

## ANEXO No 01 ESPECIFICACIONES TECNICAS

### LOTE 1 COMPUTADORES

<b>Nombre Comercial del Producto</b>	<b>COMPUTADOR TIPO 1- MADS</b>
<b>Calidad</b>	Norma Energy Star: Debe cumplir con la norma Energy Star 6.0, Gold EPEAT y ROHS, Green Guard
<b>Generalidades</b>	Computadores personales que sean diseñados para ser usado en una ubicación fija, en un escritorio, color negro, soporte para montaje compatible VESA
<b>Requisitos Generales</b>	La CPU, teclado y mouse serán de la misma marca de los equipos ofertados. Deben ser equipos tipo all in one, corporativo.
	Cada equipo debe tener software de administración propietario del fabricante que permita el soporte para recuperación de datos de restauración con las siguientes funcionalidades: <ul style="list-style-type: none"> <li>✓ Software de Respaldo con derecho de uso del fabricante que permita restauración de la maquina a su estado original de fábrica.</li> <li>✓ Restauración de la máquina, recuperación de la información seleccionable por el usuario sin requerir de la apertura del sistema, posibilidad de realizar copia de seguridad a medio externo tales como Disco USB, CD/DVD, Red, Disco secundario o Disco Local.</li> </ul>
	Soporte y garantía: 3 años por: partes o maquinaria, servicio de Hardware en sitio luego del diagnóstico remoto, cambio de partes o componentes en caso de falla.
<b>Requisitos Específicos</b>	Color negro de escritorio, fuente de poder interna con conexión directa a la fuente de alimentación, y dos (2) altavoces de 2W cada uno o superior.
	Procesador Intel Core i 7 de sexta generación, frecuencia de reloj base de 3.4Ghz 4 núcleos, 8MB caché
	Chip de seguridad TPM versión 1.2 o superior integrado a la board o superior
	Memoria RAM 8 GB crecimiento mínimo a 16GB DDR4 a 2133 MHz
	Disco Duro de 500 GB 7200RPM de 2.5" con sistema de encriptación (AES-256) de datos para una partición del disco o las que se requieran
	Tarjeta de red integrada a la tarjeta principal de 10/100/1000RJ-45
	Gráficos integrados compatible DirectX 12. 1Gb mínimo de direccionamiento dinámico, Pantalla: Mínimo 23.8" No Touch, FHD (1920x1080) TFT color, ángulo de visión 89°, panel LCD panorámico con formato 16:9 y retroiluminación LED, 250 nits, 1000:1 contrast ratio, anti-reflejo. Cámara integrada, El stand debe permitir grado de inclinación fr -5 a 60 grados, 90 grados de giro y una altura de 110 mm. O similar.
	Fuente de poder interna de máximo 180 watts con eficiencia mínimo del 85% o 90%
	Unidad óptica DVD+/-RW interna, con Bandeja de carga automática (DVD+/-RW), lectura y escritura de DVD
	Un Puerto Paralelo, No PS/2, Puertos de audio Un puerto combinado de auriculares y micrófono de 3.5mm, puertos de USB: 4 puertos USB 2.0, 2 puertos USB 3.0, VGA No, Un puerto Display Port, Audio HD de mínimo 2.1, certificado DOLBY AUDIO, Sonido interno Parlantes internos de mínimo 2 de 2W cada uno
	Mouse USB óptico de la misma marca del equipo sin publicidad
	2 Pad mouse de color negro con soporte para muñeca por cada equipo
	Teclado Multimedia español de la misma marca del equipo
	Sistema operativo Windows ® 10 Professional 64 Bits OEM con licencia y llave de activación incorporada en la BIOS (OEM Activation 3.0 (OA3)), en español última versión liberada en el mercado, con el servicepack última versión en español. Los equipos a entregar deberán tener instalado el sistema operativo Microsoft Windows 10 64 Bits Professional (con último Service pack disponible) a través de derechos de downgrade.
	Patch Cord de tres (3) metros de fábrica termoformado categoría seis A(6A),
<b>Empaque y Rotulado</b>	Cada uno de los equipos será entregado con sus respectivas cajas individuales y

	Manuales técnicos, manuales de operación, cargador, interfaces de conexión software de configuración(drivers) en medios digitales originales para cada uno de los componentes del equipo que garanticen su pleno funcionamiento. Los manuales deben contener idioma español
	Los computadores deben tener un sticker adhesivo con el nombre de la empresa que suministra los equipos y el número del contrato de comisión.
	Los equipos serán entregados y probados (Procedimientos básicos de encendido, cargue de sistema operativo, reconocimiento de dispositivos instalados, verificación de configuración, instalación de software), No se aceptan equipos remanufacturados o refurbished
<b>Presentación</b>	Unidad

## LOTE 2 (SIEM)

Nombre Comercial del Producto	SISTEMA SIEM
<b>Requisitos Generales</b>	<p>Se requiere una plataforma del tipo Next Generation - Security Information and Event Manager (Next Generation SIEM) que permita coleccionar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad.</p> <p>La plataforma deberá Colectar los eventos de seguridad de múltiples marcas para lo cual se deberá incluir el licenciamiento necesario para esto y los servicios descritos en el numeral 2.</p> <p>La plataforma deberá tener la capacidad de comportarse como una herramienta del tipo CMDB.</p> <p>La plataforma deberá monitorear los cambios en los archivos de configuración de los servidores que la entidad defina.</p> <p>La plataforma deberá ser del tipo Virtual Appliance con el fin de que la entidad pueda asignar recursos virtuales a la misma a medida que se requieran.</p> <p>La solución deberá con un sistema de bases de datos híbrida, lo que quiere decir que esté basado en NoSQL y SQL, no se aceptan soluciones basadas únicamente en motores de bases de datos del tipo SQL, esto con el fin de que soportar grandes volúmenes de datos sin afectar la estabilidad de la solución.</p> <p>La solución deberá soportar características multi-tenancy</p> <p>La plataforma al ser un SIEM de nueva generación deberá contar con características NOC y SOC, por lo cual deberá realizar:</p> <ul style="list-style-type: none"> <li>▪ Actualización constante de la base de datos de contextos, configuraciones, software instalado y servicios corriendo de los dispositivos monitoreados.</li> <li>▪ Análisis constante el desempeño de las aplicaciones lo cual permita realizar una clasificación (triage) de la seguridad.</li> <li>▪ Visor personalizado de log de tráfico.</li> <li>▪ Herramienta de búsqueda sobre los logs de tráfico.</li> </ul> <p>La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante, licenciamiento a tres años, con actualizaciones.</p> <p>Se requiere Capacitación Certificada por el Fabricante en la administración avanzada de esta plataforma para 3 empleados de la entidad, los exámenes y demás materiales requeridos para obtener dicha certificación, deberán estar totalmente incluidos en la oferta.</p>
<b>Desempeño</b>	<p>La solución de SIEM debe dar soporte a las siguientes características mínimas:</p> <ul style="list-style-type: none"> <li>▪ Numero de Dispositivos 50.</li> <li>▪ Numero de Eventos por Segundo (EPS): 1000</li> <li>▪ HyperVisor Soportado: VMWare ESXi 5.5 o Superior</li> <li>▪ Número de Agentes Windows Avanzados: 50</li> </ul> <p>Nota: la entidad suministrara el hardware y entorno de procesamiento requerido para la implementación de la solución.</p>
	<ul style="list-style-type: none"> <li>▪ Deberá tener la capacidad coleccionar archivos de configuración de red de los dispositivos monitoreados, almacenada en un repositorio de versiones.</li> <li>▪ Deberá tener la capacidad de Colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones.</li> <li>▪ Deberá contar con la característica de detección automática de los cambios en la configuración de red de las plataformas monitoreadas.</li> <li>▪ Deberá contar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas.</li> <li>▪ Deberá contar con la característica de detección automática en cambios en archivos y</li> </ul>

<p><b>Funciones de Monitoreo y Disponibilidad.</b></p>	<p>carpetas, de las plataformas Windows y Linux monitoreadas, donde se detalle el "Quien" y el "Que".</p> <ul style="list-style-type: none"><li>▪ Deberá contar con la característica de detección automática basada en agente, de cambios en el registro de los sistemas Windows monitoreados.</li><li>▪ Deberá contar con la característica de Monitoreo del sistema via SNMP, WMI y PowerShell.</li><li>▪ Deberá contar con la característica de Monitoreo de aplicaciones via JMX, WMI y PowerShell.</li><li>▪ Deberá contar con la característica de Monitoreo de Hipervisor tales como VMWARE y Hype-V.</li><li>▪ Deberá poder Monitorear plataformas de almacenamiento tales como EMC, NetAPP, Nutanix, Nimble, etc a nivel de desempeño y uso de almacenamiento.</li><li>▪ Deberá poder Monitorear sistemas del tipo Directorio Activo y Exchange basado en WMI y PowerShell.</li><li>▪ Deberá poder Monitorear motores de Bases de datos SQL Server, Oracle, MySQL entre otras via JDBC.</li><li>▪ Deberá poder Monitorear Infraestructura VoIP via IPSLA, SNMP, CDR y CMR.</li><li>▪ Debe realizar Análisis del desempeño y flujo de las aplicaciones via NetFlow, Sflow, Cisco AVC y NBAR.</li><li>▪ Debe tener la Capacidad de definir métricas customizadas.</li><li>▪ Debe tener la Capacidad de detectar desviaciones de una línea base de la infraestructura monitoreada.</li><li>▪ Debe tener la Capacidad de monitorear dispositivos del entorno tales como Liebert UPS, HVAC, FPC y APC.</li><li>▪ Deberá monitorear las caídas e inicios de los sistemas via Ping, SNMP, WMI, así como análisis del inicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage.</li><li>▪ Deberá hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos.</li></ul>
--------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p><b>Dispositivos y Aplicaciones Soportados</b></p>	<p>La solución deberá soportar al menos las siguientes plataformas a nivel de monitoreo de seguridad y de rendimiento:</p> <p><b>Antivirus</b></p> <ul style="list-style-type: none"> <li>• Kaspersky</li> <li>• Symantec Endpoint Protection</li> <li>• McAfee EPO</li> <li>• Trend Micro OfficeScan</li> <li>• Trend Micro Intrusion Defense Firewall (IDF)</li> <li>• Sophos Endpoint Security and Control</li> <li>• ESET NOD32</li> <li>• Cisco Security Agent (CSA)</li> <li>• Entre otros</li> </ul> <p><b>Application Servers</b></p> <ul style="list-style-type: none"> <li>• Microsoft ASP.NET</li> <li>• Oracle WebLogic</li> <li>• IBM WebSphere</li> <li>• Red Hat JBoss</li> <li>• Sun GlassFish</li> <li>• Apache Tomcat</li> <li>• Entre otros</li> </ul> <p><b>Authentication Servers</b></p> <ul style="list-style-type: none"> <li>• Cisco Access Control Server (ACS)</li> <li>• Juniper Steel-Belted Radius</li> <li>• Microsoft Internet Authentication Service (IAS)</li> <li>• Alcatel AAA RADIUS</li> </ul> <p><b>Blade Servers</b></p> <ul style="list-style-type: none"> <li>• Cisco Unified Computer System (UCS)</li> <li>• HP BladeSystem</li> <li>• Dell Blade Server</li> <li>•</li> </ul> <p><b>Cloud Services</b></p> <ul style="list-style-type: none"> <li>• Amazon EC2</li> <li>•</li> </ul> <p><b>Databases</b></p> <ul style="list-style-type: none"> <li>• IBM DB2</li> <li>• MySQL</li> <li>• Microsoft SQL Server</li> <li>• Oracle Database Server</li> </ul> <p><b>Directory Services</b></p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory 2000, 2003, 2008, 2012</li> <li>•</li> </ul> <p><b>DNS/DHCP Servers</b></p> <ul style="list-style-type: none"> <li>• Infoblox DNS/DHCP</li> <li>• BIND DNS</li> <li>• Linux DHCP</li> <li>• Microsoft DHCP/DNS 2003, 2008</li> </ul> <p><b>Email</b></p> <ul style="list-style-type: none"> <li>• Microsoft Exchange</li> <li>• Postfix Mail Server</li> <li>• Sendmail</li> <li>•</li> </ul> <p><b>Environmental</b></p> <ul style="list-style-type: none"> <li>• APC UPS</li> <li>• Liebert UPS, HVAC, FPC</li> <li>• APC NetBotz</li> <li>• Generic UPS</li> <li>•</li> </ul> <p><b>File Monitoring</b></p> <ul style="list-style-type: none"> <li>• Linux</li> <li>• Microsoft Windows</li> </ul>
------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Dispositivos y Aplicaciones  
Soportados**

**Firewalls**

- Cisco ASA, IOS
- Cisco Firewall Services Module (FWSM), Private Internet eXchange (PIX)
- Juniper Networks Secure Services Gateway (SSG), Integrated Security Gateways (ISG)
- Palo Alto Networks
- Check Point FireWall-1, Provider-1, IPSO
- Check Point VSX
- Fortinet FortiOS
- Linux ipchains
- McAfee Enterprise (Sidewinder)
- Dell SonicWALL SonicOS
- WatchGuard
- Microsoft Internet Security and Acceleration (ISA) Server
- Astaro

**Hardware Monitoring**

- Dell servers
- HP servers
- IBM servers
- VMware ESX servers
- Network devices
- Storage devices

**Host OS**

- Microsoft Windows 2000, 2003, 2008, 2012, XP, Vista, Windows 7
- CentOS Linux
- Fedora Linux
- Red Hat Linux
- Debian Linux
- SUSE Linux
- HP-UX
- IBM AIX
- IBM OS/400
- Oracle Solaris, SunOS

**Internet Security Gateways**

- Blue Coat ProxySG
- Cisco IronPort Mail and Web
- Barracuda Spam Firewall
- FortiGate
- McAfee Web Gateway
- Websense Web Filter
- Websense Email Security Gateway
- Microsoft Internet Security and Acceleration (ISA) Server
- Squid
- Untangle Secure Gateway
- Astaro Security Gateway

**Network Intrusion Prevention Systems (IPS)**

- Cisco IPS
- Snort IPS
- FortiGate
- FireEye
- Juniper IDP
- IBM Security/ISS SiteProtector
- McAfee IntruShield
- HP TippingPoint Next-Generation Intrusion Prevention System (IPS)
- Check Point SmartDefense
- ForeScout
- SourceFire IPS appliances and DefenseCenter

**Load Balancers / Application Firewall**

- F5 BIG-IP Local Traffic Manager
- F5 BIG-IP WebAccelerator
- F5 BIG-IP Application Security Manager
- Citrix NetScaler

<p><b>Dispositivos y Aplicaciones Soportados</b></p>	<p><b>Network Flow</b></p> <ul style="list-style-type: none"> <li>• Cisco NetFlow v5, v9</li> <li>• sFlow</li> <li>• Cisco Application Visibility and Control (AVC)</li> </ul> <p><b>Routers and Switches</b></p> <ul style="list-style-type: none"> <li>• Cisco IOS, Nx-OS, CatOS</li> <li>• Juniper Junos</li> <li>• Alcatel-Lucent TiMOS, AOS</li> <li>• Brocade/Foundry IronWare</li> <li>• HP ProCurve</li> <li>• Cisco MDS</li> <li>• Avaya (Nortel) ERS, Nortel Passport</li> <li>• HP/3Com Comware</li> <li>• Huawei VPR</li> <li>• Extreme ExtremeWare XOS</li> <li>• Mikrotik Router</li> </ul> <p><b>Storage</b></p> <ul style="list-style-type: none"> <li>• EMC Data Domain</li> <li>• EMC Isilon</li> <li>• EMC VNX</li> <li>• NetApp Data ONTAP Filer</li> <li>• EMC CLARiiON</li> <li>• EMC VNX</li> <li>• Dell EqualLogic</li> <li>• VMware and Host attached storage</li> </ul> <p><b>Virtualization</b></p> <ul style="list-style-type: none"> <li>• VMware ESX, ESXi, vSphere, vCenter</li> </ul> <p><b>Wireless LAN</b></p> <ul style="list-style-type: none"> <li>• Cisco WLAN</li> <li>• Aruba ArubaOS</li> <li>• NetMotion Mobility XE</li> </ul> <p><b>Vulnerability Scanners</b></p> <ul style="list-style-type: none"> <li>• McAfee Foundstone</li> <li>• Qualys QualysGuard</li> <li>• Rapid7 Nexpose</li> <li>• Tenable Nessus</li> <li>• nCircle</li> </ul>
<p><b>Protocolos Soportados</b></p>	<p>La solución deberá soportar los siguientes protocolos de colección y/o monitoreo:</p> <ul style="list-style-type: none"> <li>▪ Web – HTTP/HTTPS</li> <li>▪ DNS</li> <li>▪ FTP/SCP</li> <li>▪ Generic TCP/UDP</li> <li>▪ ICMP</li> <li>▪ IMAP4</li> <li>▪ JDBC</li> <li>▪ LDAP</li> <li>▪ POP3</li> <li>▪ POP3S</li> <li>▪ SMTP</li> <li>▪ SOAP</li> <li>▪ SSH</li> <li>▪ Telnet/SSH</li> <li>▪ SNMP</li> <li>▪ WMI</li> <li>▪ JMX</li> </ul>

<b>Características de Análisis de Seguridad en Tiempo Real.</b>	<p>El módulo de analítica de eventos de seguridad deberá cumplir con mínimo las siguientes características:</p> <ul style="list-style-type: none"> <li>▪ Deberá soportar la Correlación de Eventos de múltiples fuentes, tales como Firewalls, UPS, Servidores, estaciones de trabajo entre otros.</li> <li>▪ Deberá soportar Correlación cruzada de eventos.</li> <li>▪ Integración por medio de API's con fuentes de información externa sobre amenazas, tales como Dominios de Malware, IPs, URLs, Hash y Nodos de Tor</li> <li>▪ Integración Nativa con fuentes de información de terceros tales como ThreatStream, CyberArk, SANS y Zeus</li> <li>▪ Deberá tener la Capacidad de Colección de logs, parsing de logs, indexación de logs a una tasa de 10.000 EPS.</li> <li>▪ Capacidad de hacer Monitoreo de la Integridad de Archivos o FIM basada en agente tanto para Windows como Linux.</li> <li>▪ Deberá tener la capacidad de modificar los parsers por medio de interface gráfica, sin que esta modificación afecte la colección de logs o genere caídas en los servicios de la solución.</li> <li>▪ Deberá permitir la creación de Parsers customizados a partir de platillas XML.</li> <li>▪ Deberá tener la capacidad de Colectar logs de forma segura, desde dispositivos remotos.</li> <li>▪ Deberá contar con un framework de notificación de incidentes el cual deberá estar basado en políticas.</li> <li>▪ Deberá tener la capacidad de ejecutar scripts de remediación cuando un incidente ocurra.</li> <li>▪ Deberá contar con un sistema propio de tickets</li> <li>▪ Deberá tener la capacidad de integrarse con sistemas de tickets externos en caso que la entidad lo requiera, dicha integración deberá ser por API y mínimo deberá soportar ServiceNow, ConnectWise, and Remedy.</li> <li>▪ Debe ser capaz de detectar anomalías en la línea base definida.</li> <li>▪ La detección de incidentes deberá ser en tiempo real anterior al almacenamiento del evento, utilizando técnicas del tipo "Correlación Distribuida".</li> <li>▪ Deberá contar con una consola de visualización de logs y eventos correlacionados la cual cuente con un sistema para el filtrado de los mismos por medio de condiciones Booleanas.</li> <li>▪ Deberán poder realizarse filtros por medio de expresiones regulares.</li> <li>▪ El reporte de incidentes deberá poder ser priorizado por los servicios críticos.</li> <li>▪ Deberá permitir la identificación dinámica de usuarios.</li> </ul>
<b>Administración y Reportes</b>	<p>La solución deberá contar con las siguientes características de administración y reportes:</p> <ul style="list-style-type: none"> <li>▪ La plataforma deberá poder ser administrada vía HTTPS.</li> <li>▪ La plataforma deberá tener una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas y tablas, lo cual permita tener una visión global de los incidentes de seguridad.</li> <li>▪ La comunicación de los módulos deberá ser asegurada por temas de confidencialidad por medio de HTTPS.</li> <li>▪ Deberá contar con un módulo para el cálculo de los SLA.</li> <li>▪ Deberá contar con un módulo grafico que muestre la infraestructura existente, las conexiones de las mismas y los eventos generados en cada activo.</li> <li>▪ Deberá contar con un dashboard que permita identificar en un mapa los incidentes y su ubicación geográfica.</li> <li>▪ Deberá contar con un módulo para administrar las políticas de correlación.</li> <li>▪ Deberá contar con un módulo para la administración de los agentes.</li> <li>▪ Deberá contar con un módulo de administración para la característica de CMDB.</li> <li>▪ La plataforma deberá tener un gran número de reportes predefinidos y deberá permitir crear reportes customizados.</li> </ul>
<b>Servicios Profesionales y de Soporte</b>	<p>El oferente deberá entregar la plataforma en Bogotá DC, en la Calle 37 No 8 -40.</p> <p>El oferente deberá realizar la instalación y configuración de los equipos con personal que cuente con experiencia en soluciones de seguridad.</p> <p>La implementación deberá comprender los siguientes puntos.</p> <ul style="list-style-type: none"> <li>▪ Planeación de cada una de las actividades con el fin de disminuir los tiempos de implementación de la solución.</li> <li>▪ Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.</li> <li>▪ Planeación de la implementación a realizar asesorando a la entidad en el alcance de la correlación de seguridad a realizar en los dispositivos que se acuerden.</li> <li>▪ Planeación de la implementación a realizar asesorando a la entidad en el alcance del monitoreo a realizar en los dispositivos que se acuerden</li> <li>▪ Creación de los conectores necesarios para un correcto monitoreo/correlación de las plataformas que se requieran.</li> <li>▪ Desarrollar un plan de pruebas que permita garantizar la correcta operación del sistema integrado a la infraestructura actual.</li> </ul>

	<ul style="list-style-type: none"> <li>El oferente deberá presentar una certificación suscrita a través de su representante legal dirigida al, Ministerio de Ambiente donde conste que debe incorporara al proyecto el siguiente equipo de trabajo exigido:</li> </ul> <p>1. Un Líder de servicio o Gerente de Proyecto: Un ingeniero de sistemas electrónico o de telecomunicaciones, con mínimo 5 años de experiencia en instalaciones, soporte y/o mantenimiento en soluciones de seguridad o de red, específicamente en Implementación de sistemas SIEM. Para el cumplimiento del objeto contractual tendrá una dedicación de 50%.</p> <p>2. Dos (2) Ingenieros de Soporte certificados expertos en la solución ofertada, Ingenieros de sistemas, electrónicos o de telecomunicaciones, con mínimo 3 años de experiencia en instalaciones, soporte y/o mantenimiento en soluciones de seguridad o de red, específicamente en Implementación de SIEM. Para el cumplimiento del objeto contractual tendrá una dedicación de 100 % cada Uno.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### LOTE 3 (SOLUCION DE BALANCEO DE SERVIDORES Y ENLACES)

Nombre Comercial del Producto	
<b>SOLUCION DE BALANCEO DE SERVIDORES Y ENLACES ADC</b>	
<b>Requisitos Generales</b>	<p>Contar con una solución de balanceo de servidores y de enlaces que permita mejorar el desempeño de las mismas y al mismo tiempo generar un esquema de alta disponibilidad, donde se deberán ofrecer listas ya incluidas para ser utilizadas, las funcionalidades que se detallan en el presente documento.</p> <ul style="list-style-type: none"> <li>Solución en alta disponibilidad, dos equipos de la misma referencia funcionando en modo clúster.</li> <li>El dispositivo debe ser un equipo de propósito específico.</li> <li>Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.</li> <li>La solución debe ser desarrollada por el fabricante y no debe incluir desarrollos de terceros</li> </ul>
<b>Rendimiento</b>	<p>El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:</p> <ul style="list-style-type: none"> <li>Rendimiento Capa 4: 15 Gbps</li> <li>Rendimiento Capa 7: 12 Gbps</li> <li>Rendimiento Compresión: 8Gbps</li> <li>Conexiones por Segundo SSL: 12.000</li> <li>Transacciones por Segundo Capa 7: 600.000</li> <li>Dominios Virtuales: 5</li> </ul>
<b>Conectividad</b>	<p>El equipo deberá contar con las siguientes interfaces de conexión como mínimo, con sus respectivos conectores o licenciamiento en caso de ser necesario:</p> <ul style="list-style-type: none"> <li>4 puertos de 10Gbps SPF+.</li> <li>4 puertos de 1Gbps SPF.</li> <li>4 puertos de 1Gbps RJ45.</li> </ul>



**Funcionalidades básicas mínimas de Balanceo.**

- La solución debe estar diseñada para proveer aceleración en Layer-4 y Layer-7
- La solución debe ser capaz de balancear tráfico ICMP, UDP, TCP y poseer entendimiento de protocolos como HTTP/s, FTP y RADIUS.
- La solución debe ser capaz de balancear carga de manera transparente o utilizando NAT basándose en información obtenida de Layer-7 como URL, Cookie, SSL ID, etc.
- La solución debe poseer distintos métodos de balanceo como round robin, weighted round robin, least connection y shortest response
- La solución debe ser capaz de hacer routing/switching inteligente de contenido en Layer-7 basándose en la información enviada por el cliente (URL, HTTP header, cookie, URL, etc)
- La solución debe proveer persistencia en Layer-4 basándose en la dirección IP de origen y puerto. Adicionalmente la persistencia en Layer-7 debe poder ser configurada basándose en la información del cliente como URI, HTTP headers, hostname, SSL session ID y Cookies.
- La solución debe ser capaz de hacer SSL Offloading
- La solución debe ser capaz de realizar balanceo entre datacenters (GSLB)
- La solución debe poseer la capacidad de proteger aplicaciones y servidores de ataques SYN-Flood y cantidad de conexiones. Además debe ser capaz de integrar tabla de conexiones statefull para IPv4 e IPv6.
- La solución debe poder ser administrada vía interfaz gráfica (GUI) e interfaz de línea de comandos (CLI)
- La Solución propuesta deberá proveer alta disponibilidad, failover transparente y escalabilidad para las aplicaciones
- La solución propuesta deberá permitir la creación de hasta 23 dominios virtuales mínimo.
- tener un puerto dedicado para un failover rápido entre dos unidades de menos de un segundo, soporte de configuración activo-activo o activo-pasivo, todas las direcciones IP virtuales de las aplicaciones deberán ser soportadas por un clúster virtual, la configuración se deberá sincronizar entre las unidades pertenecientes al clúster. Failover automático cuando los servicios reales se encuentren abajo en alguna unidad, el tiempo de failover deberá ser programable
- La solución propuesta deberá contar con un servicio de protocolo virtual de para los siguientes protocolos HTTP, HTTPS, TCP, TCPS, FTP, FTPS, UDP, DNS, SIP UDP, SIP TCP, RTSP, RDP, IP, L2IP, este servicio virtual también deberá funcionar en modo proxy reverso, proxy transparente y proxy en modo de triangulación
- La solución propuesta deberá reenviar los paquetes IP a diferentes destinos MAC para distribuir la carga a nivel de capa 2 puerto físico, a nivel de capa 3 dirección IP y rango de puertos TCP/UDP
- La solución propuesta deberá ofrecer un sistema de almacenamiento de contenido Web completamente integrado con funcionalidades de HTTP/HTTPS, compresión y funciones de administración de tráfico para almacenar y enviar objetos validando las peticiones de los clientes sin tener que consultar a los servidores reales acelerando la respuesta de las aplicaciones, reduciendo el ancho de banda y la carga de los servidores. Deberá proveer estadísticas detalladas del acceso al cache basándose en IP o en http hosts como mínimo, las coincidencias de los objetos almacenados podrán estar basadas en URL parciales. Deberá tener reglas configurables para tamaño máximo de objetos, TTL y la forma de acceso, soporte del set de caracteres extendidos
- La solución propuesta deberá tener un sistema de compresión dinámico en línea basado en hardware, en donde de forma automática deberá comprimir archivos de texto, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT y XLS, también deberá contemplar reglas para no comprimir URL seleccionados que contengan RegEx y objetos web seleccionados para el servicio virtual seleccionado y proporcionar estadísticas detalladas de la compresión.
- La solución propuesta deberá tener un sistema de aceleración de SSL basado en hardware soportando HTTPS, NNTPS, SMTPS, POPs, IMAPS y LDAPS. Soporte de SSLv3 y TLSv1 con un cifrado máximo de 2048-bits, redirección automática de HTTP a HTTPS, deberá poder actuar como servidor de SSL o como cliente de SSL al mismo tiempo, hasta 64 servicios virtuales podrán utilizar el mismo certificado. La única limitante para el almacenamiento de certificados digitales será el espacio en disco de la unidad. Autogeneración de peticiones de firma de certificados (Certificate Signing Request. CSR) para un host específico. Los certificados y llaves privadas podrán ser importados a través de TFTP soportando los formatos OpenSSL/Apache, \*.PEM", "MS IIS, \*.PFX", y "Netscape, \*.DB por lo menos

## Servicios Profesionales y de Soporte

- Instalación, Implementación y puesta en marcha de las soluciones ofertadas.
- El oferente deberá entregar los equipos en Bogotá DC. En la Calle 37 No 8 - 40
- Todas las plataformas ofertadas deberán ser mono marca
- El oferente deberá realizar la instalación y configuración de los equipos con personal certificado en un nivel profesional.
- La implementación deberá comprender los siguientes puntos.
  - Planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación en el servicio.
  - Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
  - Implementación de la solución de acuerdo a las mejores prácticas de los fabricantes, incluyendo la configuración del balanceo de los servidores y aplicativos que la entidad defina, el balanceo de los enlaces que la entidad determine y demás características soportadas por la solución, en la cuales el oferente deberá preguntar expresamente a la entidad, si se requiere o no activar las mismas explicando claramente el beneficio de hacerlo o no.
  - Pruebas de Servicio de las plataformas ofertadas.
  - Puesta en Producción de las plataformas ofertadas.
  - Estabilización de las plataformas ofertadas.
  - Entrega de la solución a satisfacción de la entidad.
- Dentro de los servicios se debe tener en cuenta la Instalación, configuración y puesta en producción de los dispositivos ofertados, así como la entrega a satisfacción de los mismos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para la entidad
- Las actividades de instalación, configuración y puesta en producción de las plataformas ofertadas, deberán ser realizadas por personal certificado por el fabricante
- El contratista deberá garantizar soporte y garantía para los Dispositivos Ofertados en un esquema 7 x 24 por 3 años en sitio.
- La entidad requiere que se realicen pruebas de detección para validar la correcta configuración de la plataforma implementada.
- El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil.
- Se deben incluir en la oferta actividades periódicas de mantenimiento preventivo con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.
- El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:
  - Revisar y afinar, las plataformas ofertadas.
  - Revisar la consistencia de los Backups realizados a la solución implementada. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en forma escrita.
  - Configurar, afinar y/o revisar las herramientas de reportes y almacenamiento de Logs.
  - Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante sin costos adicionales.
- El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.
- El oferente debe contemplar una capacitación en modalidad de transferencia de conocimientos para 3 funcionarios de la entidad, la cual debe incluir como mínimo temas de administración, Monitoreo y resolución de problemas de las plataformas objeto del presente contrato.
- El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios entre otros requerida para que el personal asignado al proyecto, pueda cumplir sus funciones.
- El oferente deberá presentar una certificación suscrita a través de su representante legal dirigida al, Ministerio de Ambiente donde conste que debe incorporar al proyecto el siguiente equipo de trabajo exigido:
  1. Un Líder de servicio o Gerente de Proyecto: Un ingeniero de sistemas electrónico o de telecomunicaciones, con mínimo 5 años de experiencia en instalaciones, soporte y/o mantenimiento en soluciones de balanceo de servidores y de enlaces, con una disponibilidad de 50%.
  2. Dos (2) Ingenieros de Soporte certificados especialistas en la solución ofertada, Ingenieros de sistemas, electrónicos o de telecomunicaciones, con mínimo 3 años de experiencia en instalaciones, soporte y/o mantenimiento en soluciones de balanceo de servidores y de enlaces, con una disponibilidad de 100% cada uno.

## LOTE 4 (IMPRESORAS PORTATILES)

<b>Nombre Comercial del Producto</b>	<b>IMPRESORAS PORTATILES</b>
<b>Calidad</b>	<p>Impresión: Negro (óptima) Renderización de hasta 600 x 600 dpi (Desde PC)</p> <p>Color (óptima) Resolución optimizada de hasta 4800 x 1200 dpi en color</p>
<b>Cantidad</b>	<b>2 UNIDADES</b>
<b>Generalidades</b>	<p>El equipo ofertado debe incluir los cartuchos de impresión iniciales y por lo menos 2 kit originales de repuesto (2 insumos multicolor y 2 insumos de blanco y negro).</p> <p>El equipo ofertado debe incluir su respectivo Adaptador CA original y su cable de alimentación</p> <p>Velocidad de impresión: Negro: Hasta 22 ppm Color: Hasta 18 ppm</p> <p>Capacidad: Hasta 500 paginas mensuales con la batería cargada</p> <p>Tecnología de inyección: Inyección térmica</p> <p>Velocidad del procesador: 200 MHz</p> <p>El equipo deberá imprimir a doble cara</p> <p>Capacidad hasta de 3 sobres</p> <p>Duración Batería: 3 horas por lo menos</p> <p>Memoria Estándar: 64 MB</p> <p>Capacidad Bandeja del papel: 50 Hojas mínimo</p> <p>Conectividad estándar: USB 2.0, 1 PictBridge, 1 Bluetooth 2.0 + EDR.</p> <p>Capacidad inalámbrica: Bluetooth 2.0 + EDR</p> <p>Alimentación: Voltaje de entrada: 90 a 132 VCA, 47 a 63 Hz; 180 a 264 VCA, 47 a 63 Hz</p> <p>Consumo de energía: 40 watts máximo, 15 watts (activa), 0,34 watts (apagado manual), 5,8 watts (en espera), 2,6 watts</p> <p>Tamaño de soporte de impresión: A4; A5 ; A6; B5 (JIS); C6; DL; L; 2L</p> <p>Soporte y garantía: 1 año de garantía ilimitada con respaldo del fabricante</p> <p>El equipo ofertado debe tener la capacidad de imprimir desde dispositivos móviles</p>
<b>Compatibilidad</b>	<p>La impresora deberá ser compatible con los siguientes sistemas operativos:</p> <p>Microsoft® Windows® 8, Windows® 7, Windows Vista® (x32 y x64), Windows® XP Professional x32, Windows® Server 2003, Windows® Server 2008</p> <p>Mac OS X v 10.5 o superior, OS X Lion, OS X Mountain Lion</p> <p>Windows Mobile® 5.0, 6.x para Pocket PC, Linux</p>
<b>Empaque y Rotulado</b>	<p>Cada uno de los equipos será entregado con sus respectivas cajas individuales y Manuales técnicos, manuales de operación, cargador, interfaces de conexión software de configuración (drivers) en medios digitales originales para cada uno de los componentes del equipo que garanticen su pleno funcionamiento. Los manuales deben contener idioma español</p>

	Los equipos deben tener un sticker adhesivo con el nombre de la empresa que suministra y el número de identificación del mismo.
	Los equipos serán entregados y probados (Procedimientos básicos de encendido, cargue, verificación de configuración, instalación de software).