CONTRATO No. 4600088239 DE 2020

CONTRATANTE:	MUNICIPIO DE MEDELLÍN - SECRETARÍA DE SUMINISTROS Y SERVICIOS
NIT:	890.905.211-1
CONTRATISTA:	Technology Partners S.A.S.
NIT:	811.032.643-5
OBJETO:	"Servicio de suscripción al soporte y actualización de las licencias del AntiSpam Barracuda 800"
VALOR INICIAL:	Ciento dieciocho millones trescientos cincuenta y siete mil cuatrocientos pesos M/L ($118.357.400) IVA Incluido.
ADICION N°1:	N/A
VALOR DEL CONTRATO INICIAL MAS ADICIONES:	Ciento dieciocho millones trescientos cincuenta y siete mil cuatrocientos pesos M/L ($118.357.400) IVA Incluido.
DURACIÓN INICIAL:	Doce (12) meses
AMPLIACIÓN N°1	N/A
DURACIÓN INICIAL MAS AMPLIACIONES:	Doce (12) meses
SUSPENSIONES:	N/A
FECHA DE INICIO:	2 diciembre de 2020
FECHA DE TERMINACIÓN:	1 diciembre de 2021
MODIFICACIÓN ACTUAL:	**ADICIÓN 01:** Por valor de cuarenta y cinco millones novecientos treinta y cuatro pesos M/L ($45.934.000) IVA Incluido, correspondiente al 37,50% del valor inicial del contrato. **OTRO SI 01:** Agregar el siguiente parágrafo a la cláusula "CUARTA: FORMA DE PAGO." del contrato 4600088239 de 2020: "El valor de la Adición 01 del contrato se pagara cuando el supervisor reciba a entera satisfacción las actividades de soporte para la identificación y cierre de brechas de seguridad informática que se agregan mediante Otrosí 01 a este contrato." Agregar actividades de soporte para la identificación y cierre de brechas de seguridad informática mediante la aplicación de las configuraciones

	actuales a la Plataforma AntiSpam Barracuda 800, con el fin de reducir los niveles de riesgo asociados al servicio de correo electrónico institucional y llevarlos a una escala aceptable para la entidad, a través de mejoras introducidas a la Plataforma con la aplicación de un Security Assesment.

ANTECEDENTES:

El Municipio de Medellín cuenta con una plataforma AntiSpam llamada Barracuda, esta sirve para la protección del correo electrónico corporativo, este equipo nos protege del ingreso de virus o correos electrónicos que puedan afectar la integridad y confidencialidad de la información que se trasmite por este medio, al igual que podría afectar la disponibilidad del servicio de correo.

El contrato en curso **Nro. 4600088239 de 2020** cuyo objeto es el "Servicio de Suscripción al soporte y actualización de las licencias del AntiSpam Barracuda 800" tiene como alcance adquirir el Servicio de Suscripción al soporte y actualización de las licencias del AntiSpam Barracuda 800, de acuerdo a los Acuerdos de Niveles de Servicio (ANS) establecidos en las especificaciones técnicas; lo anterior para la correcta operación de esta plataforma, el cual mitiga los riesgos sobre el sistema de correo electrónico de la Alcaldía de Medellín por un año.

El Servicio de Suscripción al soporte y actualización de las licencias del AntiSpam Barracuda 800, se renuevan anualmente, y tiene como fin obtener la información de las nuevas amenazas conocidas para el caso, en la actualidad el dispositivo AntiSpam, el contrato actual finaliza el 1 de diciembre de 2021.

El contrato dio inicio el día **2 de diciembre de 2020** y ha tenido un comportamiento dentro del marco jurídico, técnico y administrativo, acorde a lo contemplado en los documentos contractuales.

A la fecha de elaboración del presente documento no se presenta proceso sancionatorio ni incumplimientos por parte del contratista

- Resumen de la ejecución de los recursos:

Valor del Contrato	$118.357.400 IVA incluido
Adiciones	0
Total valor del contrato más adiciones	$118.357.400 IVA incluido
Pagos Realizados (Acumulado) al 27/08//2021	$118.357.400 IVA incluido
Saldo del contrato al 27/08/2021	0
Porcentaje de ejecución financiera	100%
Porcentaje de ejecución física	73,70%

Nota: Teniendo en cuenta que en la CLAUSULA CUARTA, forma de pago del contrato N° 4600088239 de 2021, quedo estipulado un pago único por un valor igual al 100% y este pago ya se realizó dado que el contratista cumplió con los requisitos exigidos para dicho pago, el porcentaje de ejecución financiera del contrato a la fecha es el 100%.

JUSTIFICACIÓN:

Recientemente el país ha atravesado por un Paro Nacional de movimiento de protesta social, el cual comenzó el 28 de abril de 2021 y que a la fecha se mantiene, esto ha causado: marchas, enfrentamientos, protestas y género que el grupo de Hackers conocido a nivel internacional como "Anonymous" informara en su cuenta de Twitter el 3 de mayo de 2021 que "*If the president does not give the order to stop within 48 hours, we will enter the Colombian public system @YourAnonNews @anonops - Si el presidente no da la orden de parar en un lapsus de 48 horas, entraremos en el sistema público colombiano. @YourAnonNews*", también publico un video:
https://www.youtube.com/watch?v=ZnJbdOC7IyQ,
https://twitter.com/YourAnonNewsESP/status/1389439480688488449?s=20,
https://www.asuntoslegales.com.co/actualidad/anonymous-tumbo-pagina-del-ejercito-colombiano-y-modifico-su-descripcion-en-wikipedia-3164315

Posteriormente, el colectivo "Anonymous" el 4 de mayo de 2021 revelaría correos y contraseñas de al menos 168 miembros de las Fuerzas Armadas https://ghostbin.co/paste/zwh8g8a/raw y a su vez intervino de forma irregular la página del ejército https://twitter.com/YourAnonNewsESP/status/1389648429488484352?s=20, https://www.eltiempo.com/tecnosfera/novedades-tecnologia/anonymous-revela-correos-y-contrasenas-de-miembros-del-ejercito-de-colombia-585874, https://caracol.com.co/radio/2021/05/04/tecnologia/1620152538_277340.html

En los siguientes días otras Plataformas estatales también fueron afectadas por "Anonymous", como:

- La Página del Senado y de la presidencia de la república: https://www.elespectador.com/colombia/mas-regiones/tres-en-uno-anonymous-dice-que-hackeo-paginas-del-senado-de-colombia-y-presidencia-article/
- Se penetro la dirección fiscal y aduanera "DIAN". Sistema público colombiano https://twitter.com/YourAnonNewsESP/status/1390171652458119168?s=20, https://t.co/4nGPetObGZ?amp=1
- Infiltración de la radio de la Policía Nacional https://twitter.com/YourAnonNewsESP/status/1389794076732624901?s=20, https://t.co/HINI9kBrmf?amp=1, https://www.elespectador.com/judicial/anonymous-sigue-hackeando-ahora-fueron-las-comunicaciones-de-la-policia-article/

Adicional, a las anteriores entidades gubernamentales, en cualquier momento puede ser afectada cualquier plataforma web estatal, de acuerdo a lo informado por este colectivo el 4 de mayo de 2021: "*Saboteara cualquier tendencia que no sea relevante o que intente*

desviar la atención de la sistemática violación de los derechos humanos que se está produciendo hoy en Colombia."
https://twitter.com/YourAnonNewsESP/status/1389509089600880643?s=20 y a lo que indica el artículo:
https://colombia.as.com/colombia/2021/05/06/actualidad/1620334033_976860.html

A raíz de la situación, el CSIRT del Gobierno de Colombia (Equipo de Respuesta a Incidentes de Seguridad Informática - Csirtgob@mintic.gov.co) emitió comunicado el día 2 de mayo de 2021, sobre manifestaciones violentas cibernéticas por grupos cibercriminales que estarían realizando actividades de reconocimiento, escaneo e identificación a infraestructuras críticas del país, de la misma manera amenazan con desarrollar actividades delictivas en el ciberespacio en contra de los sistemas de información de entidades públicas y privadas. Esta información se deriva por parte de 07 entidades gubernamentales en el marco del desarrollo del Paro Nacional del 28 de abril de 2021 y días subsiguientes.

- Presidencia de la República (CSIRT Presidencia)
- Ministerio de Defensa (ColCERT)
- Ministerio de Comunicaciones (CSIRT Gobierno)
- Fiscalía General de la Nación
- Fuerzas Militares (CCOCI)
- Policía Nacional (Centro Cibernético, DIPOL, DIPRO, POLFA, CSIRT PONAL)
- Dirección Nacional de Inteligencia)

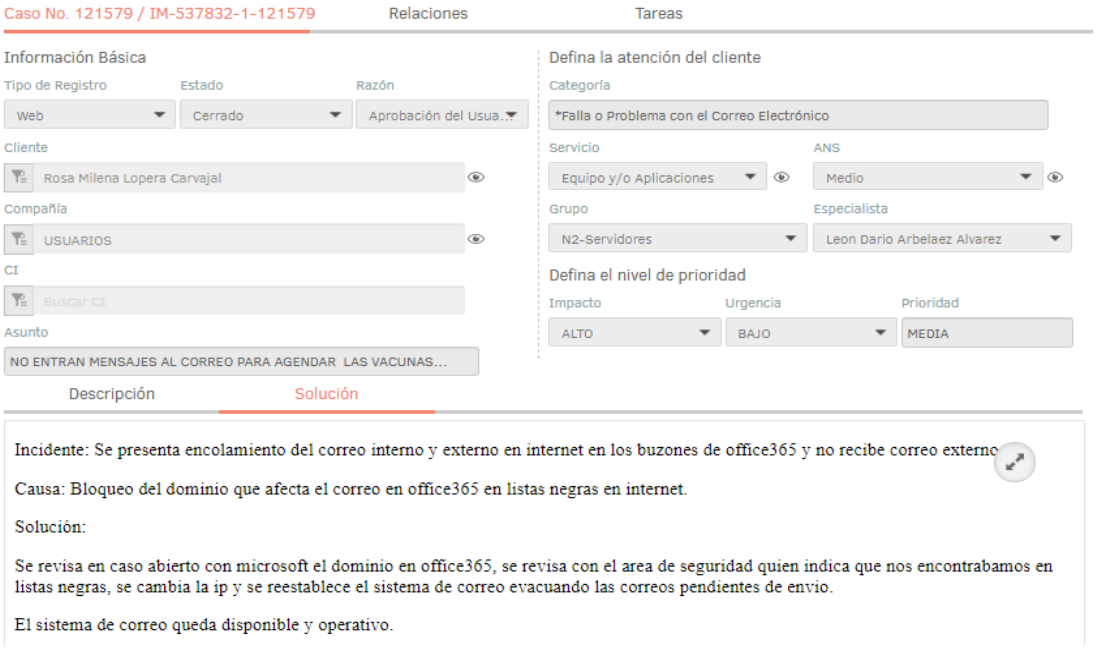
El CSIRT en dicho comunicado otorga unas recomendaciones, las cuales son: fortalecer la infraestructura, robustecer los protocolos de seguridad, realizar monitoreo constantes a los sistemas, tomar medidas necesarias de prevención, realizar actividades de mitigación frente a posibles ataques cibernéticos, poner en conocimiento cualquier situación atípica que se presente; con el fin de evitar algún incidente Informático y contrarrestar situaciones que puedan poner en riesgo la disponibilidad, la integridad y la confidencialidad de la información.https://www.itechsas.com/blog/ciberseguridad/alerta-de-seguridad-cibernetica-en-colombia/

También es importante resaltar que la mayoría de software malicioso es enviado por entes externos de dudosa procedencia a los correos electrónicos, los cuales son operados por personas, para nuestro caso los funcionarios de la entidad, teniendo como precedente que los empleados son el eslabón más débil en la estrategia de Seguridad Informática, ya que estos e-mails tienen esquemas de ingeniería social convincentes que pueden provocar filtraciones de información confidencial y pérdidas financieras potencialmente enormes, generando una seria amenaza para la organización.

Evidenciando los eventos que demuestran el aumento del nivel de riesgo de seguridad informática, como se observa en el hackeo de los correos de miembros de las Fuerzas Armadas y de la DIAN, así mismo adoptando las recomendaciones que realiza el CSIRT del Gobierno de Colombia, donde se indica que se deben tomar medidas necesarias de prevención, y buscando una solución a la situación actual, se inició trámite al interior de la

secretaria de Innovación Digital, el 22 de junio de 2021, día que se remite solicitud a revisión del equipo interno de apoyo a la contratación, evidenciando que es necesario efectuar un análisis y mejora en la capacidad de "filtro" AntiSpam Barracuda 800 y que este análisis es posible mediante unas actividades de soporte de características especiales y que para estas actividades es indispensable una adición al contrato 4600088239 dado que a través de este contrato el Municipio de Medellin obtiene la actualización y soporte de dicha plataforma. Es necesario que el contratista efectúe, entre otras actividades de soporte, un estudio de Security Assesment y efectúe la mayor cantidad de "actualizaciones" posibles a Barracuda 800 disminuyendo así la vulnerabilidad de esta en el mayor grado posible.

Aparte del incremento en los niveles de riesgo ya citados y las recomendaciones realizadas por el CSIRT, condiciones que ya por si solas obligan a reevaluar y fortalecer el sistema de control del correo electrónico institucional, en la actualidad sean detectado eventos que cada vez demuestran con más urgencia la necesidad de realizar las tareas de identificación de brechas por los bloqueos que se han presentado en la entrega de correos electrónicos de los servidores internos de correo de la organización a otros servidores en internet, detectados el domingo 6 de junio y el sábado 12 de junio y registrados mediante los incidentes en el sistema Aranda CSC con números 121579 y 122136, los cuales indican que la dirección IP del correo electrónico estaba en listas negras:



Las dos afectaciones citadas fueron evidenciadas por las quejas recibidas en el mes de junio de 2021, cuando diversos usuarios que hacen uso del correo electrónico institucional, así como el personal de la Secretaria de Salud, reportaron que los mensajes que enviaban no estaban siendo recibidos por los destinatarios de correos externos a la Alcaldía de Medellín.

A parte de lo anterior, en las semanas más reciente se han continuado identificando eventos que podrían indicar situaciones en las que mensajes correos electrónicos potencialmente maliciosos llegaron a los buzones de los usuarios de la Alcaldía de Medellín y que dan cuenta de la urgencia que se requiere tomar cartas en el asunto, se anexa recuento de incidentes más relevantes a la fecha:

Numero Incidente CSC - Aranda	Asunto	Fecha de registro
128913	Alerta Malware circulando en la red	01/09/2021 15:30
128894	Revisión de posible compromiso de cuenta	01/09/2021 14:14
128868	MENSAJES SPAM	01/09/2021 11:44
128849	Correo Spam	01/09/2021 10:43
128839	Mensaje recibido considerado sospechosos	01/09/2021 10:05
128814	Correo sospechoso	01/09/2021 8:28
128813	Gestionar Correo Sospechoso	01/09/2021 8:18
128174	Alerta ante sitio fraudulento que suplanta	24/08/2021 14:39
128014	Alerta de Phishing circulando en la red	23/08/2021 14:42
127681	Revisión de correo sospechoso	19/08/2021 8:55
127536	Reporte de mensaje sospechoso	17/08/2021 15:52
127435	Correo malicioso	17/08/2021 9:17
127057	Correo sospechoso	11/08/2021 10:51
126964	Mensaje de correo tipo Spam	10/08/2021 15:50
126874	Correo Sospechoso de amenaza de Virus.	10/08/2021 9:30
126374	Correo sospechoso	05/08/2021 9:12
126366	correo sospechoso	05/08/2021 8:35
126106	Correo sospechoso	03/08/2021 8:47
125718	Correo sospechoso	30/07/2021 9:02
123623	CORREO SOSPECHOSO	06/07/2021 16:09
123615	CORREO SOSPECHOSO	06/07/2021 15:08
123391	Correo Electrónico sospechoso	01/07/2021 11:21
123090	Posible ingreso de correo Falso	28/06/2021 9:08

De esta manera una vez revisada la situación del aumento en los métodos de amenazas en el correo electrónico:

- Se comienza a realizar un estudio en busca de soluciones con diferentes proveedores.
- Al explorar el mercado se encuentra que varios proveedores tienen la posibilidad de ofrecer el soporte para la identificación y cierre de brechas de seguridad para el

AntiSpam Barracuda 800, que precisamente tiene por objeto atender situaciones problemáticas como la descrita, pero que no fue incluido en el contrato existente.

- Se encuentra conveniente, e incluso necesario, que sea Technology Partners quien ejecute estas actividades adicionales, dado que no solo ofrece el costo más bajo por su realización, sino que estas implican intervenir el equipo AntiSpam Barracuda 800, y si un tercero lo manipulara se perdería el soporte y garantía que actualmente está contrato con Technology Partners, quienes son los proveedores actuales del contrato 4600088239 de 2020.

Este soporte, al tratarse de intervenciones técnicas de nivel especializado sobre la solución AntiSpam Barracuda 800, dado que enmarca tareas que buscan revisar y ajustar el funcionamiento de la solución y que tienen la finalidad de propender por la correcta operación de esta plataforma, al igual que mitigar los riesgos sobre el sistema de correo electrónico de la Alcaldía, se entiende cubierto en el alcance del contrato 4600088239 de 2020 que está establecido como:

"Servicio de suscripción al soporte y actualización de las licencias AntiSpam Barracuda 800, de acuerdo a los Acuerdos de Niveles de Servicio (ANS) establecidos en las especificaciones técnicas; lo anterior para la correcta operación de esta plataforma, el cual mitiga los riesgos sobre el sistema de correo electrónico de la Alcaldía de Medellín por un año."

Es de anotar que el citado soporte, si bien están cubiertas dentro del alcance del contrato actual, no fue incluido originalmente en el mismo, toda vez que éste contrato se suscribió en diciembre de 2020 antes de que ocurriera el evento sobreviniente de aumento abrupto en los niveles de amenaza informática que ya ha sido explicado que viene ocurriendo desde el primer semestre de 2021. Lo anterior teniendo presente que las actividades de soporte inicialmente incluidas en el contrato se refieren, como en todos los años anteriores, a actividades orientadas a resolver fallas de servicio sobre la plataforma, es decir aquellas en las que la solución deja de funcionar o deja de aplicar las reglas de control de configuradas, cosa distinta a la situación actual, ya que el equipo opera normalmente pero hay indicios que este funcionamiento ya no es suficiente. Se aclara que este enfoque de resolución de fallas operativas para las actividades se soporte ha sido el aplicado en los contratos anteriores para la solución Barracuda desde 2011, sin que en los años anteriores hubiera surgido una situación sobreviniente como la actual que obligara a agregar actividades, los contratos anteriores son:

CONTRATO No 4600035935 DE 2011
CONTRATO No 4600044584 DE 2012
CONTRATO No 4600051822 DE 2013
CONTRATO No 4600057154 DE 2014
CONTRATO No 4600062730 DE 2015
CONTRATO No 4600070865 DE 2017
CONTRATO No 4600076392 DE 2018
CONTRATO No 4600083178 DE 2019

Adicionalmente se remarca que este soporte para la identificación y cierre de brechas de seguridad que se solicita agregar al contrato actual, aportan al fortalecimiento y la postura de seguridad informática del correo electrónico de la Alcaldía de Medellín, frente al reciente cambio en los niveles de amenaza que se han generado en el marco de los movimientos de protesta social que vive el país y los eventos de bloqueo registrados.

Por qué se debe realizar la adición en este momento:

- Porque el contrato 4600088239 finaliza el 1 de diciembre de 2021 y es urgente realizar las actividades mencionadas anteriormente, ante las recomendaciones dadas por el CSIRT ya citadas, donde se deben tomar medidas necesarias de prevención.
- Estas actividades se deben hacer y no tiene espera por las alertas realizadas desde el colectivo de hackers llamado Anonymous expuestas anteriormente.
- Porque mientras no se realicen estas actividades, no se podrá conocer la magnitud del riesgo que la entidad sea víctima de un ataque informático que comprometa el correo electrónico, sea porque se afecte su funcionamiento, porque los piratas informáticos expongan información sensible gestionada por correo electrónico, o porque las cuentas de correo de la Alcaldía de Medellín sean comprometidas y usadas para actividades maliciosas como enviar mensajes falsos a los ciudadanos pidiendo pagar deudas inexistentes en servicios de pagos que van a terceros.
- Porque recientemente se ha identificado un aumento en el número de mensajes maliciosos que alcanzan a llegar a los buzones de correo de la entidad, como por ejemplo los mensajes con intentos de phishing (suplantación digital)
- Porque si se espera hasta el 2 de diciembre de 2021 para realizar las actividades planteadas, no solo transcurrirán varios meses en los que la entidad corre un riesgo no valorado y evaluado, sino que de identificarse actividades de tratamiento urgentes que requieran la aplicación de recursos financieros, sería prácticamente imposible ejecutarlas oportunamente debido al cierre de la vigencia fiscal.

Manera cuantificable por el tiempo restante de ejecución del contrato el valor de la adición solicitada

Valor del contrato actual	Duración	Valor por mes
$118.357.400	12	$9.863.117

Valor de la adición	Tiempo restante del contrato en meses	Valor por mes
$45.934.000	2	$15.311.333

Es de anotar que las actividades que se incluyen son más especializadas, por esto el valor entre un mes y otro incrementa.

Porcentaje del valor de la adición.

Valor Inicial Contrato	$	118.357.400,00
Año Celebración contrato		2020
Salarios Minimos		134,83
Adicion 01	$	45.934.000,00
Año adición		2021
Adicion SMMLV		50,56
% Adición SMLV		37,50%

Propuesta Económica:

DESCRIPCIÓN	VALOR
BARRACUDA-EMAIL GATEWAY SECURITY (Actividades de soporte y actualización acordadas en el Contrato 4600088239 DE 2020)	0
Security Assesment	$38.600.000
IVA	$7.334.000
Valor Total	**$45.934.000**

SOLICITUD:

Se solicita al Comité Interno de Planeación de la Secretaria de Suministros y Servicios, aprobar la siguiente necesidad:

ADICIÓN 01: Por valor de cuarenta y cinco millones novecientos treinta y cuatro pesos M/L ($45.934.000) IVA Incluido, correspondiente al 37,50% del valor inicial del contrato.

OTRO SI 01: Agregar el siguiente parágrafo a la cláusula “CUARTA: FORMA DE PAGO.” del contrato 4600088239 de 2020:

“El valor de la Adición 01 del contrato se pagara cuando el supervisor reciba a entera satisfacción las actividades de soporte para la identificación y cierre de brechas de seguridad informática que se agregan mediante Otrosí 01 a este contrato.”

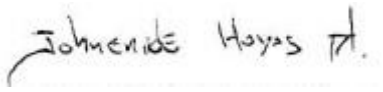
Agregar actividades de soporte para la identificación y cierre de brechas de seguridad informática mediante la aplicación de las configuraciones actuales a la Plataforma AntiSpam Barracuda 800, con el fin de reducir los niveles de riesgo asociados al servicio de correo electrónico institucional y llevarlos a una escala aceptable para la entidad, a través de mejoras introducidas a la Plataforma con la aplicación de un Security Assesment.

Las modificaciones incluidas en la presente solicitud fueron aprobadas mediante CIP N°48 del 04 de octubre de 2021 de la Secretaria Innovación Digital.

ANEXOS:

- Lista de chequeo
- Solicitud de Modificación
- Oficio de Solicitud al contratista
- Aceptación por parte del contratista
- Antecedentes del contratista y representante legal y Jurídica
- CDP adición contrato
- Propuesta económica adición entregada por Technology Partners
- Análisis de Riesgos por actividades complementarias (Se revisa Matriz de Riesgos Odiseo que se anexo en la etapa precontractual y estos riesgos cubren las actividades complementarias que se van a realizar)
- Copia del acta del Comité Interno
- Listado de asistencia CIP

Atentamente,



JOHNENIDE HOYOS MONCADA
Supervisor

Revisó: Duber Alexis Londoño Chavarría.
Apoyo jurídico
Subsecretaría de Ejecución de la Contratación
Secretaría de Suministros y Servicios.

Revisó: Yessica Hernández Ramos.
Apoyo administrativo, Financiero y Contable
Subsecretaría de Ejecución de la Contratación
Secretaría de Suministros y Servicios.

Revisó: Luis Miguel Sierra Saldarriaga.
Apoyo jurídico
Secretaría de Innovación Digital.