística oficial que requiere el país para la comprensión y solución de las problemáticas sociales, económicas y ambientales.

Otro aspecto importante a considerar en la implementación de herramientas de seguridad cuando se trata de entornos de nube es cumplir con la exigencias de la reserva estadística y la protección de datos personales, algunas de estas reglas conocidas como GDPR, o reglamento europeo de protección de datos personales, un conjunto de normas para privacidad de datos que requieren que proteja, administre y proporcione derechos y control sobre la información personal almacenada en la infraestructura de TI, incluidas las instalaciones locales y en la nube. En el caso colombiano la Ley 1581 o Ley de Protección de Datos fue creada para garantizar la seguridad y protección de los datos personales que se encuentran almacenados en las diferentes bases de datos de entidades de naturaleza pública o privada y que realicen algún tipo de tratamiento sobre los datos. El incumplimiento de las normativas de privacidad de datos puede provocar importantes multas.

Debido a la estructuración de nuevas operaciones estadísticas y a la definición de nuevos servicios, se incrementa la contratación de colaboradores a través de órdenes de servicio, lo cual expone a la Entidad en nuevos riesgos derivados de la contratación de personal, por lo cual la Entidad también debe contemplar cómo puede garantizar la seguridad de la información, de las aplicaciones y de los recursos a través de dispositivos de tipo personal (BYOD – trae tu propio dispositivo) incluso para sus colaboradores directos dadas las condiciones laborales actuales que hablan de trabajo remoto desde casa o teletrabajo, ya que el ingreso o acceso a los recursos de la nube se hace desde sus dispositivos propios, y que en apego a las normas la Entidad no tiene cómo controlar o gestionar directamente, aquí surge entonces la aplicación del concepto "Zero Trust Network Access" (acceso a la red de confianza cero), este concepto que se viene escuchando de hace poco más de tres años, pero que con la pandemia por Covid-19 creció en reconocimiento, debe entenderse en la forma de *"confiamos en la persona, pero no confiamos en lo que puede hacer con sus dispositivos"*, es decir, puede la Entidad exigir el uso de herramientas personales como antivirus, firewalls, VPNs, pero nadie puede garantizar que sus proveedores realmente cumplan con este mandato, ¿entonces, cómo se puede garantizar la seguridad de los recursos en la nube?

Es la misma Entidad la que debe asumir la protección de sus elementos y servicios de red en la nube, herramientas que brinden una protección adicional a los que provee intrínsecamente el proveedor de nube, poder gestionar y administrar estos recursos es clave para lograr el objetivo principal de la Entidad que es garantizar que su información siempre debe estar protegida, segura, inalterable por medios no autorizados, garantizando la reserva estadística y los pilares de la seguridad de la información que son parte de las obligaciones del DANE y que los usuarios aprenderán a usar también los mecanismos dispuestos ya implementados para un uso seguro de los servicios en la nube.

El más reciente informe de cibercrimen entregado por el Centro Cibernético Policial Nacional y la Dijín, reveló que, durante el 2022, los delitos asociados a crímenes vía internet se incrementaron, siendo el acceso abusivo a sistema informático, la violación de datos personales y el hurto por medios informáticos, los delitos más comunes. "El balance oficial indicó que el robo por canales informáticos encabeza la lista de los ciberdelitos desde 2020, con más de 13.000 casos; seguido por la violación de datos personales, con 7.001 casos; suplantación de delitos web, con 4.353; transferencias no consentidas de activos, con 2.362 e interceptación de datos informáticos, con 1.231."[1]

Además de todo lo anterior, podemos anotar que como resultado de la situación que se presentó con el COVID19, ocasionó un incremento considerable del uso de uso de herramientas colaborativas en la nube. En la Entidad Office 365 se adoptó como la solución para habilitar el trabajo remoto permitiendo la continuidad de las operaciones de las áreas administrativas desde cualquier lugar. Dado que es una de las herramientas principales de trabajo en el día a día, es importante seguir robusteciendo el esquema de seguridad con el cual se está protegiendo actualmente la solución. Es importante anotar que las herramientas colaborativas no están cubiertas por el sistema antivirus y los demás sistemas de seguridad de la Entidad, dado que estos sólo protegen la infraestructura "on premise", es decir todo lo local.

La Entidad pasó de tener por el orden de 6.000 cuentas de correo on premise en el 2019, a migrar 4.000 de estos servicios en nube con el objetivo de llevar mesas de trabajo virtuales y utilizar las herramientas colaborativas debido a la emergencia en el 2020.

Dado que la Entidad para cumplir con su misión se interrelaciona con otras entidades del estado como lo son: Ministerios, Institutos, entes reguladores, auditores, entre otras, y al mismo tiempo con empresa privadas que se involucran en el funcionamiento del país, se requiere fortalecer opciones de protección contra suplantación de identidad, al mismo tiempo tener detección avanzada de phishing y de configuración para inteligencia en suplantación de identidad.

Debido a que la Entidad tiene una implementación híbrida de mensajería (Microsoft Office 365 en la nube y Zimbra en Centro de Procesamiento de Datos en DANE Central), se requiere configurar protección a todo el entorno de mensajería y controlar el enrutamiento de correo para el filtrado de correo entrante al ecosistema de la Entidad.

Conscientes de las implicaciones del cumplimiento de las fases requeridas para el proceso estadístico especificaciones de necesidades, diseño, construcción, recolección, procesamiento, análisis, difusión y evaluación, implica para la Entidad un tráfico considerable de archivos que conlleva la necesidad de requerir una capa adicional de protección para los datos adjuntos de correo electrónico antes de entregarse a los destinatarios con el fin de salvaguardar entre otras la reserva estadística, de esta forma es fundamental se implemente protección del tipo antimalware y de suplantación de identidad que contribuya a la credibilidad y confianza de las fuentes.

Como la Entidad tiene presencia en varias Redes Sociales e interactúa con diferentes organismos estadísticos en el mundo como Naciones Unidas y sus diferentes oficinas, la OCDE, CEPAL, entre otros, la protección contra enlaces fraudulentos es imprescindible para salvaguardar la integridad de las estadísticas oficiales del país. Es requerido poder realizar análisis de direcciones URL en tiempo real, con reescritura de mensajes de correo electrónico entrantes en el flujo de correo, realizar comprobación con tiempo de clic de direcciones URL y vínculos en mensajes de correo electrónico y otras ubicaciones.

[1] https://www.semana.com/tecnologia/articulo/ojo-estos-son-los-ciberdelitos-que-mas-se-cometen-en-colombia/202127/

El examen de vínculos seguros ayuda a la Entidad a la protección contra enlaces malintencionados que se usan en la suplantación de identidad (phishing) y otros ataques. Se requieren capacidades de investigación y respuesta de amenazas, y usar el aprendizaje en simulación de ataques para ejecutar escenarios realistas en la Entidad. Estos ataques simulados pueden ayudar a identificar y encontrar usuarios vulnerables antes de que un ataque real impacte en la línea de fondo.

Las herramientas de protección avanzadas, soportadas en Inteligencia Artificial - IA y Machine Learning - ML, permiten que el equipo de operaciones de seguridad funcione de forma más eficaz. Las capacidades de IA y ML en conjunto incluyen procesos de investigación automatizados en respuesta a amenazas conocidas que existen actualmente y que permiten proteger toda la información estadística que se maneja por medio de estas herramientas colaborativas en la nube. Las acciones de corrección apropiadas esperan la aprobación, lo que permite al equipo de operaciones de seguridad responder a las amenazas detectadas.

Desde la ventana de administración y gestión en el portal de la herramienta se deben poder identificar y categorizar los ataques de suplantación de identidad en el servicio. Estas vistas pueden ayudar a:

1. Investigar y responder eficazmente a los ataques de suplantación de identidad.
2. Entender mejor el alcance del ataque.
3. Proporcionar información a los responsables de la toma de decisiones.
4. Obtener una perspectiva general del ataque más completa y más rápidamente.

Estas capacidades fortalecen la gestión y mitigan el riesgo de seguridad informática.

Por estas razones se hizo necesario en 2021 la adquisición de servicios de seguridad para la identidad en herramientas de colaboración, por medio de la OC 82720, renovadas en 2022 por medio de la orden de compra OC 102216. Este conjunto de programas informáticos facilita las labores diarias del personal de la Entidad, pues son usadas desde su estación personal a través de la nube disminuyendo el riesgo de pérdida de información o de retrasos en los procesos por sobrecargas en la red.

En el 2023, a través de la orden de compra OC 108135, la Entidad renovó la suscripción de licencias de herramientas colaborativas y correo y adquirió unas nuevas, finalizando con 5.031 licencias de Office 365, es por esta razón se requiere adquirir igual cantidad de servicios de seguridad que cubran las 5.031 licencias existentes. Es importante aclarar que no se están adquiriendo licencias de Office 365, estamos contratando servicios de seguridad para las herramientas colaborativas de Office 365 en nube.

Por lo tanto, se requiere adelantar un proceso de contratación para renovar suscripciones y adquirir adicionales que permitan el fortalecimiento de los servicios de seguridad en las herramientas colaborativas que actualmente tiene la Entidad con la Suite Microsoft Office 365 nube a través de la Tienda Virtual del Estado Colombiano (TVEC) Software por Catálogo, Instrumento de Agregación por Demanda CCE-139-IAD-2020.

2. DESCRIPCIÓN DEL OBJETO A CONTRATAR

2.1. Objeto

"Contratar las suscripciones de seguridad en la nube para los servicios de trabajo colaborativo Microsoft Office 365, según las especificaciones técnicas definidas por la Entidad."

2.2. Clasificación en la Codificación UNSPSC

El objeto del presente proceso tiene relación con los siguientes códigos de la UNSPSC:

Número	Segmentos	Familias	Clases	Productos
1	81. Servicios basados en ingeniería, investigación y tecnología	11. Servicios informáticos	15. Ingeniería de software o hardware	00. Todos
2	81. Servicios basados en ingeniería, investigación y tecnología	11. Servicios informáticos	25. Servicios de alquiler o arrendamiento de licencias de software de computador	01. Servicio de licencias del software del computador
3	81. Servicios basados en ingeniería, investigación y tecnología	16. Entrega de servicios de tecnología de información	18. Servicios de alquiler o arrendamiento de equipos o plataformas de voz y datos o multimedia	01. Servicio de arriendo o leasing de plataformas o equipos de comunicación de datos
4	43. Difusión de Tecnologías de Información y Telecomunicaciones	23. Software	27. Software de aplicaciones de red	01. Software de servidor de aplicaciones
5	43. Difusión de Tecnologías de Información y Telecomunicaciones	23. Software	27. Software de aplicaciones de red	04.Software de servicios de directorio por internet

2.3. Especificaciones técnicas

Los ítems que se van a adquirir son los siguientes:

Ítem	Código Catálogo	Descripción	Unidad de medida	Cantidad
1	FSZ-00002EAEASAP	Microsoft Defender O365 P2 Subscription Per User_EA_EAS_AP por 17 meses	Unidad	85.527
2	CE6-00003EAEASENT	Microsoft EMS E5 Subscription Per User_EA_EAS_Ent por 17 meses	Unidad	85.527

Nota: Para los ítems 1 y 2 y teniendo en cuenta que en el catálogo y el simulador de productos Microsoft no están relacionadas las licencias para suscripción anual, se seleccionan las de suscripción mensual y se multiplica la cantidad de licencias (5.031) por el número de meses requerido (17) para calcular el valor total. Para los dos Ítems es 5.031 X 17 = 85.527, obteniendo el valor que aparece en el simulador.

Es deber del proveedor conocer a cabalidad los Términos y condiciones de uso de la TVEC, el instrumento de agregación de demanda y sus Anexos Técnicos.

2.4. Plazo de Ejecución

El plazo de ejecución será de cinco (5) días hábiles contados a partir de la suscripción del acta de inicio entre el contratista y el supervisor del contrato, previo cumplimiento de los requisitos de perfeccionamiento y ejecución de la orden de compra, sin superar el 24 de noviembre de 2023.

Nota: La vigencia de las licencias será de diecisiete (17) meses contados a partir de la activación de la suscripción.

2.5. Sitio de entrega o de prestación del servicio

El desarrollo del objeto contractual se realizará en la ciudad de Bogotá; D.C., en la en la carrera 59 No. 26-70, Interior 1, edificio DANE Bogotá D.C., – Oficina de Sistemas o donde el supervisor lo considere pertinente.

2.6. Identificación del contrato a celebrar

Será una orden de compra dentro del Instrumento de Agregación de Demanda para la Adquisición de Software por Catálogo CCE-139-IAD-2020, derivado del proceso de contratación directa No CCE-116-IAD-2020.

2.7. Tipo de Contrato

Acorde con la naturaleza del objeto a contratar, el contrato resultante de este proceso se considera como un contrato de prestación de servicios.

3. OBLIGACIONES

3.1. OBLIGACIONES DEL CONTRATISTA O PROVEEDOR:

1. Cumplir con las condiciones para la adquisición de Software del Acuerdo Marco IAD Software por Catálogo CCE-139-IAD-2020 y con las especificaciones técnicas definidas en el numeral 2.3 del presente documento.
2. Cumplir con las obligaciones contenidas en la cláusula 12 -Obligaciones de los Proveedores - del Instrumento de Agregación de Demanda - Software por Catálogo CCE-139-IAD-2020. .
3. Entregar y prestar los productos objeto del proceso, de acuerdo a las condiciones establecidas en este documento y en el Instrumento de Agregación por Demanda CCE-139-IAD-2020.
4. Responder los reclamos, consultas y/o solicitudes eficaz y oportunamente.
5. Entregar oportunamente la información requerida por el DANE para registrar al proveedor en sus sistemas de pago.
6. Cumplir con las demás obligaciones derivadas de los Términos y Condiciones de Uso de la TVEC, las demás inherentes al objeto y naturaleza del contrato, así como aquellas indicadas por el supervisor del mismo para el cabal cumplimiento del objeto contractual.

3.2. OBLIGACIONES DEL DANE:

1. Velar por el cumplimiento de todas las cláusulas contractuales.
2. Exigir al proveedor la ejecución idónea y oportuna del objeto del contrato.
3. Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones, así como garantías a que hubiere lugar.
4. Entregar oportunamente al proveedor toda la información necesaria para la ejecución del objeto contratado.
5. Exigir la calidad de los servicios prestados objeto del contrato.
6. Cumplir con la forma de pago establecida, previo recibo a satisfacción por parte del DANE.
7. Las demás inherentes al objeto y naturaleza del contrato, así como aquellas indicadas en el Instrumento de Agregación de Demanda CCE-139-IAD-2020.

4. VALOR, IMPUTACIÓN PRESUPUESTAL, FORMA DE PAGO Y FACTURACIÓN:

4.1. Valor:

De acuerdo con los cálculos realizados en el Análisis del Sector, se tiene que el presupuesto total estimado para la contratación requerida asciende a la suma de: **CUATRO MIL OCHOCIENTOS DIECIOCHO MILLONES SETECIENTOS TREINTA Y NUEVE MIL NOVECIENTOS NOVENTA Y SEIS PESOS CON NOVENTA Y OCHO CENTAVOS M/CTE ($4.818.739.996,98).**

La siguiente tabla detalla el presupuesto estimado:

íte m	Código Catálogo SKU	Descripción del Producto	Unidad	Cantidad	Precio Unitario Sin Descuento	Precio Total Sin Descuento	Descuento	Precio Unitario con Descuento	Precio Total con Descuento	IVA	Total
1	FSZ-00002EAEASAP	Microsoft Defender O365 P2 Subscription Per User_EA_EAS_AP	Unidad	85.527	$19.545,50	$1.671.659.425,80	40%	**$11.727,24**	$1.002.995.655,48	N/A	**$1.002.995.655,48**
2	CE6-00003EAEASENT	Microsoft EMS E5 Subscription Per User_EA_EAS_Ent	Unidad	85.527	$63.735,40	$5.451.063.345,00	30%	**$44.614,50**	$3.815.744.341,50	N/A	**$3.815.744.341,50**
TOTAL											**$4.818.739.996,98**

Según el numeral 21 del artículo 10 de la Ley 1943 de 2018, los servicios de suministro de páginas web, servidores (hosting), computación en la nube (cloud computing) están excluidos del Impuesto a las Ventas (IVA), como también se puede comprobar en el mensaje arrojado por el simulador:

"El numeral 24 del artículo 476 del Estatuto Tributario - Decreto 624 de 1989 - adicionado por el artículo 187 de la Ley 1819 de 2016 y modificado por el numeral 10 de la Ley 1943 de 2018- señala que, el suministro de páginas web, servidores (hosting) y computación en la nube (cloud computing) están excluidos del impuesto sobre las ventas. Algunos productos de este catálogo pueden estar excluidos de IVA. Consulte con el proveedor/fabricante para más información."

Los recursos para atender el objeto de este proceso provienen del presupuesto del DANE, correspondiente a la presente vigencia fiscal de conformidad con el certificado de disponibilidad presupuestal.

4.2. Imputación presupuestal:

El presente proceso de contratación cuenta con el debido respaldo presupuestal contenido en el Certificado de Disponibilidad Presupuestal – CDP número 116723 del 2023 por valor total de $4.597.320.857,22.

CÓDIGO RUBRO	C-0499-1003-5-0-0499001-02 recurso 10
DESCRIPCIÓN DEL RUBRO	ADQUISICIÓN DE BIENES Y SERVICIOS - SERVICIOS DE INFORMACIÓN PARA LA GESTIÓN ADMINISTRATIVA - FORTALECIMIENTO Y MODERNIZACIÓN DE LAS TICS QUE RESPONDAN A LAS NECESIDADES DE LA ENTIDAD A NIVEL NACIONAL
FUENTE	Nación
VALOR	$4.818.739.996,98

4.3. Forma de pago y facturación:

El DANE pagará al contratista el valor del contrato así:

Un (1) único pago al momento de recibir la activación de los servicios, previa verificación de las cantidades de las licencias adquiridas en el servicio de administración de identidades de Microsoft (Tenant), por parte del supervisor del contrato y de acuerdo con las siguientes condiciones:

1-Previa presentación de factura y/o cuenta de cobro de acuerdo con las condiciones establecidas en el Instrumento de Agregación de Demanda CCE-139-IAD-2020 de la Tienda Virtual del Estado Colombiano.
2-Previa presentación de la certificación de cumplimiento a satisfacción generada por el encargado de ejercer el control y vigilancia del contrato.

Nota 1: El pago estará sujeto a lo establecido por el DANE, en el numeral 3 de la Circular No. 008 del 22 de marzo de 2020, el cual cita:

"(…)
Solo se recibirán cuentas de cobro radicadas electrónicamente por parte de los supervisores de los contratos con las siguientes indicaciones:

- *Se debe enviar un correo por cada cuenta de cobro radicada electrónicamente.*
- *Los documentos deben ser allegados con firmas.*
- *En el ASUNTO deben ir los siguientes datos: nombre o razón social completo del contrista, número del contrato.*
- *El correo hará las veces de radicado y así mismo tendrá autorización directa por parte del supervisor, para realizar el respectivo trámite de pago de la cuenta.*

(…)".

Nota 2. En cumplimiento del literal a) del numeral 3 de la Circular No. 008 del 22 de marzo de 2020 del DANE, la cuenta de cobro o factura se radicará a través de la ventanilla de atención al usuario de la Entidad (https://www.dane.gov.co/index.php/ventanilla-unica/pqr-s) dirigida al funcionario designado como supervisor del contrato. La factura debe contener la información necesaria de acuerdo a las normas comerciales y tributarias.
Nota 3. El pago se hará dentro de los treinta (30) días calendario, contados a de la fecha en que se radique de manera correcta los documentos mencionados en la forma de pago.
Si los documentos en mención no se presentan o son devueltos por falta de información o mal diligenciados, la Entidad contará hasta con treinta (30) días más, adicionales a los señalados, para realizar el pago, los cuales iniciaran a partir de la subsanación de los documentos.
Nota 4. En todo caso el pago está sujeto a la programación y aprobación del Programa Anual Mensualizado de Caja –PAC, situación que el contratista conoce y acepta.
Nota 5. El IVA, retención en la fuente, tasas y demás impuestos a que se tenga lugar, que deban realizarse al pago o abono en cuenta, se hará de acuerdo con las disposiciones legales que regulan la materia.
Nota 6. EL CONTRATISTA deberá acreditar el pago de los aportes establecidos en el artículo 50 de la Ley 789 de 2002, lo cual se hará mediante certificación expedida por el revisor fiscal o el representante legal si no se encuentra obligado a tener revisor fiscal, según corresponda.
Nota 7. El pago se realizará a través de la cuenta de ahorros o corriente que disponga el contratista, según sea el caso, acorde con la certificación expedida por la Entidad financiera.

Nota 8. El DANE no reconocerá pagos sobre pedidos o entregas de elementos y/o equipos según corresponda, que no hubieren sido previamente requeridos o autorizados por el Supervisor del contrato.
Nota 9. Para dar cumplimiento al derecho a turno, contemplado en el artículo 19 de la Ley 1150 de 2007, se deberá presentar toda la documentación necesaria para los pagos.

5. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

El parágrafo 5° del artículo 2 de la Ley 1150 de 2007, establece que los acuerdos marco de precios, permitirán fijar las condiciones de oferta para la adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización a las entidades estatales durante un período de tiempo determinado, en la forma, plazo y condiciones de entrega, calidad y garantía establecidas en el acuerdo. La selección de proveedores como consecuencia de la realización de un acuerdo marco de precios, les dará a las entidades estatales que suscriban el acuerdo, la posibilidad que, mediante órdenes de compra directa, adquieran los bienes y servicios ofrecidos. En consecuencia, entre cada una de las entidades que formulen órdenes directas de compra y el respectivo proveedor se formará un contrato en los términos y condiciones previstos en el respectivo acuerdo.

De conformidad con lo establecido en el artículo 2.2.1.2.1.2.7 del Decreto 1082 de 2015, que establece en su la procedencia del Acuerdo Marco de Precios que, "Las entidades Estatales de la Rama Ejecutiva del Poder Público del orden nacional, obligadas a aplicar la Ley 80 de 1993 y la Ley 1150 2007, o las normas que modifiquen, aclaren, adicionen o sustituyan, están obligadas a adquirir Bienes y Servicios de Características Técnicas Uniformes a través los Acuerdos Marco Precios vigentes."

Las entidades Estatales de la rama ejecutiva del orden nacional sometidas al Estatuto General de Contratación de la Administración Pública, están obligadas a adquirir los Bienes y Servicios de Características Técnicas Uniformes que requieren, al amparo del Acuerdo Marco de Precios existente según lo dispuesto en el Artículo 2.2.1.2.1.2.7 del Decreto 1082 de 2015, sin embargo, frente a los Instrumentos de Agregación de Demanda – IAD emitidos por Colombia Compra Eficiente, no existe normatividad vigente que los obligue a adherirse a ellos.

Así las cosas, la obligación de que trata el Articulo 2.2.1.2.1.2.7 del Decreto 1082 de 2015, solo hace referencia a Acuerdos Marco de Precios.

Los instrumentos de agregación de demanda son un mecanismo previsto por la ley para que las entidades Estatales suman sus necesidades y actúen en forma coordinada en el mercado para obtener eficiencia en el gasto y un mejor provecho de los recursos públicos.

Los Acuerdos Marco son un tipo de instrumento de agregación de demanda. En los Acuerdos Marco Colombia Compra Eficiente convoca al público en general a través de una licitación pública de bienes o servicios de características técnicas uniformes.

Las ventajas que aporta hacer la compra por IAD son superiores, por ejemplo, permiten lograr mejores precios, resultados y ahorros en términos de valor por dinero, así como reducir los costos administrativos del proceso de compra, tanto para las entidades como para los proveedores, como se logró evidenciar en los análisis y cálculos realizados en el Análisis del Sector.

Por estas razones la Entidad opta por realizar la compra por el instrumento de agregación por demanda de CCE.

6. FACTORES DE SELECCIÓN DE LA OFERTA MÁS FAVORABLE

De conformidad con lo establecido en el Instrumento de Agregación por Demanda CCE-139-IAD-2020, la Entidad seleccionara al Proveedor que haya cotizado el menor precio total para la adquisición de Software por catálogo.

7. ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS

Para el presente proceso, las garantías aplicables, son las estipuladas en la Cláusula 18.2. del instrumento de agregación de demanda CCE-139-IAD-2020.

Los Proveedores deben constituir una garantía de cumplimiento dentro de los tres (3) días hábiles siguientes a la colocación de la Orden de Compra a favor de la Entidad Compradora, por el valor, amparos y vigencia establecidos en la siguiente tabla.

El valor de los amparos de la garantía de cumplimiento es calculado de acuerdo con el valor de la Orden de Compra.

Amparo	Suficiencia	Vigencia
Cumplimiento del contrato	15% de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad de los Bienes	20% del Valor de la Orden de Compra	Duración de la Orden de Compra y un (1) año más
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5% del Valor de la Orden de Compra	Duración de la Orden de Compra y (3) tres años más

La vigencia de la garantía y sus amparos debe iniciar desde la colocación de la Orden de Compra.

Los Proveedores deberán ampliar la garantía dentro de los tres (3) días hábiles siguientes a la fecha en la que la Orden de Compra sea modificada, adicionada y/o prorrogada. La vigencia de la garantía debe ser ampliada por los plazos señalados en la tabla anterior. En todo caso de conformidad al Decreto 1082 de 2015 la garantía de cumplimiento debe estar vigente hasta la liquidación.

La Entidad Compradora deberá aprobar la garantía de cumplimiento correspondiente a la orden de compra, de conformidad con las disposiciones establecidas en el manual de supervisión y de contratación de cada Entidad.

En caso de declaratoria de incumplimiento que afecte la garantía de cumplimiento o alguno de sus amparos, el Proveedor deberá ajustar la suficiencia de la garantía, en los amparos respectivos, de forma tal que cumpla con lo señalado en la cláusula 18 después de haber sido afectada

8. SUPERVISIÓN DEL CONTRATO

La supervisión del contrato será ejercida por el jefe de la Oficina de Sistemas Luis Martín Barrera Pino (lmbarrerap@dane.gov.co). En todo caso, el ordenador del gasto podrá variar unilateralmente la designación del supervisor, sin que implique una modificación contractual.

En el ejercicio de sus funciones el (la) Supervisor(a) deberá realizar el seguimiento del cumplimiento de los términos y condiciones del Acuerdo Marco y de la Orden de Compra, revisar y aprobar la factura correspondiente, verificar que la Entidad pague el valor de la factura aprobada en los términos establecidos en el Acuerdo Marco de Precios, así como informar sobre cualquier eventualidad que dé lugar a un incumplimiento del proveedor. También deberá dar cumplimiento a las demás obligaciones como supervisor y deberá atender las funciones señaladas en la Constitución Política de Colombia, la Ley y los reglamentos tanto legales como internos del DANE.

9. APLICACIÓN DE ACUERDO MARCO DE PRECIOS

De acuerdo con lo establecido en el artículo 2.2.1.2.1.2.9 del Decreto 1082 de 2015, se adelantó la revisión delos Acuerdos Marcos de Precios vigentes en la dirección https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/acuerdos-marco, se determinó que para el presente proceso **NO existe un Acuerdo Marco de Precios** vigente aplicable, lo que aplica en este caso es el instrumento de agregación por demanda que tiene Colombia compra eficiente.

10. VERIFICACIÓN DEL PLAN ANUAL DE ADQUISICIONES

El área requirente manifiesta que revisó el Plan Anual de Adquisiciones que se encuentra publicado en la plataforma de Colombia Compra Eficiente (CCE) y verificó que los bienes, obras y/o servicios que se pretenden adquirir por medio de este proceso están debidamente relacionados en el mismo y por una cuantía igual o superior al presupuesto oficial estimado

También certifica que esta contratación podrá celebrarse y ejecutarse en su totalidad en la presente vigencia de acuerdo con el principio de anualidad

Proyectó: Frank Córdoba – Profesional Especializado Oficina de Sistemas.
Revisó: Ángel Yesid Ducuara Cruz – Coordinador plataforma tecnológica.