Fecha: Julio 18 de 2017

Dependencia subgerente del proyecto:
Subgerencia Corporativa

Nombre del proyecto:
Renovación de licenciamiento de los procesos de seguridad de la información y soporte y mantenimiento requerido (logmain – antivirus - firewall)

Rubro presupuestal imputable:
Mantenimiento de Bienes Muebles e Inmuebles

Clase de gasto:
Gastos Generales

Descripción del problema a resolver, actividad o necesidad que se pretende crear, fortalecer o satisfacer con la contratación (Análisis de Conveniencia y Oportunidad):

La Terminal de Transporte S.A. es una sociedad de economía mixta del orden Distrital, con autonomía administrativa, financiera y patrimonio independiente, que tiene como función principal prestar servicios conexos al transporte público, una de las funciones de la subgerencia corporativa es dirigir y orientar su gestión para garantizar el fortalecimiento institucional y la prestación de los servicios tecnológicos, para el cumplimiento de la misión de la empresa, de acuerdo con los recursos disponibles, las necesidades y los procesos de la misma.

En ese orden de ideas y con el propósito de disminuir los riesgos asociados a la integridad, confiabilidad y disponibilidad de la información de la Terminal de Transporte, se hace necesario contar con herramientas que blinden a la plataforma tecnológica y por ende a todos los datos que a través de la misma circulan, con el objeto de preservar la seguridad informática interna, basada en el control del tráfico de datos de las redes, regulando así el acceso a los servidores de datos de la Terminal. Dado lo anterior, la entidad requiere adquirir la renovación anual de las licencias Firewall Cyberoam UTM, antivirus y acceso remoto, herramientas que ofrecen protección a la data center de la entidad y permiten a los dispositivos conectados a la red de datos de la misma, estar debidamente protegidos contra los ataques informáticos evitando que se pierda información almacenada en documentos y bases de datos. Es así como, el licenciamiento del software antivirus, la renovación de los servicios, mantenimiento y soporte de Cyberoam y el acceso remoto, le permite a la entidad proteger todos los equipos y la información contra los peligros que representan los ataques informáticos y minimizar así las fallas a las que está expuesta la información y los diferentes archivos almacenados, por lo anterior:

1. Para la Terminal es conveniente y prioritario proteger todos los equipos de cómputo con la renovación de las licencias y antivirus protegiendo los equipos, ya que en su mayoría permanecen prendidos las 24 horas del día, por ende, las amenazas de virus son muy altas o frecuentes y con la citada renovación, se busca mitigar estos inconvenientes para garantizar la prestación de los servicios ofrecidos por la Terminal sin interrupciones.
2. Que con la adquisición del antivirus, la Entidad genera las políticas de seguridad para tener control de las aplicaciones instaladas en los equipos de cómputo, control de filtros de contenido, control y bloqueo total de USB para lectura y poder generar políticas de acceso a internet por usuario.
3. Que con la renovación del licenciamiento del firewall (sistema de seguridad informática perimetral) se pretende fortalecer y proteger la información que ingresa y sale de la Terminal de Transporte S.A. por cuanto se trata de una herramienta que opera como un filtro que examina todos los paquetes que se dirigen hacia la red de la Entidad y compara la información del encabezado con reglas previamente

establecidas. Si la dirección IP y el puerto son válidos según las reglas, el paquete es entregado. En caso contrario, se desecha. La misma operación es realizada con los paquetes que son enviados desde el interior hacia el internet. Este permite generar e implementar unas políticas de seguridad entre la red privada de la Terminal y el internet y es una herramienta para restringir el acceso entre el internet y la red corporativa interna. Típicamente se instala un firewall en un punto estratégico donde una red o redes se conectan a la internet, con el propósito de impedir que extraños accedan a los PC desde internet, lo que proporciona una frontera de protección que ayuda a mantener fuera a los invasores no deseados de internet.

4. Que con esta renovación se pretende reducir la probabilidad de que los hacker y cracker desde un sitio de internet, puedan atacar los sistemas corporativos y redes internas y así mismo, controla y evitar que los propios usuarios internos comprometan la seguridad de la red al enviar información peligrosa como passwords no encriptados o datos sensitivos para la organización hacia el mundo externo.
5. Que con la renovación de un acceso remoto se busca contar con una solución para acceder remotamente y brindar soporte vía internet a diferentes computadores de operación misional donde todas las comunicaciones utilizan algoritmos y protocolos estándares del sector cifrado y autenticación en caso de que se tenga que remitir información de un equipo a otro manteniendo la integridad y confidencialidad de la información enviada.
6. Que se pretende establecer la comunicación vía internet desde cualquier parte donde se tenga acceso a internet a cinco (5) equipos de cómputo de las tres Terminales para poder dar soporte remoto y mantener el normal funcionamiento de la venta de la tasa de uso en estas Terminales y demás servicios conexos a la operación misional de la Entidad.
7. Que con la renovación del licenciamiento del firewall, antivirus y acceso remoto se pretende suministrar las herramientas necesarias para poder garantizar el funcionamiento de los equipos de cómputo, servidores y no interrumpir las labores diarias por causa del ingreso de hacker y cracker, virus al computador, ocasionando pérdida de información generando traumas en la prestación del servicio.
8. Que con la adquisición y licenciamiento de una herramienta que detenga los ataques de ransomware la Terminal pretende mitigar estos ataques y si llegasen a suceder que esta herramienta cuente con la funcionabilidad de detener el ransomware antes de que secuestre nuestros archivos y mantenerlos en un lugar seguro
9. Que la Subgerencia Corporativa de la Terminal de Transporte adelantó el estudio previo correspondiente definiendo los requerimientos mínimos a la Gerencia General, para adelantar la contratación citada.
10. Que para la realización de estas actividades es necesario contratar una empresa con experiencia en la prestación del servicio.

La Dirección de Recursos Tecnológicos certifica que con estas cinco (5)) licencias de acceso remoto, son suficientes para garantizar la prestación de estos servicios y dar cumplimiento a lo exigido por la Ley 603 de 2000 "Derechos de Autor"

Objeto del proyecto:
Renovación de licenciamiento de (firewall – antivirus y logmain)

Plazo (debe ser adecuado y acorde al objeto del contrato):
Un año (1) contados a partir de la firma del acta de inicio

Lugar de ejecución: Terminal de Transporte S.A.

Supervisión: Dirección de Recursos Tecnológicos o quien designe la Gerente General

Valor estimado del contrato y la justificación del mismo:
Se estima como presupuesto oficial para esta contratación el valor de Cuarenta y Dos Millones De Pesos M/cte. incluido IVA ($42.000.000)

Forma de Pago:
La Terminal de Transporte S.A. cancelará el valor del contrato así:

1.) Un pago único por el ciento por ciento (100%) con el suministro del licenciamiento adquirido

Para tramitar los pagos se deben adjuntar los siguientes documentos:

1. Factura de cobro en donde se relacione el licenciamiento.
2. Certificado expedido por el supervisor del contrato, en donde conste el cumplimiento del producto objeto de pago, acorde a las obligaciones del contrato y su alcance.
3. Acreditación del pago de aportes de seguridad social integral, de acuerdo con lo señalado en la normatividad vigente.

La Terminal de Transporte S.A. no se hace responsable por las demoras presentadas en el trámite para el pago al CONTRATISTA cuando ellas sean ocasionadas por encontrarse incompleta la documentación soporte o por no ajustarse a cualquiera de las obligaciones establecidas en el presente contrato o en la oferta presentada.

La Terminal de Transporte S.A. hará las retenciones a que haya lugar sobre el pago de acuerdo a las disposiciones legales vigentes.

Perfil específico de los proponentes o futuros contratistas (Requisitos de Experiencia y/o formación profesional, Financieros y jurídicos):

Podrán participar las personas jurídicas nacionales o extranjeras, ya sea en forma individual, en consorcio o unión temporal, o promesas de sociedad, debidamente registradas ante la Cámara de Comercio, cuya actividad comercial se encuentre directamente relacionada con el objeto a contratar y estén interesadas presentar su propuesta para satisfacer la necesidad de la Terminal de Transporte.

El proponente deberá demostrar la ejecución a satisfacción de al menos dos (2) contratos similares en empresa pública o privada que sumen un presupuesto igual o superior al dispuesto para el presente proyecto, para estos efectos adjuntará el RUP y acreditar personal idóneo para atender los requerimientos propios de la instalación, mantenimiento y soporte

Especificaciones técnicas y cantidades del bien o servicio a contratar, autorizaciones, permisos y licencias necesarias para la ejecución del proyecto:

El contratista se obliga a:

1. Renovar el licenciamiento de un (1) firewall Cyberoam CR100ING – 10.6.2 MR1 que actualmente tenemos en la Terminal o Suministrar un (1) sistema de seguridad informática perimetral tipo firewall de nueva generación con su respectivo licenciamiento
2. Renovar o licenciar mínimo ciento cincuenta (150) licencias de antivirus.
3. Renovación de cinco (5) licencias de acceso remoto
4. Adquisición de Ciento cincuenta (150) licencias mínimo de anti-ransomware
5. Instalar las actualizaciones de los productos antes mencionados durante un (1) año
6. Dar el respectivo soporte de los productos antes mencionados durante un año
7. Vigencia del licenciamiento y soporte por doce (12) meses

Obligaciones específicas y productos esperados (deben ser armónicos con el objeto del contrato):

1.. El Contratista se obliga para con La Contratante a:

Cumplir con los requerimientos técnicos, administrativos y de gestión para renovar, suministrar, licenciar, configurar, actualizar y dar soporte en las instalaciones de la Terminal de Transporte S.A., por una año a:

A. **FIREWALL (Cyberoam CR100ING – 10.6.2 MR1) o** Adquisición, implementación y puesta en Funcionamiento de un sistema de seguridad informática perimetral interna tipo Firewall de nueva Generación implementando las políticas designadas por la Terminal y debe tener ya incluida y disponibles, las funcionalidades y especificaciones técnicas Mínimas indicadas a continuación.

ITEM	REQUERIMIENTO MÍNIMO	CUMPLE SI	CUMPLE NO
	REQUISITOS GENERALES		
1	Adquisición de un sistema de seguridad informática perimetral e interna tipo Firewall de Nueva Generación, que debe tener ya incluidas y disponibles, las funcionalidades indicadas a continuación		
2	Throughput de por lo menos 20 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6.		
3	Soporte a por lo menos 2 millones de conexiones simultaneas		
4	Soporte a por lo menos 130 mil nuevas conexiones por segundo		
5	Throughput de al menos 9 Gbps de VPN IPSec		
6	Estar licenciado para, o soportar sin necesidad de licencia, 2 mil túneles de VPN IPSec site-to-site simultáneos		
7	Estar licenciado para, o soportar sin necesidad de licencia, 5 mil túneles de clientes VPN IPSec simultáneos		
8	Throughput de al menos 900 Mbps de VPN SSL		
9	Soportar al menos 300 clientes de VPN SSL simultáneos		
10	Soportar al menos 6 Gbps Mbps de throughput de IPS		

11	Soportar al menos 1 Gbps de throughput de Inspección SSL		
12	Soportar un Throughput de 1.8 Gbps de Next generation Firewall		
13	Throughput de al menos 1.2 Gbps de protección de amenazas		
14	Permitir gestionar al menos 32 Access Points		
15	Tener al menos 18 interfaces 1Gbps en cobre (UTP)		
16	Tener al menos 4 interfaces de 1 Gbps disponibles SFP de fibra.		
17	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance		
18	Soporte de al menos 10.000 políticas de Firewall		
19	El dispositivo debe ser un equipo de propósito específico para ofrecer un alto rendimiento y baja latencia		
20	El dispositivo debe soportar prevención de intrusos basada en anomalías, desfragmentación de paquetes y descarga de checksum		
21	El equipo debe soportar VPN, CAPWAP, aceleración de túneles IP, traffic shaping y prioridad de colas		
22	El dispositivo deberá incluir aceleración de inspección de contenido basada en firmas, trafico cifrado y texto claro		
23	El fabricante de la solución debe estar validado a nivel de rendimiento y seguridad por los siguientes laboratorios de pruebas de terceros, líderes en la industria de protección: NSS Labs, VB100, AV Comparatives e ICSA		
24	El dispositivo debe controlar miles de aplicaciones, bloquear los últimos exploits y filtrar trafico web basado en millones de clasificaciones de URLs en tiempo real		
25	El equipo debe estar respaldado por un laboratorio de investigación y desarrollo que ofrezca inteligencia en tiempo real entregando actualizaciones de seguridad completas, investigadores de amenazas de seguridad		
26	El equipo debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 3 años en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono		
27	El dispositivo debe proporcionar información granular para aplicaciones basadas en nube, tales como: YouTube, Dropbox, Baidu, Microsoft Office 365, Amazon, entre otras		
28	El dispositivo debe realizar balanceo de carga de enlaces estático mediante el uso de los siguientes algoritmos de balanceo de carga: Ancho de banda, Sesiones, Spillover, Ip Fuente - IP Destino, IP Fuente.		
29	El equipo deberá poder ser configurado en capa 2 o en capa 3 en la red		
30	La solución soportará políticas basadas en dispositivo. Esto significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (móvil, laptop) que tenga el usuario. Esta característica no requerirá ningún tipo de licenciamiento adicional		
31	Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, de esta forma se es lo más granular posible en la definición de políticas		
32	El equipo deberá poder contar con la característica de modo de aprendizaje para políticas de firewall, cuyo objetivo sea monitorear el tráfico para determinar cuáles restricciones y protecciones se deben aplicar		
	TRADUCCIÓN DE DIRECCIONES DE RED (NAT)		
33	Debe soportar NAT de origen y NAT de destino de forma simultánea;		
34	Debe ser compatible con NAT dinámica (muchos-a-muchos y varios a 1);		
35	Debe ser compatible con NAT Origen;		
36	Debe soportar NAT estática (1-a-1);		
37	Debe ser compatible con NAT64 y NAT46;		
38	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;		
39	Debe ser compatible con NAT estático bidireccional 1-a-1;		
40	Debe admitir NAT estática (muchos-a-muchos);		
41	Debe ser compatible con NAT de destino;		
42	Debe ser compatible con la traducción de puertos (PAT);		
	REQUISITOS MÍNIMOS DE FUNCIONALIDAD		

43	Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario;		
44	Permitir la visualización de los dispositivos inalámbricos conectados por canal		
45	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;		
46	Permitir la visualización de los dispositivos inalámbricos conectados por IP		
47	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;		
48	Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración;		
49	Soportar OSPF graceful restart;		
50	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);		
51	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;		
52	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);		
53	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones SYN, ICMP , UDP, etc;		
54	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)		
55	La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP		
56	El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces		
57	El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico		
58	Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis		
59	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3 y BGP);		
60	La solución debe soportar ECMP (Equal Cost Multi-Path)		
61	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);		
62	La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow		
63	La solución podrá habilitar políticas de ruteo en IPv6		
64	La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6		
65	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP		
66	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;		
67	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs		
68	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;		
69	Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad		
	VPNS		
70	Soporte de VPNs IPSec sitio a sitio y cliente – sitio		
71	La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI		
72	Las características de VPN SSL se deben cumplir con o sin el uso de agentes;		
73	Asignación de DNS en la VPN de cliente remoto;		
74	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);		
75	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);		
76	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y el Grupo 14;		

77	La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;		
78	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;		
79	La VPN IPSec debe ser compatible con 3DES;		
80	Soportar VPN SSL;		
81	Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;		
82	La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;		
83	Soporte a certificados RSA X.509 para construcción de VPNs cliente a sitio (client-to-site)		
84	En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall		
85	Soporte a SSL 2.0 y 3.0, TLS 1.0,1.1 y 1.2		
86	Soporte para modo de operación basado en web o modo túnel		
87	Soporte a certificados RSA X.509 para construcción de VPNs SSL		
88	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN		
89	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;		
90	Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos o basados en software		
91	Validación de equipos de plataformas Windows mediante la comprobación de sistema operativo, firewall de Windows, antivirus para obtener acceso mediante VPN SSL		
92	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet		
93	La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS		
94	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL		
95	La VPN SSL Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios		
96	La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información		
	ALTA DISPONIBILIDAD		
97	La configuración de alta disponibilidad debe sincronizar Sesiones		
98	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;		
99	El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6		
100	Debe soportar Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico		
101	Posibilidad de definir al menos dos interfaces para sincronía		
102	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red		
103	Será posible definir interfaces de gestión independientes para cada miembro en un clúster		
104	Debe ser posible definir que Firewall Virtual estará activo sobre que miembro del Cluster para hacer una distribución de carga en caso se der necesario		
105	El equipo debe soportar hasta 4 equipos en esquema de HA		

106	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad;		
107	La configuración de alta disponibilidad debe sincronizar las asociaciones de seguridad VPN;		
108	La configuración de alta disponibilidad debe sincronizar: configuración, incluyendo, pero no limitados políticas de Firewalls, NAT, QoS y objetos de la red;		
	ANTIMALWARE		
109	Debe mitigar las siguientes amenazas: Virus, gusanos, troyanos, ransomware, scareware, spyware, adware, botnets, entre otros		
110	El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma		
111	El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión		
112	Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;		
113	El antivirus debe permitir las siguientes opciones de inspección: amenazas en ejecutables Windows que se encuentran embebidas en un adjunto de correo electrónico y protección para malware de dispositivos móviles		
114	El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6		
	FILTRADO WEB		
115	La solución debe permitir filtrado de contenido web, filtrado de URLs y servicio de filtrado web basado en firmas desarrolladas por laboratorio de investigación y desarrollo propio del fabricante		
116	Tener por lo menos 75 categorías de URL y clasificación de por lo menos 47 millones de páginas web;		
117	Debe poder categorizar contenido Web requerido mediante IPv6		
118	Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;		
119	Debe tener la funcionalidad de exclusión de URLs por categoría		
120	Capacidad de filtrado de scripts en páginas web (JAVA/Active X)		
121	La solución de Filtrado de Contenido debe soportar la característica de "Safe Search" o "Búsqueda Segura" para prevenir imágenes y sitios web con contenido explícito en los resultados de búsqueda. Esto debe ser soportado para los siguientes sitios: Google, Yahoo, Bing y Yandex		
122	Será posible exceptuar la inspección de HTTPS por categoría		
123	El filtrado de contenido web debe permitir la definición de palabras, frases, patrones, wildcards y expresiones regulares Perl para prevenir acceso a páginas con material cuestionable		
124	El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en categoría, grupo de categoría o clasificación		
125	El filtrado debe ser sobre tráfico HTTP y HTTPS		
	IPS		
126	El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror		
127	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP		
128	Deberá ser posible seleccionar el sistema operativo, protocolo, severidad y objetivo para la configuración de perfiles IPS		
129	Debe tener los siguientes mecanismos de inspección IPS: análisis para detectar anomalías de protocolo		

130	Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones		
131	Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico		
132	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets)		
133	Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: permitir, permitir y generar registro, bloqueo, bloqueo del IP del atacante durante un tiempo y enviar tcp-reset;		
134	Debe tener los siguientes mecanismos de inspección IPS: análisis de decodificación de protocolo;		
135	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;		
136	Capacidad de detección de más de 4000 ataques		
137	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		
138	Actualización automática de firmas para el detector de intrusos		
139	Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP		
	CONTROL DE APLICACIONES		
140	Debe basarse en categorías que permitan seleccionar grupos de firmas basados en un tipo de categoría		
141	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor		
142	Reconocer al menos 2.300 aplicaciones diferentes, incluyendo, pero no limitado a: el tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;		
143	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.		
144	Actualización de la base de firmas de la aplicación de forma automática;		
145	Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;		
146	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, hacer traffic shapping, registrar en log, ver firmas y bloquear acceso a una aplicación por un periodo de tiempo específico basado en días, horas y minutos		
147	Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;		
148	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log		
149	Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping		
150	Debe ser posible inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados		
	VISIBILIDAD Y ADMINISTRACIÓN		
151	El equipo debe permitir la visualización de la topología física y lógica, con el fin de obtener mayor información de los dispositivos y conexiones		
152	El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Políticas: Permite monitoreo de actividad de políticas, con el fin de discernir cuales políticas no se usan y pueden ser borradas.		
153	El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Interfaces: Permite realizar monitoreo actual e histórico de ancho de banda por interfaz		
154	El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Países: Filtrado de trafico de acuerdo a países fuente y destino		
155	El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Traffic shaping: Permite monitoreo de traffic shappers configurados		

156	El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Mapa de amenazas: Permite monitorear riesgos provenientes de varias ubicaciones internacionales llegando a una ubicación específica		
157	El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Autenticaciones fallidas: Permite determinar si el NGFW presenta un ataque de fuerza bruta, así como: acceso no autorizado a interfaz por telnet, SSH, HTTP y HTTPS, fallas para hacer una consulta por SNMP, intentos fallidos para establecer conexión de una VPN IPSec Dial-up, conexiones de VPNs IPSec Sitio a Sitio y conexiones de VPNs SSL		
158	La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional		
159	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;		
160	Deber permitir el bloqueo de vulnerabilidades		
161	Mostrar los orígenes del tráfico o usuarios que lo generan.		
162	Mostrar las aplicaciones y su categorización según riesgo.		
163	Visibilidad de aplicaciones Cloud usadas por el usuario.		
164	Visibilidad de destinos del tráfico.		
165	Visibilidad de los sitios web mas consultados por los usuarios.		
166	Visibilidad de las amenazas o incidentes que han ocurriendo en la red		
167	En la información de fuentes, aplicaciones, navegación debe ser posible con un doble-click filtrar la información para ser más específica la búsqueda.		
168	Se deben ver aplicaciones, sitios, amenazas por cada usuario.		
169	Se debe ver el tiempo de navegación por cada sitio o categoría de sitios.		
170	De las aplicaciones Cloud que permitan compartir archivos como Dropbox debe ser posible ver que archivos fueron subidos y descargados por los usuarios		
171	Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)		
172	Interfaz basada en línea de comando (CLI) para administración de la solución.		
173	Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.		
174	Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH)		
175	El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.		
176	Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.		
177	El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.		
178	El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.		
179	Soporte de SNMP versión 2		
180	Soporte de SNMP versión 3		
181	Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos		
182	Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.		
183	Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.		

184	Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.		
185	Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.		
186	Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).		
187	Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.		
188	Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación		

B. **ANTI-RANSOMWARE:** El ransomware debe cumplir con mínimo las siguientes especificaciones:

- Licenciamiento para 150 usuarios
- Que detenga los ataques de ransomware antes de que secuestre nuestros archivos y mantenerlos en un lugar seguro
- Browser Exploit Prevention
- Exploit Prevention
- Malicious Traffic Detection (MTD)
- Automated Malware Remova
- Synchronized Security Heartbeat
- Root Cause Analysis

C. **ANTIVIRUS:** El antivirus debe cumplir con mínimo las siguientes especificaciones:

- Licenciamiento para 150 licencias
- Actualización de versiones nuevas por un (1) año
- Cobertura: Estaciones de trabajo, servidores de archivos Windows y servidor de correo Exchange Server
- Protección para: Virus, spyware, hackers, rootkits, malware, troyanos, etc. Que proteja el Spam a estaciones de trabajo Firewall
- Control de dispositivos: Para lectura, escritura y bloqueo total, incluyendo el serial de las USB que desea permitir en la red, evitando propagación de virus y control de fuga de información.
- Control de aplicaciones: Permite el bloqueo de aplicaciones que usuarios descargan y se consume el ancho de banda como ARES, etc.
- Filtro de contenidos: Genera bloqueo de los sitios Web no permitidos y los permitidos, evitando el consumo del ancho de banda de la red.
- Control de acceso a internet por tiempos: Puede bloquear el acceso a internet de los usuarios que determine y en los horarios deseados, ayudando a administrar mejor el ancho de banda.
- Consola vía web, que no consuma tanto recurso de máquina, con dos motores propios de firmas, soporte ilimitado en sitio, visitas periódicas
- Análisis de archivos anti-malware
- Análisis del comportamiento de la pre-ejecución / HIPS
- Bloqueo de aplicaciones potencialmente no deseadas (PUA)

- Prevención de pérdida de datos
- Análisis del comportamiento en tiempo de ejecución / HIPS
- Detección de tráfico malicioso (MTD)
- Eliminación automatizada de software malicioso

D. PRO LOGMEIN o HERRAMIENTA DE ACCESO REMOTO:

El contratista se obliga a entregar la Renovación del licenciamiento para la solución de acceso remoto vía internet para cinco (5) equipos de cómputo que funcione como contingencia para dar soporte a puestos de trabajo misionales existentes en la Terminal Central, Sur y Norte, por un (1) año.

E. SOPORTE y ACTUALIZACIONES: El contratista debe garantizar el soporte y actualizaciones por un año a los productos y licencias ofertadas

- Soporte Técnico 7X24X365, con soporte remoto y presencial.
- Solución a fallas técnicas máxime en dos (2) horas desde el momento en que se le reporta hasta la solución del inconveniente
- Revisión cada 30 días de las tablas de filtrado, detección de virus, filtrado de contenidos web y antiespam, tablas de enrutamiento, reglas de filtrado y actualización del software cuando sea necesario, revisión de la protección contra spyware
- Actualizaciones de software cuando sean necesarias

2. Atender los requerimientos del supervisor que conduzcan a un desempeño excelente del objeto del contrato.

3. Generar un informe mensual de las actividades realizadas durante las visitas de preventivas y revisiones.

6. Elaborar una lista de chequeo y bitácoras de cada una de los equipos y que políticas tiene configuradas.

7. Elaborar una bitácora con cada uno de los incidentes presentados y la forma como se soluciono.

8. Soporte con servicio de alta disponibilidad en routers Mikrotik, enrutamiento dinámico OSPF, rutas estáticas, túneles EoIP y VPN para las Terminales central, sur y norte.

9. Tiempos de Respuesta: a) La Terminal de Transporte S.A., solicitará un tiempo de respuesta a los requerimientos realizados en caso de fallar el **Cyberoam CR100_ING** o el sistema de seguridad informática perimetral tipo firewall de nueva generación con su respectivo licenciamiento ofrecido y la solución del mismo de máximo dos (2) horas, desde el momento en que se le informa hasta la solución de la misma. b) Si el requerimiento no se soluciona, La Terminal solicitará un equipo de soporte igual o superior a las características del equipo en problemas máximo en un tiempo de dos (2) horas.

10. Soporte Remoto: La Terminal de Transporte S.A., solicitará un tiempo de respuesta para brindar el soporte remoto de máximo dos (2) hora, contados a partir desde el momento en que se les informa hasta la solución del mismo.

11. El contratista debe contar con el servicio de Centro de Operaciones de Seguridad (SOC) para monitoreo y atención a incidentes 7x 24 x 365.

12. Perfil del equipo de trabajo: Ofrecer como mínimo dos (2) personas técnicas o profesionales que cumplan el siguiente perfil: a) Mínimo dos (2) años de experiencia comprobada en el soporte y configuración de políticas del equipo Cyberoam CR100ING o de la solución propuesta, para su validación deben allegar las hojas de vida, b) Que sean certificados por el fabricante o por un centro de entrenamiento aprobado por éste, para su validación deben allegar los certificados o diplomas donde se acredite que las personas ofrecidas realizaron el respectivo entrenamiento y que están capacitados para realizar el respectivo soporte y configuración a los equipos ofrecidos

Análisis de riesgos que deben ser amparados en la Garantía Única y la forma de mitigarlo (si aplica):

MATRIZ DE ANÁLISIS, VALORACIÓN DE RIESGOS DE LA CONTRATACIÓN

No.		1	2	3	4
Clase		GENERAL	GENERAL	GENERAL	GENERAL
Fuente		EXTERNO	EXTERNO	EXTERNO	EXTERNO
Etapa		EJECUCIÓN	EJECUCIÓN	EJECUCIÓN	CONTRATACIÓN
Tipo		OPERACIONAL	TECNOLÓGICO	TECNOLÓGICO	TECNOLÓGICO
Descripción (Que puede pasar y como ocurre el riesgo)		Que los productos no estén licenciados por empresas autorizadas	Que los productos objeto de la contratación no estén licenciados correctamente o en las cantidades requeridas	Que no se de respuesta a los requerimientos de la Terminal en los tiempos estipulados.	La falta de personal capacitado para atender los requerimientos de la Terminal
Causas (Que origina el riesgo) y consecuencia de la ocurrencia del evento		No cumple con lo ofrecido en el contrato y no se encuentra registro de las licencias en la casa matriz	Utilización de software ilegal, incumplimiento la ley 603 de 2000 derechos de autor	Que la necesidad de la contratación no sea suplida a tiempo	Demoras en la respuesta a las solicitudes realizadas, reprocesos y controles ineficientes generando opción de ataques externos a la plataforma tecnoogica
Probabilidad		3	3	2	2
Impacto		4	6	8	5
Calificación Total		7	9	10	7
Riesgo		Alto			Alto
A quién se le asigna?		Contratista	Contratista	Contratista	Contratista
Tratamiento/ controles a ser implementados		Requerir al contratista de inmediato para que instale los productos con empresas autorizadas y poder evidenciarla a nombre de la terminal en la casa matriz	Implementación de controles de verificación del licenciamiento instalado y validación de cantidades y de versiones permanentemente	Requerir al contratista de inmediato para que de respuesta a los requerimientos dentro de los tiempos estipulados	Requerimiento inmediato para el cambio de personal por uno más idóneo.
Impactos después del tratamiento	Probabilidad	1	1	1	1
	Impacto	2	2	5	3
	Calificación	3	3	6	4
	Calificación Total	3	3	6	4
¿Afecta el equilibrio económico del contrato?		No	No	No	No
Persona responsable por implementar el tratamiento		Contratista	Contratista/ Supervisor	Contratista / Supervisor	Contratista

Fecha estimada en que se indica el tratamiento		Una vez	Cada vez que se instale un equipo en la red de la Terminal	Cada vez que se dé una novedad	Cada vez que se dé una novedad
Fecha estimada en que se completa el tratamiento		Cuando el contratista entregue el soporte de las licencias y evidenciemos en la casa matriz están a nombre de la terminal	En la configuración del equipo ingresado	Una vez el contratista haya solucionado la novedad	Una vez el contratista haya cambiado el personal por personal idóneo y certificado
Monitoreo y revisión	**¿Cómo se realiza el monitoreo?**	Con el seguimiento de donde se compraron las licencias.	Seguimiento a las instalaciones de equipos en la red	Seguimiento a los tiempos de los requerimientos	Una vez se haya aprobado, cambiado el equipo de trabajo y se compruebe su idoneidad
	Periodicidad ¿Cuándo?	Una única vez	mensual	Semana	Una única vez

Matriz adaptada de M-ICR-01 Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación Colombia Compra Eficiente http://www.colombiacompra.gov.co/sites/default/files/manuales/cce_manual_riesgo_web.pdf

El proveedor favorecido se compromete a constituir a favor de la Terminal de transporte S.A., de una parte, una garantía única que ampare el cumplimiento de las obligaciones surgidas del contrato y de su liquidación, expedida por una compañía de Seguros establecida legalmente en Colombia que cubra todos los riesgos en las cuantías y vigencias que se establecen a continuación.

RIESGO	%	SOBRE EL VALOR	VIGENCIA DEL AMPARO
Cumplimiento del contrato	10	Del Contrato	Plazo del contrato y seis (6) meses más
Calidad del servicio	10	Del Contrato	Plazo del contrato y seis (6) meses más, a partir del recibo a satisfacción.
Calidad de los Bienes	10	Del Contrato	Plazo del contrato y seis (6) meses más, a partir del recibo a satisfacción.
Pago de Salarios y prestaciones sociales.	5	Del Contrato	Plazo del contrato y un año más, a partir del recibo a satisfacción

Requisitos Ambientales y de Seguridad y Salud en el Trabajo:

El Proveedor deberá cumplir con la legislación ambiental vigente sin que LA TERMINAL DE TRANSPORTE SA le efectúe requerimiento expreso. Por lo anterior, para adelantar sus actividades, le corresponde obtener previamente las licencias, permisos, o autorizaciones necesarias y cumplir con las especificaciones que para el respectivo contrato sean indicadas por la Entidad.

Requisitos de Seguridad y Salud en el Trabajo: En cumplimiento del artículo 2 de la Ley 1562 de 2012 que modificó el artículo 13 del Decreto legislativo 1295 de 1994, el contratista se obligará a afiliarse a la administradora de riesgos laborales – ARL, que ampare los riesgos laborales identificados para la TERMINAL DE TRANSPORTE SA Entregar para el pago, la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o complemente.

Impacto: Población objetivo que se beneficiará con la ejecución del proyecto (si aplica) y beneficios que obtendrá la Terminal de Transporte S.A con su ejecución (según el objeto social y funciones señalados en el artículo 2 de los estatutos):

(La Terminal de Transporte S.A. y usuarios que hacen uso de los servicios que brinda la Terminal) y beneficios que obtendrá la Terminal de Transporte S.A con su ejecución (mejorar en la prestación de los servicios donde utilizaremos estos equipos al contar herramientas que garantizaran la seguridad de la información que se está

transmitiendo, que no les va a entrar virus, que la información está segura y que la Terminal esta dando cumplimiento a la Ley 603 de 2000 Derechos de Autor):

Modalidad de contratación de acuerdo al Manual de Contratación de la Empresa:
De acuerdo al presupuesto asignado al presente proyecto y de acuerdo con el numeral 15.2 del Manual de contratación la modalidad que corresponde adelantar es la de Solicitud Simplificada de Oferta

Criterios para determinar la oferta y/o propuesta más favorable para la empresa: Menor Precio

Requisitos Habilitantes:

- ✓ Cámara de Comercio con una antelación no mayor a 30 días calendario, donde el objeto social de la persona jurídica o la cámara de comercio de la actividad comercial incluya el objeto del contrato.
- ✓ Distribuidor autorizado y/o partner de la solución ofrecida.
- ✓ El contratista debe contar con el servicio de Centro de Operaciones de Seguridad (SOC) para monitoreo y atención a incidentes 7x 24 x 365
- ✓ Acreditar una experiencia mínima de dos (2) años a través de dos (2) certificaciones de contratos cuyo objeto sea igual a la solución requerida por la Terminal.
- ✓ El Perfil del equipo de trabajo: Ofrecer como mínimo dos (2) personas técnicas o profesionales que cumplan el siguiente perfil: a) Mínimo dos (2) años de experiencia comprobada en el soporte y configuración de políticas del equipo Cyberoam CR100ING o de la solución propuesta, para su validación deben allegar las hojas de vida, b) Que sean certificados por el fabricante o por un centro de entrenamiento aprobado por éste, para su validación deben allegar los certificados o diplomas donde se acredite que las personas ofrecidas realizaron el respectivo entrenamiento y que están capacitados para realizar el respectivo soporte y configuración a los equipos ofrecidos

Para efectos de la evaluación de la oferta de menor valor que cumpla con todas las condiciones y exigencias de la invitación a ofertar se definen las siguientes clausulas de rechazo:

CAUSALES GENERALES:

- El proponente que se halle incurso en alguna de las causales de inhabilidad o incompatibilidad para contratar establecidas en la Constitución o en la ley.
- La propuesta sea presentada por personas jurídicamente incapaces para obligarse
- Existan varias propuestas presentadas por el mismo proponente ya sea en forma individual o en calidad de integrante de un consorcio o unión temporal
- El proponente señale su desacuerdo o imposibilidad de cumplir las obligaciones y condiciones previstas en la invitación publica, o presente condicionamiento para su adjudicación
- Cuando la propuesta se presente extemporáneamente o no se presente en el lugar u hora establecidos en la invitación publica
- Cuando el proponente no responda a cualquiera de los requerimientos efectuados por la entidad en el término previsto en la invitación pública o en la solicitud que de forma particular haga la entidad
- Cuando de conformidad con la información a su alcance, la entidad estime que el valor de una oferta resulta artificialmente bajo y una vez requerido el proponente para la sustentación del valor ofertado, el mismo no de razones suficientes para el comité evaluador
- Cuando en el certificado de existencia y representación se verifique que el objeto del proponente (o de cualquiera de los integrantes cuando sea un consorcio o Unión Temporal) no permita desarrollar la actividad, gestión y operación que se solicita en el presente proceso
- Se demuestre que, a la fecha de presentación de su propuesta, el proponente que siendo persona natural no se encuentra al día, durante los últimos seis (6) meses con el cumplimiento en el pago de los aportes

al sistema de seguridad social en salud, pensión, y riesgos laborales y los aportes a parafiscales cuando a ello hubiere lugar

- Cuando se acrediten circunstancias ocurridas con posterioridad al cierre del proceso
- Cuando de conformidad con el certificado de existencia y representación expedido por la cámara de comercio o autoridad competente, con los estatutos de la persona jurídica o con certificación juramentada proveniente del representante legal del proponente, se determine que su duración no es igual a la del plazo para la ejecución del contrato y tres (3) años más
- Cuando verificada la información aportada por cualquiera de los proponentes y/o de los integrantes del consorcio y/o unión temporal, se determine por parte de la Terminal de Transporte S.A., que ella no corresponde a la realidad.
- En los demás casos que contemple la ley y/o los estudios previos y/o la invitación pública que rige el presente proceso de selección.

Indicación de Acuerdos Comerciales aplicables al proceso de contratación (no aplica a contratos con una sola oferta): N/A

Viabilidad Técnica y Económica del Proyecto

El Líder del Proyecto conceptúa que la contratación es viable técnicamente y cumple con las especificaciones determinadas para satisfacer la necesidad objeto del proyecto descrito en la presente formulación.
El Subgerente Corporativo conceptúa que el proyecto cumple con las condiciones financieras y económicas necesarias para su ejecución.
El Subgerente Jurídico conceptúa que el proyecto cumple con las condiciones jurídicas necesarias para su ejecución.

Firma

JULIO CESAR MOSQUERA SANTOS
Líder del Proyecto

NELSON MUÑOZ LEGUIZAMÓN
Subgerente Corporativo (e)

VoBo: (En caso que aplique)

NELSON MUÑOZ LEGUIZAMÓN
Subgerente Jurídico