MINIMA CUANTIA No VJ-VPRE-MC-010-2016

En Bogotá D.C., a los quince (15) días del mes de junio de 2016, la Agencia Nacional de Infraestructura, por medio del presente documento se permite dar respuesta a las observaciones allegadas la invitación del proceso de mínima cuantía No VJ-VPRE-MC-010-2016, en los siguientes términos:

N°	NOMBRE DE LA PERSONA QUE OBSERVA	OBSERVACIÓN REALIZADA	RESPUESTA DE LA AGENCIA	Clasificación
1	De: Andrea Velez [mailto:Andrea.Velez@i2ss.com] Enviado el: martes, 14 de junio de 2016 4:11 p. m. **Andrea Velez Estupiñan** **Directora de Operaciones y HSEQ** **I2 Sistemas y Seguridad Informatica Ltda.**	Con el presente nos permitimos realizar las siguientes observaciones al pliego de condiciones definitivo del proceso en referencia cuyo objeto es "Contratar la compra e instalación de una solución de antivirus para la Agencia Nacional de Infraestructura – ANI" **Observación 1:** 1. En el documento Anexo 1 Técnico, pág. 3 subtitulo Otras Especificaciones Generales la entidad solicita para la solución antivirus "Deberá detectar y eliminar/desinfectar al menos los siguientes tipos de amenazas: Spyware, Adware, Rogues, Ransomware, Keyloggers, Troyanos, Worms, Virus, etc." Observación: Ninguna solución antivirus por si sola hace la detección y eliminación de RAMSOWARE, en razón a que ésta detección del ataque depende de las variantes nuevas, que pueden no estar incluidas en las firmas del día. Adicionalmente la razón más importante de la no detección por si sola, es que por tratarse de un ataque dirigido al usuario final, su efectividad depende del comportamiento del usuario final y no del antivirus.	**Respuesta Observación 1:** No se acepta la observación, RAMSOWARE es un tipo de virus informático (malware) y el objeto del proceso es un antivirus que permita bloquear, borrar, eliminar y proteger los equipos y a la información de la Entidad. Independiente del uso que haga el funcionario final, el acceso a páginas sospechosas está controlado por el firewall perimetral de la red ANI; por consiguiente no depende del usuario final si no del antivirus que haga su función.	Técnica

		Por lo anterior respetuosamente solicitamos a la entidad modificar en el documento Anexo 1 Técnico, que la solución: deberá detectar y eliminar o desinfectar al menos los siguientes tipos de amenazas: Spyware, Adware, Rogues, Ransomware, Keyloggers, Troyanos, Worms, Virus, etc, siempre y cuando la variante en cuestión se encuentre dentro de las firmas del último día. **Observación 2:** 2. En el documento Anexo 1 Técnico, pág. 4 subtitulo Otras Especificaciones Generales, la entidad solicita "El Endpoint debe contar con la certificación Gold OPSWAT para las categorías de antiphishing, antispyware, antivirus, cliente de copia de seguridad, cortafuego y filtrado de URLs" Observación: Respetuosamente solicitamos a la entidad modificar este ítem por: El Endpoint debe contar con la certificación Gold OPSWAT para las categorías inherentes a su función como antiphishing, cortafuego o antimalware. Lo anterior en razón a que las categorías de OPSWAT no contemplan todo lo requerido por la entidad en el aparte mencionado. Cordial Saludo,	**Respuesta Observación 2:** No se acepta la Observación, La certificaciones Gold OPSWAT cumple en forma directa sobre las categorías de antiphishing, antispyware, antivirus, cliente de copia de seguridad, cortafuego y filtrado de URLs.	Técnica
2	De: CARLOS MAURICIO PEREZ CORTES [mailto:cperez@itaca-la.com] Enviado el: miércoles, 15 de junio de 2016 10:29 a. m.	Con el presente nos permitimos realizar las siguientes observaciones al pliego de condiciones definitivo del proceso en referencia cuyo objeto es "Contratar la compra e instalación de una solución de antivirus para la Agencia Nacional de Infraestructura – ANI" De manera atenta, a continuación emitimos las observaciones referentes al proceso, esperando que sean tenidas en cuenta por ustedes para garantizar la pluralidad de oferentes en el mismo: **Observación 1:**	**Respuesta Observación 1:** No se acepta la observación, el proponente debe incluir en su	Técnica

	Carlos Mauricio Pérez C. **ITACA LATINOAMERICA** **Gerente Comercial**	✓ Revisando las especificaciones técnicas se puede establecer que el proceso se está cerrando a una sola marca violando con esto el principio de la pluralidad de oferentes y de la selección objetiva; lo cual no permite que los proponentes puedan ofertar otro tipo de marcas que cumplirían con la finalidad requerida. A manera de ejemplo citamos algunos de estos requerimientos: ○ Se solicita que la solución incluya un control por palabras para el correo electrónico con el fin de evitar fugas de información. Esto significa que se requiere incluir un módulo DLP a nivel del correo electrónico? Pues muchos fabricantes de antivirus no incluyen esta funcionalidad DLP como parte del EndPoint y debe licenciarse como un módulo o producto por separado (Ej: Symantec y Mcafee). Por ende esto puede encarecer los costos de la oferta o hacer inviable presentarse con ciertas marcas cerrando así el proceso solo al fabricante que pueda cumplir este requerimiento. Solicitamos respetuosamente aclarar este requerimiento o si es posible eliminarlo o ponerlo como un requisito opcional. **Observación 2:** ✓ Debido a que el sitio web del SECOP ha estado fuera de línea o intermitente durante esta semana, no hemos podido descargar todos los documentos del proceso para su revisión. Por este motivo, solicitamos respetuosamente la posibilidad de ampliar el plazo de presentación de ofertas para el viernes 17 o si es posible lunes 19 de junio de 2016 dando tiempo a. Quedamos atentos y en espera de sus respuestas.	oferta y asumir los respectivos costos del antivirus de tal forma que garantice los múltiples filtros de anti-spam, a través de listas de rechazos, filtrado por IP y otras tecnologías avanzadas que vengan incluidas en el antivirus, para proporcionar un porcentaje de captura de más 99% y con un mínimo de positivos falsos asegurando la entrega del correo importante. **Respuesta Observación 2:** No se acoge la observación, teniendo en cuenta que los términos se encuentran establecidos de acuerdo al Decreto 1082 de 2015, considerando que los mismos son suficientes para la presentación de las propuestas.	Jurídica

Proyectó aspectos técnicos: Javier Alonso Zuñiga Gómez – Experto GIT de Sistemas de Información y Tecnología - Vicepresidencia de Planeación, Riesgos y Entorno.
Proyectó aspectos juridicos: Daniel Correa Calderon – abogado / GIT Contratacion
Revisó aspectos juridicos: Gabriel Eduardo del Toro Benavides – Gerente / GIT Contratacion