



ANEXO No. 6
ANEXO TECNICO

Señores

IDIGER/FONDIGER

Proceso de Selección No. IDIGER-SA-SI-xxx-2026

Yo _____, en mi calidad de representante legal del oferente _____, me comprometo a cumplir con todas y cada una de las especificaciones técnicas establecidas en los estudios previos, el documento complementario de invitación pública, las adendas, respuestas a observaciones, los anexos del proceso y documento complementario minuta contractual, durante toda la ejecución del contrato que resulte del proceso de SELECCIÓN ABREVIADA SUBASTA INVERSA ELECTRONICA No. IDIGER SA-SI-xxx-2026, cuyo objeto es **“CONTRATAR LA RENOVACIÓN DEL LICENCIAMIENTO, GARANTÍA Y SOPORTE DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL, INCLUYENDO LOS COMPONENTES TECNOLÓGICOS Y SERVICIOS ASOCIADOS REQUERIDOS PARA SU ADECUADA OPERACIÓN, ASÍ COMO LA IMPLEMENTACIÓN DE UN ESQUEMA DE REDUNDANCIA QUE PERMITA GARANTIZAR LA DISPONIBILIDAD Y CONTINUIDAD DE LOS SERVICIOS CRÍTICOS INSTITUCIONALES, CONTRIBUYENDO AL FORTALECIMIENTO Y MEJORAMIENTO DEL DESEMPEÑO INSTITUCIONAL Y AL CONOCIMIENTO DEL RIESGO EN EL DISTRITO CAPITAL.”** así:

ESPECIFICACIONES TECNICAS

Se deberá ofertar en su totalidad, cumpliendo con las especificaciones técnicas descritas en el presente anexo, que hace parte del presente pliego y las escritas a continuación

A. RENOVACIÓN:

NOTA: GARANTIZAR RENOVACIÓN DE TODOS Y CADA UNO DE LOS ELEMENTOS ENUNCIADOS, TENIENDO EN CUENTA EL INICIO DEL CONTRATO Y SU VIGENCIA DE 06 MESES. TENER EN CUENTA QUE LOS ELEMENTOS DEBEN TENER LA MISMA FECHA DE EXPIRACIÓN.

ITEM	MODELO PRODUCTO	NUMERO SERIAL	SERVICIO A RENOVAR	CANT.
1	FortiGate 600E Renovación Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS; Video Filtering, Antispam, Service, and FortiCare Premium)	FG6H0ETB21906925 FG6H0ETB21907117	Incluye soporte 7x24	2
2	FortiGate FG-50G Renovación Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS; Video Filtering, Antispam, Service, and FortiCare Premium)	FG50GTK25021731	Incluye soporte 7x24	1
3	FortiAnalyzer 150G FortiAnalyzer 150G, FortiCare Premium Support, Indicators of Compromise	FAZ15GT221000504	Incluye soporte 7x24	1

	Service, Outbreak Detection Service, Security Rating Update			
4	FortiSwitch 524D FortiCare Premium Support	S524DNTV21000375 S524DNTV21000394	Incluye soporte 7x24	2
5	FortiClient EMS / FortiSASE HERRAMIENTA ZTNA BÁSICO	FCTEMS8824010582	Incluye soporte 7x24	1
	 FortiGate Cloud Sandbox FortiClient EMS Cloud  Licensed (Expiration Date: 2026/10/31)  Licensed (Expiration Date: 2026/11/14)			
6	FortiWeb Cloud Service (WAF)	FWBCLD0000002077	Incluye soporte 7x24	1
7	FortiAP 231F ACCESS POINTS INDOOR.	FP231FTF23031867 FP231FTF23031880 FP231FTF23031916 FP231FTF23032046 FP231FTF23032073 FP231FTF23032088	Incluye soporte 8x5	6
8	FortiAP 431-G ACCESS POINTS INDOOR.	FP431GTY25006324 FP431GTY24004797 FP431GTY25005969	Incluye soporte 8x5	3

Consideraciones a tener en cuenta

Para la renovación o desarrollo de cada uno de los ítems solicitados, se deberá garantizar que las características y/o funcionalidades establecidas se mantengan sin alteraciones al momento de su actualización, asegurando así la continuidad operativa y técnica del servicio.

A. RENOVACION. Se debe garantizar que las características y funcionalidades aca descritas sigan en funcionamiento.

DESCRIPCIÓN
RENOVACION DE FORTIGUARD OUTBREAK DETECTION SERVICE Y FORTIGUARD IOC (INDICATORS OF COMPROMISE) SERVICE PARA EL FORTIANALYZER – CORRESPONDIENTE AL ITEM 3
Proporcionar renovación de licencias del servicio FortiGuard Indicators of Compromise Service y FortiGuard Outbreak Detection Service para el equipo FAZ150G, de acuerdo a la duración del contrato
Soportar más de tres millones de sensores desplegados en todo el mundo, incluyendo dispositivos y honeypots, para brindar una alerta temprana sobre la actividad en el ciberespacio global.
Emplear técnicas de aprendizaje automático para capturar IOC - FortiGuard IOC and Outbreak Detection Service, tales como direcciones IP, dominios y URL incorrectos. La tecnología requerida deberá utilizar inteligencia artificial para rastrear Internet en busca de sitios maliciosos, asegurando así una protección proactiva contra amenazas emergentes.
HERRAMIENTA ZTNA BÁSICO - FORTICLIENT EMS – CORRESPONDIENTE AL ITEM 5
Licenciado para mínimo 350 dispositivos de acuerdo a la duración del contrato
Permitir integración con Directorio Activo LDAP On-Premise y Azure
Permitir uso de LDAP para la autenticación de usuarios y la generación de políticas de acceso
Permitir el acceso remoto de los usuarios a aplicaciones WEB y no WEB como SSH, RDP, Directorio activo, etc.
Evitar el uso de IP públicas de la entidad para exponer servicios de conexión remota.

Permitir validar la postura de seguridad de los usuarios que se conectan de forma remota y poder tomar decisiones basadas en reglas para permitir o denegar el acceso a los recursos de la red interna.
Generar un análisis de riesgo a nivel de aplicaciones, servicios nube y usuarios, según sus comportamientos en el uso de los servicios de navegación.
Generar acciones en las políticas como permitir, bloquear, alertar y generar alertas personalizadas para ser mostradas a nivel del agente o del navegador.
Permitir análisis de malware sin restricción del ancho de banda que genere el usuario dentro de la red corporativa o por fuera de ella.
Contar con plantillas pre-configuradas para la identificación de los diferentes activos de la red y así como la posibilidad de ofrecer auditorías de configuración, con el fin de comprender rápidamente dónde están las vulnerabilidades.
Contar con capacidades de Machine Learning y análisis profundo para detectar amenazas desconocidas, anomalías y comportamientos sospechosos.
Contar con agente ZTNA para acceso seguro que soporte MFA
Garantizar que los agentes ZTNA que se instalen en los dispositivos deben soportar Microsoft Windows, Mac OS, iOS, Android, entre otros.
Generación de reglas de etiquetado de seguridad
Permitir realizar gestión centralizada a través de una única consola de gestión.
Permitir la visualización de vulnerabilidades y su posible remediación
Permitir establecer conexiones de VPN SSL que soporten MFA
Permitir establecer conexiones VPN IPSEC que soporten MFA
Permitir el filtrado de video y web por medio de su plataforma de inteligencia de amenazas.
Tener funciones de CASB para proteger en tiempo real las aplicaciones SaaS de la entidad.
Permitir registro y centralización de informes.
Permitir reducir la superficie de ataque escaneando los puntos finales en busca de vulnerabilidades y compartiendo esa información para tomar las medidas adecuadas.
Permite realizar verificación de salud de equipos, telemetría, identidad y certificados de puntos finales
Permite realizar supervisión continua de Endpoint Posture Check
Permite realizar Inventario de software en los equipos instalados
RENOVACION DE SERVICIO DE WEB APPLICATION FIREWALL EN NUBE - FORTIWEB CLOUD SERVICE – CORRESPONDIENTE AL ITEM 6
Permitir la implementación rápida y sencilla de controles basados en políticas internas para la protección de los servidores web de la entidad.
Permitir restaurar automáticamente los portales web en caso de una modificación no autorizada.
Compatibilidad total con IPv6.
Permite identificar vulnerabilidades en al menos cinco dominios de aplicaciones web de la entidad sin la necesidad de licencias adicionales.
Garantizar el tener actualizado el servicio conforme a las actualizaciones lanzadas por fabricante durante la vigencia el contrato.
Garantizar su actualización continua con las últimas definiciones de seguridad durante todo el periodo contratado (Cross-Site Scripting (XSS), SQL Injection, Remote File Inclusion, Local File Inclusion, OS Commands, Troyanos y virus, Exploits, Fugas de Información, entre otros).
Integrar una base de datos de firmas de amenazas y ataques conocidos, y debe contar con la capacidad de proteger contra ataques de día cero.
Incorporar funcionalidades de aprendizaje automático (Machine Learning).
Garantizar su integración de manera nativa con la actual solución de gestión de logs y el firewall Fortigate implementado en la entidad.
Garantizar protección de las siguientes amenazas, entre otras: Adobe Flash Binary (AMF) protocol Attack, Botnet, Browser Exploit Against SSL /TLS, Clickjacking, Cookie Tampering, Cross Site request forgery, Cross site Scripting, DoS, HTTP Header Overflow, Local File Inclusion, Malicious Robots, Man in the Middle, Remote File Inclusion, Server information leakage, SQL Injection, Malformed XML)

Contar con un módulo anti-defacement que permita monitorear las aplicaciones web, alertar sobre cualquier cambio no autorizado y restaurarlas automáticamente en caso de modificaciones no autorizadas.
Contar con la capacidad de monitorear la integridad de los archivos a través de protocolos como FTP, SSH o SMB, sin la necesidad de instalar agentes adicionales.
Permitir el realizar análisis exhaustivos de vulnerabilidades en las aplicaciones web protegidas, permitiendo la identificación de todas las vulnerabilidades presentes en los aplicativos web de la entidad de manera ilimitada, sin necesidad de licencias adicionales.
Incluir un módulo de prevención contra ataques de denegación de servicio (DoS) en protocolos HTTP y HTTPS, que proteja eficazmente las aplicaciones web frente a este tipo de amenazas. Este módulo deberá ofrecer, como mínimo, las siguientes capacidades: alertar sobre ataques detectados, denegar solicitudes maliciosas y bloquear las fuentes de ataque por un periodo de tiempo definido.
Contar con la funcionalidad de auto aprendizaje que le permita crear una línea base del comportamiento de la aplicación para la creación de diferentes políticas de protección.
Disponer de un módulo de escaneo AntiMalware para examinar los archivos que se carguen o suban a las aplicaciones web, con la capacidad de detectar y bloquear malware.
Contar con protección de ataques basados en la localización geográfica del atacante (protección basada en geolocalización).
Contar con un módulo para la prevención de fugas de información, que permita establecer reglas personalizadas basadas en patrones. Este módulo deberá estar completamente funcional desde la solución, sin necesidad de licencias adicionales o integraciones con plataformas de terceros.
Contar con un módulo para la prevención de ataques de fuerza bruta contra los portales de autenticación de la entidad, el cual permita bloquear al atacante por un periodo de tiempo parametrizable por la entidad.
Garantizar la capacidad de inspeccionar en profundidad los protocolos HTTP y HTTPS, haciendo una revisión como mínimo de los siguientes parámetros: Hostname, Versión, Método del Request, Tamaño del Request, Tamaño del Contenido, Tamaño del Body, Tamaño del Header, Numero de Cookies en el request, Numero de Parámetros en la URL.
Permitir la gestión de la plataforma se llevará a cabo a través de HTTPS y contará con una API basada en el método RESTful sobre HTTPS.
Disponer de dashboards que presenten, como mínimo, información en tiempo real del tráfico, historial de ataques, sesiones por política e información del sistema.
Soportar ambientes multitenant, lo que permitirá dividir la administración y aplicar políticas de WAF de manera independiente para entornos de producción y desarrollo, o según los criterios definidos por la entidad.
Garantizar un desempeño mínimo en: ● Soportar mínimo 5 dominios ● Desempeño promedio de 20 Mbps ● Vigencia durante todo el contrato ● Capacidad de aumentar los sitios WEB soportados Capacidad de aumentar el desempeño.
FORTIAP 231F – CORRESPONDIENTE AL ITEM 7. Renovación de licenciamiento para los equipos AP, los cuales tienen las siguientes características:
Numero de radios: 3 + 1 BLE Antenas Internas / Externas Antenas omnidireccionales de banda dual integradas. ● Radio 1: ○ Capabilities Frequency band: 2.4GHz ○ Channel width: 20/40MHz ○ Modulation: BPSK, QPSK, 64/256/1024 QAM ○ MIMO Chains: 2x2 Service ● Radio 2: ○ Capabilities Frequency band: 5.0GHz ○ Channel width: 20/40/80MHz ○ Modulation: BPSK, QPSK, 64/256/1024 QAM

○ MIMO Chains: 2x2 Service ● Radio 3: ○ Capabilities Frequency bands: 2.4GHz and 5.0GHz
MIMO Chains: 1x1 Frequency Scanning
Puerto Gigabit Ethernet compatible con 802.3af Power over Ethernet (PoE) (pines de entrada de alimentación RJ-45); Admite inyector de alimentación a través de Ethernet 802.3af / 802.3at; Alimentación PoE IEEE 802.3af.
SSIDs (Service Set Identifier) simultáneas: Mínimo 6 por radio.
Número de dispositivos conectados: Cada AP debe soportar mínimo 512 equipos conectados.
Interfaces 2x 10/100/1000 Base-T RJ45, 1x Type 2.0 USB, 1x RS232 RJ45 Serial Port
Antenna Type and Peak Gain: Omni Directional antenna
Dual band: 4.5dBi for 2.4Ghz and 5.5dBi for 5GHz
BLE antenna 4.0dBi at 2.4GHz band
Incluir al menos soporte para Autenticación por AP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAPMSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, AP-FAST
Los equipos deben ser administrados desde una controladora física (de la misma marca de los AP) y Directamente desde los AP por interfaz web.
Compatible con IEEE Estándares 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bz
PoE Mode: 802.3at PoE default. 1 port powered by 802.3at - full system functionality. USB support. 1 port is connected to 802.3af - no USB support.
Frequency Bands (GHz): 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
User/Device Authentication: WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blocklist and allowlist
Maximum Tx Power (Conducted): Radio 1: 2.4GHz: 23 dBm / 200 mW (2 chains combined) * Radio 2: 5GHz: 22 dBm / 158 mW (2 chains combined)
FORTIAP 431G – CORRESPONDIENTE AL ITEM 8. Renovación de licenciamiento para los equipos AP, los cuales tienen las siguientes características:
Número de radios: 3 + 1 BLE Antenas Internas / Externas Antenas de banda dual integradas. ● Radio 1: ○ Capabilities Frequency band: 2.4GHz ○ Channel width: 20/40MHz ○ Modulation: BPSK, QPSK, 64/256/1024 QAM ○ MIMO Chains: 4x4 Service ● Radio 2: ○ Capabilities Frequency band: 5.0GHz ○ Channel width: 20/40/80/80 + 80MHz ○ Modulation: BPSK, QPSK, 64/256/1024 QAM ○ MIMO Chains: 4x4 Service ● Radio 3: ○ Capabilities Frequency band: 6.0GHz ○ Channel width: 20/40/80/160 MHz ○ Modulation: BPSK, QPSK, 64/256/1024 QAM ○ MIMO Chains: 4x4 Service and 2x2 scanning
Puerto Gigabit Ethernet compatible con 802.3af Power over Ethernet (PoE) (pines de entrada de alimentación RJ-45); Admite inyector de alimentación a través de Ethernet 1 802.3bt PoE default or x2 802.3at PoE (Dual PoE current sharing)
SSIDs (Service Set Identifier) simultáneas: Mínimo 6 por radio.
Número de dispositivos conectados: Cada AP debe soportar mínimo 512 equipos conectados.
Interfaces x2 100/1000/2500/5000 Base-T RJ45, 1 Type 3.0 USB, 1 RS-232 RJ45 Serial Port

Antenna Type and Peak Gain: PIFA antenna.
Dual band: 4.0 dBi for 2.4GHz, 5.6 dBi for 5 GHz Tr-band: 4.0 dBi for 2.4GHz, 6.0 dBi for 5 GHz & 5.7dBi for 6GHz band
BLE antenna: 5.1dBi for 2.4Ghz Band
Incluir al menos soporte para Autenticación por EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Los equipos deben ser administrados desde una controladora física (de la misma marca de los AP) y Directamente desde los AP por interfaz web.
Compatible con IEEE Estándares 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.1X, 802.3ad, 802.3at, 802.3bt, 802.3az
PoE Mode: Dual PoE sharing with 2x 802.3at PoE (GPI-130) or Single 802.3at PoE (GPI-130) with No USB and reduced Transmit power
Frequency Bands (GHz): 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850, 5.925–6.425, 6.425–6.525, 6.525–7, 5.925–6.875, 6.875–7.125
User/Device Authentication: WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blocklist and allowlist
Maximum Tx Power (Conducted): Radio 1: 2.4GHz: 27 dBm / 501 mW (4 chains combined) Radio 2: 5GHz: 26 dBm / 400 mW (4 chains combined) Radio 3: 6GHz: 24 dBm 251 mW (4 chains combined @ 160MHz BW)

- B. ADQUISICIÓN NUEVAS SOLUCIONES:** Para el cumplimiento de los siguientes ítems, el contratista deberá suministrar todos los elementos necesarios para la instalación y configuración de los equipos, incluyendo, pero sin limitarse a: cable UTP Categoría 6A, patch panel, jacks, tuberías, cajas y demás componentes que se requieran. La ejecución deberá ajustarse a la distribución y lineamientos establecidos por el supervisor del contrato.

	ESQUEMA DE CONECTIVIDAD REDUNDANTE TIPO FIBRA – 06 MESES	CUMPLE
1	Suministrar un canal redundante que actúe como respaldo de los canales principales existentes, tanto para el acceso a Internet como para la comunicación entre las sedes de la Entidad (Fontibón y Normandía).	
	Velocidad mínima garantizada: 500 Mbps de conexión efectiva hacia Internet desde Sede Normandía 200 Mbps de conexión efectiva hacia Internet desde Sede Fontibón	
	Los canales deberán implementarse con una tecnología de alta eficiencia, velocidad y disponibilidad, que asegure la continuidad operativa de los servicios críticos.	
	El esquema de conectividad deberá permitir la conmutación automática entre el canal principal y el canal redundante en caso de falla, sin intervención manual y sin afectar la continuidad del servicio.	
	En caso de requerirse un traslado físico de la conexión o los equipos asociados, el contratista deberá asumir la reubicación y puesta en funcionamiento sin costos adicionales para la Entidad.	
	Garantizar medición del tiempo que tarda un paquete IP ir y volver entre el router de la entidad y el punto de distribución durante la vigencia del servicio. La medición se debe hacer por canal	
	El contratista deberá incluir todos los costos relacionados con adecuaciones, instalación, configuración, pruebas y demás actividades necesarias para garantizar la disponibilidad y funcionamiento del canal redundante.	
	El servicio debe incluir monitoreo proactivo de la disponibilidad y del tráfico del canal, con capacidad de generar alertas y reportes que faciliten la gestión operativa y la identificación de incidentes.	



ACUERDOS DE NIVELES DE SERVICIO: El contratista debe garantizar de manera ininterrumpida la atención telefónica para prestar el servicio de soporte, el cual debe incluir la atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil.

Así mismo, deberá contar con un Software de Mesa de Servicio, donde se puedan registrar casos o incidentes de forma web, correo o teléfono, y así realizar el seguimiento correspondiente.

El contratista debe poner a disposición de IDIGER, durante el desarrollo del contrato y por el tiempo de cobertura de las Garantías exigidas, el recurso físico y humano necesario, para cumplir con los niveles de servicio y compromisos para la efectiva prestación del servicio, en un modelo de 7X24, es decir, los siete días de la semana, las veinticuatro horas del día todos los días del año, para atender los requerimientos de la Entidad, como se describe a continuación:

SERVICIO DE SOPORTE TÉCNICO:

SOPORTE TELEFÓNICO: Ilimitado. El contratista deberá atender las llamadas de emergencia para la solución de problemas sencillos que no ameriten visita en modalidad 7 X 24, durante toda la vigencia del contrato.

SOPORTE REMOTO: Ilimitado. El contratista deberá disponer de un correo electrónico y acceso vía internet en modalidad 7 X 24, durante toda la vigencia del contrato. El oferente debe contar con una mesa de servicios y/o mesa de ayuda que esté certificada bajo la norma internacional vigente del Sistema de Gestión de Servicios en su versión más reciente, aplicable a los procesos de seguridad y soporte de servicios. Esta certificación asegurará la calidad, gestión y mejora continua de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida directamente al oferente por el ente certificador autorizado.

SOPORTE PRESENCIAL: Ilimitado. El contratista deberá brindar soporte en las instalaciones del IDIGER, cuando el problema sea de alta complejidad y no haya podido resolverse a través de otros canales y que demande la intervención del personal competente que señale la entidad, proporcionado por el Proveedor en sitio o, cuando sea solicitado por el IDIGER en modalidad 7 X 24, durante la vigencia del contrato.

NIVELES DE SERVICIO				
MATRIZ PRIORIDADES	ALTO IMPACTO	MEDIO IMPACTO	BAJO IMPACTO	NULO IMPACTO
ALTA URGENCIA	Prioridad 1	Prioridad 2		
MEDIA URGENCIA	Prioridad 2	Prioridad 2	Prioridad 3	Prioridad 4
BAJA URGENCIA	Prioridad 3	Prioridad 3	Prioridad 4	Prioridad 4
NULA URGENCIA			Prioridad 4	Prioridad 5
TIEMPO DE ATENCIÓN				
PRIORIDAD	TIEMPO DE RESPUESTA INICIAL			
1	2 HORAS			
2	6 HORAS			
3	2 DÍAS HÁBILES SIGUIENTES			
4	4 DÍAS HÁBILES SIGUIENTES			
5	5 DÍAS HÁBILES SIGUIENTES			



FIRMA DEL REPRESENTANTE LEGAL O APODERADO
NOMBRE DEL PROPONENTE:
NOMBRE DEL REPRESENTANTE LEGAL:
DIRECCIÓN:
CORREO ELECTRÓNICO:
TELÉFONO: