ANEXO ESPECIFICACIONES TÉCNICAS Y OBLIGACIONES

OBJETO: Adquirir licencias de agente cortex XDR para protección de endpoint, firewall de propósito específico y servicios adicionales.

1	**CARACTERÍSTICAS DE AGENTE CORTEX XDR**
1.1	Se debe incluir los agentes para al menos 184 dispositivos que se puedan instalar en sistemas operativos Windows, MacOS, Linux sin necesidad de reiniciar, que deben ser compatibles con los que actualmente cuenta la entidad y funcionen sobre la misma plataforma de gestión (actualmente cuenta con la solución de CORTEX XDR)
1.2	Los agentes deben poderse instalar en equipos físicos, máquinas virtuales, en contenedores, en dispositivos móviles, en entornos de nube privada, nube publica, nube hibrida.
1.3	El agente debe tener un footprint mínimo que no impacte la experiencia de usuario y que soporte las siguientes versiones de sistemas operativos: Windows XP* (32-bit, SP3 o posterior), Windows Vista (32-bit, 64-bit, SP1 o posterior; FIPS mode), Windows 7 (32-bit, 64-bit, RTM & SP1; excepto Home), Windows Embedded 7 (Standard & POSReady), Windows 8* (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit; FIPS mode), Windows Embedded 8.1 Pro, Windows 10 Pro (32-bit and 64-bit), Windows 10 Enterprise LTSB, Windows 10 Education, Windows 10 Update 1809, Windows Server 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter. OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14. CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16
1.4	Debe incluir la capacidad de examinar los datos de los equipos terminales que tengan los agentes instalados, las alertas de terceros y los datos de logs.
1.5	Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
1.6	Debe permitir que las VPN client-to-site operen usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
1.7	Debe soportar para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V.
1.8	Debe soportar para máquinas virtuales en nube publica y ambientes de contenedores de servicio como: Google Kubernetes (GKE), Amazon Elastic Kubernetes Service (EKS) y Azure Kubernetes Service (AKS)

1.9	Debe tener la capacidad para configurar la captura de datos que serán enviados a la nube para su almacenamiento, procesamiento y análisis en una consola de detección y respuesta a incidentes.
1.10	Debe incluir la capacidad de realizar inspección de datos a nivel de información del host: Información del Host: Nombre de host, Dirección MAC, Sistema operativo
1.11	La protección de los equipos terminales (end points) debe incluir la búsqueda y destrucción de amenazas, indexando todos los archivos de los equipos con sistemas operativos Windows, Linux, MacOS que pueda encontrar y eliminar los archivos maliciosos en tiempo real.
1.12	Debe estar en capacidad de evaluar las vulnerabilidades, que le permitan una total visibilidad en tiempo real de la exposición a la vulnerabilidad y los niveles actuales de parches en sus endpoints para priorizar la mitigación.
1.13	Cada endpoint debe ser protegido por un solo agente.
2	**EQUIPOS FIREWAL DE NUEVA GENERACIÓN OSS (On Site Spare)**
2.1	**GENERALIDADES**
2.1.1	Adquisición de dos equipos de propósito dedicado para la protección de red con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial con la licencia de prevención de amenazas, filtrado URL, seguridad de DNS, protección de malware por lo menos por 3 años, que este en capacidad de soportar HA tanto en modo activo-activo como activo-pasivo. La solución debe ser de la misma marca que el software de seguridad para detección y respuesta de ataques sofisticados con el que cuenta la entidad (CORTEX XDR). Los equipos deberán quedar configurados uno en activo y el otro pasivo, que en caso de falla se pueda quedar configurado como activo.
2.1.2	El fabricante debe pertenecer al cuadrante de líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” en los últimos 5 reportes.
2.1.3	El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
2.1.4	El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
2.1.5	La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
2.1.6	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.

2.1.7	Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware. Asimismo, el soporte del fabricante deberá brindar herramientas de evaluación de configuraciones del NGFW alineadas a las buenas prácticas de la industria y propuestas por el fabricante.
2.1.8	Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Postor.
2.1.9	Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante.
2.2	**CAPACIDAD**
2.2.1	Throughput de Next Generation Firewall de 2,8 Gbps medido con tráfico real (transacciones http 64KB o transacciones usando tráfico mixto de aplicaciones similar a un tráfico empresarial). No se aceptarán mediciones hechas con tráfico UDP o bajo el marco de RFCs no actualizados como los 3511, 2544, 2647 o 1242, o empleando tráfico mixto que no especifique tamaño de transacciones o paquetes.
2.2.2	Throughput de Threat Prevention de 1350 Mbps medido con tráfico de real (transacciones http 64KB o transacciones usando tráfico mixto de aplicaciones similar a un tráfico empresarial), con las siguientes funcionalidades habilitadas simultáneamente: Firewall con clasificación y control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Anti-malware de red, Antispyware (o AntiBot), control de amenazas avanzadas de día cero (Sandboxing), control de archivos y logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o empleando tráfico mixto que no especifique tamaño de transacciones o paquetes.
2.2.3	No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
2.2.4	La plataforma de hardware debe soportar hasta 290.000 sesiones simultaneas y 50.000 sesiones por segundo
2.2.5	Capacidad de Descifrado de sesiones SSL de al menos 38.000 sesiones concurrentes
2.2.6	Disco interno de 128 GB
2.2.7	Mínimo 8 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red
2.2.8	1 (una) interfaz de red tipo RJ45 de 1 Gbps dedicada para administración tipo Fuera de banda (Out of band)
2.2.9	1 (una) interfaz de tipo consola

2.2.10	1 Puerto de consola Micro-USB tipo A
2.2.11	Capacidad mínima de 5 instancias de routing virtuales
2.2.12	Capacidad mínima de 75 zonas de seguridad
2.2.13	El equipo debe contar de manera nativa con interfaz gráfica web (GUI), Línea de comandos (CLI) e Interfaz de programación de aplicaciones (Rest API)
2.3	**CARACTERÍSTICAS GENERALES**
2.3.1	El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
2.3.2	Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
2.3.3	Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
2.3.4	Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
2.3.5	Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
2.3.6	Soportar túneles GRE como punto inicio o finalización del túnel.
2.3.7	Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
2.3.8	Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
2.3.9	Debe permitir el bloqueo de ataques de Denegación de Servicio (DoS), definiendo un umbral máximo de conexiones por segundo por tipo de paquete (SYN, ICMP, UDP).
2.3.10	Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
2.4	**FUNCIONALIDADES DE FIREWALL**
2.4.1	Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
2.4.2	Permitir el agendamiento de las políticas de seguridad.
2.4.3	Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
2.4.4	Permitir añadir un comentario de auditoria cada vez que se haga un cambio o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada.

2.4.5	Al crear o editar políticas de seguridad, se debe poder forzar el uso de una descripción, tag o comentario de auditoria. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.
2.4.6	Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
2.4.7	Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:
2.4.8	- Mostrar la primera y última vez que se utilizó una regla de seguridad
2.4.9	- Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso desde un período definido.
2.5	**DESCIFRADO DE TRÁFICO SSL/TLS**
2.5.1	Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
2.5.2	Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
2.5.3	Debe permitir los algoritmos de cifrado para negociar la conexión SSL/TLS, deberá soportar como mínimo los siguientes: RSA, DHE, ECDHE, 3DES, AES-128-GCM, AES-128-CBC, AES-256-GCM, AES-256-CBC, CHACHA20-POLY1305, MD5, SHA1, SHA256, SHA384.
2.5.4	Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido
2.5.5	Debe poder bloquear las sesiones cuyo certificado no es válido o el emisor no es confiable a pesar de no aplicar descifrado al tráfico SSL/TLS
2.5.6	Debe soportar certificados que utilice Subject Alternative Name (SAN).
2.5.7	Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
2.5.8	Debe permitir reenviar el tráfico descifrado por una interfaz Port Mirror o Snnifer a un equipo externo al Firewall, como por ejemplo un DLP.
2.5.9	Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.
2.5.10	Capacidad de poder hacer de cifrado a por lo menos TLS v1.1, v1.2 y v1.3
2.5.11	Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de explorar de las claves privadas, para evitar un uso indebido por parte de los administradores.

2.5.12	La solución tiene que contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL / TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo tiene que tener varios estados de trobleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (ej: informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).
2.6	**IDENTIFICACION Y CONTROL DE APLICACIONES**
2.6.1	Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
2.6.2	Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
2.6.3	Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
2.6.4	Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
2.6.5	Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
2.6.6	Permitir nativamente la creación de firmas personalizadas basadas en expresiones regulares de aplicaciones propietarias desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
2.6.7	Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad. Con el objetivo de poder permitir acceder por ejemplo a Office365, Google G Suites para dominios manejados por la organización y no otras cuentas de SaaS dentro de esas nubes.
2.6.8	Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.
2.6.9	Las políticas de seguridad tienen que poder ser creadas en base a las aplicaciones y no en base a puertos TCP/UDP.
2.6.10	La aplicación de seguridad tienen que ser 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto de comunicaciones, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación.
2.6.11	Debe poder identificar y crear políticas de aplicaciones de redes industriales (Redes OT), como ser Scada, modbus, dnp3, iccp, opc, siemens, etc

2.6.12	Debe poder permitirse granularidad de aplicaciones de redes industriales, es decir, en las aplicaciones de este tipo de redes poder identificar acciones como lectura, escritura, apertura, llamadas, etc
2.6.13	Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las políticas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación.
2.6.14	Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.
2.7	**PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)**
2.7.1	Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood y Otros ataques basados en Floods de IP
2.7.2	La medida de defensa contra ataques Flood deberán basarse en mecanismos de early drop o random early detection
2.7.3	Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa
2.7.4	La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Next Generation Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
2.7.5	La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS
2.7.6	Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
2.7.7	La protección contra ataques de escaneo deberá permitir alertar el ataque, activar la protección bloqueando la IP que supera el umbral definido y adicionalmente definir un tiempo de bloqueo
2.7.8	La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP, a los cuales no se le aplicarán la protección (por ejemplo, en caso de una herramienta de escaneo legítimo)
2.7.9	Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
2.7.10	Debe proteger contra ataques basado en paquetes TCP, como mínimo Split Handshake, paquetes TCP SYN y TCP SYN/ACK con datos contenidos durante el handshake, Validación del Three Handshake.

2.7.11	Debe proteger contra ataques basado en paquetes ICMP, como mínimo paquetes con Ping ID 0, paquetes ICMP fragmentados, paquetes ICMP extensos
2.7.12	Debe proteger contra ataques basado en paquetes IPv6 e ICMPv6
2.7.13	Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA y otros), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).
2.7.14	Debe contar con un mecanismo que proteja contra la saturación del buffer de paquetes por cada interfaz de datos de la solución
2.7.15	Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia un equipo protegido
2.7.16	Debe permitir reglas de prevención contra ataques DoS de tal forma que se pueda definir la IP y grupo de usuario origen, la IP destino, Puertos y regla de protección DoS
2.7.17	Se debe poder definir un horario para que automáticamente se aplique la regla de prevención contra ataques DoS
2.8	**PREVENCION DE AMENAZAS**
2.8.1	Se debe incluir, para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Antispyware/Antibot
2.8.2	Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por Spyware en entornos corporativos
2.8.3	Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
2.8.4	Cuando se utilicen las funciones de IPS, Antivirus y Antispyware/Antibot, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Antivirus y Antispyware habilitadas simultáneamente.
2.8.5	El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
2.8.6	Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
2.8.7	Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
2.8.8	Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.
2.8.9	Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.

2.8.10	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1,2 y 3), SMTP, IMAP y POP3. Deberá tener cobertura tanto en IPv4 como en IPv6 para los protocolos en mención
2.8.11	Previene ataques utilizando Inteligencia de amenazas global
2.8.12	Protección contra cargas ocultas en tipos de archivos comunes, como documentos de Microsoft® Office y PDF.
2.8.13	Debe combinar un motor de prevención de amenazas en tiempo real con una base de datos URL completa y elementos de identificación de aplicaciones para limitar la transferencia no autorizada de datos y archivos y detectar y bloquear una amplia gama de exploits, malware, navegación web peligrosa y objetivos y amenazas desconocidas.
2.8.14	Debe admitir la conversión de firmas de snort configuradas correctamente. Snort Intrusion Prevention System (IPS) y firmas del Sistema de nombres de dominio (DNS) se puede convertir en listas dinámicas externas.
2.8.15	IPS Las protecciones incluyen tanto la detección de anomalías como la coincidencia de firmas, utilizando la coincidencia de patrones con estado para comprender el orden y la secuencia de llegada de los paquetes..
2.8.16	Debe proteger la red de amenazas comunes y amenazas persistentes avanzadas (APT)
2.9	**IDENTIFICACION DE USUARIOS**
2.9.1	Debe tener la posibilidad de incluirse la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.
2.9.2	Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
2.9.3	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios.
2.9.4	Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
2.9.5	Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
2.9.6	Debe permitir la definición de grupos dinámicos de usuarios.
2.9.7	Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server.

2.9.8	Debe de permitir la identificación de los usuarios de la red utilizando una variedad de métodos de acceso y sistemas operativos, incluidos Microsoft Windows, Apple iOS, Mac OS, Android y Linux / UNIX.
2.9.9	Debe de poder leer las direcciones IPv4 o IPv6 de los usuarios desde el encabezado X-Forwarded-For (XFF) en las solicitudes del cliente HTTP cuando el firewall se implementa entre Internet y un servidor proxy que de otro modo ocultaría las direcciones IP del usuario.
2.9.10	Debe de tener un API para actualizar ID de usuario, así como la capacidad de analizar syslogs para mapeos de ID de usuario.
2.10	**CALIDAD DE SERVICIO (QOS)**
2.10.1	Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.
2.10.2	Soportar la creación de políticas de QoS por: dirección de origen y destino, por usuario y grupo de LDAP/AD, por aplicaciones, por puerto.
2.10.3	El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
2.10.4	Soportar marcación de paquetes DSCP, inclusive por aplicaciones;
2.10.5	Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.
2.11	**FILTRO DE DATOS**
2.11.1	Los archivos deben ser identificados por extensión y firmas.
2.11.2	Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
2.11.3	Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.
2.12	**VPN**
2.12.1	Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
2.12.2	La VPN IPSec debe soportar como mínimo:
	- DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
	- Autenticación MD5, SHA-1, SHA-2
	- Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
	- Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
2.12.3	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.

2.12.4	Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
2.12.5	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.
2.12.6	Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
2.12.7	Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
2.12.8	Debe soportar Split Tunel, de tal forma que el tráfico hacia internet no se en rute por la VPN
2.12.9	Debe permitir configurar Split Tunel inteligente, que permita seleccionar el tráfico a enrutar en base a la aplicación y dominio de internet. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
2.12.10	Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
	- Antes del usuario se autentique en la estación;
	- Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
	- Bajo demanda del usuario;
2.12.11	Debe asignar una IP a cada cliente que se conecte a la VPN en formato IPv4 e IPv6, de forma automática mediante un pool de IP.
2.12.12	El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.
2.12.13	Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
2.12.14	Debe permitir la conexión a la VPN sin necesidad de instalar el agente (clientless).
2.12.15	La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada. La identificación de equipos colocados en cuarentena se debe basar en un ID inmutable del Cliente VPN, de tal forma que la restricción no pueda ser eludida (por ejemplo, si la cuarentena se hace a una IP, el malware puede modificar la IP del equipo para eludir la cuarentena)
2.12.16	Debe ser posible colocar equipos en cuarentena de forma manual o automática.
2.12.17	Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.
2.12.18	Debe permitir la configuración de políticas de seguridad de VPN basado en las características del equipo, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.

2.12.19	El Perfilamiento y postura mencionado en el punto anterior, tiene que poder efectuarse inclusive dentro de la red, entre dos o más segmentos de red que controle el firewall, sin necesidad de armar un túnel de VPN, sino solamente utilizando el perfilamiento y postura del equipo de punto final sobre las políticas de seguridad del NGFW
3	**SERVICIOS**
3.1	Se debe realizar la instalación y puesta en servicio de los equipo NGFW
3.2	Se debe incluir el servicio de soporte por 36 meses, 8x5 remoto que incluye: Gestión de reemplazo de partes, Soporte de incidencias telefónico, Atención nuevos requerimiento telefónico, remoto, tanto para la solución del NGFW como para el SOFTWARE DE SEGURIDAD PARA DETECCION Y RESPUESTA DE ATAQUES SOFISTICADOS
3.3	En caso de falla o caída total del equipo FWNG se debe realizar el soporte en sitio 24x7 con tiempo de respuesta inferior a 4 horas
3.4	Se debe realizar labores de servicios de configuración en el software de seguridad para, detección y respuesta de ataques sofisticados, deben incluir:
	Implementación de la funcionalidad de App-ID en la red del cliente y cambio de políticas de acuerdo a la adopción.
	Conversión de todas las aplicaciones conocidas por la solución de Palo Alto Networks de reglas basadas en puertos a reglas basadas en aplicaciones.
	Aislamiento de las reglas de tráfico que manejan tráfico TCP/UDP desconocido. (unknown).
	Implementación de la funcionalidad de User-ID en la red del cliente con una (1) fuente de identificación (802.1x, RADIUS, LDAP, XML API).
	Configuración de asociación de grupos de acuerdo al User-ID. (Group Mapping).
	Desarrollo y despliegue de políticas de Descifrado SSL para categorías de alto riesgo de acuerdo a los requisitos del cliente. No se incluye despliegue de certificado.
	Habilitación de la función de Descifrado SSL en dispositivos seleccionados.
	Despliegue de políticas de descifrado basado en categorías definidas por el cliente.
	Validación a través del monitoreo de logs, descifrado activo de sesiones para las categorías definidas en los requisitos del cliente.
	Configuración de la función de Filtrado de Contenido de PANDB basado en los requisitos del cliente.
	Bloqueo de categorías de alto riesgo (high-risk) basado en requisitos del cliente.
	Habilitación de Content-ID – Revisión del tráfico de red y documentar cambios como sea necesario.
	Inclusión de recomendación de Anti-virus y Anti-Spyware.
	Configuración de mejores prácticas de Zone Protection
	Configuración de EDL en políticas generales, solo EDL públicas de Palo Alto Networks. No Incluye EDL personalizadas.

	Análisis de un 10% de políticas de seguridad del cliente y los perfiles de seguridad asociados a las mismas. (Impacto al tráfico por la configuración de elementos del Content-ID
	Personalización de reportes de operación de seguridad, mantenimiento de los firewalls, detección de compromiso y detección de fallos en la configuración.
	Habilitar con el usuario un ambiente de reportes de toda la red
	Identificar generación de logs hacia SNMP y SNMP trap necesarios.
	Configuración de QoS
	Integración con herramientas de terceros

ENTREGABLES

El contratista debe suministrar:

1. Dos equipos Firewall instalados y en funcionamiento con licenciamiento para operar en activo – pasivo, con soporte de fábrica por 3 años.
2. 184 licencias de agentes CORTEX XDR para usuarios finales (End Point) con certificado de licenciamiento por 3 años.
3. Manuales de usuario y técnico de la solución incluyendo firewall y agente de usuarios finales (End Point).
4. Informe de actividades donde se consigne los servicios y configuraciones realizadas en el software de seguridad de entidad, según el objeto y las especificaciones técnicas del contrato. El informe debe entregarse después de finalizada la entrega de las licencias y el Firewall en operación.

OBLIGACIONES DE LAS PARTES

OBLIGACIONES DEL DISTRITO ESPECIAL DE CIENCIA TECNOLOGÍA E INNOVACIÓN DE MEDELLÍN

1. Designar supervisor y equipo de supervisión de apoyo, los cuales velarán por el cumplimiento efectivo del contrato y servirán de enlace al contratista.
2. Cancelar al Contratista el valor del contrato, de acuerdo a la forma de pago establecida, previa presentación de la documentación requerida.
3. Dar respuesta en forma oportuna a los requerimientos y comunicados presentados por el contratista.
4. Verificar el cumplimiento de cada uno de los requerimientos señalados en las presentes especificaciones técnicas.

5. Acompañar y apoyar en forma permanente al contratista en los aspectos que sean competencia de la Administración Distrital durante la ejecución del contrato.
6. Garantizar los recursos financieros para la ejecución del contrato.
7. Suministrar la información que requiera EL CONTRATISTA en ocasión a la ejecución del presente contrato.
8. Efectuar por escrito y de manera oportuna requerimientos al contratista ante incumplimientos a lo estipulado en las especificaciones técnicas, para el establecimiento de los correctivos necesarios.
9. Adoptar las medidas necesarias para mantener el equilibrio económico del contrato, de acuerdo con lo previsto en la ley.
10. Vigilar que, durante toda la ejecución del contrato, el contratista aplique las medidas necesarias de protección y bioseguridad de todos los trabajadores y de toda la cadena de producción, transporte y distribución, para disminuir las fuentes de contacto y probabilidad de infección en época de pandemia
11. Las demás que sean necesarias para coadyuvar a la supervisión del contrato y para la correcta ejecución del mismo.

OBLIGACIONES DEL CONTRATISTA

1. Cumplir con el objeto del contrato, en los términos y condiciones establecidos de conformidad con lo estipulado en el contrato, los estudios, especificaciones técnicas, así como con la oferta presentada.
2. Asumir todos los gastos y riesgos que implica el desarrollo del contrato en los términos, condiciones y exigencias consagradas en la propuesta.
3. Notificar a la Secretaría de Seguridad y Convivencia– Distrito Especial de ciencia, Tecnología e Innovación de Medellín y a la supervisión del contrato, dentro de las veinticuatro (24) horas siguientes al conocimiento de hechos o circunstancias que puedan incidir en la no oportuna o debida ejecución del contrato o que puedan poner en peligro los intereses legítimos del Distrito Especial de ciencia, Tecnología e Innovación de Medellín
4. Desarrollar la gestión conforme a las normas legales y a los requerimientos del Distrito Especial de ciencia, Tecnología e Innovación de Medellín.
5. Desplegar toda su capacidad técnica y operativa para la ejecución de las actividades objeto del contrato cumpliendo las especificaciones técnicas.
6. Supervisar permanentemente a su personal, con el fin de que se preste un eficiente servicio y se compromete a cambiarlo cuando el Supervisor y la Secretaría de Seguridad y Convivencia del Distrito Especial de ciencia, Tecnología e Innovación de Medellín, con causa justificada, lo soliciten.

7. Adelantar los trámites contractuales requeridos para el desarrollo del presente contrato, así como los post - contractuales a que haya lugar.
8. Asistir los comités técnicos, según la regularidad establecida para ellos, y presentar el respectivo informe escrito donde se reportarán los avances del contrato.
9. Ejecutar el contrato garantizando en todo caso el cumplimiento de la normatividad aplicable, así como la eficiencia y eficacia de los recursos y la calidad de los productos y servicios prestados, desarrollando así el objeto contractual en condiciones de eficiencia, oportunidad y calidad de conformidad a los parámetros establecidos en la Secretaría de Seguridad y Convivencia – Distrito Especial de ciencia, Tecnología e Innovación de Medellín.
10. Presentar, a la supervisión del contrato designada por el Distrito Especial de ciencia, Tecnología e Innovación de Medellín, dentro de los quince (15) días calendario posterior a la instalación y puesta en funcionamiento de la solución XDR, un informe sobre las actividades realizadas. Adicionalmente, presentará cualquier otro informe que le sea solicitado por el Distrito Especial de ciencia, Tecnología e Innovación de Medellín con relación al desarrollo del contrato.
11. Pagar de su propia cuenta las tasas, impuestos, publicaciones y contribuciones a que esté obligado en virtud del contrato.
12. Deberá contar con el personal técnico y equipo necesario disponible para desarrollar el objeto contractual.
13. Cuando lo estime necesario, solicitar por escrito al supervisor previa justificación de los hechos, quedando a juicio de la Secretaría de Seguridad y Convivencia la determinación final, la ampliación de los plazos de ejecución de las actividades.
14. Cumplir con el pago oportuno de los salarios y honorarios del personal que participe en la prestación de los servicios.
15. El contratista es el único responsable por la vinculación de personal y la celebración de subcontratos, todo lo cual debe realizar en su propio nombre y por su propia cuenta y riesgo, sin que la Secretaria de Seguridad y Convivencia Distrito Especial de ciencia, Tecnología e Innovación de Medellín, adquiera responsabilidad ni solidaridad alguna por dichos actos. Por lo anterior, deberá asumir respecto de sus subcontratistas (personal dirigido a la ejecución del contrato) los honorarios o salarios, horas extras, dominicales y festivos, recargo nocturno, indemnizaciones y demás prestaciones, afiliación al Sistema de pensiones y salud, según lo ordenado por la Ley 100 de 1993 y que se causen durante la ejecución del contrato, atendiendo a la modalidad de vinculación que aplique con las personas naturales que subcontrate.

16. El contratista se obliga a atender todas las observaciones y requerimientos a productos por la supervisión, del Distrito Especial de ciencia, Tecnología e Innovación de Medellín distrito y demás entidades competentes.
17. Utilizar y garantizar personal idóneo y calificado para adelantar todas las gestiones necesarias para cumplir con el contrato así como los medios técnicos y tecnológicos necesarios.
18. Cualquier discrepancia debe ser aclarada prontamente con el supervisor.
19. Otorgar las garantías exigidas para amparar los riesgos del contrato.
20. Facilitar la liquidación del contrato dentro del plazo establecido.
21. Garantizar durante la ejecución el cumplimiento de las especificaciones Técnicas y las Normas vigentes
22. El contratista deberá entregar toda la información generada en desarrollo del contrato, en medio físico y magnético, con el fin de entregar a los diferentes organismos de control y seguimiento con que cuenta el Distrito, tales como SAP, Informes de Seguimiento mensual, entre otros garantizando la cadena de custodia.
23. Cumplir con los acuerdos de niveles de servicio (ANS) tal como se describen en las especificaciones técnicas que hacen parte integral del contrato.
24. El contratista debe presentar informe técnico final sobre las actividades realizadas durante la ejecución del contrato.
25. El contratista es el encargado del mantenimiento, la formación y el servicio de atención al cliente remoto 24/7/365.
26. El contratista es responsable soporte 24/7/365, cliente dedicado y equipo de soporte técnico.
27. Las demás señaladas en la Constitución, la Ley, las cláusulas contractuales, la propuesta y las que correspondan a la naturaleza o tipo de contrato y su efectiva ejecución.

OBLIGACIONES DEL CONTRATISTA REFERENTE AL CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST):

El contratista debe cumplir las disposiciones contempladas en el Decreto 1072 de 2015 y la Resolución 0312 de 2019 y las demás disposiciones vigentes en materia de Seguridad Social y Seguridad y Salud en el Trabajo.

Esta obligación será verificada por los supervisores o interventores según aplique, con los siguientes documentos:

1. La Autoevaluación del SGSST o autoevaluaciones del año en curso. Conforme a los resultados de la autoevaluación que aporte el contratista, éste asume unas obligaciones que están expresas en el artículo 28 Resolución 0312 de 2019, las cuales serán verificadas por el supervisor según sea el caso.
2. Plan de Trabajo del SG-SST acorde a la autoevaluación o autoevaluaciones del año en curso.
3. En los contratos donde el contratista deba dotar de elementos de protección personal, el supervisor debe constatar en campo dicha obligación, y solicitar al contratista formato de entrega de los elementos de protección personal que lleve la firma de los trabajadores que están prestando sus servicios en el Distrito Especial de Ciencia, tecnología e innovación de Medellín, dejando todas las evidencias en el informe parcial de supervisión, y debe ser revisada en cada pago.

HORACIO GRISALES NOREÑA
Técnico

BALMES JUANICO MENA MOSQUERA
Jurídico