UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
VICERRECTORIA ADMINISTRATIVA Y FINANCIERA
CONVOCATORIA PUBLICA N° 013-2018 CONVOCATORA PUBLICA

OBJETO: *"CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE EQUIPOS, LICENCIAS Y COMPONENTES, QUE PERMITAN LA ACTUALIZACIÓN Y EL REFORZAMIENTO, DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES Y DE LA SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, MEDIANTE DOS COMPONENTES: SISTEMA DE SEGURIDAD PERIMETRAL Y EQUIPOS ENRUTADORES".*

ADENDO No. 01

Dentro del marco de la Ley 30 de 1992, el Acuerdo No 03 de 2015 expedido por el Consejo Superior Universitario, la Resolución No 262 de 2015 expedida por la Rectoría de la Universidad Distrital y demás normas que la complementan, adicionan o reglamentan y teniendo en cuenta las respuestas aceptadas a las observaciones presentadas por los oferentes interesados en el proceso. El Comité Asesor de Contratación aprueba por unanimidad modificar los Pliegos de Condiciones mediante el presente Adendo, tal como se describe a continuación:

1. Modificar el numeral 2.3.1 EXPERIENCIA DEL PROPONENTE, que en lo sucesivo queda así:

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), mínimo tres (3) y máximo cinco (5) contratos en los últimos cinco (5) años para cada componente, contados retroactivamente desde la fecha del cierre del presente proceso de selección, cumpliendo con las siguientes condiciones:

Para cada uno de los componentes:

- ✓ El objeto de estos contratos deberá consistir o estar relacionado con el objeto del presente proceso de selección.
- ✓ 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, es decir, respecto del presupuesto establecido para cada uno de los componentes en relación con el cual se oferta, esto es, 500 millones de pesos para el componente uno (1) y 270 millones, para el dos (2).
- ✓ 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.
- ✓ 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).
- ✓ 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 una de los componentes a los que se presente, y que se señalan a continuación:

CLASIFICACION UNSPSC	DESCRIPCIÓN
32151800	Dispositivos de control de seguridad
43220000	Equipos o plataformas y accesorios de redes multimedia o de voz y datos
43221700	Equipo fijo de red y componentes
43222500	Equipo de seguridad de red
43222600	Equipo de servicio de red
43223100	Componentes y equipo de infraestructura de redes móviles y digitales
43223300	Dispositivos y equipos para instalación de conectividad de redes y Datacom
43230000	Software
43232800	Software de administración de redes
43233200	Software de seguridad y protección

La actualización a "pesos de hoy" del valor de los contratos ejecutados, se calculará en relación con el valor del salario mínimo del año de la fecha de terminación, es decir, el valor de los ítems se expresará en salarios mínimos correspondientes al año de terminación. Para efectos del cálculo correspondiente, se anexa la siguiente tabla sobre los valores del SMLMV de los últimos años:

PERIODO	MONTO
Enero 1 de 2013 a Dic. 31 de 2013	$ 589.500
Enero 1 de 2014 a Dic. 31 de 2014	$ 616.000
Enero 1 de 2015 a Dic. 31 de 2015	$ 644.350
Enero 1 de 2016 a Dic. 31 de 2016	$ 689.455
Enero 1 de 2017 a Dic. 31 de 2017	$ 737.717
Enero 1 de 2018 a la fecha.	$ 781.242

NOTA: TENIENDO EN CUENTA QUE EL REGISTRO ÚNICO DE PROPONENTES –RUP- NO CONSIGNA EL TIEMPO DE EJECUCIÓN DE LOS CONTRATOS Y PORCENTAJES DE PARTICIPACIÓN, CUANDO EL PROPONENTE FUERE PLURAL, ÉSTE DEBERÁ ACREDITAR LA EXPERIENCIA CONSIGNADA EN EL RUP, ADJUNTANDO LAS CERTIFICACIONES Y/O COPIA DE LOS CONTRATOS EN LOS CUALES SE PUEDA EVIDENCIAR DICHOS ASPECTOS.

- NOTA: En dicho documento (RUP), se verificará que el oferente esté inscrito antes de la fecha de cierre en la clasificación que se establece en el anterior cuadro.

- ✓ Para el caso de experiencias que sean presentadas como integrante de consorcio, unión temporal o promesa de sociedad futura, se tendrá en cuenta únicamente el valor correspondiente al porcentaje de su participación, por tanto, la certificación lo debe señalar.

- ✓ Cuando el proponente incluya valores que no correspondan a la experiencia general o especifica, aqui señaladas, este valor será descontado del valor total del contrato certificado respectivo.

- ✓ Los proponentes que se presenten en Consorcio, Unión Temporal o Promesa de Sociedad Futura deberán cumplir en conjunto con la experiencia requerida, lo cual significa que deberá ser acreditada por todos, algunos o uno de los integrantes.

- ✓ En caso de requerirlo, la Universidad podrá solicitar la copia del contrato, así como del o de los OTROSI que se hubieran firmado.

- ✓ La Universidad se reserva el derecho de verificar toda la información y documentación que los proponentes presenten en su propuesta. De presentarse inconsistencias, la propuesta será rechazada.

- ✓ EN CUANTO A PERSONAS NATURALES EXTRANJERAS DOMICILIADAS EN COLOMBIA Y PERSONAS JURÍDICAS EXTRANJERAS CON SUCURSAL EN EL PAÍS, deberán acreditar este requerimiento como lo haría una persona jurídica de origen nacional. En cuanto a personas naturales y personas jurídicas privadas extranjeras no inscritas en el RUP, por no tener domicilio o sucursal en el país, el requisito exigido es el mismo, pero deberá ser aportado mediante contratos, certificaciones de contratos o documentos equivalentes.

  Sin embargo, es necesario tener en cuenta que todos los documentos otorgados en el exterior para acreditar lo dispuesto en este numeral, deberán presentarse legalizados en la forma prevista en el Código General del Proceso y el Artículo 480 del Código de Comercio. Si se tratare de documentos expedidos por autoridades de países miembros del Convenio de La Haya de 1961, se requerirá únicamente de la Apostille.

- ✓ Las certificaciones o contratos para las personas naturales y jurídicas extranjeras no domiciliadas en Colombia, deben tener como mínimo la siguiente información:

a. Nombre o razón social de la entidad que certifica
b. Valor del contrato
c. Objeto del contrato y alcance del mismo, de ser el caso
d. Fecha de suscripción e iniciación
e. Fecha de terminación: Estos contratos deberán estar terminados y, de ser el caso, liquidados, antes de la fecha de cierre del presente proceso
f. Porcentaje de participación, en tratándose de consorcio, unión temporal o promesa de sociedad futura
g. Nombre Completo, cargo, dirección y número de Teléfono de la Persona que expide la Certificación

NOTA: Aquella experiencia que sea calificada en el cumplimiento del contrato como "malo", "regular" o expresiones similares, que demuestren o que indiquen, que durante su ejecución fueron sujetas a multas o sanciones debidamente impuestas por la administración, no se aceptarán por la Universidad.

Otras Consideraciones importantes:

- ✓ Confidencialidad

El proponente respetará el carácter confidencial de toda la información obtenida dentro del marco de la ejecución del contrato y no deberá divulgarla a terceros, sin acuerdo previo y por escrito con la Universidad Distrital Francisco José de Caldas.

- ✓ El oferente deberá anexar en su propuesta, carta en donde se compromete a realizar todas las actividades establecidas en las presentes especificaciones técnicas.

- ✓ El oferente deberá registrarse en el Sistema de Registro de Proponentes de la Universidad Distrital (Sistema ÁGORA).

2. Modificar el numeral 2.4.1.1 ESPECIFICACIONES TÉCNICAS COMPONENTE 1, ITEM 80, que en lo sucesivo queda así:

Los factores que deben ser ofertados, deben cumplir, en su totalidad, con las caracteristicas técnicas mínimas de carácter obligatorio. De no cumplir con estas características, la propuesta no será aceptada por no permitir la escogencia objetiva del contratista.

La evaluación de orden técnico se hará a partir de la siguiente tabla y, por lo tanto, el proponente debe diligenciar cada uno de los ítem en la celda correspondiente a la columna con título: "Ubicación en la propuesta y Link a página WEB del fabricante (No. de Página)", la cual debe ser confirmada mediante documentación oficial y pública en la Web del fabricante (guías de administración, manuales y/o guías técnicas), en medio físico y digital, en el cual se debe referenciar para cada característica un link a página WEB oficial, donde se encuentre la documentación y número de página del documento encontrado en el link, donde se puede validar el cumplimiento de la especificación técnica. En el caso de las certificaciones y servicios solicitados, se debe relacionar el número de página (folio) de la propuesta entregada.

	ÍTEM	CARACTERÍSTICA	Ubicación en la propuesta y Link a página WEB del fabricante (No. de Página)
GENERALIDADES	1	El Sistema de Seguridad Perimetral (HA) debe estar compuesto por todo el hardware, software y licenciamiento necesarios para su funcionamiento incluyendo alta disponibilidad HA.	
	2	El sistema debe contar con máximo dos equipos con el fin de minimizar los puntos de falla, optimizar el espacio en el data center, optimizar el uso de las conexiones de red y facilitar la administración incluyendo el sistema de monitoreo y reportes. Estos deben trabajar de forma redundante entre sí en Alta disponibilidad (HA) soportando todos los servicios que presta el sistema de seguridad perimetral HA.	
	3	El hardware y software que ejecuten las funcionalidades del sistema deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operativo de uso genérico	
	4	Los equipos ofrecidos deben ser adecuados para montaje en rack 19". Cada equipo puede ocupar máximo 3 unidades de Rack.	

	5	El software del sistema deberá ser ofertado en la última versión estable y recomendada por el fabricante.	
	6	El sistema debe tener la capacidad de identificar al usuario de red con integración a Microsoft Active Directory, sin la necesidad de instalación de agente en el Controlador de dominio, ni en las estaciones de los usuarios.	
	7	Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready	
	8	El sistema debe incluir actualización automática de firmas de prevención de intrusos (IPS), bloqueo de archivos maliciosos (Antivirus y Antispyware), Filtrado WEB por categorías e identificación de aplicaciones	
	9	Motor de procesamiento en paralelo: el módulo de hardware del plano de control y el módulo de hardware del plano de datos deben estar separados y deben estar embebidos en cada equipo.	
	10	Los equipos ofertados NO deben estar en anuncio de fin de vida (end-of-life) y fin de venta (end-of-sale) por parte del fabricante	
	11	Debe permitir el control de políticas por identificación de País.	
	12	El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner Silver (o equivalente a la marca) o superior de los productos adquiridos con el licenciamiento, teniendo en cuenta que en orden ascendente los niveles de certificación son: Silver, Gold, Platinum (o equivalente a la marca).	
ALTA DISPONI	13	Soporta configuración de alta disponibilidad (HA) en los modos Activo/Pasivo y Activo/Activo en modo transparente y en layer 3	
	14	El HA (modo de Alta-Disponibilidad) debe permitir monitoreo de fallo de link.	
CAPACIDAD Y CANTIDADES	15	Throughput para cada equipo de mínimo 8 Gbps con la funcionalidad de control de aplicaciones habilitada y logs habilitados para todas las firmas (actualizaciones) que el fabricante disponga.	
	16	Throughput para cada equipo de mínimo 4 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas firmas (actualizaciones) que el sistema disponga debidamente activadas y actuando con logs habilitados para: control de aplicaciones, IPS, Antivirus y Antispyware.	
	17	Cada equipo debe tener la Capacidad de procesar mínimo 3 millones de conexiones de red simultáneas (concurrentes)	
	18	Cada equipo debe tener la Capacidad de procesar mínimo 135.000 nuevas conexiones en red por segundo.	
	19	Cada equipo debe tener Fuente 120V AC, redundante y hot-swappable (dos fuente en redundancia)	

	20	Cada equipo debe incluir Disco de Estado Sólido (SSD) o arreglo de discos (SSD) de mínimo 240 GB para almacenamiento del sistema y logs	
	21	Mínimo 8 Interfaces Ethernet base-TX 10/100/1000 de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	
	22	Mínimo 4 Interfaces 10Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración) incluyendo Mínimo 2 optical transceiver SFP+ 10-Gigabit multi-mode	
	23	Mínimo 1 Interfaz para alta disponibilidad a 1 Gbps (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)	
	24	Mínimo 1 Interfaz adicional para alta disponibilidad a 10 Gbps SFP+ (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)	
	25	Interfaz dedicada para administración 10/100/1000 para cada equipo	
	26	1 interfaz de tipo consola	
	27	Capacidad de mínimo 60 zonas de seguridad	
SERVICIOS Y PROTOCOLOS DE RED	28	Soporte de mínimo 1024 VLAN Tags 802.1q	
	29	Soporte de Agregación de links 802.3ad	
	30	Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2) Para IPv4	
	31	Debe soportar enrutamiento estático y dinámico (OSPFv3) Para IPv6	
	32	Capacidad de balancear varios enlaces de internet con o sin el uso de políticas especificas	
	33	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QoS y SSL Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no hay contrato de licenciamiento con el fabricante.	
CONTROL POR POLÍTICA DE FIREWALL	34	Soportar controles por zona de seguridad	
	35	Controles de políticas por puerto y protocolo.	
	36	Control de políticas por aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.	
	37	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.	
	38	Soportar objetos y Reglas multicast.	

	39	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.	
CONTROL DE APLICACIONES	40	El sistema deberá tener la capacidad de reconocer aplicaciones, independiente del puerto y protocolo	
	41	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.	
	42	Detectar y limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD	
	43	Para mantener la seguridad de la red, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas	
PREVENCIÓN DE AMENAZAS	44	Para seguridad del ambiente contra ataques informáticos, el sistema de seguridad debe poseer módulo de IPS, Antivirus y Anti-Spyware integrados en los equipos que componen el sistema	
	45	El sistema debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.	
	46	Debe incluir seguridad contra ataques de denegación de servicios.	
	47	Debe permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3	
	48	Soportar bloqueo de archivos por tipo	
	49	Debe ser posible la configuración de diferentes politicas de control de amenazas y ataques basados en políticas del firewall donde cada política pueda incluir como mínimo Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad	
	50	El sistema debe ofrecer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta.	
	51	El sistema debe ser capaz de enviar archivos sospechosos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado.	
FILTRO URL	52	Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad	
	53	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando URLs a través de la integración con servicios de directorio, autentificación vía LDAP, Active Directory, E-Directory y base de datos local	

	54	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL	
	55	Debe permitir al menos 60 categorías de URLs	
	56	Debe soportar la creación de categorías URL custom	
	57	Debe soportar la exclusión de URLs del bloqueo por categoría	
IDENTIFICACIÓN DE USUARIOS	58	Debe permitir integración con Radius, ldap, Active Directory, E-directory y base de datos local, para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	
	59	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC via syslog, para la identificación de direcciones IP y usuarios	
	60	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tienen estos servicios	
	61	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.	
CALIDAD DE SERVICIO	62	Como la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc.) y tener un alto consumo de ancho de banda, el sistema debe controlarlas por políticas de máximo ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.	
	63	Soportar la creación de políticas de QoS por: - Dirección de origen - Dirección de destino - Por usuario y grupo de LDAP/AD - Por aplicaciones - Por puerto	
	64	El QoS debe permitir la definición de clases por: - Ancho de Banda garantizado - Ancho de Banda Máximo - Cola de prioridad.	
	65	Soportar priorización RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.	
	66	Soportar marcación de paquetes Diffserv	

FILTRO DE DATOS	67	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, mas no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos via expresión regular	
	68	Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados	
VPN	69	Debe soportar VPN IPSec Nativa Client-To-Site y Site-to-Site (Incluyendo conexión Site-to-Site con infraestructuras en la nube mínimo con: Amazon, Microsoft Azure)	
	70	La VPN IPSEc debe soportar mínimo: - 3DES; - Autenticación MD5 y SHA-1; - Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; - Algoritmo Internet Key Exchange (IKEv1 & IKEv2); - AES 128 y AES 256 (Advanced Encryption Standard) - Autenticación via certificado IKE PKI.	
	71	Debe poseer interoperabilidad VPN IPSec mínimo con los siguientes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall	
	72	Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operativo del equipo cliente o por medio de interfaz WEB	
	73	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local	
	74	Permite establecer un túnel VPN client-to-site del cliente al sistema de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon	
	75	Debe permitir que las conexiones VPN SSL o VPN IPSec sean establecidas de las siguientes formas: - Antes o durante la autenticación del usuario en la estación - Después de la autenticación del usuario en la estación - Manualmente por el usuario	
	76	El cliente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10	
	77	Capacidad de soportar mínimo 2000 clientes de VPN SSL simultáneos sin uso de licenciamiento o licenciado a perpetuidad	
	78	Capacidad de soportar mínimo 1000 túneles de VPN IPSEC simultáneos sin uso de licenciamiento o licenciado a perpetuidad	
CONSOLA	79	El sistema debe incluir consola de administración y monitoreo, incluyendo el licenciamiento de software necesario para las dos funcionalidades, como también el hardware dedicado para el funcionamiento de las mismas	

	80	La consola de administración y monitoreo debe residir en el mismo appliance de seguridad de red, lo cual implica que ésta posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función	
	81	La administración del sistema debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta	
	82	La administración en la consola debe permitir/hacer: - Creación y administración de políticas de firewall y control de aplicaciones - Creación y administración de políticas de IPS y Anti-Spyware - Creación y administración de políticas de filtro de URL - Monitoreo de logs - Herramientas de investigación de logs - Debugging - Captura de paquetes	
	83	Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing)	
	84	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas	
	85	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó y el horario del cambio	
	86	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la Universidad	
	87	Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Anti Spyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes	
	88	Debe ser posible acceder remotamente al sistema a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.	
	89	Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto): - Debe mostrar la situación del dispositivo y del clúster - Debe poder mostrar las principales aplicaciones - Debe poder mostrar las principales aplicaciones por riesgo - Debe poder mostrar los administradores autenticados en la plataforma de seguridad - Debe poder mostrar el número de sesiones simultáneas - Debe poder mostrar el estado de las interfaces - Debe poder mostrar el uso de CPU	

SERVICIOS	90	Soporte y cambio de partes 7x24 durante 3 años: El proveedor debe prestar el Soporte técnico de todos los componentes del sistema durante los 3 años contratados, con servicio en sitio, remoto, telefónico o a través correo electrónico, por personal certificado en la marca. Cuando el diagnóstico sobre los equipos o partes determine falla total o parcial, el contratista deberá realizar el proceso de RMA. El equipo entregado o partes por RMA debe contar con iguales o superiores características y capacidades tanto en hardware como en software que el equipo o parte reemplazada. La atención de soporte será en esquema 7x24xNBD: 7 días de la semana las 24 horas del día, con reemplazo de hardware al siguiente día hábil, el tiempo de atención no puede superar las 4 horas. Estos servicios hacen parte de la oferta incluyendo todos costos asociados para su cumplimiento (fletes, impuestos, transporte, importación, entre otros).	
	91	Instalación, configuración, migración, puesta en funcionamiento y optimización del sistema: hardware, software, licenciamiento y todas las funcionalidades adquiridas, incluyendo todos los cables, accesorios y demás elementos necesarios.	
	92	Licenciamiento en HA durante 3 años incluyendo todas las funcionalidades descritas en este documento	
	93	Transferencia de conocimiento certificada por el fabricante para dos personas del equipo técnico de la Red de Datos UDNET	

El contenido del presente ADENDO No.1, forma parte integral del Pliego de Condiciones y modifica en lo pertinente los numerales que le sean contrarios. Las demás condiciones continúan como están establecidas en el Pliego de Condiciones

Dado en Bogotá, D. C. a los nueve días del mes de octubre de dos mil diez y ocho (2018)

COMITÉ ASESOR DE CONTRATACIÓN DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS