ANEXO 1. FICHA TÉCNICA SOLUCIÓN DE SEGURIDAD PERIMETRAL
SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO
DIRECCIÓN DE GESTIÓN CORPORATIVA - SUBDIRECCIÓN DE INFORMÁTICA Y SISTEMAS

Objeto: Adquirir una solución integral de seguridad perimetral compuesta por hardware y licenciamiento de software, incluidos los servicios conexos de instalación, configuración y soporte especializado

CARACTERÍSTICAS GENERALES	
Denominación técnica del bien	Equipo de seguridad de red
Unidad de medida	Unidad
Descripción General	Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico de red.
Cantidad	**Un (1) Firewall de Próxima Generación (NGFW) con funciones SD-WAN** **Debe incluir:** **-Licenciamiento*** **-Solución de WAF** **-Protección de red, protección web, protección de amenazas, protección de correo electrónico, protección inalámbrica, protección de servidor web,sandbox** **-Servicio de Soporte Técnico y Garantias Directo del Fabricante en modalidad 7x24** ***Para todas las licencias: tres (3) años de Subscripción.**
CÓDIGOS UNSPSC	43222501, 43222600, 43233203, 43233204

REQUISITOS TÉCNICOS MÍNIMOS OBLIGATORIOS

Ite	Firewall	Tipo de Requisito
0	Indicar Marca y Modelo del hardware que hace parte de la solucion ofertada	Técnico Obligatorio
0.1	Indicar licencia del software de la solución ofertada	Técnico Obligatorio
0.2	El proponente debe adjuntar obligatoriamente con su oferta la ficha técnica oficial de la solución NGFW ofertada, emitida por el fabricante, donde se evidencie al menos la marca, modelo, características, funcionalidades y capacidades que permitan validar el cumplimiento de los requerimientos. La información debe ser consistente y verificable con la oferta presentada. La ausencia, incompletitud o inconsistencia de este documento será causal de rechazo de la propuesta por incumplimiento de requisitos técnicos.	Habilitante
1	Rendimiento mínimo de Firewall de 100 Gbps con funciones básicas de firewall habilitadas, conforme a especificaciones oficiales del fabricante	Técnico Obligatorio
2	Rendimiento mínimo del sistema de prevención de intrusiones (IPS) de 20 Gbps con firmas activas y bajo condiciones estándar de laboratorio del fabricante.	Técnico Obligatorio
3	Rendimiento mínimo en túneles IPSec VPN de 20 Gbps, medido con cifrado AES-256 y tráfico bidireccional, conforme a ficha técnica oficial del fabricante.	Técnico Obligatorio
4	La solucion debe soporte un mínimo 10'000.000 conexiones concurrentes.	Técnico Obligatorio
5	La solucion debe soporte minimo 1.000 usuarios concurrentes VPN Ipsec.	Técnico Obligatorio
6	Soporte de minimo 1.000 usuarios concurrentes para SSL debidamente licenciados	Técnico Obligatorio
7	Conexiones mínimas por segundo: 468.000	Técnico Obligatorio
8	El equipo deberá contar con interfaces de red suficientes para soportar la arquitectura actual de la entidad, incluyendo como mínimo: • 8 puertos minimo 10GbE ópticos SFP • 4 puertos minimo 10/25 10GbE SFP+ • 8 puertos RJ45 1GbE • 4 puertos minimo 10/25GbE (nativos o mediante expansión)	Técnico Obligatorio
9	El equipo deberá contar con recursos de hardware (memoria, almacenamiento y procesamiento) suficientes para soportar los niveles de tráfico y funcionalidades de seguridad requeridas por la Entidad, incluyendo como mínimo 64 GB de memoria RAM y dos (2) discos SSD SATA-III de mínimo 480 GB en configuración RAID por hardware o equivalente. Adicionalmente, la solución podrá complementarse con plataformas de almacenamiento y análisis centralizado de logs del mismo fabricante, con el fin de optimizar la gestión, retención y análisis de eventos de seguridad.	Técnico Obligatorio
10	La solución deberá acreditar su posicionamiento como solución empresarial de seguridad perimetral mediante evidencias verificables tales como: documentación oficial del fabricante, certificaciones técnicas internacionales, y/o evaluaciones independientes de terceros. El oferente deberá adjuntar soportes y referencias documentales	Habilitante
11	El lanzamiento oficial al mercado de la solución ofertada no debe ser mayor a dos (2) años, lo cual debe ser acreditado por el fabricante.	Habilitante
12	La solución debe contar con mínimo de seis (6) transceptores de mínimo 10 Gigabit Ethernet (GbE) SFP+	Técnico Obligatorio
13	La solución deberá permitir expansión de interfaces de red mediante módulos o tarjetas adicionales que soporten: * Puertos Multi-Gigabit de Cobre: Cuatro (4) puertos que soporten velocidades de 10/25 Gbps utilizando interfaces estándar (SFP+/SFP28) o cobre (RJ45). * Puertos Gigabit de Alta Densidad: Doce (12) puertos que soporten el estándar 1 Gigabit Ethernet (GE) sobre cableado de cobre (RJ45).	Técnico Obligatorio
14	La solución debe soportar mínimo 700 usuarios	Técnico Obligatorio
15	La solución debe contar con capacidad de fuente redundante para que ante cualquier fallo inminente se mantenga la disponibilidad física del equipo.	Técnico Obligatorio
	Software y Licenciamiento	
16	Tanto el hardware como el software que hacen parte de la solución deben ser totalmente compatibles con el protocolo IPV6 y debe configurarse con la dirección IPV6 suministrada por la entidad.	Habilitante
17	La solución deberá contar con el licenciamiento necesario para habilitar, como mínimo, capacidades de seguridad NGFW y servicios avanzados de protección (web/URL filtering, IPS, antimalware, antbot, sandbox/zero-day). Para funciones especializadas de WAF, protección de correo y protección inalámbrica, se aceptará que se provean integradas en el NGFW o mediante componentes del mismo fabricante o interoperables, plenamente compatibles y soportados, sin afectar la operación centralizada y la trazabilidad. Debe incluir Soporte Técnico Directo del Fabricante 7x24.	Técnico Obligatorio
18	La solución debe incluir como mínimo las siguientes capacidades: Firewall (NGFW), control y filtrado web/URL, IPS, antimalware, antibot y sandbox/zero-day. Para Web Application Firewall (WAF), se aceptará su provisión integrada en el NGFW o mediante un componente dedicado del fabricante o interoperable, plenamente compatible y con administración centralizada.	Técnico Obligatorio
19	Toda comunicación de administración en la solución debe ser cifrada y autenticada mediante certificados PKI.	Técnico Obligatorio
20	La solución debe soportar los siguientes métodos de autenticacion para el control de acceso y la funcionalidad de VPN: Tokens, TACACS, Radius y certificados digitales.	Técnico Obligatorio
21	La solución debe soportar una base de datos interna para autenticar y autorizar usuarios sin necesidad de alguna integración.	Técnico Obligatorio
22	La solución debe permitir integración con LDAP o un sistema que haga sus veces.	Técnico Obligatorio
23	La solución debe soportar funcionalidad de DHCP como servidor.	Técnico Obligatorio
24	La solución debe soportar la funcionalidad de proxy HTTP y HTTPS tanto e forma explicita como transparente.	Técnico Obligatorio
25	La solución debe inspeccionar trafico IPv6 en las funcionalidades de detección de intrusos, identificación de aplicaciones, identificación de usuarios, "firewall", filtrado de URLs, AntiVirus, AnitBot, SandBoxing y Prevención de fuga de datos.	Técnico Obligatorio
26	La solución debe soportar túneles "NAT 6-to-4" o "NAT 4-to-6".	Técnico Obligatorio
27	La solución deberá integrarse con el Directorio Activo de la entidad para la gestión de usuarios y políticas basadas en identidad. Para ello, se permitirá el uso de métodos estándar como LDAP, RADIUS, SAML 2.0 u OIDC. Asimismo, se aceptará el uso de agentes o conectores propietarios del fabricante destinados a garantizar la transparencia en la autenticación del usuario, la validación de postura y la aplicación de políticas de seguridad sin intervención del usuario final.	Técnico Obligatorio
	Dirección General	
28	Interfaz de administración gráfica avanzada con capacidades de agrupación y visualización de reglas a gran escala.	Técnico Obligatorio
29	Compatibilidad con autenticación de dos factores (contraseña de un solo uso) para acceso de administrador, portal de usuario, IPSec y SSL VPN	Técnico Obligatorio
30	Herramientas avanzadas de resolución de problemas en GUI (por ejemplo, captura de paquetes)	Técnico Obligatorio
31	Interfaz de línea de comandos (CLI) completa accesible desde la GUI	Técnico Obligatorio
32	Administración basada en roles	Técnico Obligatorio
33	Notificación automatizada de actualización de firmware con un sencillo proceso de actualización automatizado y funciones de reversión	Técnico Obligatorio
34	Definiciones de objetos de sistema reutilizables para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores	Técnico Obligatorio
35	Portal de usuario de autoservicio	Técnico Obligatorio
36	Seguimiento de cambios de configuración	Técnico Obligatorio
37	Control de acceso a dispositivos flexible para servicios por zonas	Técnico Obligatorio
38	Opciones de notificación de captura de correo electrónico o SNMP	Técnico Obligatorio
39	Compatibilidad con SNMPv3 y uno que haga sus veces para el monitoreo, y Netflow	Técnico Obligatorio
40	Soporte de administración centralizada de múltiples dispositivos mediante una consola unificada, ya sea en modalidad local (on-premises) o en modalidad cloud, según arquitectura definida por la Entidad.	Técnico Obligatorio
41	Notificaciones automáticas por correo electrónico para cualquier evento importante	Técnico Obligatorio
42	Configuraciones de copia de seguridad y restauración: localmente, a través de FTP o correo electrónico; bajo demanda, diariamente, semanalmente o mensualmente	Técnico Obligatorio
43	API para la integración de 3rd party	Técnico Obligatorio
44	Cambio de nombre de la interfaz	Técnico Obligatorio

Uso Público

45	La solución deberá permitir el acceso remoto seguro y auditado para soporte técnico del fabricante o del contratista autorizado, bajo control y aprobación de la Entidad, utilizando mecanismos cifrados (TLS), con trazabilidad de sesiones (logs) y opción de habilitación temporal (just-in-time).	Técnico Obligatorio
46	Gestión de licencias basada en la nube a través del Portal de licencias	Técnico Obligatorio
47	Soporte técnico de Syslog	Técnico Obligatorio
48	Monitoreo de flujo en tiempo real	Técnico Obligatorio
49	Indicadores visuales de estado del sistema y servicios.	Técnico Obligatorio
50	Información instantánea de un vistazo	Técnico Obligatorio
51	Indicadores visuales de estado del sistema y servicios.	Tecnico
52	SNMP con una MIB personalizada y soporte para túneles VPN IPSec	Técnico Obligatorio
53	Compatibilidad con zonas WAN virtuales en puertas de enlace personalizadas para el uso de un solo brazo después de la implementación	Técnico Obligatorio
54	Recomendable la solucion debe conecrarse con una amplia gama de plataformas de virtualización y también se puede implementar como un dispositivo de software.	Tecnico
55	Recomendable la solucion debe conecrarse con sistemas de Nutanix AHV y Nutanix Flow	Tecnico
56	Recomendable la solucion debe conecrarse con sistemas de algoritmo hash de contraseña más fuerte (requiere un cambio de contraseña)	Tecnico
	Gestión del Firewall	
57	La gestión y la generación de informes para varios firewalls proporcionan gestión de políticas de grupo y una única consola para los productos de seguridad	Técnico Obligatorio
58	La administración de directivas de grupo permite que los objetos, la configuración y las directivas se modifiquen una vez y se sincronicen automáticamente con todos los firewalls del grupo	Técnico Obligatorio
59	El Administrador de tareas proporciona una pista de auditoría histórica completa y supervisión del estado de los cambios en las directivas de grupo	Técnico Obligatorio
60	La solucion debe tener como minimo la capacidad de almacenar múltiples versiones de respaldo de configuración de los componentes	Técnico Obligatorio
61	Actualizaciones de firmware que ofrecen actualizaciones de firmware con un solo clic para aplicar a cualquier dispositivo	Técnico Obligatorio
62	La solución de seguridad perimetral deberá soportar implementación sin contacto (Zero Touch Deployment – ZTD), que permita realizar la configuración inicial del equipo de forma automática, sin intervención manual directa en sitio. La funcionalidad de implementación sin contacto deberá estar disponible sin requerir desarrollos adicionales ni soluciones de terceros no certificadas por el fabricante.	Técnico Obligatorio
63	Programación de actualizaciones de firmware	Técnico Obligatorio
64	Guardar, programar y exportar informes	Técnico Obligatorio
65	Informes de múltiples firewalls entre grupos de firewall	Técnico Obligatorio
	Firewall, Redes y Enrutamiento	
66	Firewall de inspección profunda de paquetes con estado	Técnico Obligatorio
67	Arquitectura de procesamiento de paquetes que proporciona niveles extremos de visibilidad, protección y rendimiento a través del procesamiento de paquetes basado en secuencias	Técnico Obligatorio
68	Inspección TLS con alto rendimiento, soporte para TLS 1.3 sin degradación, puerto independientes, políticas de nivel empresarial, visibilidad única del panel y solución de problemas de compatibilidad	Técnico Obligatorio
69	La solución deberá contar con un motor de inspección profunda de paquetes (DPI) de alto rendimiento que permita la aplicación simultánea de múltiples perfiles de seguridad sin degradación significativa del rendimiento	Técnico Obligatorio
70	Inspección en un solo motor de alto rendimiento	Técnico Obligatorio
71	Acelera el tráfico SaaS, SD-WAN y en la nube, como VoIP, video y otras aplicaciones confiables.	Tecnico
72	la solucion como minio debe peritir tener soporte para listas de exclusión preconfiguradas y personalizables	Tecnico
73	Directivas basadas en usuarios, grupos, tiempo o redes	Técnico Obligatorio
74	Políticas de tiempo de acceso por usuario/grupo	Técnico Obligatorio
75	Aplicar directivas en todas las zonas, redes o por tipo de servicio	Técnico Obligatorio
76	Firewall basado en zonas	Técnico Obligatorio
77	La solución ofertada debe operar bajo una arquitectura de "Firewall Basado en Zonas" (Zone-Based Firewall) permitiendo crear, nombrar y personalizar ilimitadas zonas de seguridad (incluyendo LAN, WAN, DMZ, WiFi, etc.) permitiendo la segmentación lógica de la red y la aplicación de políticas de seguridad entre segmentos sin depender de configuraciones predeterminadas del fabricante.	Técnico Obligatorio
78	Soporte completo de VLAN	Técnico Obligatorio
79	Aislamiento de zonas y VLAN y compatibilidad con políticas basadas en zonas.	Técnico Obligatorio
80	La solución deberá permitir la integración con plataformas de Endpoint (EDR/XDR) mediante APIs documentadas o protocolos estándar para aplicar políticas dinámicas basadas en postura de seguridad	Tecnico
81	Zonas personalizadas en LAN o DMZ	Técnico Obligatorio
82	Políticas NAT personalizables con enmascaramiento de IP y soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un conveniente asistente de reglas NAT para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics	Técnico Obligatorio
83	Protección contra inundaciones: Bloqueo DoS, DDoS y portscan	Tecnico
84	Bloqueo de países por geo-IP	Tecnico
85	Enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF) con soporte completo de VLAN 802.1Q	Técnico Obligatorio
86	Compatibilidad con proxy ascendente	Técnico Obligatorio
87	Enrutamiento de multidifusión independiente del protocolo con snooping IGMP	Técnico Obligatorio
88	Puente con soporte STP y reenvío de difusión ARP	Técnico Obligatorio
89	Compatibilidad y etiquetado de VLAN DHCP	Técnico Obligatorio
90	Compatibilidad con puentes VLAN	Técnico Obligatorio
91	Equilibrio de enlaces SD-WAN: múltiples conexiones a Internet, comprobación de estado de vínculos automáticos, conmutación por error automática, equilibrio automático y ponderado y reglas granulares de múltiples rutas	Técnico Obligatorio
92	Compatibilidad con WAN inalámbrica (n/a en implementaciones virtuales)	Tecnico
93	Agregación de enlaces de interfaz 802.3ad	Técnico Obligatorio
94	Configuración completa de DNS, DHCP y NTP	Técnico Obligatorio
95	DNS dinámico (DDNS)	Técnico Obligatorio
96	Certificación de aprobación del programa IPv6 Ready Logo	Tecnico
97	Compatibilidad con túneles IPv6, incluida la implementación rápida de 6 pulgadas 4, 6to4, 4 pulgadas6 e IPv6 (6ª) a través de IPSec	Técnico Obligatorio
	SD-WAN	
98	Soporte para múltiples opciones de enlace WAN, incluyendo VDSL, DSL, cable y celular 3G / 4G / LTE con monitoreo esencial, balanceo, conmutación por error	Técnico Obligatorio
99	Selección y enrutamiento de rutas de aplicaciones, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP	Técnico Obligatorio
100	El NGFW debe ser capaz de consumir información de identidad y estado de salud de la plataforma de Endpoint y utilizar esta información para optimizar la selección de rutas (SD-WAN) y priorizar el tráfico (QoS) de aplicaciones críticas, o degradar la prioridad de tráfico de hosts comprometidos.	Tecnico
101	Enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas	Técnico Obligatorio
102	Implementación asequible, flexible y sin contacto o de bajo contacto	Técnico Obligatorio
103	Soporte VPN robusto que incluye IPSec y SSL VPN	Técnico Obligatorio
104	Orquestación VPN centralizada	Técnico Obligatorio
105	La solución de seguridad perimetral deberá permitir la interconexión segura, centralizada y administrada de sedes remotas, mediante mecanismos basados en estándares abiertos, que permitan la extensión de la red institucional sin requerir tecnologías propietarias específicas de un fabricante.	Técnico Obligatorio
	Conformación de tráfico base y cuotas	
106	Gestión de Calidad de Servicio (QoS) y Control de Tráfico: La solución debe permitir la creación de políticas de gestión de ancho de banda (Traffic Shaping) con las siguientes capacidades mínimas: Priorización y Garantía: Capacidad de definir ancho de banda garantizado, límites máximos (burst) y prioridades de tráfico (clases). Granularidad: Las políticas deben poder aplicarse de forma individual o combinada basándose en: Dirección IP/Segmento de red, Identidad de Usuario/Grupo (Directorio Activo) y Aplicación específica Visibilidad: La consola de gestión debe permitir la visualización en tiempo real del consumo de ancho de banda por cada una de estas categorías para facilitar la resolución de incidentes de saturación.	Técnico Obligatorio
107	Establecer cuotas de tráfico basadas en el usuario en la carga/descarga o tráfico total y cíclico o no cíclico	Técnico Obligatorio
108	Optimización de VoIP en tiempo real	Tecnico
109	Marcado DSCP	Técnico Obligatorio
110	Conexión inalámbrica segura	Tecnico
111	La solución deberá permitir el aprovisionamiento simplificado de puntos de acceso inalámbricos (AP), ya sea mediante descubrimiento automático o a través de una plataforma de gestión centralizada.	Tecnico
112	Soporte para estándares inalámbricos IEEE 802.11ac Wave 2 o superior, conforme a las capacidades del fabricante.	Tecnico
113	Supervisión y gestión centralizada de puntos de acceso y clientes inalámbricos mediante plataforma de control unificada, ya sea integrada en el firewall o mediante controlador dedicado interoperable.	Tecnico
114	Capacidad de asignar AP a LAN, VLAN o zonas de seguridad independientes, con opciones de aislamiento de cliente.	Tecnico
115	Soporte para múltiples SSID por radio, incluyendo opciones de visibilidad configurable.	Tecnico
116	Soporte para estándares actuales de seguridad inalámbrica, incluyendo WPA2-Personal/Enterprise y WPA3 según disponibilidad del fabricante.	Tecnico
117	Configuración flexible de ancho de canal conforme a estándares IEEE aplicables.	Tecnico
118	Compatibilidad con autenticación IEEE 802.1X mediante integración con servidores RADIUS primarios y secundarios.	Tecnico
119	Soporte para IEEE 802.11r (Fast Transition) o tecnologías equivalentes de transición rápida.	Tecnico
120	Optimización automática de selección de canales para reducción de interferencias y mejora de desempeño	Tecnico
121	Las funcionalidades inalámbricas serán aplicables únicamente en caso de que la entidad decida implementar puntos de acceso compatibles con la solución ofertada.	Tecnico

122	Compatibilidad con el inicio de sesión HTTPS	Tecnico
	ZTNA	
123	Zero Trust Network Access (ZTNA) para ofrecer una forma segura y sencilla para que los usuarios se conecten de forma segura a aplicaciones y datos importantes.	Tecnico
124	Conecte de forma segura a los usuarios a las aplicaciones	Tecnico
125	Soporte de aplicaciones en la nube y locales	Tecnico
126	Acceso remoto desde cualquier lugar	Tecnico
127	El firewall debe intercambiar información de estado (salud, cumplimiento, nivel de amenaza) de los dispositivos finales (endpoints) con la plataforma de gestión de seguridad centralizada (XDR/EDR) en tiempo real, utilizando APIs documentadas o protocolos abiertos.	Tecnico
	Autenticación	
128	La solución NGFW deberá integrarse con servicios empresariales de directorio y autenticación, tales como Active Directory, LDAP, SAML y RADIUS, así como con soluciones de control de acceso a la red (NAC), permitiendo la correlación de direcciones IP con usuarios autenticados para la aplicación de políticas basadas en identidad. La solución deberá soportar mecanismos de integración como SSO (clientless u otros), así como capacidades de correlación y visibilidad de usuarios en tiempo real, sin requerir la instalación obligatoria de agentes propietarios y permitiendo diferentes mecanismos de integración de acuerdo con la arquitectura de la solución.	Técnico Obligatorio
129	Autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS+	Técnico Obligatorio
130	Agentes de autenticación de servidor para SSO e integración con AD/LDAP mediante Kerberos/NTLM/SAML/OIDC o equivalente	Técnico Obligatorio
131	Inicio de sesión único: Active Directory, eDirectory, RADIUS Accounting	Técnico Obligatorio
132	La solución deberá permitir la autenticación multifactor (MFA) y la configuración de tiempos de expiración de sesión para accesos administrativos y de usuarios, con capacidad de aplicar políticas diferenciadas según el tipo de acceso, perfil de usuario y nivel de riesgo, sin limitar su aplicación a un escenario específico.	Técnico Obligatorio
133	Agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64	Tecnico
134	Autenticación SSO (Kerberos/NTLM/SAML/OIDC o equivalente) según arquitectura del oferente.	Técnico Obligatorio
135	Portal cautivo del navegador	Técnico Obligatorio
136	Certificados de autenticación para iOS y Android	Técnico Obligatorio
137	Servicios de autenticación para IPSec, SSL, L2TP, PPTP	Técnico Obligatorio
138	Autenticación basada en API	Técnico Obligatorio
139	recomandable la compatibilidad con la creación de usuarios con formato UPN para la autenticación RADIUS	Tecnico
	Portal de autoservicio del usuario	
140	Descargue Authentication Client	Tecnico
141	Descargar el cliente de acceso remoto SSL (Windows) y los archivos de configuración (otro sistema operativo)	Tecnico
142	La solución deberá permitir la gestión de acceso de usuarios a la red o a los servicios protegidos, mediante mecanismos de autenticación o integración con servicios de directorio o tecnologías equivalentes, según las capacidades de la solución ofertada.	Tecnico
143	Cambiar nombre de usuario y contraseña	Tecnico
144	Ver el uso personal de Internet	Tecnico
145	La solución deberá permitir la integración con las plataformas de correo electrónico existentes en la Entidad, garantizando la visibilidad, monitoreo y control del tráfico asociado, así como la generación de registros, aplicación de políticas de seguridad y análisis del tráfico relacionado con los servicios de correo electrónico, conforme a las capacidades del equipo ofertado, sin requerir la inclusión obligatoria de una solución independiente de seguridad de correo electrónico dentro del alcance del NGFW, salvo que el oferente la contemple como parte de su propuesta.	Tecnico
	Opciones básicas de VPN	
146	Túneles VPN IPSec y SSL	Técnico Obligatorio
147	Orquestación basada en asistente	Técnico Obligatorio
148	VPN de sitio a sitio: La solución deberá soportar túneles SSL e IPsec utilizando estándares de cifrado robustos, incluyendo AES-GCM (128/256 bits). Se requiere soporte para Perfect Forward Secrecy (PFS), certificados X.509, claves pre-compartidas (PSK) y algoritmos de integridad de la familia SHA-2 (hasta HMAC-SHA-512). Asimismo, deberá permitir el intercambio de llaves mediante grupos Diffie-Hellman de curva elíptica (ECDH) para asegurar una alta resistencia criptográfica. Queda excluido el uso del algoritmo 3DES por considerarse obsoleto.	Técnico Obligatorio
149	Túnel VPN de sitio a sitio de dispositivo remoto con VPN IPSec/SSL/SD-WAN equivalente.	Técnico Obligatorio
150	L2TP y PPTP	Técnico Obligatorio
151	VPN basada en rutas	Técnico Obligatorio
152	Acceso remoto: SSL, IPsec, soporte de cliente VPN para iPhone / iPad / Cisco / Andriod	Técnico Obligatorio
153	Soporte IKEv2	Técnico Obligatorio
154	Cliente SSL para Windows y descarga de configuración a través del portal de usuario	Técnico Obligatorio
155	La solución deberá soportar la aplicación de TLS 1.3 para túneles VPN SSL. Adicionalmente, deberá permitir el uso de DTLS (Datagram Transport Layer Security) o mecanismos que garanticen un comportamiento equivalente, para túneles de sitio a sitio y de acceso remoto, con el fin de optimizar el rendimiento de aplicaciones sensibles a la latencia (VoIP, Video, RDP) y evitar la degradación por retransmisiones de paquetes.	Técnico Obligatorio
	Cliente VPN	
156	Compatibilidad con IPSec y SSL	Técnico Obligatorio
157	Fácil aprovisionamiento e implementación	Técnico Obligatorio
158	Soporte mínimo 1.000 usuarios concurrentes (VPN IPSec/SSL) debidamente licenciados con autenticación mediante AD/LDAP y MFA.	Técnico Obligatorio
159	Autenticación: clave precompartida (PSK), PKI (X.509), token y XAUTH	Técnico Obligatorio
160	El acceso remoto (VPN SSL/IPsec) debe requerir y validar el estado de seguridad (postura) del dispositivo del usuario (e.g., antivirus activo, parches al día, ausencia de malware) antes de otorgar o restringir el acceso a la red interna.	Técnico Obligatorio
161	Túnel dividido inteligente para un enrutamiento óptimo del tráfico	Tecnico
162	Compatibilidad con NAT-traversal	Técnico Obligatorio
163	Client-monitor para obtener una visión general gráfica del estado de la conexión	Tecnico
164	Compatibilidad con Mac y Windows	Técnico Obligatorio
165	Aprovisionamiento de políticas IPSec de acceso remoto	Técnico Obligatorio
	Prevención de intrusiones (IPS)	
166	Motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se pueden aplicar sobre la base de reglas de firewall para obtener el máximo rendimiento y protección	Técnico Obligatorio
167	Protección contra amenazas de día cero	Técnico Obligatorio
168	Defensas perimetrales	Técnico Obligatorio
169	Miles de firmas	Técnico Obligatorio
170	Selección granular de categorías	Técnico Obligatorio
171	Compatibilidad con firmas IPS personalizadas	Técnico Obligatorio
172	Los filtros inteligentes de directiva IPS habilitan directivas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones	Técnico Obligatorio
	Dispositivos de Extensión Seguro	
173	Dispositivo perimetral SD-WAN	Técnico Obligatorio
174	Acceso y gestión centralizada de todos los dispositivos	Tecnico
175	Sin configuración: se conecta automáticamente a través de un servicio de aprovisionamiento basado en la nube	Tecnico
176	Cifrado de nivel empresarial	Tecnico
177	Opciones de túnel dividido	Tecnico
178	Túnel cifrado seguro mediante certificados digitales X.509 y cifrado AES de 256 bits	Tecnico
179	Ethernet virtual para una transferencia confiable de todo el tráfico entre ubicaciones	Tecnico
180	Administración de direcciones IP con configuración de servidor DHCP y DNS definida de forma centralizada	Tecnico
181	Desautorizar de forma remota el dispositivo remoto después de un período selecto de inactividad	Tecnico
182	Compresión del tráfico del túnel	Tecnico
183	Opciones de configuración del puerto VLAN	Tecnico
184	Opciones inalámbricas integradas	Tecnico
	Clientles VPN	
185	La solución deberá proveer un mecanismo de acceso remoto seguro que soporte la validación de la postura de seguridad del dispositivo (ej. verificación de antivirus, parches de SO, certificados de equipo). Se aceptarán soluciones basadas en agentes VPN seguros o arquitecturas ZTNA que garanticen que solo dispositivos autorizados y seguros puedan acceder a los recursos internos (RDP, SSH, aplicaciones web, etc.).	Técnico Obligatorio
	Protección y Control Web	
186	Proxy totalmente transparente para antimalware y filtrado web	Técnico Obligatorio
187	Protección avanzada contra amenazas mejorada	Técnico Obligatorio
188	La solución deberá contar con servicio de inteligencia de amenazas actualizado en tiempo real, respaldado por infraestructura global de análisis de amenazas.	Técnico Obligatorio
189	Políticas de tiempo de cuota de navegación por usuario/grupo	Técnico Obligatorio

190	Políticas de tiempo de acceso por usuario/grupo	Técnico Obligatorio
191	Escaneo de malware: bloquee todas las formas de virus, malware web, troyanos y spyware en HTTP / S, FTP y correo electrónico basado en la web	Técnico Obligatorio
192	La solución deberá contar con capacidades de protección y análisis de tráfico web, permitiendo la identificación, inspección y control de contenido web, incluyendo elementos activos como scripts (por ejemplo, JavaScript), con el fin de prevenir riesgos asociados a la navegación y el uso de aplicaciones web.	Tecnico
193	Consultas en tiempo real a servicios de inteligencia de amenazas en la nube para validación de reputación de archivos, URLs y dominios	Tecnico
194	La solución ofertada debe contar con protección contra Malware (Anti-Malware) de alta eficacia, con actualizaciones en tiempo real y capacidad de análisis de archivos por inteligencia de amenazas y/o sandboxing avanzado.	Técnico Obligatorio
195	Escaneo en tiempo real o en modo por lotes	Técnico Obligatorio
196	Protección Pharming	Técnico Obligatorio
197	Análisis HTTP y HTTPS por usuario o directiva de red con reglas y excepciones personalizables	Técnico Obligatorio
198	Detección y enforcment de túneles de protocolo SSL	Técnico Obligatorio
199	Validación de certificados	Técnico Obligatorio
200	Almacenamiento en caché de contenido web de alto rendimiento	Tecnico
201	Almacenamiento en caché forzado para actualizaciones	Tecnico
202	Filtrado de tipos de archivo por tipo mime, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)	Técnico Obligatorio
203	Aplicación de políticas específicas sobre plataformas de video bajo criterios definidos por la entidad.	Tecnico
204	Aplicación de SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario/grupo)	Tecnico
205	Monitoreo y aplicación de palabras clave web para registrar, informar o bloquear palabras clave coincidentes con contenido web listas con la opción de subir listas de aduanas	Técnico Obligatorio
206	Bloquear aplicaciones potencialmente no deseadas (PUAs)	Técnico Obligatorio
207	El NGFW deberá permitir el bloqueo y control de transferencia de archivos por tipo y firma real (no solo por extensión), en tráfico web, correo electrónico y aplicaciones, mediante inspección profunda de paquetes (DPI) y sandbox.	Técnico Obligatorio
208	Opción de anulación de directivas web para que los profesores o el personal permitan temporalmente el acceso a sitios o categorías bloqueados que son totalmente personalizables y administrables por usuarios seleccionados	Tecnico
209	Filtrado web automático de sitios identificados por Internet Watch Foundation (IWF) que contienen abuso sexual infantil	Tecnico
	Visibilidad de aplicaciones en la nube	
210	Desglose para obtener detalles sobre los usuarios, el tráfico y los datos	Tecnico
211	Acceso con un solo clic a las políticas de configuración del tráfico	Tecnico
212	Filtrar el uso de aplicaciones en la nube por categoría o volumen	Tecnico
213	Informe detallado de uso de aplicaciones en la nube personalizable para obtener informes históricos completos	Tecnico
	Protección y Control de Aplicaciones	
214	La solución deberá permitir intercambio de información de amenazas con soluciones de Endpoint mediante mecanismos estandarizados o APIs documentadas.	Tecnico
215	Control de aplicaciones basado en firmas con patrones para miles de aplicaciones	Técnico Obligatorio
216	Visibilidad y control de aplicaciones en la nube para descubrirShadow IT	Tecnico
217	Filtros inteligentes de control de aplicaciones que habilitan directivas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones	Tecnico
218	Detección y control de micro aplicaciones	Tecnico
219	Control de aplicaciones basado en categorías, características (por ejemplo, ancho de banda y consumo de productividad), tecnología (por ejemplo, P2P), y nivel de riesgo	Técnico Obligatorio
220	Aplicación de directivas de control de aplicaciones por usuario o regla de red	Técnico Obligatorio
	Conformación de tráfico web y de aplicaciones	
221	Opciones personalizadas de conformación de tráfico (QoS) por categoría web o aplicación para limitar o garantizar la carga/descarga o la prioridad total del tráfico y la tasa de bits de forma individual o compartida	Tecnico
	Análisis de Sandbox Dinámico	
222	Integración completa en el panel de control de su solución de seguridad	Tecnico
223	Inspecciona ejecutables y documentos que contienen contenido ejecutable (incluidos .exe, .com y .dll, .doc, .docx, docm y .rtf y PDF) y archivos que contienen cualquiera de los tipos de archivo enumerados anteriormente (incluidos ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)	Tecnico
224	Análisis agresivo del comportamiento, la red y la memoria	Tecnico
225	Detecta el comportamiento de evasión de sandbox	Tecnico
226	La tecnología de aprendizaje automático con aprendizaje profundo analiza todos los archivos ejecutables eliminados	Tecnico
227	Selección opcional del centro de datos y opciones flexibles de directivas de usuario y grupo sobre el tipo de archivo, las exclusiones y las acciones en el análisis	Tecnico
228	Soporta enlaces de descarga de una sola vez	Tecnico
229	Análisis de archivos estáticos de aprendizaje profundo	Tecnico
230	Múltiples modelos de aprendizaje automático	Tecnico
231	Análisis dinámico de sandboxing	Tecnico
232	Archivos sospechosos sometidos a análisis de inteligencia de amenazas en paralelo con el análisis completo de sandbox	Tecnico
	Orquestación SD-WAN	
233	Orquestación SD-WAN y VPN con creación fácil y automatizada basada en asistente de túneles VPN de sitio a sitio entre ubicaciones de red utilizando una arquitectura óptima (hub-and-spoke, full mesh o alguna combinación).	Tecnico
234	Soporta túneles IPSec, SSL o dispositivo remoto VPN. Se integra a la perfección con las características SD-WAN para la priorización de aplicaciones, la optimización del enrutamiento y el aprovechamiento de múltiples enlaces WAN para la resiliencia y el rendimiento.	Tecnico
	Protección de firewall de aplicaciones web	
235	Proxy inverso	Técnico Obligatorio
236	Motor de endurecimiento de URL con vinculación profunda y prevención de recorrido de directorios	Técnico Obligatorio
237	Motor de endurecimiento de formularios	Técnico Obligatorio
238	Protección de inyección SQL	Técnico Obligatorio
239	Protección de secuencias de comandos entre sitios	Técnico Obligatorio
240	La solución deberá contar con motor(es) antimalware de alta eficacia con capacidad de análisis en tiempo real y actualización continua de firmas.	Tecnico
241	Descarga de cifrado HTTPS (TLS/SSL)	Técnico Obligatorio
242	Firma de cookies con firmas digitales	Técnico Obligatorio
243	Enrutamiento basado en rutas	Técnico Obligatorio
244	Compatibilidad con el protocolo outlook en cualquier lugar	Técnico Obligatorio
245	Autenticación inversa (descarga) para la autenticación básica y basada en formularios para el acceso al servidor	Técnico Obligatorio
246	Abstracción de servidor virtual y servidor físico	Tecnico
247	El equilibrador de carga integrado distribuye a los visitantes en varios servidores	Técnico Obligatorio
248	Omita las comprobaciones individuales de forma granular según sea necesario	Técnico Obligatorio
249	Hacer coincidir las solicitudes de las redes de origen o las direcciones URL de destino especificadas	Técnico Obligatorio
250	El WAF debe permitir la creación de políticas avanzadas mediante la combinación de múltiples condiciones con operadores lógicos (AND, OR, NOT), incluyendo la capacidad de correlacionar diferentes atributos de la solicitud en una misma regla, con motor de inspección flexible y personalizable.	Tecnico
251	El WAF debe contar con capacidades avanzadas de personalización que permitan la creación de excepciones, perfiles y ajustes granulares por aplicación, URL, parámetros y firmas, sin afectar otras políticas, garantizando la operación en entornos con implementaciones no estándar.	Tecnico
252	Opciones para cambiar los parámetros de rendimiento de Web Application Firewall	Tecnico
253	Opción de límite de tamaño de escaneo	Técnico Obligatorio
254	Permitir/Bloquear rangos de IP	Técnico Obligatorio
255	Compatibilidad con comodines para rutas de acceso y dominios de servidor	Técnico Obligatorio
256	Anexar automáticamente un prefijo/sufijo para la autenticación	Técnico Obligatorio
	Informes de Firewall	
257	Informes predefinidos con opciones de personalización flexibles	Técnico Obligatorio
258	Informes para firewalls (hardware, software, virtual y nube)	Técnico Obligatorio
259	La interfaz de usuario intuitiva proporciona una representación gráfica de los datos	Técnico Obligatorio
260	El panel de informes proporciona una vista rápida de los eventos de las últimas 24 horas	Técnico Obligatorio
261	Identifique fácilmente las actividades de red, las tendencias y los posibles ataques	Técnico Obligatorio
262	Copia de seguridad sencilla de los registros con recuperación rápida para las necesidades de auditoría	Técnico Obligatorio
263	Implementación simplificada sin necesidad de conocimientos técnicos	Técnico Obligatorio
264	Cree informes personalizados con potentes herramientas de visualización	Técnico Obligatorio
265	30 días de almacenamiento de datos en la nube o local para informes históricos de firewall con funciones avanzadas para guardar, programar y exportar informes personalizados.	Técnico Obligatorio
266	Búsqueda y visualización de Syslog	Técnico Obligatorio
267	Almacenamiento de datos Syslog	Técnico Obligatorio
268	Almacenamiento en la nube de 7 días para informes de Firewall	Tecnico
269	Informe sobre la nueva aplicación en la nube (CASB)	Tecnico
270	Sin requerir licenciamiento adicional distinto al ofertado.	Tecnico
271	Informes agregados de múltiples firewalls	Tecnico
272	Guardar plantillas de informe personalizadas	Técnico Obligatorio
273	Informes programados	Técnico Obligatorio
274	Exportar informes en formato PDF, CFV o HTML	Técnico Obligatorio

275	La solución deberá contar con una capacidad de almacenamiento de reportes analíticos y gráficos en línea (Hot Storage) por un periodo mínimo de treinta (30) días, permitiendo la visibilidad inmediata de eventos de seguridad. Asimismo, el sistema deberá garantizar la retención de registros de eventos (logs) de auditoría por un periodo de un (1) año, permitiendo para ello la exportación automática de dichos registros a un repositorio externo de la entidad mediante mecanismos seguros y estándar como Syslog y/o SFTP. El uso de otros mecanismos podrá ser considerado de manera opcional, siempre que no comprometa la seguridad de la información.	Técnico Obligatorio
276	Búsqueda y visualización de Syslog	Técnico Obligatorio
277	Almacenamiento de datos Syslog	Técnico Obligatorio
278	Informes bajo demanda	Técnico Obligatorio
279	Informe a través de varios firewalls	Técnico Obligatorio
280	Guarde, exporte y programe sus informes Sin cargo adicional	Técnico Obligatorio
281	Generación de alertas por correo electrónico	Técnico Obligatorio
282	El NGFW debe proporcionar herramientas robustas de registro (log) y reportes	Técnico Obligatorio
283	El NGFW debe proporcionar herramientas como Paneles Operacionales y de Seguridad (Dashboards): Vistas en tiempo real del estado de la red, rendimiento, principales amenazas, y uso de aplicaciones.	Técnico Obligatorio
284	El NGFW debe proporcionar herramientas como Informes Personalizables y Predefinidos: Generación de reportes detallados sobre el uso de la red (aplicaciones, usuarios, tráfico web), eventos de seguridad (IPS, Anti-Malware, Zero-Day Sandbox), y el estado de la conexión (VPN).	Técnico Obligatorio
285	El NGFW debe Ofrecer reportes predefinidos o plantillas personalizables diseñadas para asistir en la auditoría y el cumplimiento de marcos normativos globales y regionales (como PCI-DSS, HIPAA, SOC 2, ISO 27001, etc.).	Técnico Obligatorio
286	El NGFW debe tener la capacidad de exportar todos los registros de tráfico y eventos de seguridad en formatos estándar, como Syslog, para la integración transparente con soluciones SIEM de terceros (ej. Splunk, Microsoft Sentinel). Adicionalmente, se valorará el soporte de formatos como CEF y/o LEEF.	Técnico Obligatorio
287	Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS	Técnico Obligatorio
288	Anonimización de informes	Tecnico
289	Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles	Técnico Obligatorio
290	La solución deberá permitir la exportación de informes en formatos como HTML, PDF y Excel (XLS) o formatos equivalentes (como CSV), que garanticen la adecuada visualización, análisis y manipulación de la información.	Técnico Obligatorio
291	Marcadores de informe	Tecnico
292	Personalización de la retención de registros por categoría	Tecnico
293	Soporte de Syslog	Técnico Obligatorio
294	Visor de registros en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de filtro y búsqueda, ID de regla con hipervínculos y personalización de la vista de datos	Técnico Obligatorio
	Garantía de hardware y RMA con intercambio avanzado	
295	Servicio de Soporte Técnico Directo del Fabricante en modalidad 7x24", que incluya acceso ilimitado (sin restricciones de horas) al Centro de Asistencia Técnica global para la apertura de casos, con derecho a escalamiento a ingenieros expertos de máximo nivel para la resolución de incidentes críticos.	Habilitante
296	Actualizaciones y parches de seguridad durante un periodo de tres (3) años	Habilitante
297	Actualizaciones y mejoras de características de software durante un periodo de tres (3) años	Habilitante
	Paquete de Protección Avanzada	
298	Licencia base: Redes, Inalámbrico, Arquitectura , VPN de acceso remoto, VPN de sitio a sitio, informes.	Técnico Obligatorio
299	La solución debe incluir un conjunto completo de protección de red que abarque: a. Inspección de Contenido Cifrado: Motor de inspección SSL/TLS (DPI) de alto rendimiento. b. Prevención de Intrusiones: Sistema de Prevención de Intrusiones (IPS/IDS). c. Protección Avanzada contra Amenazas (ATP): Módulos para detectar y mitigar malware, ransomware y zero-days. d. Conectividad Segura: Funcionalidad completa de Red Privada Virtual (VPN) de sitio a sitio (IPsec) y de acceso remoto (SSL/IPsec). e. Interoperabilidad: Mecanismos de intercambio de telemetría de amenazas bidireccional entre el firewall y las soluciones de Endpoint (EDR/XDR) a través de APIs documentadas. f. Visibilidad: Capacidades robustas de generación de logs e informes de tráfico y amenazas	Técnico Obligatorio
300	Protección web: motor TLS y DPI, seguridad y control web, control de aplicaciones, informes	Técnico Obligatorio
301	Soporte mejorado: soporte 24/7, actualizaciones de funciones, garantía de hardware de reemplazo avanzada por término	Habilitante
302	Email Protection: Antispam, AV, DLP, cifrado en caja	Técnico Obligatorio
303	Web Application Firewall (WAF)	Técnico Obligatorio
304	Protección de día cero: aprendizaje automático y análisis de archivos de espacio aislado, informes	Técnico Obligatorio
305	Orquestación central: orquestación de VPN SD-WAN, informes avanzados de firewall central (30 días)	Técnico Obligatorio
306	Soporte Técnico Especializado: El contratista deberá garantizar un Servicio de Soporte Técnico Directo del Fabricante en modalidad 24x7, que incluya acceso ilimitado (sin restricciones de horas) al Centro de Asistencia Técnica (TAC) global para la apertura de casos, con derecho a escalamiento a ingenieros expertos de Nivel 3 para la resolución de incidentes críticos y garantía de hardware (HW) para los componentes o complementos de la solución.	Habilitante
307	Gestión de firewall de grupo, gestión de copias de seguridad, programación de actualizaciones de firmware	Técnico Obligatorio
308	Almacenamiento en la nube conforme al esquema de licenciamiento ofertado.	Tecnico
309	ZTNA: administración Zero Trust Network Access	Habilitante
	Soporte y Transferencia de Conocimiento	
310	El soporte debe ser en sitio, remoto, vía e-mail, web, telefónico, fax, o a través de chat; y debe incluir servicios profesionales de configuración, Actualizaciones y aplicación de suplementos y parches liberados por el fabricante. Tiempo de respuesta: 4 horas	Habilitante
311	El oferente deberá garantizar que los equipos ofertados contarán, durante los tres (3) años de la vigencia contractual, con soporte oficial del fabricante, el cual deberá incluir como mínimo: i) Atención técnica 24/7 ii) Acceso a actualizaciones y mantenimiento de software y firmware iii) Soporte remoto especializado iv) Reemplazo de hardware bajo esquema de garantía del fabricante, con tiempos de atención y reposición definidos (NBD o superior)	Habilitante
312	Garantizar que el dispositivo pueda recibir cobertura de actualizaciones de software durante minimo tres (3) años contados a partir de la fecha del acta de recibido a satisfacción por parte de la SDDE	Habilitante
313	Acuerdo de servicio por tres (3) años de servicios profesionales soporte y mantenimiento	Habilitante
314	El Oferente deberá ofrecer soporte 7x24 por el periodo de la vigencia de suscripción de las licencias.	Habilitante
315	El Oferente deberá ofrecer una transferencia de conocimiento de mínimo 12h en las soluciones implementadas. Máximo 5 funcionarios.	Habilitante
	Otras Generalidades	
316	El contratista en conjunto con el fabricante, el contratista deberá elaborar el cronograma con las actividades que se desarrollarán para la implementación de la solución del presente proceso, la cual debe ser presentada al supervisor de contrato para su aprobación dentro de los primeros 15 días calendario siguientes a la aprobación de la garantía única.	Habilitante
317	Los alcances del presente proceso deben estar soportados en la confidencialidad, integridad, disponibilidad y criticidad de la información.	Técnico Obligatorio
318	El contratista deberá conocer suficientemente la topología de conexión y la disponibilidad para conectar los equipos en la infraestructura del centro de datos de la SDDE, la cual podrá verificar personalmente mediante visita técnica, allí se darán a conocer los detalles de los componentes y elementos instalados en el centro de datos, ya que por motivos de seguridad no se pueden publicar los detalles técnicos en este pliego.	Habilitante
319	Si el equipo ofertado supera las capacidades técnicas disponibles en el centro de datos, el contratista deberá proveer los componentes de electricidad y conectividad de datos necesarios para la puesta en funcionamiento de la plataforma de backup ofertada.	Habilitante
320	Garantizar la compatibilidad con la infraestructura instalada de los elementos y componentes de cableado en cobre y/o fibra óptica que se instalen en el centro de datos y certificada en sus puntos de enlace LAN.	Habilitante
321	Todo el cableado estructurado debe contar con servicio especializado certificado en el peinado de rack de datos, asegurando el cumplimiento de normas de marquillado y organización de cableado de datos.	Habilitante
322	La solución del presente proceso cumplirá con el ámbito de aplicación de normatividad y reglamentaciones de acuerdo a las mejores prácticas y estándares de la industria y el fabricante.	Habilitante
323	El contratista debe realizar todos los trabajos y tareas preliminares que sean necesarios para la ejecución del presente proceso.	Habilitante
324	El contratista será el responsable de entregar en correcto funcionamiento todos los bienes suministrados para la ejecución del presente procesos de contratación por ellos dentro de su oferta económica debe incluir el costo de todas las actividades requeridas para ese fin. Cualquier actividad adicional, así como cualquier labor de planeación, programación, desarrollo, tiempos de disponibilidad de personal, suministro de equipos, componentes de conectividad y software, que se requieran para garantizar el pleno y adecuado funcionamiento de la solución, deben ser incluida por el contratista y por ningún motivo generaran costos adicionales a la SDDE.	Habilitante

325	El contratista deberá garantizar la disponibilidad del personal de profesionales las 24 horas de los 7 días del plazo de ejecución del contrato para la realización de las tareas y actividades requeridas en la solución ofertada.	Habilitante
326	El proveedor de la solución ofrecida debe acreditarse como canal o distribuidor en la categoría Gold o Platinum (o sus equivalentes en las categorías superiores del fabricante).	Habilitante
327	La Entidad aceptará soluciones técnicamente equivalentes o superiores que acrediten el cumplimiento de los requisitos funcionales y de desempeño establecidos en el presente documento, en observancia del principio de pluralidad de oferentes y selección objetiva	Técnico Obligatorio
	Instalación y Configuración de la Solución	
328	Incluir todos los elementos físicos y lógicos, así como los servicios de instalación y configuración necesarios para que la Entidad cuente con el sistema de seguridad perimetral, con óptima configuración que respalde los firewall e información alojada al interior de la SDDE.	Técnico Obligatorio
329	Entregar la plataforma instalada y configurada, esto es el conjunto de todos los equipos con los productos según la arquitectura y requerimientos definidos. Se considera que la plataforma se entregará funcionando en perfecto estado y con las aprobaciones que se requieran para su ejercicio.	Técnico Obligatorio
330	La solución instalada debe ser entregada con un informe de prueba pruebas documentadas del rendimiento con funciones de seguridad activas (IPS, SSL/TLS inspection) con el «security profile» activado.	Técnico Obligatorio
331	Instalación en rack y conexión eléctrica.	Técnico Obligatorio
332	Instalación de licencias de la solución ofertada.	Técnico Obligatorio
333	Actualización e instalación de últimos parches de seguridad, cuando sea necesario.	Técnico Obligatorio
334	Servicio de Soporte Técnico y Garantías Directo del Fabricante en modalidad 7x24 por un periodo de tres (3) años	Técnico Obligatorio
335	Instalación de la consola administrativa y verificación de acceso a la administración de la solución, por los diferentes métodos (web, ssh, telnet, serial, cliente o local).	Técnico Obligatorio
336	Asesoramiento remoto o presencial para las configuraciones requeridas por la SDDE, en el piloto operativo buscando no afectar los servicios de la entidad.	Técnico Obligatorio
337	Informe de prueba de vulnerabilidades	Técnico Obligatorio
338	La solución instalada debe ser entregada con un informe de prueba de vulnerabilidades. El proveedor de la solución ofertada debe garantizar la mitigación y buenas prácticas de configuración a la solución entregada.	Técnico Obligatorio
	Guía de Instalación, Configuración y Transferencia Tecnológica	
339	Además de los servicios de instalación y configuración, el contratista deberá entregar, una guía de instalación y configuración que permita, de forma autónoma, a la Subdirección de Informática y Sistemas de la SDDE, efectuar la reconfiguración de la totalidad de los elementos que conforman la solución. La guía deberá considerar como mínimo los siguientes aspectos: a) Arquitectura técnica de la solución. b) Configuración e instalación de los componentes físicos (hardware) de gestión de ancho de banda y seguridad perimetral. c) Configuración del software del sistema de gestión de ancho de banda y de seguridad perimetral. d) Configuración e instalación del software adicional que pueda requerirse. e) Políticas de respaldo y recuperación de las configuraciones de los sistemas de gestión de ancho de banda y de seguridad perimetral. f) Recomendaciones técnicas para proyectar mejoras en la solución. g) Manual de técnico y de usuario de la solución ofertada en Inglés y Español. La documentación podrá basarse en documentos existentes, pero deberá adaptarse a las condiciones y aspectos particulares de la instalación y configuración requeridas por la SDDE. En el mismo conjunto de documentos deberán presentarse al finalizar el contrato: las recomendaciones, previsiones y todo aquello que sea necesario para proyectar las mejoras en la solución en el mediano plazo. Durante el período de la garantía se deberá prestar la atención a problemas que se presenten, en un lapso no superior a cuatro (4) horas. Si el proveedor no puede solucionar el problema en este tiempo debe poner a disposición de la Entidad máximo dentro de los dos (2) días hábiles siguientes un equipo de soporte que sea de las mismas características o superiores, durante el tiempo que dure la reparación del equipo dañado.	Técnico Obligatorio

Firma Ficha Técnica

ADRIANA MONTOYA RIOS
Subdirectora de Informática y Sistemas

Uso Público