

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.																																						
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral																																				
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software																																				
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO																																				
1.1.	Aspectos Generales	En la actualidad, la Entidad cuenta con una robusta plataforma de seguridad perimetral FORTINET, aprovisionada en alta disponibilidad e integrada por equipos, appliances, licenciamientos y suscripciones de funcionalidades específicas, que se relacionan a continuación: <table> <tr> <th>Item</th><th>Serial</th><th>Funcionalidad</th></tr> <tr> <td>1</td><td>FGT2KE3916900296</td><td>Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.</td></tr> <tr> <td>2</td><td>FGT2KE3916900051</td><td>Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.</td></tr> <tr> <td>3</td><td>FAZ1KFTA21000133</td><td>Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service). FortiAnalyzer Attack Surface Security Rating and Compliance 24x7.</td></tr> <tr> <td>4</td><td>FSA3KE3R16000019</td><td>Sandbox Threat Intelligence subscription. Includes Sandbox Engine, File Query, Industrial Security (OT) plus essential FortiGuard Services (Antivirus, IPS, Web Filtering) and FortiCare Premium 24x7.</td></tr> <tr> <td>5</td><td>FI1K5FTE24000015</td><td>FortiCare Premium 24x7</td></tr> <tr> <td>6</td><td>FV-2KET620000044</td><td>24x7 Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation).</td></tr> <tr> <td>7</td><td>FV-2KET621000014</td><td>24x7 Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation).</td></tr> <tr> <td>8</td><td>FGVM08TM22005233</td><td>Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.</td></tr> <tr> <td>9</td><td>FSMP000000001702</td><td>FortiSIEM Indicators of Compromise (IOC) Service, 24x7x4 FortiCare Premium 24X7 Threat Detection service, 24x7 Email, 24x7 Comprehensive Support, Firmware & General Updates.</td></tr> <tr> <td>10</td><td>FSRVMSTM21000135</td><td>FortiSOAR Enterprise Subscription plus FortiCare Premium 24X7 and FortiCare Best Practice Service - 2 User Logins included.</td></tr> <tr> <td>11</td><td>FDLPEP0000000655</td><td>FortiDLP Enterprise Premium Subscription for 1000 Endpoints. Includes cloud-native Endpoint DLP, Insider Risk, SaaS integration hosted on a premium PoP location with FortiCare Premium. Endpoints MOQ 500. Refer to documentation for Security PoP locations + Best Practice</td></tr> </table> Dicha plataforma es la estrategia institucional de ciberdefensa que protege el ámbito de red corporativo, evitando accesos no autorizados a sistemas y datos confidenciales, actuando como barrera entre Internet y la red interna segura.	Item	Serial	Funcionalidad	1	FGT2KE3916900296	Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.	2	FGT2KE3916900051	Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.	3	FAZ1KFTA21000133	Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service). FortiAnalyzer Attack Surface Security Rating and Compliance 24x7.	4	FSA3KE3R16000019	Sandbox Threat Intelligence subscription. Includes Sandbox Engine, File Query, Industrial Security (OT) plus essential FortiGuard Services (Antivirus, IPS, Web Filtering) and FortiCare Premium 24x7.	5	FI1K5FTE24000015	FortiCare Premium 24x7	6	FV-2KET620000044	24x7 Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation).	7	FV-2KET621000014	24x7 Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation).	8	FGVM08TM22005233	Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.	9	FSMP000000001702	FortiSIEM Indicators of Compromise (IOC) Service, 24x7x4 FortiCare Premium 24X7 Threat Detection service, 24x7 Email, 24x7 Comprehensive Support, Firmware & General Updates.	10	FSRVMSTM21000135	FortiSOAR Enterprise Subscription plus FortiCare Premium 24X7 and FortiCare Best Practice Service - 2 User Logins included.	11	FDLPEP0000000655	FortiDLP Enterprise Premium Subscription for 1000 Endpoints. Includes cloud-native Endpoint DLP, Insider Risk, SaaS integration hosted on a premium PoP location with FortiCare Premium. Endpoints MOQ 500. Refer to documentation for Security PoP locations + Best Practice
Item	Serial	Funcionalidad																																				
1	FGT2KE3916900296	Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.																																				
2	FGT2KE3916900051	Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.																																				
3	FAZ1KFTA21000133	Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service). FortiAnalyzer Attack Surface Security Rating and Compliance 24x7.																																				
4	FSA3KE3R16000019	Sandbox Threat Intelligence subscription. Includes Sandbox Engine, File Query, Industrial Security (OT) plus essential FortiGuard Services (Antivirus, IPS, Web Filtering) and FortiCare Premium 24x7.																																				
5	FI1K5FTE24000015	FortiCare Premium 24x7																																				
6	FV-2KET620000044	24x7 Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation).																																				
7	FV-2KET621000014	24x7 Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation).																																				
8	FGVM08TM22005233	Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 24x7.																																				
9	FSMP000000001702	FortiSIEM Indicators of Compromise (IOC) Service, 24x7x4 FortiCare Premium 24X7 Threat Detection service, 24x7 Email, 24x7 Comprehensive Support, Firmware & General Updates.																																				
10	FSRVMSTM21000135	FortiSOAR Enterprise Subscription plus FortiCare Premium 24X7 and FortiCare Best Practice Service - 2 User Logins included.																																				
11	FDLPEP0000000655	FortiDLP Enterprise Premium Subscription for 1000 Endpoints. Includes cloud-native Endpoint DLP, Insider Risk, SaaS integration hosted on a premium PoP location with FortiCare Premium. Endpoints MOQ 500. Refer to documentation for Security PoP locations + Best Practice																																				

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.2.	Funcionalidad implementada	La plataforma de seguridad perimetral Institucional detallada en el numeral 1.1. Aspectos Generales, ofrece características técnicas integradas e implementadas en la Entidad, a saber: ✓ FortiGate (Firewall) para el control de tráfico y prevención de amenazas ✓ FortiWEB (WAF) para la protección de aplicaciones web ✓ FortiAnalyzer para análisis de registros y visibilidad de amenazas ✓ FortiDDoS para la mitigación de ataques DDoS en la capa de red y aplicación ✓ FortiSandbox para la detección de malware avanzado y desconocido ✓ FortiSIEM (Security Information and Event Management) para la gestión centralizada de eventos de seguridad ✓ FortiSOAR (Security Orchestration, Automation, and Response) para automatizar y orquestar la respuesta a incidentes. ✓ FortiDLP para la prevención de pérdida de datos (Data Loss Prevention) mediante monitoreo y control de información sensible en reposo, en uso y en tránsito. Las funcionalidades anteriormente relacionadas, se encuentran configuradas en esquema de alta disponibilidad, estableciendo una defensa integral a la Entidad, que incluye: detección de amenazas avanzadas, gestión centralizada de la seguridad y automatización para simplificar su administración, manteniendo así la seguridad de la información institucional, la seguridad de dispositivos y usuarios y de aplicaciones organizacionales.

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.											
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral									
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software									
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO									
1.3.	Requerimiento	La Entidad requiere la renovación del Licenciamiento, Soporte y Actualización de su Plataforma de Seguridad Perimetral, manteniendo las Garantías sobre los equipos y funcionalidades descritas en numerales 1.1. y 1.2., de la suite FORTINET, como se describe a continuación: ✓ Renovación de Licenciamiento, Soporte y Actualización y Mantenimiento de sus plataformas de Seguridad FORTINET. ✓ Implementación y puesta en marcha de las renovaciones requeridas. ✓ Cobertura de la Garantía de Fabrica de doce (12) meses a partir del vencimiento del licenciamiento vigente, para todos los elementos componentes de la suite, implementados en la Entidad. ✓ Realizar la actualización, migración, optimización, configuración de todos los elementos pertenecientes a la solución implementada, según corresponda. ✓ Los equipos a renovar deben ser compatibles y permitir coexistencia con IPV6/IPV4. ✓ Generar un informe inicial del estado actual de los dispositivos y funcionalidades, distribución y arquitectura de la solución, estado de las configuraciones, mejoras a implementar de acuerdo a las mejores prácticas de fabricante y mejoras propuestas sobre la arquitectura. ✓ Validación del estado del Security Fabric y ejecución de ajustes necesarios sobre configuraciones, para garantizar la integración de toda la solución. Así mismo y en consideración al EOSL (Fin de Vida Útil del Servicio) y cambio generacional de los appliances y funcionalidades implementadas de SANDBOX (Ítem 4 del numeral 1.1. Aspectos Generales) y WAF (Ítems 6 y 7 del numeral 1.1. Aspectos Generales), es indispensable realizar su reemplazo por modernización tecnológica de dichos módulos, por los relacionados a continuación: <table> <tr> <th>Servicio</th><th>Funcionalidad</th><th>CANTIDAD</th></tr> <tr> <td>FSA-CLOUD-PAAS</td><td>Sandboxing PaaS Appliance with Advanced AI Sandbox subscription. Expands the number of Cloud VMs by 1, up to a maximum limit of 200 VMs. FortiCare Premium support included. Licenciado para 40 maquinas virtuales Windows y Microsoft Office</td><td>UNO (1)</td></tr> <tr> <td>FORTIWEB</td><td>FWB-2000F 24x7 FortiCare Premium, AV, FortiWeb Security Service, and IP Reputation</td><td>DOS (2)</td></tr> </table> ✓ Planeación, diseño, Instalación, configuración e implementación de las nuevas funcionalidades y appliances suministrados. ✓ Configuración en alta disponibilidad de los módulos FortiWEB suministrados ✓ Migración de configuraciones, reglas, políticas, etc., implementadas en las versiones anteriores de los appliances y funcionalidades a renovar. ✓ Integración de los nuevos appliances y funcionalidades con la infraestructura implementada actualmente. ✓ Realizar todas las pruebas necesarias para garantizar el correcto funcionamiento de los appliances y funcionalidades implementadas ✓ Puesta en producción los appliances y funcionalidades implementadas	Servicio	Funcionalidad	CANTIDAD	FSA-CLOUD-PAAS	Sandboxing PaaS Appliance with Advanced AI Sandbox subscription. Expands the number of Cloud VMs by 1, up to a maximum limit of 200 VMs. FortiCare Premium support included. Licenciado para 40 maquinas virtuales Windows y Microsoft Office	UNO (1)	FORTIWEB	FWB-2000F 24x7 FortiCare Premium, AV, FortiWeb Security Service, and IP Reputation	DOS (2)
Servicio	Funcionalidad	CANTIDAD									
FSA-CLOUD-PAAS	Sandboxing PaaS Appliance with Advanced AI Sandbox subscription. Expands the number of Cloud VMs by 1, up to a maximum limit of 200 VMs. FortiCare Premium support included. Licenciado para 40 maquinas virtuales Windows y Microsoft Office	UNO (1)									
FORTIWEB	FWB-2000F 24x7 FortiCare Premium, AV, FortiWeb Security Service, and IP Reputation	DOS (2)									

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.4.	Actualizaciones de Software	✓ Actualización de las versiones de sistema operativo y firmware de los equipos relacionados. ✓ Ofrecer un esquema de acceso a las actualizaciones de software, disponibles para todos los componentes de la solución, durante la vigencia de las garantías. ✓ Actualización del software durante la vigencia de las garantías, a la última versión disponible y estable, para optimizar funcionalidades de ciberseguridad, cada vez que se requiera. ✓ Realizar la actualización de firmas de ataques de intrusión en el sistema, durante la vigencia de las garantías. ✓ Realizar la instalación y configuración de las actualizaciones menores (updates) y mayores (upgrades), sobre todos los componentes de la solución implementada. ✓ Realizar las configuraciones necesarias para las integraciones de la solución implementada con Security Fabric de FORTINET.
1.5.	Instalacion de Hardware y software	Efectuar instalaciones y configuraciones requeridas de software y hardware de componentes de la plataforma y puesta en producción en óptimas condiciones de funcionamiento, abarcando las siguientes consideraciones: ✓ Planeación, Instalación, configuración e implementación de cada una de las plataformas y actividades necesarias con el fin de disminuir los tiempos de afectación en el servicio. ✓ Realizar las actividades planeadas de acuerdo con las mejores prácticas del fabricante garantizando la integración, disponibilidad y operación de la plataforma implementada y sus funcionalidades. ✓ Pruebas de funcionamiento. ✓ Estabilización de la plataforma. ✓ Suministro de todos los dispositivos, elementos y accesorios requeridos para llevar a cabo la implementación, sin costo adicional para la Entidad.

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.6.	Servicio de Soporte Avanzado de Fabrica	Servicios avanzados de soporte directamente por fabricante, con cubrimiento de todas las plataformas ofertadas y renovadas en el presente proceso, con las siguientes características: ✓ Asignación de profesionales idóneos (ingeniero principal y suplente), para la prestación del servicio, directamente de fábrica. ✓ Reporte de Análisis de causa raíz para eventos de alta severidad / prioridad. ✓ Recomendaciones para mejorar el desempeño de los componentes de la plataforma. ✓ Recomendaciones sobre las mejores prácticas e indicadores clave de rendimiento, para garantizar una óptima gestión de los dispositivos FORTINET. ✓ Notificaciones anticipadas acerca de novedades de seguridad y/o vulnerabilidades del PSIRT. ✓ Soporte Técnico Extendido de 12 meses a partir del vencimiento del licenciamiento vigente, que provee gestión de incidencias y correcciones de software más allá del fin del ciclo de vida estándar de la plataforma, asegurando la continuidad de la operación de esta y la resolución de errores a través del servicio FortiCare. Incluye la gestión de tickets técnicos para resolver problemas. ✓ Asistencia en horario No Hábil de mínimo dieciséis (16) horas, durante la vigencia del contrato y el periodo de garantía, para actividades críticas como: evaluación de actualización de software, contrato de servicio con visita en sitio, informe estándar de análisis de malware, configuración y prueba de comunicaciones, informe experto de malware, verificación de hardening de configuración, verificación de rendimiento de dispositivos, webinars personalizados de transferencia de conocimiento, talleres personalizados con laboratorio remoto, auditoría de ciclo de vida de productos, pruebas de readiness del cliente, día de servicios profesionales y paquetes de consultoría para acelerar la adopción de soluciones Fortinet.

FICHA TECNICA
INSTITUTO DE DESARROLLO URBANO – IDU
PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.7.	Servicio de Soporte	✓ El servicio de soporte debe incluir atención de requerimientos, incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil, en un esquema de atención 7x24x365x4, es decir, los siete días de la semana, las veinticuatro horas del día todos los días del año y con un máximo tiempo de respuesta de cuatro (4) horas en sitio, para los elementos integrales de la solución implementada: Componentes de Hardware, Software y/o Firmware, Configuración de Servicios, Software Especializado, etc. ✓ Revisar y afinar las plataformas FORTINET, en cada uno de los componentes descritos en los numerales 1.1. y 1.2., ejecutando ajustes y configuraciones requeridas para garantizar el óptimo desempeño de la solución implementada y su integralidad. ✓ Revisar la consistencia de los backups realizados. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma. ✓ Las actividades de soporte y afinamiento de la plataforma objeto de esta contratación, deberán ser realizadas por personal certificado por el fabricante. ✓ Configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante para todas las plataformas adquiridas, durante la vigencia de las garantías. ✓ Prestar soporte sobre los componentes de la plataforma FORTINET, de acuerdo a las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura. ✓ Realizar pruebas del funcionamiento en alta disponibilidad de la plataforma objeto de esta contratación y presentar un informe de la operatividad de las mismas.
1.8.	Centro de Soporte	Se debe garantizar acceso al centro de soporte durante el período de Soporte y Garantía, en la modalidad 7*24*365*4 (Siete días a la semana, Veinticuatro horas al día durante 365 días del año), con cuatro (4) horas máximo de respuesta. Tipo de solicitudes: El IDU podrá registrar en el centro de soporte, las fallas que presente cualquier elemento integral de la solución, requerimientos de soporte técnico y requerimientos de solución de problemas. Registro y seguimiento de solicitudes: El IDU recibirá del Contratista un número de registro de caso reportado y contará con un mecanismo para efectuar seguimiento y escalamiento de solicitudes en el centro de soporte.
1.9.	Niveles de Servicio	El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil. El contratista debe disponer para el IDU, durante el tiempo de Soporte y Garantía, el recurso físico, técnico y humano necesario, para cumplir con los niveles de servicio, en un modelo de 7*24*365*4, es decir, los siete días de la semana, las veinticuatro horas del día todos los días del año y con un máximo tiempo de respuesta de cuatro (4) horas en sitio y tiempo de solución de ocho (8) horas hábiles a partir de la solicitud de servicio, para atender los requerimientos de la Entidad, tras haberse solicitado por el Supervisor del Contrato, en lo relacionado con: componentes de Hardware, Software o Firmware; configuración de servicios y, en general, toda solicitud de la Entidad, relacionado con la solución implementada.

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.10.	Lugar de Servicio	Instituto de Desarrollo Urbano - IDU Sede Principal: CL 22 6 27 - Bogotá D.C. Datacenter NEBULA, Tocancipá – Cundinamarca Zona Franca de Tocancipá, Vereda Verganzo, Km 1.5 vía Briceño-Zipacquirá, Int 9, Tocancipá, Cundinamarca, Colombia.
1.11.	Entregables	El contratista deberá entregar documentación idónea que evidencie la renovación de garantía, licenciamiento y soporte, así como la modernización tecnológica, expresada en el numeral 1.3. Requerimiento: ✓ Hardware, software, suscripciones y servicios que cumplan con los requerimientos de la presente Ficha Técnica. ✓ Certificación que indique que el Licenciamiento de los componentes de la solución implementada, esté actualizado a la fecha requerida. ✓ La adquisición de servicios, soporte y garantía de la Solución implementada en la Entidad; incluido el licenciamiento involucrado, suministrado directamente por el fabricante. ✓ La ejecución de los requerimientos incluidos en el presente documento, desde la etapa de planeación y diseño hasta la entrega a satisfacción por parte del Supervisor del contrato. ✓ Manuales de instalación, configuración, administración, actualización, informe definitivo de implementación, diagramas técnicos y toda aquella documentación técnica que el fabricante libere, sobre la totalidad de los componentes entregados dentro de la Solución.

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.12.	Equipo Mínimo de Trabajo	El contratista debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado por: ✓ Gerente de Proyecto: Ingeniero de Sistemas, Telecomunicaciones, Electrónico o afines con especialización o certificación PMP, con mínimo dos (2) años de experiencia liderando proyectos de infraestructura tecnológica en la implementación de los servicios descritos en la presente Ficha Técnica. ✓ Especialistas en servicios: Ingenieros de Sistemas, Telecomunicaciones, Electrónicos o afines, con especialización, experiencia mínima tres (3) años en implementación y soporte en servicios y funcionalidades de la suite FORTINET, descritos en la presente Ficha Técnica, certificados por el Fabricante FORTINET, certificado NSE4, NSE5, NSE6 y NSE7 para la prestación del servicio. Deberá entregar dentro de los cinco (5) días hábiles siguientes a la firma del contrato las hojas de vida del personal solicitado en la ficha técnica, a fin de que estas sean avaladas por la supervisión del contrato. En caso de que las mismas no sean aprobadas, el contratista deberá presentar las nuevas hojas de vida en un término no mayor a dos (2) días hábiles, las cuales deben cumplir con los requisitos solicitado: Las hojas de vida del personal mínimo requerido, junto con los siguientes documentos: ● Certificados de experiencia. ● Copia de la cédula de ciudadanía. ● Certificación de formación académica con copia de la Tarjeta profesional de la rama de ingeniería de sistemas y afines. ● Certificaciones vigentes de antecedentes expedidos por la Personería Distrital, Procuraduría General de la Nación y Contraloría General de la República, con 30 días de expedido ● Certificado de REDAM vigente ● Certificado de afiliación a los sistemas de seguridad social y Cajas de Compensación Familiar de conformidad con la ley 100 de 1993 y sus decretos reglamentarios, con 30 días de expedido ● Certificado de Antecedentes Judiciales y registro de medidas correctivas expedidos por la Policía Nacional, con 30 días de expedido ● Tratándose de hombres menores de 50 años se deberá acreditar la definición de la situación militar.

FICHA TECNICA

INSTITUTO DE DESARROLLO URBANO – IDU

PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.13.	Mantenimiento Preventivo	El mantenimiento preventivo abarca una serie de actividades que aseguran el correcto funcionamiento y optimización de las plataformas de seguridad. Su efectividad se consolida de manera continua a través de revisiones periódicas, afinamientos, actualizaciones y monitoreo constante, incluyendo como mínimo dos (2) visitas al año: ✓ Revisar y afinar las plataformas implementadas, como mínimo cada seis (6) meses, previa coordinación con el Supervisor. ✓ Limpieza lógica de los equipos y elementos, que comprende configuraciones y ajustes de configuración. Verificación del aspecto físico. Revisión de indicadores visuales. Verificación del rendimiento de cada una de las plataformas. ✓ Análisis de logs de eventos y alarmas de las plataformas. ✓ Alertar el cambio de partes deterioradas de ser necesario. ✓ Afinamiento periódico de las plataformas que incluye: validación de reglas no activas o sobrepuestas, así como la activación de nuevas funcionalidades para garantizar un mejor desempeño y efectividad. ✓ Revisar la consistencia de los Backups realizados a la solución implementada. ✓ Hacer uso de herramientas de detección, diagnóstico y resolución de novedades para conservar la estabilidad y el óptimo rendimiento de la plataforma. ✓ Configuración y afinamiento de herramientas de reportes y almacenamiento de logs, reportes existentes y configuración de aquellos que la entidad requiera. ✓ Mantener actualizados los niveles de Firmware de los componentes implementados de acuerdo con las últimas versiones estables liberadas por el fabricante. ✓ Monitorear permanente de la plataforma tecnológica de seguridad involucrada, para lo cual el contratista debe referir su metodología y contar con herramientas de apoyo. ✓ Brindar acompañamiento técnico para la puesta en producción de servicios internos y externos publicados, con el fin de establecer los lineamientos técnicos de seguridad. Esta actividad genera un documento técnico con recomendaciones y un plan de trabajo. ✓ El horario de atención para el mantenimiento debe ser de 7x24x365, en sitio y sin costo adicional para la entidad, lo que permite una respuesta continua a cualquier necesidad. ✓ Al finalizar cada visita de mantenimiento, el contratista generará un informe técnico de servicio que incluye un resumen de las actividades realizadas, incidentes presentados, soluciones ejecutadas, evidencia de versionamiento de software, ajustes en la configuración y recomendaciones Para las actividades de Mantenimiento Preventivo se deberá realizar la planeación de cada una de ellas, validadas en conjunto con el Supervisor del contrato o a quien este delegue.

FICHA TECNICA
INSTITUTO DE DESARROLLO URBANO – IDU
PROCESO: ADQUIRIR LA RENOVACIÓN, ACTUALIZACIÓN, SOPORTE Y MANTENIMIENTO DEL LICENCIAMIENTO PARA LA PLATAFORMA DE SEGURIDAD PERIMETRAL DEL IDU.

ÍTEM 1: Adquirir la renovación, actualización, soporte y mantenimiento del licenciamiento para la plataforma de seguridad perimetral del IDU.		
Denominación Técnica:		Equipos y Servicios de Seguridad Perimetral
Códigos UNSPSC		43222500: Equipo de seguridad de red 43233200: Software de seguridad y protección 81111800: Servicios de sistemas y administración de componentes de sistemas 81112200 – Mantenimiento y Soporte de Software
ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
1.14.	Mantenimiento Correctivo	✓ En caso de determinarse que un incidente no puede ser resuelto dentro de las Ocho (8) horas hábiles siguientes, el contratista debe reemplazar el elemento averiado teniendo en cuenta los SLA impuestos por los licenciamientos de soporte de las diferentes soluciones. ✓ Al finalizar cada visita el contratista generará un informe de servicio que contiene el resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones implementadas y recomendaciones. De igual forma quedará constancia en acta o informe de servicio, si hubo actualización de software o ajustes en la configuración actual. ✓ El horario de atención para el mantenimiento debe ser de 7x24x365, en sitio y sin costo adicional para la Entidad. ✓ Planeación de cada una de las actividades, validadas en conjunto con la Supervisión del contrato. ✓ El servicio o repuestos requeridos para la ejecución de mantenimiento correctivo, no significará costo adicional alguno para la Entidad.
1.15.	Transferencia de Conocimiento	Realizar transferencia de conocimiento técnica, a profesionales designados por la STRT, intensidad horaria mínima de veinte (20) horas posteriores a la implementación, con respecto a configuración y administración de la Solución. Esta será realizada por personal certificado por Fábrica. La Transferencia de conocimiento deberá incluir evidencias de las sesiones, temarios, presentaciones y material de apoyo. Dichas sesiones serán grabadas y entregadas a la Entidad.
1.16.	Certificación Directa de Fabrica	El contratista debe evidenciar membresía de Partner Advanced o Expert, con especialización en Cloud Security, Operational Technology y Security Operations en Colombia. De igual manera, estar en capacidad técnica de instalar, configurar, mantener y dar soporte técnico a la solución implementada. En consecuencia, debe presentar certificación FORTINET que lo acredite conforme a las condiciones mencionadas anteriormente. Dicha certificación debe estar dirigida al Instituto de Desarrollo Urbano – IDU. La documentación deberá haber sido expedida máximo noventa (90) días calendario anteriores a la fecha de cierre del proceso de selección (si se prorroga dicha fecha, esta certificación valdrá con la fecha inicial de cierre).

Elaborado por	Aprobado por
Firma: 	Firma: 
MARCO FIDEL GUERRERO PARADA Profesional STRT	HÉCTOR PULIDO MORENO Subdirector Técnico de Recursos Tecnológicos (e)