**EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS - ESU**

**NIT 890.984.761-8**

| **CONTRATO No.** |
|---|
| **202500241** |

**FT-M3-GJ-01**
**Versión: 11**

| **CONTRATISTA** | **NIT** | **TELÉFONO** | **FECHA DE SUSCRIPCIÓN** | |
|---|---|---|---|---|
| BOYRA S.A.S. | 830.100.010-4 | 6019156130 | LEGALIZADO POR FIRMA ELECTRONICA | |
| **REPRESENTANTE LEGAL** | **CÉDULA** | **DIRECCIÓN DE CONTACTO** | | **TEL./CEL. CONTACTO** |
| Luis José Ignacio Quintero Cusguen | 79131510 | Diagonal 61C Bis 24 44 | | 6019156130 |
| **CORREO ELECTRÓNICO** | **CIUDAD DE EJECUCIÓN** | **RADICADO REQUERIMIENTO** | **BIENES O SERVICIOS** | **DISPONIBILIDAD PRESUPUESTAL** |
| luis.quintero@boyra.com | Medellín | 20251006543 | Bienes | **2025001140** |

| **CONVENIO** | **CENTRO DE COSTOS** | **RUBRO PRESUPUESTAL** | **DESCRIPCIÓN RUBRO** | **VALOR CONTRATO** | **COMPROMISO PRESUPUESTAL** |
|---|---|---|---|---|---|
| 4600105849 DE 2025 | 33408 | 23202020080460-1 / 83159 | FORTALECIMIENTO DATA CENTER | $3.170.006.562 IVA Incluido | 2025001348 |

**OBJETO**
Adquisición y soporte de licencias y hardware para el fortalecimiento de la seguridad de la información, orientados a la modernización y transformación de las soluciones tecnológicas de seguridad ciudadana.

**ALCANCE DEL OBJETO**
El alcance del presente proceso comprende:

1. Adquisición y soporte de licencias para orientados a la modernización y transformación de las soluciones tecnológicas de seguridad ciudadana.
2. Adquisición de hardware para la seguridad de la información.

**ESPECIFICACIONES TÉCNICAS**
Las especificaciones de los servicios se encuentran descritas en el anexo No 1 del presente contrato.

1. **RFP firewall PA-3430 CoreSec+GP+DLP.**

| | | |
|---|---|---|
| 1 | | **SUMINISTRO DE HARDWARE DE SEGURIDAD PERIMETRAL** |
| 1,1 | Generalidades | Suministro de dos (2) appliances de seguridad para actualización de la plataforma de seguridad perimetral. Los appliances deben soportar la función de balanceo de cargas sin requerir un software adicional, ni licenciamiento adicional. La entidad desea contar con la funcionalidad de alta disponibilidad en modo Activo-Pasivo, con las respectivas suscripciones y soportes de cada equipo por 21 meses entre ellas GP, DLP, BND, PLUS. |
| | | La entidad requiere de la renovación o adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red. |
| | | La solución tiene que ser ofrecida en alta disponibilidad en cada una de las sedes, se entiende por alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones. |
| | | El fabricante debe pertenecer al cuadrante de líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” en los últimos 10 reportes. |
| | | La solución propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS. |
| | | La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7. |
| | | 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. Debe cubrir cinco años de vida útil para el servicio en la Entidad. |
| | | 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. |
| | | 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. |
| | | 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 y de manera autónoma, a cursos en línea sobre las diversas tecnologías del fabricante. |
| | | Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de |

| | | |
|---|---|---|
| | | configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución. |
| | | Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. |
| | | El contratista y personal de la entidad deberán poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma o cuando lo requiera la Entidad entregando un informe de las mejoras y buenas prácticas. |
| | | El Postor deberá ejecutar la evaluación de buenas prácticas de forma periódica por lo menos dos veces durante la vigencia del contrato, con el objetivo de proporcionar un servicio de mejora continua sobre las configuraciones del Next Generation Firewall. |
| | | Si se identifica actividad sospechosa y/o maliciosa en la red, o sufra una brecha de seguridad luego de implementar las buenas prácticas de seguridad sugeridas por la herramienta de evaluación, la Entidad tendrá la potestad de contar con un servicio el cual incluye: |
| | | ▪ Expertos, herramientas especializadas de inteligencia de amenazas y prácticas de cacería de amenazas. |
| | | ▪ Análisis de logs e indicadores de compromiso. |
| | | ▪ Evaluación de la configuración del NGFW que incluya recomendaciones personalizadas. |
| | | ▪ Recomendaciones de pasos siguientes a realizar. |
| 1,2 | Capacidades NGFW | Throughput de Next Generation Firewall de 29 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). En el caso que el fabricante tenga mediciones con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes, deberá garantizar este Throughput con el máximo nivel de inspección del fabricante. |
| | | Throughput de Prevención de Amenazas de 15 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), DNS Security, Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar un throughput mínimo medido con el nivel o modo más alto de inspección. Se debe garantizar |

| | | |
|---|---|---|
| | | que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. |
| | | 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. |
| | | La plataforma de hardware debe soportar mínimo 2.5 millones de sesiones simultáneas y mínimo 240 Mil sesiones por segundo. |
| | | Fuente de poder redundante. |
| | | Disco (de estado sólido) interno mínimo 480 GB o superior. |
| | | Mínimo 12 interfaces de red 1G/2.5G/5G/10G en cobre, formato RJ45 para tráfico de datos de la red. |
| | | Mínimo 10 interfaces de red 1G/10G SFP/SFP+ para el tráfico de datos de la red. |
| | | Mínimo 4 interfaces de red 25G SFP28 para el tráfico de datos de la red y mínimo 2 interfaces 40G/100G QSFP/QSFP28. |
| | | La plataforma deberá contar con al menos una interface adicional RJ45 de 100/1000 para administración o interfaces SFP+ de 10 Gbps dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad. |
| | | Capacidad de virtualización de router de mínimo 10 instancias. |
| 1,3 | Características de red | Capacidad de etiquetas VLAN 802.1Q por equipo/interfaz: 4,094/4,094. |
| | | 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. |
| | | Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). |
| | | 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. |
| | | Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP. |
| | | 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. |

| | | |
|---|---|---|
| | | 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. |
| | | Soportar DNS Dinámico en las interfaces de red del equipo de seguridad. |
| | | 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. |
| | | Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo. |
| | | 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. |
| 1,4 | Alta disponibilidad | Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3). |
| | | La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red. |
| | | Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces. |
| | | Para la funcionalidad de HA y Clustering no debe requerirse de dispositivos o software externos a los NGFW. |
| | | Se deben tener interfaces dedicadas para la función de HA, estas interfaces deben estar asociadas al plano de datos y ser independiente de las interfaces de tráfico. |
| | | Se debe poder crear clusters de más de dos dispositivos para la sincronización de sesiones. Esta funcionalidad no debe requerir licenciamiento. |
| | | La funcionalidad de clustering debe permitir incorporar al mismo tiempo dispositivos independientes, así como dispositivos configurados en HA. |
| 1,5 | Funcionalidades de Firewall | 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. |
| | | Permitir el agendamiento de las políticas de seguridad. |

| | | |
|---|---|---|
| | | Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa. |
| | | Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. |
| | | Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria. |
| | | 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). |
| | | Debe mostrar la primera y última vez que se utilizó una regla de seguridad. |
| | | Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad. |
| | | Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red. |
| 1,6 | Descifrado de tráfico SSL/TLS | Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos. |
| | | Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall. |
| | | Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido |
| | | Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS |
| | | Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI). |
| | | Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards. |
| | | Debe permitir reenviar el tráfico descifrado por una interfaz Port Mirror o Snnifer a un equipo externo al Firewall, como por ejemplo un DLP. |
| | | Capacidad de poder hacer descifrado a por lo menos TLS v1.1, v1.2 y v1.3 |
| | | Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar de las claves privadas, para evitar un uso indebido por parte de los administradores. |

| | | |
|---|---|---|
| | | Debe 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 debe tener varios estados de troubleshooting 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 (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros). |
| 1,7 | Identificación y control de aplicaciones | Reconocer por lo menos 4550 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. |
| | | Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2 |
| | | Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. 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. |
| | | Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado. |
| | | Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada. |
| | | 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. |
| | | 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 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. |
| | | Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como: |
| | | • Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol). |
| | | • Nivel de riesgo de las aplicaciones. |
| | | • Categoría y sub-categoría de aplicaciones. |

| | | |
|---|---|---|
| | | Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda. |
| | | La aplicación de políticas de seguridad debe tener la posibilidad de 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. |
| | | 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. |
| | | Debe contar con la posibilidad de 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. |
| 1,8 | Protección ante ataques de denegación de servicio (DoS) | 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 |
| | | Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa |
| | | 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) |
| | | Deberá permitir configurar límites o umbrales que permitan proteger contra ataques de denegación de servicios como syn flood, escaneo de puertos, inundación udp, inundación icmp, entre otros. |
| | | 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 |
| | | 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) |
| | | Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route |
| | | 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. |

| | | |
|---|---|---|
| | | Debe proteger contra ataques basado en paquetes ICMP, como mínimo paquetes con Ping ID 0, paquetes ICMP fragmentados, paquetes ICMP extensos |
| | | Debe proteger contra ataques basado en paquetes IPv6 e ICMPv6 |
| | | Debe contar con un mecanismo que proteja contra la saturación del buffer de paquetes por cada interfaz de datos de la solución |
| | | 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. |
| | | Debe permitir reglas de prevención contra ataques DoS de tal forma que se pueda definir la IP, la IP destino, Puertos y regla de protección DoS. |
| | | Se debe poder definir un horario para que automáticamente se aplique la regla de prevención contra ataques DoS |
| 1,9 | Prevención de amenazas | Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Antispyware/Antibot |
| | | Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por Spyware en entornos corporativos |
| | | La solución debe ser capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas. |
| | | La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA). |
| | | Debe poder clasificar los dominios maliciosos en categorías como: malware, DGA, DNS tunneling, Comando y Control, DNS dinámicos, phising o dominios recientemente registrados. |
| | | 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. |
| | | 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. |
| | | El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot. |

| | | |
|---|---|---|
| | | 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. |
| | | 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. |
| | | Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad. |
| | | Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto. |
| | | 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 |
| | | Previene ataques utilizando Inteligencia de amenazas global |
| | | Protección contra cargas ocultas en tipos de archivos comunes, como documentos de Microsoft® Office y PDF. |
| | | 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. |
| | | 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. |
| | | IPS protections include both anomaly detection and signature matching, using stateful pattern matching to understand packet arrival order and sequence. |
| | | Debe proteger la red de amenazas comunes y amenazas persistentes avanzadas (APT) |
| 1.10. | Análisis de malware de día cero (Sandboxing) | La solución debe contar con un mecanismo interno basado en ML que permita detectar el malware de día cero que se propaga por la red en tiempo real y sin depender de firmas de antivirus. |
| | | Adicionalmente, la solución propuesta debe incluir la detección de amenazas de día cero complejas a través de una integración con una plataforma Sandboxing. |
| | | El dispositivo debe poder acceder y descargar protecciones contra malware de día 0 en tiempo real. |

| | | |
|---|---|---|
| | | En caso se trate de sandbox cloud, deberá ser una nube gestionada en su totalidad por el fabricante y deberá contar con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 2 o FedRAMP |
| | | La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac. |
| | | Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows 8, Windows 10, Mac OS X, Linux y Android. |
| | | Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante. |
| | | Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. |
| | | Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado. |
| | | El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6. |
| | | Debe permitir al administrador la descarga del archivo original analizado por el Sandbox. |
| | | Debe permitir reportar al fabricante eventos que son falso-positivo y falso negativo en el análisis de malware de día cero a partir de la propia consola de administración. |
| | | Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado. |
| | | Permitir la subida de archivos al sandbox de forma manual y vía API. |
| | | Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host. |

| | | |
|---|---|---|
| | | La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales. |
| | | La capacidad mínima de archivos por minuto que debe poder enviarse a análisis debe ser de 70 archivos. |
| | | La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales. |
| 1.11. | Filtro de contenido Web | Capacidad de poder aplicar técnicas de aprendizaje de máquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevos sitios de phishing, con la capacidad de poder bloquear los mismos. |
| | | Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora) |
| | | Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local. |
| | | Debe soportar un caché local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs |
| | | Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing. |
| | | Debe permitir la creación de categorías personalizadas. |
| | | Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas. |
| | | Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad. |
| | | Debe permitir la customización de la página de bloqueo. |
| | | Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site. |
| | | Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing. |
| 1.12. | Identificación de usuarios | Debe incluir 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. |

| | | |
|---|---|---|
| | | 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. |
| | | 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. |
| | | Debe permitir la definición de grupos dinámicos de usuarios. |
| | | 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. |
| | | 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. |
| | | Debe de tener un API para actualizar ID de usuario, así como la capacidad de analizar syslogs para mapeos de ID de usuario. |
| 1.13. | Filtrado de datos - DLP | Los archivos deben ser identificados por extensión y firmas. |
| | | 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. |
| | | 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. |
| 1.14. | Conexiones remotas seguras (VPN) | Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL. |
| | | 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); |
| | | Las VPN deberán estar en la capacidad o tener disponible en futuras actualizaciones la capacidad de configurar PPK poscuánticas en IKEv2 y se deben basar en el estándar RFC 8784. |

| | | |
|---|---|---|
| | | Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN. |
| | | 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 y soportar una cantidad mínima de 1800 usuarios concurrentes. |
| | | Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN clientto-site. |
| | | Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA). |
| | | 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. |
| | | Debe soportar Split Tunel, de tal forma que el tráfico hacia internet no se enrute por la VPN |
| | | 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. |
| | | 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. |
| | | 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. |
| | | 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. |
| | | 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 |

| | | |
|---|---|---|
| | | Debe permitir aislar el dispositivo de la red y mantenerlo en cuarentena de forma dinámica, en caso se detecte alguna actividad maliciosa |
| | | Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN. |
| | | El agente de VPN client-to-site debe ser compatible al menos con:, Windows 10, Windows 11, MacOS X, Linux, Android y iPhone. |
| | | La capacidad de establecer VPN's cliente a sitio con agente debe permanecer funcional para equipos windows y Mac aún con el vencimiento del licenciamiento y soporte. |
| 1.15 | Administración | Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino) |
| | | Debe permitir la visualización de los logs del tráfico de red, tráfico malicioso, envíos de archivos al sandbox, filtro web, eventos de sistema |
| | | Debe permitir la visualización de los logs con información del Usuario y Dirección IP asignada, esto deberá ser visible en la interfaz gráfica |
| | | Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración |
| | | Debe ser capaz de enviar los logs vía SNMP Trap, Correo Electrónico, Syslog y HTTP (vía API) |
| | | Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico. |
| | | Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables. |
| | | La autenticación deberá estar disponible localmente o integrado con plataformas SAML, Kerberos, RADIUS, TACACS+ y LDAP |
| | | Ante escenarios donde existan dos o más administradores logueados en el Next Generation Firewall, y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. |

| | | |
|---|---|---|
| | | Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política. |
| | | Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules). |
| | | Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup). |
| | | Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada. |
| | | Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema. |
| | | La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML. |
| 1.16. | Protección avanzada de DNS | La solución debe ser alimentada por un servicio de inteligencia global capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas. |
| | | El servicio de protección de DNS debe poder habilitarse sin modificar la configuración de DNS de la red local o desviar el tráfico DNS a servidores externos. |
| | | La solución debe ser un servicio que funcione integrado en la plataforma de NGFW, sin requerir adicionar hardware adicional y sin impactar el rendimiento del NGFW. |
| | | El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros. |
| | | La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA). |
| | | Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca antes vistos autogenerados por algoritmos DGA |
| | | Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios. |
| | | Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS |
| | | Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams para detectar posibles intentos de tunelización. |

| | | |
|---|---|---|
| | | Debe permitir como acción ante peticiones DNS maliciosas: alertar, bloquear las conexiones y además responder a la petición con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas. |
| | | Debe poder clasificar los dominios maliciosos en categorías como: malware, DGA, DNS tunneling, Comando y Control, DNS dinámicos, phising o dominios recientemente registrados. |
| | | Debe perimir la acción a tomar dependiendo de la categoría a la que pertenezca el dominio, pudiendo tomar acciones diferentes para cada tipo de categoría. |
| | | La solución debe brindar el contexto de cada dominio incluyendo historial completo para informar el origen y reputación de cada dominio. |
| | | Debe brindar analítica de cada consulta DNS: frecuencia de visita, marca de tiempo, información del DNS pasiva, WHOIS y cualquier etiqueta de malware asociada. |
| | SDWAN | La solución debe contar con una consola de monitoreo con la capacidad de poder identificar fácilmente las aplicaciones y enlaces, sus estados dentro de la red de SD-WAN (aplicaciones con problemas de jitter, latencia, pérdida de paquetes y sus diferentes estados dentro de la red) pudiendo ver el estado de las mismas en por lo menos en los últimos 5 minutos, última hora, último día o bien haciendo filtros personalizados. |
| | | La solución debe contar con la posibilidad de hacer reportes del estado de los enlaces y aplicaciones, indicando volúmenes de datos con respecto a las veces que fueron degradados o afectados. |
| | | Capacidad de poder cambiar dinámicamente de camino al detector alguna degradación del enlace sin afectar o cortar la sesión establecida de la aplicación, es decir, que el usuario no perciba corte en la aplicación o tener que reiniciar la sesión. |
| | | Soportar algoritmo de corrección de errores (FEC - Forward Error Correction) con el objetivo de poder garantizar una experiencia alta en el uso de aplicaciones de voz y video a través de la red de SD-WAN |
| | | Soportar la trasmisión de paquetes duplicados por diferentes enlaces al utilizar la red de SD-WAN con el objetivo de mantener una calidad de experiencia alta al usar aplicaciones de misión crítica y prevenir la pérdida de paquetes, incremento de latencia, jitter, etc. |
| | | Capacidad de monitorear la salud de los enlaces a través de aplicaciones de SaaS y aplicaciones de Cloud, para poder determinar si esas aplicaciones son enviadas a internet de manera directa o bien a través de algún camino a través de la red de SD-WAN. |

## 2. XSIAM

La solución XSIAM es un upgrade de características de las soluciones con la que ya cuenta la entidad (Cortex XDR y Pro Per GB), consiste en una plataforma unificada capaz de gestionar y automatizar el proceso de operaciones de ciberseguridad (XSOAR). La plataforma está basada en Inteligencia Artificial para la detección, triage, investigación y respuesta ante amenazas.

XSOAR RFP + Pro per GB

| **Requerimiento** |
|---|
| Ser una solución auto-contenida, instalada en la Infraestructura de EL CLIENTE, la cual deberá integrarse con otras herramientas y soluciones mediante diferentes medios como ser: API, Correo electrónico, Syslog. Ajuste de almacenamiento (228 GB) para el registro y retención de incidentes. |
| Contar con una plataforma de orquestación, automatización y respuesta, y un amplio conjunto de integraciones con otros sistemas ya desarrolladas (Fuentes de Threat Intelligence, MISP, etc). |
| Contar con una librería de integraciones y automatizaciones con el equipamiento y/o software de los fabricantes más conocidos de la industria. |
| Contar con cifrado de las comunicaciones. |
| Contar con diferentes interfaces para que usuarios ajenos al sistema puedan reportar incidentes sin afectar la licencia (ejemplos: Portal de auto gestión, mail, app, etc.). |
| **Necesidades para analistas** |
| Integración con el SIEM IBM QRadar con el objetivo de interactuar con las ofensas generadas por QRadar bidireccionalmente. |
| Automatización de procedimientos de respuesta a incidentes de forma parcial o total, pudiendo tomar acciones locales o en sistemas remotos. |
| Contar con herramientas de diseño de procedimientos de respuesta de forma gráfica y simple, posibilitando todas las opciones por medio de ayudas contextuales. |
| Contar con una biblioteca de procedimientos de respuesta genéricos pre-cargados y customizables. |
| Categorización de severidad de incidentes automatizada en base a información contextual. |
| Enriquecimiento del incidente agregando datos de diferentes fuentes, tanto propias (del mismo sistema) como de terceros. Ejemplo: Información de actividad maliciosa de una IP dada. |
| Condicionar el acceso a la información contenida en los incidentes dependiendo del rol del usuario. Teniendo en cuenta que el propietario del incidente puede cambiar y por lo que el rol puede cambiar, el sistema deberá adaptar la información disponible para el nuevo propietario del incidente. |

| |
|---|
| Disponibilidad de una interfaz que permita trabajar sobre los incidentes de forma colaborativa. |
| Relacionar incidentes en base a características similares. |
| Buscador de incidentes en base a cualquier característica de estos. |
| Mapeo de incidentes con diferentes frameworks (ejemplo: Mitre Attack). |
| Guiar al analista en la toma de decisiones, siguientes pasos y seguimiento de los procedimientos después de categorizar el incidente. |
| **Necesidades de gestión** |
| Contar con Dashboards personalizables de acuerdo con el rol del usuario. |
| Contar con capacidad de reportería que permita realizar reportes automáticos y/o programados sobre cualquier conjunto de indicadores. |
| Definición de métricas en base a los datos disponibles en los incidentes. |
| Contar con la posibilidad de medir la eficiencia en la respuesta a incidentes, midiendo el tiempo que transcurre entre un conjunto de acciones dadas, tanto sean manuales como automáticas. |
| Gestión de pasaje de turno entre analistas. |
| Contar con capacidad de utilizar los datos almacenados en “reference sets” de QRadar para enriquecer incidentes. |
| Integración con otros sistemas de tickets o de gestión de incidentes (ejemplo: Service Desk, entre otros). |
| Integración con sistemas de CMDB. |
| Generación de indicadores de compromiso en base a los incidentes generados en el sistema. |
| El sistema deberá ser capaz de ser operado a través de la interfaz web, y API. |
| El sistema deberá ser capaz de agregar información a los incidentes mediante correo electrónico. |
| El sistema deberá tener la capacidad de depurar, exportar e importar los incidentes del sistema en base a un criterio dado, manteniendo opcionalmente los indicadores de compromiso asociados a este. |
| **Necesidades de automatización** |
| Generar incidentes en base a reglas de automatización del sistema. |
| Aplicar operaciones en dispositivos de terceros de forma manual o automática. Ejemplo: Aplicar una regla de bloqueo en un Firewall de un fabricante dado, etc. |
| Contar con capacidad de desarrollo para integración con herramientas y soluciones de terceros. |
| Modificar incidentes en base a reglas de automatización. |

| |
|---|
| **Se valorará que se cuente con las siguientes funcionalidades** |
| Recolección automática de evidencia contenida en el incidente (ejemplo: Captura de imagen de las URL contenidas en el incidente, escaneos de URL comparando con fuentes de inteligencia, información sobre direcciones IP, dominios, ASN, etc). |
| Integración con Herramientas tipo SIEM permitiendo ejecutar consultas directamente desde el área de trabajo del analista. |
| Gestión de fuente de inteligencia de amenazas. |
| **Varios** |
| La solución propuesta deberá ser implementada en nube y ofrecida como SAAS en formato llave en mano, donde la empresa proveedora se encargue de suministrar la instalación e implementación del producto ofrecido; así como la documentación y entrenamiento necesario para los siguientes perfiles: administradores, usuarios avanzados y analistas, contemplando todos los requerimientos y licenciamiento de la solución. |
| La implementación de la plataforma XSIAM debe ser llevada a cabo por el área de servicios profesionales del fabricante. |
| Se busca que el proveedor contemple y especifique todos los requerimientos técnicos necesarios para el funcionamiento óptimo de la solución (sistema operativo, base de datos, licencias, hardware/máquinas virtuales, networking). Así como la posibilidad de una instalación en alta disponibilidad y describir las capacidades de escalamiento de la solución. |
| Se solicita indicar el tipo de licenciamiento utilizado y la forma de venta de la solución, así como las posibilidades de crecimiento. Se debe especificar todas las posibilidades de licenciamiento disponibles explicando sus ventajas y desventajas. Deberá indicar qué datos son necesarios proporcionar para dimensionar el licenciamiento de la solución en cada una de las posibilidades. |
| Se deberá especificar el esfuerzo en cantidad de horas tanto del proveedor como de los técnicos de EL CLIENTE para la implementación y puesta en funcionamiento de la solución parametrizada, lista para utilizar. |
| Se deberá incluir dos niveles de capacitación, uno para la administración y gestión de la solución y otro para los analistas. El equipo de EL CLIENTE deberá ser capaz de formar a terceros en el uso de esta, en caso de ser necesario. Los cursos y todos los materiales utilizados deberán estar disponibles para ser utilizados en cualquier momento por EL CLIENTE durante la duración de la licencia de la solución. |
| Se deberá especificar cuáles son los diferentes esquemas de soporte y mantenimiento que puede utilizar la solución, de qué forma se accede al mismo y si es requerida alguna suscripción recurrente para la utilización de misma. |
| Se deberá especificar tiempo esperado de entrega una vez solicitado el producto. |
| **REQUERIMIENTOS DE LA SOLUCION** |
| La solución debe soportar investigaciones interactivas que permitan la colaboración, la revisión histórica y la documentación en tiempo real de todas las acciones. |

| |
|---|
| La solución debe soportar flujos de trabajo y secuencias de comandos modulares. |
| **Automatización** |
| La herramienta debe automatizar las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos. |
| La plataforma debe soportar investigaciones interactivas que permitan colaboración, revisión histórica y ejecución en tiempo real y documentación de todas las acciones. |
| Para cualquier acción de seguridad, debe ofrecer flexibilidad para automatizar manualmente ejecutar en tiempo real según los requisitos del caso de uso. |
| La automatización se debe lograr utilizando flujos de trabajo modulares y scripts. |
| Las tareas automatizadas se deben visualizar en flujos de trabajo basados en interfaz gráfica y ser impulsadas por scripts de automatización en el backend. |
| Cualquier script puede ser adjunta una tarea automatizada dentro de flujos o playbooks visuales. |
| Los flujos de trabajo que la plataforma utiliza para automatizar y ejecutar acciones deben ser compatible al menos con Python y JavaScript, debe tener la capacidad de exportar paquetes de Python a Dockers para que librerías de Python existentes puedan ser reutilizadas. |
| Debe incluir una función "BYOI" similar que permita a los analistas escribir sus propias integraciones a través de un SDK interno y un wizard. |
| La solución debe incluir nuevas integraciones de productos y automatizaciones automáticas comparte de actualizaciones de contenido. |
| La solución debe integrar las funciones de TIM (Threat intelligence Management). Deberá Automatizar y Orquestar las labores de un equipo de Threat Intel. |
| **Integraciones** |
| Herramientas forenses: Debe integrarse con un mínimo de 20 herramientas de anti-malware y forense, entre ellas Any.Run, Palo Alto Networks WildFire, VMRay, etc. |
| Herramientas TI: Debe integrarse con un mínimo de 20 servicios de TI, incluidos Box, Cisco Meraki, EasyVista, McAfee Web Gateway. |
| Herramientas Colaboración: Debe integrarse con un mínimo de 20 herramientas de colaboración incluidas ActiveMQ, Cisco Webex Teams, EWS, FCM PushNotificaciones, Kafka, etc. |
| Herramientas SIEMs: Debe tener integraciones bidireccionales con APIs de SIEM terceros, la herramienta debe recolectar incidentes desde los SIEM, buscar alertas del SIEM durante una investigación y actualizar el SIEM de ser necesario. Debe integrarse con al menos 30 soluciones de SIEM o analítica de logs, entre ellos ArcSight, RSA Netwitness, IBM Qradar, Securonix, Exabeam, LogRythm, Splunk, McAfee ESM y AlienVault |
| Endpoint Security: Debe integrarse con soluciones de punto final, incluidas McAfee, Symantec, Trend, FireEye, Crowdstrike, Cortex XDR, Cylance, Sentinel One, Cisco AMP, CybeReason y muchos más. Debe utilizar los APIs de las soluciones para hacer consultas en los productos, desencadenar nuevos |

| |
|---|
| incidentes, y activar acciones como parte de las acciones de respuesta (como por ejemplo aislar al punto final o matar procesos). |
| Seguridad de red: Debe integrarse con productos de seguridad de Red a través de API bidireccionales para realizar acciones de prevención tales como agregar reglas y desplegar IOCs. Los productos compatibles deben incluir marcas líderes del mercado como, Check Point, Forcepoint, Cisco, Palo Alto Networks, Fortinet y otros. Debe ofrecer la capacidad de agregar más productos de ser necesario. |
| Directorio Activo: Debe proveer todas las acciones permitidas por Directorio Activo vía API. Debe incluir consultar información acerca de usuarios, maquinas, contraseñas que expiran, control de afiliaciones a grupos, etc. Debe integrarse con servidores de email, permitiendo leer los buzones de correo entrante como enviar correos, actualizar usuarios, pedir aprobaciones, ejecutara tareas basadas en respuestas a correos, etc. |
| Threat Intelligence: Debe contar con más de 40 integraciones para enriquecimiento de datos y Inteligencia de amenazas, incluidas todas las principales plataformas de inteligencia de amenazas, incluidos AlienVault, AWS Sagemaker, Anomali, Cisco Umbrella, Palo Alto Networks Autofocus, etc |
| Análisis de malware dinámico: Debe integrarse con productos relacionados con análisis de malware. Debe incluir Lastline, MISP, CrowdStrike, Falcon Sandbox, Palo Alto Networks WildFire y otros. |
| Análisis de Vulnerabilidades: Debe ser compatible con soluciones de assesment de vulnerabilidades como Nssus, Rapid7 y Qualys para proveer enriquecimiento de la información y para disparar acciones de parchado de vulnerabilidades. Debe incluir integraciones con herramientas de monitoreo de nube, como GuardDuty, AWS Security Hub, servicios de compliance como Palo Alto Networks Prisma, servicios de TI (S3, EC2), loggign (CloudTrail, CloudWatch) y otros. |
| Sistemas Desarrollados localmente: Debe permitir crear integraciones propias o customizadas con soluciones locales (home-grown) (ej. portales internos y sistemas de tickets de soporte). |
| **Indicadores de compromiso** |
| La Plataforma debe poder admitir formatos de código abierto estándar como STIX , CSV, JSON, Plain Text |
| La Plataforma debe tener la capacidad de mapear datos de origen al modelo interno de datos TIP y clasificar los datos con una combinación de valores de hash, incluidos MD5, SHA1, SHA256 y SHA512 |
| La plataforma debe facilitar la atribución de amenazas con nombre: mapeo de TTP a actores de amenazas, grupos, y el marco de Mitre Att&ck |
| La plataforma debe poder admitir indicadores personalizados como IBAN, tarjetas de crédito, números de teléfonos celulares y números de identificación |
| Debe permitir al analista buscar indicadores en función de campos como etiquetas, estado o tipo de indicador para llevar a cabo acciones determinada o La plataforma debe automatizar la consolidación de la normalización tanto desde herramientas internas como externas para responder a los ataques en tiempo real |
| La plataforma debe realizar la des duplicación automática de indicadores |

| |
|---|
| La plataforma debe admitir la inclusión de indicadores internos como IP y URL en la lista blanca, para garantizar que no sean marcados como maliciosos |
| **Flujos o playbooks de automatización** |
| La herramienta debe contar con un mínimo de 200 casos de usos y playbooks de respuesta a incidentes |
| Los playbooks deben ser de código abierto y están alojados en GitHub o un repositorio público. |
| Debe permitir crear playbooks copiando flujos existentes, debe poseer una interface sencilla de utilizar que permita realizar drag-and-drop de acciones u otros flujos/playbooks |
| Debe permitir embeber un playbook dentro de otro, de forma de que este sea reutilizado continuamente |
| Un playbook puede contener acciones totalmente automatizadas o tareas manuales, tareas de collection de datos o tareas condicionadas |
| Los playbooks pueden ser ejecutadas automáticamente al crear un incidente y asociando al playbook correspondiente |
| Los playbooks deben poder ser ejecutados como tareas y también ejecutados en tiempo real. |
| La ejecución de los playbooks y la actividad relacionada por el analista debe ser automáticamente documentada para cada incidente de seguridad |
| La herramienta debe de tener la capacidad de ejecutar flujos/playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario |
| Las acciones de los playbooks deben ser totalmente personalizables por el usuario y deben poder utilizarse para adherirse a cualquier requisito de proceso organizacional o industrial. |
| Debe poseer la capacidad de asignar a cualquiera de los usuarios disponibles en el sistema basado en las capacidades RBAC. |
| La herramienta debe tener un API capaz de ejecutar las mismas funciones que la interfaz gráfica |
| **Gestión de Incidentes** |
| La herramienta debe integrarse con sistemas de ticketing de TI, debe ser compatible con Jira, ServiceNow, HP Service Manager, Remedy, etc). |
| Los usuarios pueden hacer comunicación bidireccional con estas herramientas para iniciar acciones de creación de notificaciones (tickets) como también buscar y actualizar notificaciones(tickets) con información de investigación |
| La herramienta debe proveer con una herramienta de ticketing de propósito específico de respuesta a incidentes |
| La herramienta debe soportar la asignación de tickets a usuarios o equipos de trabajo a través de roles de capacidad. Los incidentes pueden ser asignados a un equipo a través de un rol de grupo. |

| |
|---|
| La herramienta debe estandarizar o escalar la administración de SLAs |
| Debe manejar campos obligatorios a ser llenados antes de cerrar un incidente de seguridad |
| Debe enviar notificaciones mediante herramientas de integración de mensajes tales como Okta, Slack y correos sobre cambios en incidentes changes, alertas sla, etc. |
| La notificación debe poder enviarse como parte de los pasos del playbook. O La herramienta debe poder enviar recordatorios para las tareas mientras se crea el playbook. Debe poder fijar SLA y usuario mientras se crea el playbook o Los incidentes pueden ser generados usando fetch trigger en cualquiera de los productos integrados o usando un modelo de push mediante Rest API, adicionalmente también pueden ser creados manualmente. |
| La plataforma debe facilitar la de duplicaciones de incidentes, además mostrar posibles relaciones entre incidentes, y relaciones entre incidentes e indicadores. |
| Debe ofrecer una visión optimizada de cómo se relacionan los ataques en el tiempo, personalizar esa visión para adecuarse a su línea de trabajo, y codificar sus perspectivas para abordar de una mejor manera incidentes similares en el futuro. |
| Debe poseer la capacidad de asignar tags o características personalizables a los incidentes, estas características deberán poder utilizarse para distintos usos, entre ellos medir KPIs, medir estadísticas, ejecutar atomizaciones basadas en ellas, etc. |
| La solución debe permitir la delegación de tareas a otro usuario y asignar SLAs |
| **Documentación** |
| La herramienta debe incluir una instancia donde usuarios puedan ver evidencia y documentación de incidentes anteriores. |
| Debe incluir un War Room donde los incidentes se auto-documenten, ofreciendo una vista detallada de registros basada en una línea de tiempo con cada actividad realizada durante la investigación de un incidente. |
| La herramienta debe detectar alertas redundantes y agregar incidentes duplicados en uno solo, desplegando los datos de la agregación realizada. |
| Como parte de un incidente, la herramienta debe documentar cualquier cambio, los analistas parten del incidente, tareas terminadas, comandos de interacción, evidencia, chats, notas y tareas de playblooks. |
| Los usuarios pueden marcar resultados de comandos o notas como evidencia, o automatizar la recolección de evidencia dentro de un playbook. |
| Toda la información recolectada debe ser inmutable y no debe ser modificada, la documentación debe ser exportable para producir un documento de cadena de custodia. |
| Los analistas deben poder ver todos los indicadores de compromiso y el detalle alrededor de ellos. |
| Los avalistas deben ser capaces de utilizar campos customizados para por ejemplo atribuir indicadores a campañas de ataque. |

| |
|---|
| **Colaboración** |
| El producto debe proveer herramientas de colaboración en tiempo real entre usuarios, debe agrupar a todos los usuarios asociados a un incidente dentro del mismo o en un cuarto de guerra. |
| Debe integrarse con Slack, para que los usuarios de Slack puedan interactuar con los analistas de forma sencilla y ágil. |
| Los analistas deberán poder colaborar uno con otro usando la línea de comando dentro de la investigación de un incidente. |
| La colaboración puede ser extendida a grupos o equipos de trabajo terceros, como usuarios internos, grupos de recursos humanos, PR, o terceros. |
| Las tareas realizadas dentro de incidentes deben de ser respaldadas para que sirvan de documentación para entrenar a nuevos analistas. |
| La herramienta debe incluir un Canvas o mapa de investigación, el cual mediante machine learning pueda crear un mapa de ataques en tiempo real o Los resultados de los canvas deben ser exportados y compartidos por equipos ejecutivos e interesados. |
| **Indicadores de compromiso** |
| El producto debe correlacionar bidireccionalmente indicadores e incidentes. Los usuarios deben poder ver todos los indicadores de un incidente y viceversa. |
| La plataforma debe incluir playbooks de threat intel managment, que puedan ser ejecutados utilizando indicadores de compromiso. |
| Debe ser posible importar y exportar indicadores en archivos STIX y CSV o Debe poseer la capacidad de customizar la estructura de la información de los indicadores. |
| La plataforma debe poder crear whitelist so listas blancas de indicadores. |
| **Machine Learning** |
| La solución debe incluir aprendizaje dinámico de los IOCs e incidentes que se investigan y ayudar a los analistas a identificar incidentes que pueden estar relacionados. |
| La solución debe ser capaz de sugerir próximos pasos de acuerdo con el aprendizaje de maquina realizado durante investigaciones previas. |
| Debe ser capaz de aprender qué analistas son contactados usualmente por tipo de incidente y puede sugerir a los nuevos analistas a quien ellos pueden querer contactar para recibir ayuda. |
| **Arquitectura y administración** |
| |
| La solución debe soportar un despliegue en nube, capaz de conectarse a las premisas del cliente |
| La solución debe poder ser completamente SaaS, y capaz de conectarse con las premisas del cliente. |

| |
|---|
| La solución debe ofrecer Control de Acceso Basado en Rol (RBAC por sus siglas en idioma inglés) así como también el mapeo de roles a los grupos en el Directorio Activo o SAML. Los roles se corresponden con permisos granulares con inclusión de leer/escribir, leer solamente, y acceso denegado a varias áreas de la solución. |
| Debe incluir la capacidad de generar informes de incidentes, informes de estadísticas (tales como MTTR – tiempo medio de resolución) y los resúmenes o informes por incidente. |
| Debe soportar informes programados y asociarse a una lista de distribución de correos, y el motor de informes debe ser compatible con formatos PDF, DOC y CSV. |
| Debe ofrecer monitoreo y gráficos enfocados tanto a los analistas, así como a los incidentes, con el objetivo de que los CISOs y gerentes puedan medir la salud del SOC, productividad de los analistas y severidad y alcance de incidentes |
| La plataforma no limita el número de acciones, tareas, incidentes, indicadores, playbooks u otra acción operativa. La licencia debe basarse sólo en Usuarios Nombrados. |
| La plataforma debe realizar procesos automáticos preventivos y proactivos. Estos procesos deben ejecutarse con una frecuencia programada y sin necesidad de que un incidente se manifieste como tal. |
| La función de Live Backups debe ser soportada. |
| Con el fin de realizar desarrollos de manera segura la solución deberá contar con un ambiente de desarrollo ajeno al ambiente de producción. |
| - Personalizar la visualización de los indicadores: Deberá proporcionar formas escalables y personalizables para ver los datos de información sobre amenazas, permitiendo a los usuarios obtener un contexto de datos procesables. |
| - Integraciones abiertas y extensibles: La plataforma deberá permitir a los usuarios editar integraciones de productos de terceros existentes, así como agregar nuevas integraciones por sí mismos. |
| - Convergencia de incidentes y datos de indicadores: la plataforma deberá grabar y capturar automáticamente todos los indicadores presentes en los incidentes ingeridos. |
| **Automatización** |
| La plataforma permitirá ejecutar playbooks frente a un conjunto de indicadores especificados por el usuario. La plataforma también permitirá a los clientes dirigir indicadores hacia dispositivos de seguridad de tercero |
| La Plataforma permitirá a los clientes ejecutar playbooks personalizadas ante indicadores nuevos/editados/quitados |
| La plataforma proporcionará diversos playbooks listos para usar, para análisis de inteligencia de amenazas. Por ejemplo, análisis de indicadores en masa. |
| La plataforma permitirá ver y personalizar todos los códigos fuente de automatizaciones, en caso de ser necesario |

**3. Renovación VM y Panorama**

Se requiere la renovación de VM´s y Panorama existente actualmente

Paso de firewall PA-450 OSS a producción en HA con PA-450 activo: Se requiere suministro e instalación de licencia para equipo actual de 450 que se encuentra en On site Spare a High Availability.

**4. Renovación Cortex**

| Cantidad | Descripción |
|---|---|
| 250 | PAN-XDR-ADV-EP (303 days) Cortex XDR Pro for 1,endpoint, includes 30 days of data retention and standard success |
| 165 | PAN-XDR-PRO-GB (303 days) Cortex XDR Pro for daily ingested GB. Includes 30 days of ingested data retention, 180 days of alerts and incidents retention and standard success |
| 250 | PAN-XDR-HOST-INST Host Insights add-on for Cortex XDR |
| 250 | PAN-XDR-XTH Extended Threat Hunting (enhanced visibility) add-on for Cortex XDR ProEP/Cloud (price per Endpoint). Includes 30 days of data retention. |

## 5. SERVICIO DE IMPLEMENTACIÓN

La propuesta debe incluir la definición de la arquitectura a implementar, así como la orientación de ésta a las aplicaciones que la utilizarán, es la garantía para que la red cumpla con su cometido de suministrar una plataforma flexible, altamente disponible y orientada al negocio, es por ello por lo que en esta etapa se realizará la validación del diseño propuesto y el afinamiento del plan de migración de los servicios. Se debe describir el alcance del servicio.

## 6. SOPORTE

El soporte opera las 24 horas, los 7 días de la semana.

## 7. TRANSFERENCIA DE CONOCIMIENTO Y CURSOS

### 7.1 Transferencia de conocimiento

Se debe incluir transferencia de conocimiento de la plataforma implementada para máximo 6 personas de manera virtual con una duración de 4 horas divididas en 2 sesiones de máximo 2 horas cada una. El material de trabajo serán los documentos de diseño y cierre del proyecto.

### 7.2. Cursos

La propuesta debe incluir seis cupos para cursos digitales en modalidad e-learning (un cupo por persona). Estos cursos deben tener mínimo vigencia de seis (6) meses luego de su activación. Los cursos propuestos deben estar relacionados con la tecnología implementada.

### 7.3. Consideraciones de los cursos

- Curso avalado por el fabricante o el organismo certificador.
- Material oficial del curso, en formato digital, en idioma español.
- Laboratorios y/o actividades establecidas por el fabricante u organismo certificador correspondiente.

## 8. CONSIDERACIONES GENERALES

### 8.1. Premisas fuera del alcance del proyecto

- Actividades de logística de personal y equipos, adecuaciones de cualquier índole (físicas, eléctricas, ambientales, cableado, etc.), diferentes a las establecidas explícitamente en este documento no están incluidas.
- Problemas que se puedan presentar por actividades paralelas o de terceros, sobre los equipos o software relacionados en este proyecto.

- El alcance del proyecto no involucra el suministro de cableado, fibras o módulos SFP no descritos en este documento, los servicios pueden ser prestados bajo oferta adicional la cual incluirá estudio en sitio previo a ajuste de cantidades requeridas.

- Se deberá manifestar la Garantía de fabrica los equipos suministrados la cual no debe ser inferior de UN (1) año

**PLAZO**

El plazo de ejecución del contrato es hasta el treinta y uno (31) de diciembre de 2025, contados a partir de la aprobación de la garantía contractuales por parte de la Unidad de Gestión Jurídica de la ESU.

El plazo del contrato podrá ser modificado antes de su vencimiento mediante documento suscrito por las partes, previa verificación de la necesidad o conveniencia por parte del supervisor, teniendo en cuenta el cumplimiento del contrato, los precios y las condiciones de ejecución del contrato.

**VALOR**
El valor del presente contrato asciende a la suma de **TRES MIL CIENTO SETENTA MILLONES SEIS MIL QUINIENTOS SESENTA Y DOS PESOS M/CTE. ($3,170,006,562) IVA INCLUIDO**

**TITULAR DESTINATARIO**
Los bienes y/o servicios antes descritos son con destino a la Secretaria de Seguridad y Convivencia del Distrito, en virtud del Contrato Interadministrativo de administración delegada de recursos No. 4600105849 de 2025 del contrato interadministrativo suscrito con Secretaria de Seguridad del Distrito de Ciencia, Tecnología e Innovación de Medellín.

**FORMA DE PAGO**
La ESU cancelará el valor del contrato mediante pagos parciales; con el soporte de activación renovación, previo recibo a entera satisfacción por parte del supervisor del contrato.

- ✓ La respectiva factura debe cumplir con los requisitos de las normas fiscales establecidas en el Artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato y, el concepto del bien o servicio que se está cobrando.
- ✓ Las retenciones en la fuente a que hubiere lugar y todo impuesto, tasa, estampilla o contribución directa o indirecta, Nacional, Departamental o Municipal que se cause con ocasión del contrato serán a cargo exclusivo del contratista.
- ✓ Una vez recibida a satisfacción la factura o cuenta de cobro correspondiente, la ESU tendrá treinta (30) días calendario para proceder a su pago. En caso de incurrir en mora en los pagos,
- ✓ Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aporte de sus empleados al Sistema de Seguridad Social Integral y a las Entidades que administran recursos de naturaleza parafiscal; y la carta donde se especifique la Entidad y el número de cuenta bancaria a la cual se le deberá realizar el pago.
- ✓ Para el caso de proveedores que se encuentren obligados a facturar electrónicamente, la facturación deberá ser remitida al correo electrónico facturacion@esu.com.co y la fecha límite para la recepción de las mismas estará sujeta a las fechas definidas en la circular 01 del 08 de enero de 2025 documento donde adicionalmente se define la elaboración del recibo a satisfacción por parte del supervisor designado y el proceso de cierre contable en calidad de empresa industrial y comercial del estado.

**CRUCE DE CUENTAS**
Con la firma del presente contrato el contratista autoriza a la ESU, para que al momento de efectuar cualquier pago a su nombre, de manera automática y sin previo aviso, la ESU realice cruce de cuentas para compensar los dineros que el contratista adeuda a

la Entidad por cualquier concepto, salvo que sobre los mismos se tenga suscrito un acuerdo de pago entre las partes.

**LUGAR DE EJECUCIÓN**
La entrega de todos los bienes se hará en el Distrito de Medellín- secretaria de seguridad y convivencia o en el sitio que le defina la ESU, previa coordinación con el supervisor del contrato.

**GARANTÍA CONTRACTUAL**
El Contratista se obliga a constituir a favor de "**La Empresa para la Seguridad y Soluciones Urbanas - ESU y Distrito Especial de Ciencia, Tecnología e Innovación de Medellín –Secretaria de Seguridad y Convivencia**", una garantía única de las expedidas para Entidades estatales que ampare el cumplimiento de las obligaciones contractuales, otorgada por una compañía de seguros autorizada para operar en Colombia por la Superintendencia Financiera y preferiblemente con poderes decisorios en la Ciudad de Medellín, de acuerdo con la siguiente tabla:

| AMPARO | SUFICIENCIA | VIGENCIA |
|---|---|---|
| Cumplimiento | 20% | Con una vigencia igual a la duración del contrato y un (1) año más. |
| Calidad del bien (Solo para el hardware) | 20% | Con una vigencia igual a la duración del contrato y un (1) año más. |
| Salarios y Prestaciones Sociales | 5% | Con una vigencia igual a la duración del contrato y tres (3) Años más. |

**PARÁGRAFO 1**: El contratista deberá modificar el monto de la garantía cada vez que sea necesario, debido al incremento del contrato o la afectación por reclamaciones. Si el contratista se negare a constituir o a reponer la garantía exigida, la ESU directamente solicitará a la Compañía de Seguros la modificación de la misma, además podrá dar por terminado el contrato en el estado en que se encuentre, sin que haya lugar a reconocer o pagar indemnización alguna.

**PARÁGRAFO 2**: Al recibo del contrato, el contratista contará con máximo dos (2) días hábiles para la constitución de la póliza única de cumplimiento y entrega de la documentación respectiva.

**COMPRA PÚBLICA INNOVADORA, SOSTENIBLE Y SOCIALMENTE RESPONSABLE**

El contratista garantiza que durante la vigencia del contrato cumplirá con los lineamientos establecidos de ley y por la ESU sobre la compra pública innovadora, sostenible y socialmente responsable, siempre que aplique. Para tal fin presentará la evidencia correspondiente en los informes de ejecución mensuales previa coordinación con el supervisor del contrato Se deberá tener como referencia las siguientes consideraciones durante la ejecución, sin limitarse a estos cuando de lugar.

Se deberá tener como referencia las siguientes consideraciones durante la ejecución, sin limitarse a estos cuando de lugar.

**Socialmente responsable:**

- ✓ Contar con un plan de capacitación, políticas y procedimientos en temáticas relacionadas con Derechos Humanos, socializado en su personal y partes vinculadas e interesadas, fomentando el conocimiento, respeto, promoción y aplicación de las obligaciones de derechos humanos.

**OBLIGACIONES DEL CONTRATANTE**

La ESU en desarrollo del presente contrato tendrá los siguientes derechos y deberes: **1)** Exigir al contratista la ejecución idónea y oportuna del objeto contratado. **2)** Actualizar y adoptar las medidas necesarias cuando se produzcan fenómenos que alteren en su contra el equilibrio económico o financiero del contrato, previo informe del supervisor, sobre la ocurrencia de tales hechos. **3)** Adelantar las acciones conducentes a obtener la indemnización de los daños que sufran en desarrollo o con ocasión del contrato. **4)** Ejercer las acciones a que haya lugar, por las situaciones administrativas de la Entidad, como consecuencia del presente contrato. **5)** Pagar oportunamente al contratista el valor del contrato, de conformidad con lo establecido en el contrato. **6)** Facilitar al contratista lo necesario para la adecuada ejecución del objeto contractual.

**OBLIGACIONES DEL CONTRATISTA**

El contratista en desarrollo del presente contrato tendrá los siguientes derechos y obligaciones: **1)** Recibir oportunamente el pago estipulado en el contrato. **2)** Cumplir de buena fe con el objeto del presente contrato, de conformidad con la propuesta adjunta, la cual hace parte integral del contrato y en los términos del Código Civil. **3)** Designar un representante para efectos de facilitar y agilizar el manejo de la información entre las partes. **4)** Presentar los informes requeridos sobre la ejecución del contrato. **5)** Presentar las observaciones y recomendaciones para el buen desarrollo del contrato. **6)** Cumplir con el objeto contractual acordado en la forma, cantidad, lugar, fechas y especificaciones requeridas por la ESU. **7)** Constituir las garantías que le sean exigidas en el presente contrato y mantenerlas vigentes por el tiempo estipulado por la ESU. **8)** Acreditar el pago de aportes parafiscales y seguridad social para cada uno de los pagos. **9)** Acatar los requerimientos y observaciones que con ocasión de la ejecución del contrato le hagan el supervisor y/o la contratante. **10**) Considerar que las relaciones contractuales están basadas en el reconocimiento, seguimiento de las reglas, principios de la ética y la buena fe contractual; en un ambiente de respeto y de confianza que genere valor para las partes y para la sociedad en general. **11)** Rechazar las prácticas corruptas y delictivas en general; se prevendrá y combatirá el fraude, el soborno, la extorsión y otras formas de corrupción. **12)** Tanto en el desarrollo de los proyectos y procesos, como en su área de influencia, el contratista promoverá prácticas que reflejen la protección y conservación del medio ambiente, el respeto al pluralismo democrático, a las minorías étnicas, a la equidad de género y a los derechos humanos en general. **13)** Velar por el respeto de la dignidad en las condiciones de trabajo por parte de sus contratistas y subcontratistas, por lo que no se avalarán prácticas discriminatorias, trabajo forzado o de menores. **14)** Cumplir con las políticas de prevención que eviten la utilización y explotación sexual de niños, niñas y adolescentes en el desarrollo de sus actividades comerciales, así como a no contratar menores de edad en cumplimiento de

los pactos, convenios y convenciones internacionales ratificados por Colombia, según lo establece la Constitución Política de 1991 y demás normas vigentes sobre la materia, en particular aquellas que consagran los derechos de los niños. **15)** Las demás que tengan relación directa con la naturaleza y objeto del presente contrato.

**SUPERVISIÓN**
La supervisión del Contrato será realizada por el Profesional Universitario de la Subgerencia de Servicios, o quien sea designado por el funcionario competente. Al Supervisor le corresponderá realizar el seguimiento administrativo, técnico, financiero, contable, jurídico del contrato. En todo caso la designación podrá hacerse directamente por el Gerente.

**INDEMNIDAD**
De conformidad con el reglamento de contratación de la ESU **e**l Contratista se obliga a indemnizar a la Entidad con ocasión de la violación o el incumplimiento de las obligaciones previstas en el presente Contrato. El Contratista se obliga a mantener indemne a la ESU de cualquier daño o perjuicio originado en reclamaciones de terceros que tengan como causa sus actuaciones hasta por el monto del daño o perjuicio causado y hasta por el valor del presente Contrato. Igualmente, el Contratista mantendrá indemne a la Entidad por cualquier obligación de carácter laboral, o relacionadas que se originen en el incumplimiento de las obligaciones laborales que el Contratista asume frente al personal, subordinados o terceros que se vinculen a la ejecución de las obligaciones derivadas del presente Contrato.

**CLÁUSULA PENAL PECUNIARIA**
De conformidad con el artículo 1592 del Código Civil Colombiano, las partes convienen que en caso de incumplimiento del contratista en las obligaciones del contrato, o de la terminación del mismo por hechos imputables a él, pagará a la ESU en calidad de cláusula penal pecuniaria una suma equivalente al diez por ciento (10%) del valor total del contrato. El valor pactado de la presente cláusula penal es el de la estimación anticipada de perjuicios, no obstante, la presente cláusula no impide el cobro de todos los perjuicios adicionales que se causen sobre el citado valor. Si lo anterior no fuere posible, se cobrará por la vía judicial. Las partes convienen, conforme lo establece el artículo 1600 del código civil, que podrá pedirse a la vez la pena y la indemnización de perjuicios a que hubiere lugar.

**EXCLUSIÓN DE RELACIÓN LABORAL**
El contratista ejecutará el objeto de este contrato con plena autonomía técnica y administrativa, sin relación de subordinación o dependencia, por lo cual no se generará ningún tipo de vínculo laboral.

**CESIÓN DEL CONTRATO**
EL contratista no podrá ceder total o parcialmente su posición contractual sin la autorización previa, expresa y escrita de la ESU. EL contratista tampoco podrá ceder total o parcialmente derechos u obligación contractual alguna sin la autorización previa, expresa y escrita de la ESU.

**UTILIZACIÓN DE MECANISMOS DE SOLUCIÓN DIRECTA EN LAS CONTROVERSIAS CONTRACTUALES**

La ESU y el contratista buscarán solucionar en forma ágil, rápida y directa las diferencias y discrepancias surgidas de la actividad contractual. Para tal efecto, al surgir las diferencias acudirán al empleo de los mecanismos de solución de controversias contractuales, a la conciliación, a la amigable composición o a la transacción. En todo caso, la implementación de los anteriores mecanismos estará supeditada a la necesidad del servicio por parte de la ESU o de sus clientes.

**CONFIDENCIALIDAD**

En caso de que exista información sujeta a alguna reserva legal, las partes deben mantener la confidencialidad de esta información, la cual deberá estar previamente marcada como tal, para ello, debe comunicar a la otra parte que la información suministrada tiene el carácter de confidencial. Cada una de las partes acuerda mantener la confidencialidad de la información Confidencial de la otra parte durante un periodo de tres años contados a partir de la fecha de revelación.

**TERMINACIÓN**

El presente contrato se podrá dar por terminado por las siguientes causas: 1) Cuando se alcance y se cumpla el objeto del contrato. 2) Por mutuo acuerdo de las partes. 3) Cuando por razones de fuerza mayor o caso fortuito se haga imposible el cumplimiento del objeto contractual. 4) Por el incumplimiento administrativamente declarado por parte de la ESU de cualquiera de las obligaciones establecidas en el contrato. 5) Por vencimiento del término fijado para la ejecución del mismo. 6) Por las demás causales señaladas en la Ley.

**LIQUIDACIÓN**

El contrato será objeto de liquidación dentro de los cuatro (4) meses siguientes a su terminación.

Dentro de este plazo, las partes acordarán los ajustes, revisiones y reconocimientos a que haya lugar, de los cuales quedará constancia en el acta de liquidación. Si es del caso, para la liquidación se exigirá al CONTRATISTA la ampliación de la vigencia de los amparos y garantías para avalar las obligaciones que deba cumplir con posterioridad a la extinción del contrato.

En todo caso la liquidación del contrato estará sujeta a las disposiciones del reglamento de contratación de la ESU.

**INHABILIDADES E INCOMPATIBILIDADES**

El contratista con la firma del presente contrato declara bajo la gravedad de juramento que no se encuentra incurso en ninguna de las inhabilidades e incompatibilidades consagradas en la Constitución y la Ley. La contravención a lo anterior dará lugar a las sanciones de ley.

**TRATAMIENTO DE DATOS**

El contratista asume la obligación de proteger los datos personales a los que acceda con ocasión del contrato, así como las obligaciones que como responsable o encargado le correspondan acorde con la Ley 1581 de 2012 y sus decretos reglamentarios en cuanto le sean aplicables. Por tanto, deberá adoptar las medidas de seguridad, confidencialidad, acceso restringido y de no cesión en relación con los datos personales a los cuales accede, cualquiera que sea la forma de tratamiento. Las medidas de seguridad que deberán adoptarse son de tipo lógico, administrativo y físico acorde a la criticidad de la información personal a la que accede y/o recolecta, para garantizar que este tipo de información no será usada, comercializada, cedida, transferida y no será sometida a tratamiento contrario a la finalidad comprendida en lo dispuesto en el objeto contractual. En caso de tratarse de datos sensibles, de niños, niñas y adolescentes, tales como origen racial, organizaciones sociales, datos socioeconómicos, datos de salud, entre otros, las medidas de seguridad a adoptar serán de nivel alto. El contratista aportará, para la formalización del contrato, copia de su Política de Protección de Datos Personales y de Seguridad de la Información a la ESU, la cual deberá dar cumplimiento a lo establecido en las disposiciones referente a protección de datos personales. El contratista, con la presentación de la oferta manifiesta que conoce la Política de Protección de Datos de la ESU y que, de ser aceptada la oferta en el proceso del asunto, acepta y se compromete a dar cumplimiento a lo establecido en ella y demás protocolos establecidos por la ESU para el tratamiento de datos personales. Igualmente, El contratista se compromete a informar y hacer cumplir a sus trabajadores las obligaciones contenidas en esta cláusula y las demás que contenga la normativa referente a la protección de datos personales, asimismo los trabajadores de El contratista deben conocer y aceptar la Política de Protección de Datos Personales de la ESU. El contratista indemnizará los perjuicios que llegue a causar a El contratante como resultado del incumplimiento de las leyes 1266 de 2008 y 1581 de 2012, aplicables al tratamiento de la información personal, así como por las sanciones que llegaren a imponerse por violación de la misma. El incumplimiento de las obligaciones derivadas de esta cláusula se considera como un incumplimiento grave por los riesgos legales que conlleva el indebido tratamiento de datos personales, y en consecuencia será considerada justa causa para la terminación del contrato, y dará lugar al cobro de la cláusula penal pactada, sin necesidad de ningún requerimiento, a los cuales renuncia desde ahora

**IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SG - SST)**

El contratista deberá encontrarse en las adaptaciones que den lugar para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), de conformidad con el Decreto 1072 de 2015, así como sus modificaciones y los documentos que los complementen. En todo caso previo el inicio de la ejecución del contrato, el contratista deberá presentar las evidencias de las acciones realizadas en la implementación del mencionado, y el cumplimiento de la tabla de valores de la Resolución 0312 de 2019 del Ministerio del Trabajo.

**DOCUMENTOS DEL CONTRATO**

1- Disponibilidad y compromiso presupuestal. 2- Cedula de Ciudadanía. 3- Propuesta presentada por el contratista. 4- RUT. 5- Certificado de Existencia y Representación legal. 6- Certificado de paz y salvo aportes al sistema de seguridad social y parafiscal. 7- Certificado de antecedentes disciplinarios. 8- Certificado de antecedentes fiscales. 9. Certificado de antecedentes judiciales. 10- Registro Nacional de Medidas Correctivas - RNMC. 11- SPVA-44 - Consulta de Inhabilidades de la Ley 1918 de 2018 y Decreto 753 de 2019 - 12- Demás documentos que se deriven del presente contrato.

**NATURALEZA JURÍDICA DEL CONTRATO**

Este Contrato se rige por las normas comerciales y civiles, y especialmente, por el Reglamento de Contratación de la Entidad, expedido por la Junta Directiva de la ESU.

**DOMICILIO**

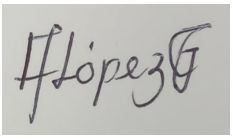
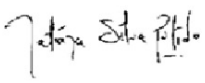
El domicilio contractual es el Distrito de Medellín

**POR LA ESU,**

**MATEO GONZÁLEZ BENÍTEZ**
Gerente ESU

**POR EL CONTRATISTA,**

**LUIS JOSÉ IGNACIO QUINTERO CUSGUEN**
Representante Legal

| | | | |
|---|---|---|---|
| Aprobó | Kamal Abdul Nassar Montoya | Secretario General |  |
| Aprobó | Angélica María López Garcés | Subgerente de Servicios |  |
| Aprobó | Nathalia Restrepo Caro | Subgerente Administrativa y Financiera |  |
| Revisó | Luis Miguel García Rendon | Profesional Universitario - Unidad de Gestión Jurídica |  |
| Proyectó | Tatiana Silva Pulido | Profesional Especializado -Unidad de Compras y Contratación. |  |