Bogotá D.C., 10 de diciembre de 2025

UDNET-284-2025

Doctor
ELVERTH SANTOS ROMERO
Vicerrector Administrativo y Financiero
Universidad Distrital
Presente –

REF: Evaluación técnica final convocatoria pública 013-2025

Respetado doctor Santos:

Atentamente se remite la evaluación técnica final de la propuesta recibida en el marco de la convocatoria pública 013-2025 cuyo objeto es: "*Contratar los servicios de adquisición y renovación del licenciamiento de la solución de seguridad antivirus para equipos servidores físicos y virtuales, pc, portátiles y máquinas virtuales propiedad de la Universidad Distrital Francisco José de Caldas, incluyendo soporte técnico 7x24 y actualizaciones (update y upgrade) conforme con las condiciones y especificaciones técnicas previstas",* como resultado se presenta el siguiente resumen:

ÍTEM	PROPONENTE	EVALUACIÓN TÉCNICA	TOTAL COTIZACIÓN
1	INFO COMUNICACIONES S.A.S.	HABILITADA	$ 487.440.000

Igualmente se presenta la tabla de asignación de puntajes:

Ítem	Criterio	INFO COMUNICACIONES S.A.S.
		Puntaje
1	Propuesta económica	850
2	Tiempo de licenciamiento y soporte adicional	0
	Total	**850**

Así mismo, se presenta la verificación de los requisitos habilitantes:

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
1.1	Software de Seguridad - Antivirus	La solución debe contar con una consola de administración on-premise o en la nube que permita tener un sistema de administración, distribución y actualización centralizada de los endpoint, así como la configuración de las características ofrecidas por el producto.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
1.2		La solución de seguridad antivirus debe ser desarrollada e integrada por un único fabricante de forma tal que tanto el soporte de la solución como sus funcionalidades se integran y administran a través de la consola de administración.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.3		La solución debe proveer un inventario de hardware y software que permita al administrador conocer el software que ha sido instalado en el endpoint.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.4		La solución debe incluir seguridad para dispositivos de usuario final (antivirus, antimalware, antispyware, IPS/IDS, firewall personal, filtro de contenido web, control de aplicaciones, protección anti-ransomware, análisis de vulnerabilidades, protección con contraseña, antivirus para correo, control de phishing - pharming, cifrado de datos y dispositivos).	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.5		La solución debe contar con una tarea que permita la desinstalación remota de las aplicaciones.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.6		La solución debe permitir que el administrador defina una Lista Blanca de dispositivos permitidos como Solo lectura o Acceso completo.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.7		El módulo de control de aplicaciones para dispositivos de usuario final y equipos servidores debe contar como mínimo con las siguientes características: Comprobación en la ejecución, verificación de aplicaciones mediante escaneo programado, definición de mensajes personalizados para los usuarios finales, incluye detección de aplicaciones ofreciendo protección automática sobre las nuevas versiones del listado de aplicaciones establecido, permitir crear listas negras y blancas de aplicaciones basadas en categorías, certificados, Metadatos, hashes, condiciones personalizadas y portables.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.8		Módulo de filtrado de contenido web debe permitir crear reglas de bloqueo de recursos web basado en categorías, url específica, tipos de datos, debe tener la capacidad de poder ser asignado a usuarios del directorio activo, así como la asignación de horarios para la aplicación de diferentes reglas de control.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.9		El filtrado de contenido web, debe tener la capacidad de bloqueo para conexiones realizadas bajo HTTP o HTTPS indistintamente.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.10		La solución debe incluir protección para sistemas operativos Mac, Linux, Windows (la última versión liberada por Microsoft, Windows 10, 11, Windows Server 2008 R2, Windows Server 2012, 2016 y 2019). La solución ofertada no debe interferir con el desempeño normal de los equipos y aplicativos instalados en los equipos.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
1.11		La solución debe permitir crear grupos y generar políticas a los mismos.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.12		La solución debe contar con un módulo de generación de reportes y notificaciones, como mínimo debe exportar las mismas en formatos XML, PDF o HTML.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.13		La solución debe ser administrable desde una única consola de administración centralizada y debe tener la capacidad de ser consultada mediante navegador web desde cualquier estación de trabajo.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.14		La solución debe permitir la configuración granular de permisos de acceso a la consola de administración permitiendo al administrador crear diferentes perfiles de acuerdo con la labor que se asigne.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.15		La consola de administración debe tener la capacidad de notificar los intentos de infección de virus de acuerdo con parámetros definidos.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.16		Debe poseer un módulo de protección de antivirus basado en firmas, las cuales se deben poder programar en un día y hora específica para ser descargadas.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.17		Desde la consola de administración de la herramienta se debe poder hacer limitación del ancho de banda que va a ser utilizado por las actualizaciones de firmas para no generar carga en la red.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.18		Permitir características de administración proactiva para brindar a los administradores información y recomendaciones de políticas antes de la generación de patrones de virus. Políticas contra epidemias de virus.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.19		Permitir una estructura jerárquica la cual ofrezca determinación en el control de acceso, como permisos y roles sobre la solución de seguridad.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.20		Permitir la limpieza de daños en tiempo real para eliminar remanentes de virus, troyanos, spyware y entradas en el registro del sistema.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.21		Realizar actualizaciones automáticas de las listas de definiciones de virus a partir de una ubicación centralizada, así mismo debe permitir un modo de actualización local y en la nube en caso de no estar disponible el repositorio local.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.22		Controlar modificaciones del endpoint contra la remoción no autorizada del agente por parte del cliente a través de una contraseña.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.23		Todos los módulos de la solución deben ser de un único proveedor y desplegados mediante un único agente.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
1.24		La solución debe permitir el cambio de la configuración de los antivirus en los clientes de forma remota y a través de reglas aplicables a un grupo de máquinas.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.25		La solución debe permitir la creación de tareas de actualización de firmas, verificación de virus y actualización del producto.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.26		La solución debe generar registros (logs) del escaneo localmente con envío posterior de su contenido al administrador.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.27		La solución debe permitir la visualización de forma rápida y sencilla del estado y estadísticas de las infecciones generadas y permitir también visualizar las endpoint y servidores donde ocurrió la detección o infección.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.28		Visualizar mediante un Dashboard en tiempo real de la incidencia de virus, estado de la actualización de las máquinas y cualquier aviso o errores que puedan ocurrir.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.29		Permitir el aprendizaje automático para detectar amenazas desconocidas que generen riesgos de seguridad en los procesos o archivos sospechosos originados desde medios de almacenamiento externos, internos, servicios web o canales de correo.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.30		Permitir manualmente registrar excepciones de archivos que ya fueron analizados y descartados de acciones maliciosas ya sea por ser procesos permitidos o aplicaciones de uso interno.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.31		La solución debe contar con una herramienta de despliegue remoto que permita la instalación remota de la solución, así como la instalación de software de terceros o que no pertenecen al fabricante, pero cuentan con un archivo ejecutable o msi para su distribución. Así mismo permitir la instalación silenciosa a través de políticas de Directorio Activo, script de logon, etc.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.32		La solución debe contar con un sistema de cifrado integral de archivos, carpetas, unidades de almacenamiento, discos duros la cual debe manejar como mínimo un algoritmo de cifrado AES 256 con el fin de elevar el nivel de seguridad de la información almacenada en caso de robo o pérdida de algunos de los dispositivos	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.33		La solución debe incluir una herramienta de soporte remoto que permita a los integrantes de soporte la posibilidad de interactuar con el equipo de manera remota y que a su vez se registren las operaciones realizadas por la persona que realizo la conexión	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.34		La solución debe contar con una herramienta de conexión remota que permita la manipulación local del equipo de usuario final guardando un registro de las acciones realizadas con los archivos en la conexión.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
1.35		La solución debe contar con un módulo de detección y respuesta (EDR) que esté integrado con la solución antivirus ofertado.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.36		La solución debe incorporar un módulo que permita realizar el análisis de una amenaza o ataque para identificar el tipo de daño que pueda causar.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.37		La solución debe contar con la opción de emplear respuestas automatizadas para erradicar la amenaza del sistema.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.38		La solución debe brindar una interfaz y funciones sencillas que permitan dar alcance de manera rápida a un incidente.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.39		La solución debe descubrir las conexiones de una amenaza y su historial mediante la visualización de la ruta de expansión del ataque.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.40		La solución debe permitir crear tareas automatizadas a partir del manejo de indicadores de compromiso, así como permitir la importación de estos a la plataforma de protección.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.41		La solución debe entregar un informe en el que se pueda visualizar el alcance del ataque y la afectación a usuarios, procesos, archivos y registro del sistema que pudieron ser comprometidos	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.42		La solución debe permitir el aislamiento de los equipos de manera automática y/o manual al encontrar un evento asociado a una amenaza de propagación rápida.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.43		La solución debe evitar que el archivo malicioso se ejecute y se propague por toda la red durante la investigación.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.44		La solución de EDR debe ser completamente administrable e integrada con la solución ofertada, no se aceptan consolas de manejo independientes.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.45		La solución de protección de correo electrónico debe verificar los mensajes en busca de virus, malware, macros, objetos cifrados y archivos comprimidos.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.46		La solución de protección de correo electrónico debe ejecutar un análisis anti-phishing de los mensajes, analizar mensajes en busca de enlaces de anuncios o enlaces maliciosos y los relacionados a software legítimo.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.47		La solución de protección de correo electrónico debe permitir verificar los mensajes en busca de spam, posible spam y correo masivo.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
1.48		La solución de protección de correo electrónico debe permitir crear y configurar reglas para procesar los mensajes.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.49		La solución de protección de correo electrónico debe contener un panel con widgets para supervisar la aplicación.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.50		La solución de protección de correo electrónico debe permitir crear listas de usuarios personalizadas de direcciones admitidas y rechazadas.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.51		La solución debe proporcionar sobre los eventos detectados en el tráfico de correo electrónico y eventos de la aplicación detectados durante el funcionamiento de la aplicación.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
1.52		La solución de protección de correo electrónico debe permitir crear informes sobre el funcionamiento de la aplicación y enviarlos por correo electrónico.	Links suministrados entre los Folios 202 al 205 del documento PARTE DOS.pdf	Cumple	
2	Distribuidor Autorizado	El proponente debe entregar certificación de fábrica como distribuidor autorizado, con un nivel de partner GOLD o superior. Dicho certificado debe estar vigente durante la validez de la propuesta.	Folio 201 del documento PARTE DOS.pdf	Cumple	
3	Experiencia	El oferente deberá acreditar su experiencia mediante la información contenida en el RUP. El oferente deberá acreditar que ha celebrado, ejecutado y liquidado (siempre y cuando el régimen de contratación exija esta liquidación), totalmente, hasta tres (3) contratos en los últimos cinco (5) años, contados retroactivamente desde la fecha del cierre del presente proceso de selección, cumpliendo con las siguientes condiciones: 1. El objeto de estos contratos deberá consistir o estar relacionado con el objeto del presente proceso de selección. 2. La sumatoria de los contratos deberá ser, como mínimo, igual o superior a una (1) vez el valor del presupuesto oficial establecido en los presentes Pliegos de Condiciones. 3. Cuando las experiencias registradas en el RUP o en las certificaciones expresen su valor en dólares, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato. 4. Cada experiencia aportada mediante el RUP se analizará por separado. En caso de tratarse de contratos adicionados, el valor de las adiciones se convertirá a salarios mínimos mensuales legales vigentes (SMMLV) a la fecha de firma de la adición y se sumará al valor del contrato principal (si fuere el caso). 5. Cuando se presente el RUP para verificar en éste la experiencia requerida, los contratos indicados por el oferente deberán cumplir con al menos uno (1) de los códigos del Clasificador de las Naciones Unidas en el tercer nivel, para cada uno de los componentes a los que se presente	Folio 014 al 106 del documento PARTE UNO - DOCUMENTOS CONVOCATORIA PUBLICA No. 013 DE 2025 - PG 1 a 106.pdf Folio 170 al 200 del documento PARTE DOS.pdf	Cumple	

Ítem	Característica	Mínimo requerido	INFO COMUNICACIONES S.A.S		
			Ubicación en la propuesta. Numero de Pagina	Cumple / No Cumple	Observaciones
4	Propuesta Económica	Propuesta Económica	Folio 214 del documento PARTE DOS.pdf	Cumple	
EVALUACIÓN TÉCNICA			**HABILITADA**		

Cordialmente,

Yuleima Ortiz Zambrano
Líder Unidad Red de Datos UDNET

	Nombre	Cargo	Firma
VoBo	Alejandro Daza Corredor	Jefe Oficina Asesora de las Tecnologías e Información	
Proyectó	Stefany Arias	CPS OATI UDNET	Stefany A