ANEXO 1. ESPECIFICACIONES TECNICAS MINIMAS DEL SERVICIO

Se requiere realizar la renovación de la Management Checkpoint del Data Center de ICETEX – Dirección General, que se integren a la infraestructura de seguridad perimetral actual. La solución debe estar en sus últimas versiones liberadas al mercado. La solución debe quedar completamente instalada e integrada con la siguiente plataforma de seguridad:

- Firewall **Checkpoint** en Data Center Principal (2).
- Firewall **Checkpoint** en Data Center Alterno (1).
- Firewall **Checkpoint** en Data Center Aguas (2)

La Management que se encuentra en operación tiene los siguientes consumos:

- Memoria(GB): 3.5 --- capacidad 3.8
- Consumo Memoria SWAP(GB): 2.3
- CPU 1: 99%
- CPU 2: 98%
- Almacenamiento /var/log: 90% de consumo almacenando solo logs del mes de Octubre
- Número máximo de Logs que maneja la MGMT per Sec: 3,000 Logs
- Número máximo de Logs que maneja la MGMT per day (GB): 3.5
- Firewall administrados: 5

La solución debe contemplar lo siguiente:

Ítem	Descripción Técnica
1.1	La Solución debe permitir la creación de perfiles de administradores, basados en roles, que accedan a secciones parciales de administración o a la totalidad, indicando también si los perfiles son de solo lectura o lectura/escritura.
1.2	Las comunicaciones establecidas entre todos los componentes de la Solución, como así también con los dispositivos administrados, debe ser encriptada con certificados propios.
1.3	La Solución debe ser del mismo fabricante que los actuales elementos/appliances de seguridad perimetral desplegados en la entidad.
1.4	La Solución debe funcionar como una CA (Certificate Authority) interna, administrando una infraestructura PKI. Siendo capaz de administrar relaciones de confianza con entidades certificantes externas.
1.5	La herramienta debe incluir una herramienta de búsqueda, que permita filtrar los objetos configurados, las reglas, los usuarios y grupos de usuarios, objetos duplicados o en uso, valido para todo aquel objeto aplicado a la política de seguridad,
1.6	La Solución debe permitir segmentar la política de seguridad con etiquetas o títulos de sección.
1.7	La Solución debe permitir realizar cambios en la configuración establecida sin impactar directamente, hasta que sea indicado por el administrador la aplicación de los cambios realizados.
1.8	La Solución debe permitir integrarse con otros fabricantes a través de API REST.
1.9	La Solución debe poseer la capacidad de funcionar en alta disponibilidad, sincronizando con los sistemas de seguridad perimetral, siendo del mismo fabricante y con compatibilidad de las versiones de software de estos sistemas.
1.10	La Solución debe permitir integrarse con Active Directory u otro servidor de seguridad (RADIUS; TACACS) para proveer autenticación de administradores.

1.11	Debe poderse integrar con un directorio LDAP, para autenticar y administrar usuarios, basados en el perfil almacenado en el LDAP.
1.12	La Solución debe integrar en una única consola gráfica segmentando el estado general de todos los dispositivos administrados, la configuración de la política de seguridad, los logs registrados y el monitoreo de toda la plataforma de seguridad perimetral.
1.13	La Solución debe poder enviar alertas a nivel de consola, correo electrónico, SNMP, syslog.
1.14	La Solución debe ser licenciada para administrar 5 dispositivos de seguridad perimetral (gateway) en forma centralizada, pudiéndose incrementar los dispositivos a administrar mediante el agregado de licencias adicionales.
1.15	La Solución de gestión centralizada no debe tener ningún límite de licencia por usuarios, por IP, por cantidad de logs generados por día, por cantidad de eventos generados por día o por almacenamiento consumido.
1.16	La Solución debe proveer una funcionalidad de auditoría de cambios.
1.17	La Solución debe proveer un acceso por sesiones de administradores, para el trabajo concurrente de los mismos.
1.18	La Solución debe permitir hacer la “apropiación” de una sesión de otro administrador.
1.19	La Solución debe permitir importar logs en formato syslog (RFC 3164).
1.20	La Solución debe estar licenciadas para almacenar logs por día y eventos correlacionados sin límite de almacenamiento.
1.21	La gestión de la solución debe ser desplegada en alta disponibilidad.
Administración de la política de seguridad	
2.1	La política de seguridad debe permitir crear reglas con los siguientes campos: Nombre, Origen, Destino, VPN, Servicio/Aplicación, Contenido, Log.
2.2	La política de seguridad debe ser integrada por objetos que indiquen un cliente de la red, un grupo de clientes de la red, una anidación de grupos, objetos dinámicos de direcciones IP, objetos de tipo DNS, usuarios, grupos de usuarios, roles y nombres de equipos registrados en el DNS.
2.3	La herramienta debe permitir administrar todas las funcionalidades de seguridad de los dispositivos de seguridad.
2.4	La herramienta debe proveer integración con Active Directory o LDAP o RADIUS para utilizar objetos de dominio como integrantes de las reglas de la política de acceso.
2.5	La herramienta debe permitir administrar toda la configuración de los accesos remotos de VPN y las VPNs de Sitio a Sitio.
2.6	La herramienta debe permitir el acceso concurrente de administradores, la modificación de la política de seguridad, la publicación de los cambios realizados antes de aplicarlos y la segregación de funciones según el administrador.
2.7	La herramienta debe permitir “impactar” la política según criterio del administrador, es decir, luego de generar un cambio, iniciar un flujo de instalación de política.
2.8	La herramienta debe permitir realizar modificaciones en la configuración sin aplicar los cambios inmediatamente.
2.9	La herramienta debe validar y verificar los cambios en las políticas de seguridad, antes de permitir la aplicación de los cambios.
2.10	La herramienta debe integrar un control de cambios y flujo de aprobación de dos etapas para los técnicos y administradores.
2.11	La herramienta debe incluir una opción de análisis de reglas según las mejores prácticas de seguridad.
2.12	La herramienta debe permitir especificar cuando generar un log por la conexión o por la sesión.
2.13	La herramienta debe permitir generar alertas, snmp traps o enviar un correo, además de loguear el tráfico que hace “match” con una regla de la política de seguridad.
Logs, Monitoreo y Provisionamiento	
3.1	Los logs, deben ser parte del mismo sistema de administración (incluido en el Servidor de Administración de la seguridad perimetral)

3.2	Debe proveer los logs de los dispositivos de seguridad y los registros de auditoria de los usuarios.
3.3	Los logs deben ser transmitidos encriptados entre los dispositivos de seguridad y el servidor de administración de seguridad centralizada.
3.4	Debe poder asociar cada IP correspondiente a usuarios internos con su correspondiente nombre de usuario y nombre de máquina.
3.5	Debe incluir una interfaz gráfica de monitoreo, que facilite la revisión del estado de los dispositivos de seguridad.
3.6	Debe incluir una interfaz gráfica de supervisión integral y unificada de los dispositivos de networking que forman parte de la plataforma de seguridad, visualizar el estado de cada dispositivo, obtener información gráfica acerca de su comportamiento y proveer alertas e indicadores de performance.
3.7	Debe proveer información del estado del hardware físico o virtual, de las transacciones de networking y el estado del licenciamiento del software.
3.8	Debe proveer el status e información detallada de cada uno de los componentes de cada dispositivo de red, el estado de los servicios que está ejecutando e información estadística de cada componente.
3.9	Debe permitir visualizar contadores de tráfico, mostrando información detallada de las transacciones que están realizando los dispositivos de red, con los servicios asociados, los protocolos, orígenes, destinos, la posibilidad de personalizar estos contadores y guardar las consultas, y generar de forma automática una lista con filtros según el contador y el ítem seleccionado.
3.10	Debe permitir visualizar contadores de sistema, mostrando información detallada de los servicios de software que están activos en la plataforma, el consumo de performance del sistema, el histórico de estos servicios y la posibilidad de crear nuevas consultas.
3.11	Debe incluir el estado de todas las conexiones de VPN del tipo site-to-site, visualizando información detallada de la conexión, los dispositivos que forman parte de la conexión, el tipo de seguridad de la conexión y permitiendo tomar acciones de reinicio del túnel.
3.12	Debe incluir el estado de todas las conexiones de VPN del tipo Client-to-Site, visualizando el usuario que estableció la conexión con información detallada relevante como por ejemplo el software del sistema operativo, la versión del software de cliente VPN, la IP de origen, la fecha y hora de conexión, el tipo de seguridad del túnel de VPN, y permitir tomar acciones de reinicio del túnel.
3.13	Debe poder reconocer funcionamientos inadecuados y problemas de conectividad entre dos puntos conectados a través de una VPN, alertar y crear logs cuando el túnel de VPN se encuentre abajo.
3.14	Debe permitir realizar actualizaciones de software, manuales o automáticas sobre los dispositivos de seguridad administrados a las últimas versiones disponibles.
3.15	Debe permitir descargar manualmente o en forma automática los nuevos paquetes de software disponibles del fabricante.
3.16	Debe permitir verificar el estado de las licencias de los dispositivos, actualizarlas con el fabricante en forma sincronizada hacia el portal de gestión del fabricante.
3.17	Debe permitir generar informes de soporte y generar casos de soporte.
3.18	Debe permitir administrar de forma centralizada la configuración del sistema operativo de los dispositivos de networking que forman parte de la plataforma de seguridad.
3.19	Debe permitir crear perfiles de configuración que permitan modificar las interfaces, el ruteo estático, los servidores de DNS, los nombres de dominio, los host de DNS, los hostnames y configuraciones de backup.
3.20	Debe permitir verificar el estado del software de un dispositivo, identificar la versión del paquete de software, distribuir un paquete de software, ejecutar de forma manual o automática la actualización del sistema operativo o de un paquete de software.
3.21	Debe incluir la habilidad de enviar y ejecutar scripts en unos o más dispositivos de seguridad administrados centralizadamente.

3.22	Debe poderse programar backups en uno o más dispositivos de seguridad.
3.23	Debe poder generar reportes de cambios realizados durante una sesión, para control del administrador y de los auditores.
3.24	Debe poder generar reportes de cambios realizados entre 2 sesiones diferentes, resumiendo todos los cambios realizados en el período de tiempo entre ambas sesiones.
3.25	Debe contar con la opción de forzar el administrador a que deba requerir la aprobación de un gerente o supervisor antes de permitir la instalación de políticas.
3.26	Debe mantener una base indexada de logs, pudiendo realizar rápidas búsquedas de logs con sintaxis estilo “google like”, agregando estadística agrupadas por los filtros de la misma búsqueda, procesando toda la información en tiempo real.
3.27	Debe permitir verificar la auditoría de los cambios realizados a la interfaz gráfica, según el usuario, la hora y la fecha y el cambio realizado.
3.28	Los logs recibidos en el servidor de administración deben ser indexados para esta a disposición del administrador.
3.29	Se debe permitir utilizar búsquedas rápidas que tengan un historial de las búsquedas mas usadas.
3.30	La indexación de logs debe permitir generar estadísticas de los orígenes, destinos, servicios, protocolos, funcionalidades, usuarios que sean los que generan mas logs.
3.31	Debe ser posible exportar la política de seguridad en un formato HTML.
3.32	Debe ser posible importar objetos desde un archivo CSV.
Consolidación de Eventos y Reportes	
4.1	La herramienta de consolidación de Eventos y Reportes debe ser desplegada en un appliance independiente con conexión segura a los appliances de Administración
4.2	Debe permitir la creación de filtros basados en cualquiera de las características del evento, tales como IP de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen o destino, etc. El administrador debe poder asignar estos filtros a diferentes líneas en un gráfico que sean actualizadas en intervalos regulares mostrando todos los eventos que concuerdan con ese filtro. Permitiendo que el operador se focalice en los eventos más importantes.
4.3	Debe mostrar la distribución de eventos por países en un mapa.
4.4	Debe permitir agrupar los eventos en base a cualquier característica de los mismos, pudiendo agrupar en varios niveles.
4.5	Debe permitir realizar búsquedas dentro del listado de eventos.
4.6	Debe poder generar automáticamente pequeños gráficos o tablas de distribución de eventos, orígenes y destinos, en la vista del listado de eventos.
4.7	Debe soportar calendarizar reportes para que se ejecuten automáticamente para extraer información en periodos regulares de tiempo (diarios, semanales y mensuales). También debe permitir al administrador la fecha y horario en que empezará a generar el reporte agendado.
4.8	Debe permitir la distribución automática de los reportes por correo electrónico.
4.9	El sistema de reportes debe proveer información consolidada sobre al menos: Top de eventos por origen Top de eventos por destino Eventos por fecha. Eventos por semana. Top de eventos por producto Top de eventos por servicios. Severidad Producto
4.10	Dichos reportes deben incluir una explicación acerca de las políticas que fueron violadas y que parte del contenido causó dicha violación. En dichos reportes deben mostrarse los usuarios a los usuarios (cuando exista una tecnología de AD).

4.11	Con el propósito de mejorar la administración, debe ser posible definir un número máximo de alertas para ser mostradas en la GUI, además poder definir un periodo de tiempo máximo para mostrar dichas alertas, por ejemplo, mostrar solo las alertas generadas hace una hora.
4.12	Debe permitir integrar múltiples dispositivos de seguridad y dominios de administración de seguridad.
4.13	Debe permitir exportar en formato XLSX o PDF los reportes generados.
4.14	Debe permitir generar “Vistas” en las cuales se aplican filtros sobre los logs previamente indexados, para obtener una “foto” del estado de seguridad de la plataforma.

Las especificaciones mínimas de procesamiento deben contar con 4 cores de 2.6 Ghz o superior, memoria RAM mínimo de 32 GB y almacenamiento de 4 Tb. **Para la Solución virtual, el Icetex asignará los recursos necesarios para el correspondiente despliegue de la solución,** como lo es procesamiento, memoria y almacenamiento en la plataforma de virtualización que se tiene disponible**.**

INSTALACIÓN: La solución suministrada dentro de este proyecto deberá ser instalada, probada y puesta en funcionamiento, además se debe realizar por parte del Proveedor la migración de todos los servicios que se encuentran actualmente configurados en la Management ubicada en el Data Center del ICETEX y que la plataforma después de su migración quede totalmente operativa e integrada con los sistemas de seguridad perimetral que cuenta el Icetex. El CONTRATISTA contemplará cualquier elemento intermedio o recurso necesario para la instalación y el funcionamiento de la solución, entregando el proyecto en perfecto funcionamiento y operatividad, garantizando una excelente calidad y terminación del trabajo sin generar costos adicionales para el ICETEX.

SERVICIO DE MANTENIMIENTO: Durante el periodo de la garantía, el CONTRATISTA deberá garantizar mantenimiento preventivo por año y los correctivos necesarios. Cuando se requiera el mantenimiento de tipo correctivo (con o sin suministro de repuesto), el CONTRATISTA deberá asegurar la restauración de las funciones básicas del equipo, y la gestión de los repuestos, equipos y servicios necesarios para lograr la puesta en operación de manera satisfactoria.

TRANSFERENCIA DE CONOCIMIENTO:
Se debe realizar una transferencia de conocimiento de la solución implementada con una intensidad de mínimo ocho (8) horas.

SERVICIO DE SOPORTE:

Niveles de servicio requeridos	Disponibilidad
Atención a reportes y requerimientos	De lunes a viernes en horario laboral
Respuesta en situaciones críticas	Máximo 6 horas después de reportado el incidente.
Soporte por teléfono	De lunes a viernes en horario laboral

El servicio de soporte local se prestará en modalidad 7x24x365 a través de la línea de atención del proveedor.

Los ingenieros de Soporte Técnico del PROVEEDOR estarán atentos y dispuestos para atender los requerimientos los 7 días de la semana, 24 horas al día, los 365 días del año, en temas referentes a:

1. Apertura y seguimiento de tickets para la resolución de inconvenientes con servicios instalados.
2. Soporte técnico de primer y segundo nivel.

Cuando se presente un problema ICETEX reportara y el PROVEEDOR deberá generar un único número de ticket y este será proporcionado y se utilizará para realizar el seguimiento desde el contacto inicial hasta que el problema sea resuelto en su totalidad.

Estructura del Soporte Técnico

- Nivel 1: Recepción de llamadas
  - ✓ Recopilación de información y determinación del nivel de gravedad del problema.
  - ✓ Búsqueda en la base de conocimiento.
  - ✓ Desarrollo y obtención de autorización por parte del ICETEX para llevar a cabo el aislamiento del problema y aprobación de un plan de implementación de la solución.
  - ✓ Escalamiento a Nivel 2 si es necesario
- Nivel 2:
  - ✓ Replicación del problema en Laboratorio con el fin de identificar problemas de diseño e interoperabilidad con los demás elementos de la red
  - ✓ Llevar a cabo resolución de problemas en sitio, si es necesario.
- Nivel 3:
  - ✓ Escalamiento a fábrica
  - ✓ Posible cambio de equipo, si es necesario

Métodos de contacto con Soporte Técnico

- El proveedor deberá contar con al menos dos (2) de los siguientes métodos de comunicación:
  - Soporte vía portal web
  - Soporte vía email
  - Soporte vía telefónica

Nombre del **Proponente**: _____
NIT del **Proponente:** _____ Régimen: _____
Representante legal del **Proponente:** _____
Documento de identidad del representante legal del **Proponente:** _____
Dirección del **Proponente:**_____ Ciudad: _____
Teléfono del **Proponente:**_____
Fax del **Proponente:**_____
***Correo electrónico del** Proponente:*_____