LICITACIÓN PUBLICA N° 012/2018

"IMPLEMENTACIÓN DE SISTEMA DE SEGURIDAD ANTI DDoS"

ACTA REUNIÓN DE ACLARACIÓN

FECHA: 26/02/2018

HORA DE INICIO: 09:00 a.m.
HORA DE CONCLUSIÓN: 11:55 a.m.

PARTICIPANTES.

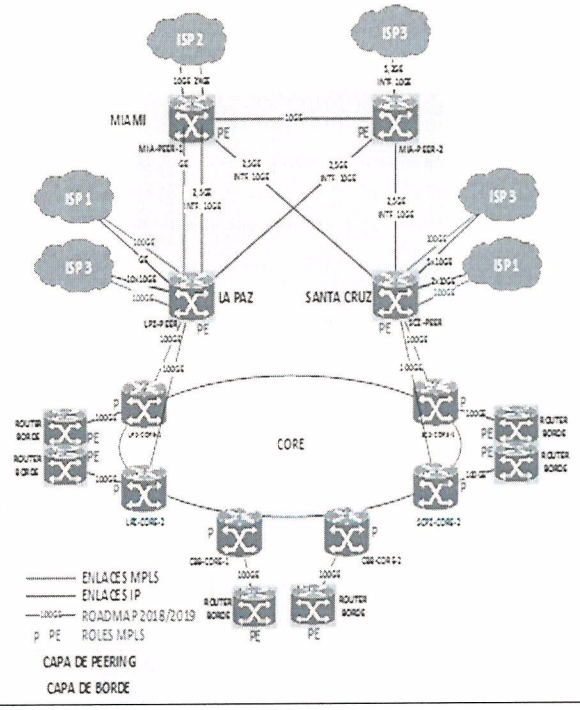
POR ENTEL SA.			
Nro.	**NOMBRE**	**UNIDAD**	**FIRMA**
1.	Marcos Pereira	Jefe Red de Transmisión y Datos IP	
2.	Jose Llampas	Profesional Implementación Proyectos de Acceso	
3.	Giovanni Mallo	Asesor Legal	
4.	Luz Andrea Ramos	Subgerente Adquisiciones a.i.	
5.	Saul Lobaton Valdez	Profesional Adquisiciones	

PROVEEDORES				
Nro.	**EMPRESA**	**NOMBRE**	**Teléfono – email**	**FIRMA**
1.	DIMA Ltda.	Ricardo Zamora	70647459 rzamora@dima.com.bo	
2.	ITC SERVICIOS	Ronald Luzio	71012806 rluzio@itcservicios.com	
3.	TLF INGENIERIA	Fernando Velasquez	73735657 ferchovelasduran@gmail.com	
4.	LOGICALIS Ltda.	Eduardo Sagarnaga	72140251 eduardo.sagarnaga@la.logicalis.com	
5.	HUAWEI TECHNOLOGIES (Bolivia) S.R.L.	Diego Zumelzu Albarracin	72035448 zumelzu.Diego@huawei.com	

Nro.	TEMAS TRATADOS	ACLARACIÓN/ MODIFICACIÓN
	PARTE LEGAL/ADMINISTRATIVA	
1.	Recomendación documentación	El asesor legal procedió a la recomendación para el cumplimiento de la totalidad de requisitos señalados en el TBC. La documentación deberá estar foliada, presentación de copias digitales, los sobres deberán presentarse de manera separada. Asimismo se deberá cumplir con la presentación de todos los documentos requeridos en el Punto 7.1 Sobre "A".
	PARTE TECNICA	
2.	Las soluciones están divididas en 2 partes: de detección y Mitigación si permite tener 2 marcar diferentes una marca por parte de detección y otra marca por la parte de mitigación.	Es factible aceptar la solución dividida. La administración de la gestión será respondida vía el portal WEB
3.	Cuáles son los volúmenes de tráfico a ser mitigado. Nosotros recomendamos cubrir el 20% de ancho de banda que Entel estaría gestionando.	Se aclara que los 10Gbps solicitados por Entel en los términos básicos de contratación son tráfico de ataque.
4.	2.- En la página 17, Numeral 3.10 se indica: "Mínimamente la solución debe realizar el bloqueo de los siguientes tipos de paquetes: "Paquetes que no sean válidos (incluidos los controles de encabezados IP malformados, fragmentos incompletos, checksum IP erróneos, fragmentos duplicados, fragmentos muy largos, paquetes pequeños, paquetes TCP pequeños, paquetes UDP pequeños, paquetes ICMP pequeños, checksums TCP/UDP erróneos, flags TCP inválidas, números ACK inválidos) y proporcionar estadísticas para los paquetes descartados. Estos valores y parámetros deben estar reflejados en los documentos de referencia de la oferta proporcionados por el fabricante" Las características solicitadas corresponder al método de operación de los equipos de un fabricante, cada fabricante tiene métodos diferentes de mitigación de ataques y en base a ello se pueden generar las políticas y estadísticas. Las características requeridas son parte del método estadístico asistido por controles manuales usados por dicho fabricante, otras fábricas usan métodos automatizados basados en el análisis de comportamiento de red. **Consulta.-** Por lo expuesto, solicitamos considerar como opcional las siguientes características solicitadas: Encabezados IP malformados Fragmentos incompletos	Se aclara que Entel requiere el tratamiento del tráfico anómalo. los oferentes deben aclarar de qué manera se realizara en tratamiento requerido por Entel del trafico anómalo

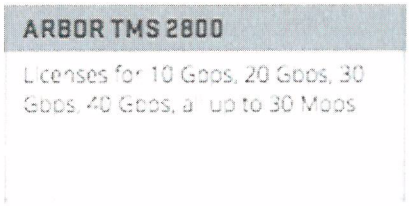
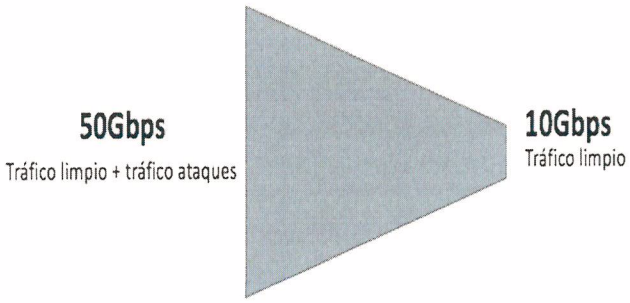
Nro.	TEMAS TRATADOS	ACLARACIÓN/ MODIFICACIÓN
	Checksum IP erróneos Fragmentos duplicados Fragmentos muy largos Paquetes pequeños Paquetes TCP pequeños Paquetes UDP pequeños Paquetes ICMP pequeños Checksums TCP/UDP erróneos Flags TCP inválidas Números ACK inválidos y permitir presentar de manera opcional: Encabezados inválidos IPv4 Encabezados inconsistentes I Inundaciones de Fragmentación T Pv6CP Checksum erróneos Paquetes de tamaño anómalo Checksum incorrecto IPv4 Flag TCP inválidos Inundaciones ACK"	
5.	Nuestra solución no se basa en la mitigación de tráfico en umbrales e IP de origen. ¿Se permitirá presentar soluciones con metodología basadas en análisis de comportamiento de red y creación automática de firmas en tiempo real?	Se aclara que el oferente debe explicar la forma del tratamiento del tráfico para el cumplimento de lo solicitado en el punto 3.10
6.	4.- En la Pagina 17, Numeral 3.10 se indica: "La solución debe permitir la prevención y mitigación de inundación suplantada de SYN TCP que autentifiquen conexiones TCP desde los hosts de origen sin impactar tráfico HTTP legítimo. Debe ser posible identificar los puertos origen y destino a ser mitigados. Debe proporcionar la capacidad para detectar y bloquear las inundaciones de SYN TCP por encima de la tasa configurada" **Consulta.-** Nuevamente la característica técnica solicitada corresponde al método de operación de un fabricante en particular, otros fabricantes líderes del mercado usan métodos y tecnologías diferentes, en ese sentido se solicita se considere como opcional el cumplimiento de "Debe ser posible identificar los puertos origen y destino a ser mitigados"	Entel requiere conocer los puertos de origen y destino en la parte de monitoreo.
7.	5.- En la Pagina 17, Numeral 3.10 se indica: "El sistema debe permitir la supresión de sesiones TCP inactivas si el cliente no envía una cantidad de datos configurable por el usuario dentro de un período de tiempo configurable por el usuario" **Consulta.-** La característica técnica solicitada corresponde al método de operación de un	Se debe cumplir el fin citado, el método a utilizarse es opcional para el oferente.

Nro.	TEMAS TRATADOS	ACLARACIÓN/ MODIFICACIÓN
	fabricante en particular. Dado que el requisito citado hace referencia a la protección contra los ataques del tipo ""low and slow"" se solicita se considere como opcional el cumplimiento del requisito referenciado y se permita ofertar la Protección específica contra ataques del tipo ""low and slow"""	
8.	6.- En la Pagina 17, Numeral 3.10 se indica "La solución debe permitir de poner en listas negras a los host después de un número de conexiones TCP consecutivas inactivas configurables por el usuario. El tráfico de los hosts en estas listas negras debe ser descartado por el sistema" **Consulta.-** Considerando que el requisito citado hace referencia la protección contra los ataques del tipo ""low and slow"" se solicita se considere como opcional el cumplimiento del requisito referenciado y se permita ofertar la Protección específica contra ataques del tipo ""low and slow"""	Se debe cumplir el fin citado como medida de prevención. El método a utilizarse es opcional para el oferente.
9.	Si se permite identificar el país de origen en la parte monitoreo.	Si se debe identificar el país de origen en la parte de monitoreo.
10.	Nosotros tenemos un sistema de alimentación diferente, y tenemos un sistema de firmas independiente, solicitamos que el SCANS Y PHISHING sea requerido de manera opcional.	Se responderá vía WEB. Se aclara que toda información de mitigación y ataques debe ser entrega a Entel.
11.	Si podemos brindas información de los ataques y amenazas sobre los cuales van a proteger las actualización, en lugar de INFORMACION DE HOST PAIS Y SISTEMA AUTONOMO.	Se responderá vía WEB.
12.	Realizamos la mitigación de ataques DNS pero no basados NXDomain y la mitigación por SIP no se realiza en base a tasa	Se debe explicar el método de mitigación por el cual no se requeriré el NXDOMAIN y el método de mitigación para SIP, se aclara que la parte de la detección es mandatorio.
13.	Podemos ofrecer más reportes que los solicitados por Entel, bajo otros indicadores	Se de explicar la equivalencia de lo requerido por Entel a lo presentado por los oferentes.
14.	Bajo qué criterios se solicita un equipo de mitigación en Miami	El criterio debe ser basado en el diseño de la solución del oferente.
15.	Dado que se tiene una plataforma RADWARE instalada en Entel consultamos si la integración al mimo puede ser presentado como un valor agregado.	Se es posible.
16.	En el pagina 16 numeral 3.9 confirma si se refiere al equipamiento para el monitoreo para el análisis de tráfico o para el equipamiento de análisis de ataques DDoS	El criterio debe ser basado en el diseño de la solución del oferente.
17.	Página 16 punto 3.9 para el componente de análisis de tráfico se requiere confirmar la cantidad de puertos disponibles en la capa de PEERING	Si se confirma que son los puestos disponibles en la capa de PEERING a nivel GE,10GE y 100GE, aclarar que los mimos deben ser incluidos en el diseño y propuesta.

Nro.	TEMAS TRATADOS	ACLARACIÓN/ MODIFICACIÓN
18.	Página 17 numeral 3.10 confirmar que si aceptaran propuestas de mitigación de: Encabezados inválidos IPv4 Encabezados inconsistentes IPV6 Inundaciones de Fragmentación T Pv6CP Checksum erróneos Paquetes de tamaño anómalo Checksum incorrecto IPv4 Flag TCP inválidos Inundaciones ACK"	Se aclara que Entel requiere el tratamiento del tráfico anómalo. los oferentes deben aclarar de qué manera se realizara en tratamiento requerido por Entel del trafico anómalo.
19.	Si se puede reutilizar equipamiento ya instalado en Entel.	Se debe proveer una solución con equipamiento nuevo y dedicado.
20.	En el punto 3.6. Sobre el esquema lógico solicitado. Consulta este detalle de información debe ser presentada en la propuesta.	Si, la información debe ser presentado en la propuesta con numeración y direccionamiento a manera de ejemplo.
21.	Punto 3.9 subpunto N° 3 debe ser posible la detecciónа 300 Gigas. Es necesario que se provea una capacidad de 300 Gigas iniciales en la detección de manera global.	Si, se debe proveer una capacidad 300 Gigas de detección de forma inicial y global
22.	Punto 3.10 sub punto 5. Habla sobre 10 gigas de tráfico malicioso con capacidad de ampliar tráfico a 40 gigas consideramos que 10 gigas no es suficiente de manera inicial para la mitigación.	La capacidad se responderá via web
23.	Punto 3.10 sub punto 5. Cuál sería la capacidad final de expansión	La capacidad de expansión es de 40 Gigas utilizando solamente licencias.
24.	En la grafica 	Si, la solución también debe contemplar la mitigación y detección en los equipos de borde del departamento de Cochabamba.

Nro.	TEMAS TRATADOS	ACLARACIÓN/ MODIFICACIÓN
	La solución debe contemplar la ciudad de Cochabamba	

CONSULTAS ESCRITAS.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
1.- En la Pagina 16, Numeral 3.9 se indica: "Debe ser posible la detección en todo el tráfico que cursa por los equipos precitados, 300Gbps, 150Gbps actuales y 150Gbps en roadmap 2018/2019". Por otro lado, en la Pagina 17, Numeral 3.10 se indica: "En cada Centro de limpieza o mitigación, se debe contar con una capacidad de mitigación de 10Gbps de tráfico malicioso con posibilidad de incrementar a 40Gbps únicamente con licencias sin modificación de hardware" Consideramos que el throughput solicitado de mitigación es insuficiente comparado con la capacidad de acceso a internet de ENTEL. Estas cifras parecen estar asociadas a una solución en particular y no a la previsión de ataques para la capacidad de internet indicada en las especificaciones técnicas:  Con un acceso de 150Gbps actual y un proyectado a 300Gbps la capacidad de 10Gbps solicitada consideramos que debería ser únicamente de tráfico legítimo y la capacidad total de mitigación debería ser como mínimo de 50Gbps para poder asegurar una adecuada protección de la red core de Entel y de sus clientes contra ataques de Denegación de Servicios. **Consulta:** Solicitamos que se modifique el requisito a 50 Gbps de capacidad Total de Mitigación (Tráfico limpio + Tráfico de Ataques) y 10Gbps de tráfico limpio. 	Las capacidades planteadas son consideradas suficientes dentro el Proyecto. Dado que las características de los ataques son aleatorias y según requerimiento del documento, se debe disponer de la información necesaria para que los ataques puedan ser mitigados en capas superiores de la red.
2.- En la página 17, Numeral 3.10 se indica: "Mínimamente la solución debe realizar el bloqueo de los siguientes tipos de paquetes: "Paquetes que no sean válidos (incluidos los controles de encabezados IP malformados, fragmentos incompletos, checksum IP erróneos, fragmentos duplicados, fragmentos muy largos, paquetes pequeños,	Las características solicitadas son necesarias para la mitigación DDoS y el método a utilizarse es opcional para el oferente.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
paquetes TCP pequeños, paquetes UDP pequeños, paquetes ICMP pequeños, checksums TCP/UDP erróneos, flags TCP inválidas, números ACK inválidos) y proporcionar estadísticas para los paquetes descartados. Estos valores y parámetros deben estar reflejados en los documentos de referencia de la oferta proporcionados por el fabricante" Las características solicitadas corresponder al método de operación de los equipos de un fabricante, cada fabricante tiene métodos diferentes de mitigación de ataques y en base a ello se pueden generar las políticas y estadísticas. Las características requeridas son parte del método estadístico asistido por controles manuales usados por dicho fabricante, otras fábricas usan métodos automatizados basados en el análisis de comportamiento de red. **Consulta.-** Por lo expuesto, solicitamos considerar como opcional las siguientes características solicitadas: Encabezados IP malformados Fragmentos incompletos Checksum IP erróneos Fragmentos duplicados Fragmentos muy largos Paquetes pequeños Paquetes TCP pequeños Paquetes UDP pequeños Paquetes ICMP pequeños Checksums TCP/UDP erróneos Flags TCP inválidas Números ACK inválidos y permitir presentar de manera opcional: Encabezados inválidos IPv4 Encabezados inconsistentes IPv6 Inundaciones de Fragmentación TCP Checksum erróneos Paquetes de tamaño anómalo Checksum incorrecto IPv4 Flag TCP inválidos Inundaciones ACK"	
3.- En la Pagina 17, Numeral 3.10 se indica: "La solución debe permitir el bloqueo basado en la tasa y volumen de tráfico, detectando fuentes que envíen cantidades excesivas de tráfico bajo umbrales configurables, para después colocar esas fuentes en listas de hosts bloqueados temporalmente" La característica técnica solicitada corresponde al método de operación de los equipos de un fabricante, otros fabricantes líderes en el mercado, usan metodologías superiores de mitigación basadas en análisis de comportamiento de red que permiten automatizar las tareas de mitigación y evitar los falsos positivos. **Consulta.-** Se solicita se considere como opcional las características citadas y se permita ofertar Tecnologías que permitan bloquear ataques de Denegación de Servicios basados en análisis de	La solución, además de ser requerida para tiempo real también es requerida para prevención, por tanto se deben cumplir estos requisitos.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
comportamiento de red y creación automática de políticas en tiempo real.	
4.- En la Pagina 17, Numeral 3.10 se indica: "La solución debe permitir la prevención y mitigación de inundación suplantada de SYN TCP que autentifiquen conexiones TCP desde los hosts de origen sin impactar tráfico HTTP legítimo. Debe ser posible identificar los puertos origen y destino a ser mitigados. Debe proporcionar la capacidad para detectar y bloquear las inundaciones de SYN TCP por encima de la tasa configurada" **Consulta.-** Nuevamente la característica técnica solicitada corresponde al método de operación de un fabricante en particular, otros fabricantes líderes del mercado usan métodos y tecnologías diferentes, en ese sentido se solicita se considere como opcional el cumplimiento de "Debe ser posible identificar los puertos origen y destino a ser mitigados"	La opción de identificar los puertos origen y destino debe estar disponible para que los ataques puedan ser mitigados en capas superiores de la red.
5.- En la Pagina 17, Numeral 3.10 se indica: "El sistema debe permitir la supresión de sesiones TCP inactivas si el cliente no envía una cantidad de datos configurable por el usuario dentro de un período de tiempo configurable por el usuario" **Consulta.-** La característica técnica solicitada corresponde al método de operación de un fabricante en particular. Dado que el requisito citado hace referencia a la protección contra los ataques del tipo ""low and slow"" se solicita se considere como opcional el cumplimiento del requisito referenciado y se permita ofertar la Protección específica contra ataques del tipo ""low and slow"""	Se debe cumplir el fin citado, el método a utilizarse es opcional para el oferente.
6.- En la Pagina 17, Numeral 3.10 se indica "La solución debe permitir de poner en listas negras a los host después de un número de conexiones TCP consecutivas inactivas configurables por el usuario. El tráfico de los hosts en estas listas negras debe ser descartado por el sistema" **Consulta.-** Considerando que el requisito citado hace referencia la protección contra los ataques del tipo ""low and slow"" se solicita se considere como opcional el cumplimiento del requisito referenciado y se permita ofertar la Protección específica contra ataques del tipo ""low and slow"""	Se debe cumplir el fin citado como medida de prevención. El método a utilizarse es opcional para el oferente.
7.- En la Pagina 17, Numeral 3.10 se indica: "La solución deberá permitir autentificar solicitudes DNS desde el host origen, y suprimir aquellas que no puedan ser autentificadas dentro de un tiempo específico. Debe permitir limitar el número de consultas DNS por segundo a una velocidad configurable por el usuario. La solución debe permitir bloquear el tráfico desde cualquier host que genere más solicitudes DNS fallidas consecutivas del límite configurado y poner al host origen en una lista negra" **Consulta.-** La característica técnica solicitada corresponde al método de operación de un fabricante en particular e introduce una vulnerabilidad al convertir el sistema stateful al aplicar esta política. Para poder contar con tecnologías superiores, se solicita se considere como opcional el cumplimiento del requisito "La solución debe permitir	Estas funcionalidades son requeridas para la protección y prevención para DNS. El método a utilizarse es opcional para el oferente.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
bloquear el tráfico desde cualquier host que genere más solicitudes DNS fallidas consecutivas del límite configurado y poner al host origen en una lista negra"	
8.- En la Pagina 17, Numeral 3.10, se indica: "Debe permitir bloquear tráfico en base al país de origen del mismo" **Consulta.-** La característica técnica solicitada asociada a otros requerimientos del pliego corresponde al método de operación de los equipos de un fabricante e introduce un alto riesgo de falsos positivos pues en el presente panorama mundial de DDoS, los botnets se pueden ubicar en múltiples países que también generan tráfico legítimo; en caso se bloquee el tráfico de dicho país se bloqueará también el tráfico válido, en ese sentido se solicita se considera como opcional el cumplimiento del requerimiento referenciado	Dadas las características aleatorias de los ataques DDoS, la funcionalidad debe estar disponible.
9.- En la Pagina 18, Numeral 3.12 se indica: "El servicio de actualización debe estar basado en procesos de investigación y análisis por parte del fabricante para poder mitigar las amenazas y ataques actuales. Por lo cual se deberá contar con algún sistema de inteligencia donde se esté monitoreando las amenazas de Internet a nivel mundial y deberá proporcionar información sobre: • Botnets • DDoS • FastFlux Bots • Scans • Phishing Proporcionando información por host, país y sistema autónomo de BGP. Estos datos deberán estar públicos en el sitio web del fabricante" **Consulta.-** Se solicita se considere como opcional el cumplimiento de las siguientes especificaciones: "• Scans, • Phishing proporcionando información por host, país y sistema autónomo de BGP. Estos datos deberán estar públicos en el sitio web del fabricante"	Dada la amenaza que representan los tipos citados, deben estar disponibles en la solución. La información permitirá que los ataques puedan también ser mitigados en capas superiores de la red.
10.- En la Pagina 18, Numeral 3.15 se indica: "Para detección y mitigación, la solución deberá proporcionar mínimamente los siguientes valores: pps/bps para bloqueos de umbrales, tasa de peticiones HTTP por segundo, tasa de objetos HTTP por segundo, tasa de peticiones DNS, tasa de respuestas DNS NXDomain, tasa de mensajes SIP, tasa de bps y pps para ICMP, UDP y fragmentación" **Consulta.-** La característica técnica solicitada corresponde al método de operación de un fabricante en particular y por lo tanto imposibilita el cumplimiento de fabricantes líderes del mercado que usan métodos y tecnologías diferentes, en ese sentido se considere como opcional el cumplimiento de las siguientes especificaciones: "tasa de respuestas DNS NXDomain, tasa de mensajes SIP"	Se debe proveer indicadores sobre respuestas DNS NXDomain y mensajes SIP.
11.- En la Pagina 18, Numeral 3.18 se indica: "Se debe proveer un sistema de gestión centralizado que permita el monitoreo de toda la solución a ser provista, cumpliendo con las características detalladas a continuación" Una tendencia global en los principales operadores de	Por políticas de ENTEL, la gestión debe estar centralizada en la empresa, por lo tanto se debe proveer este sistema.

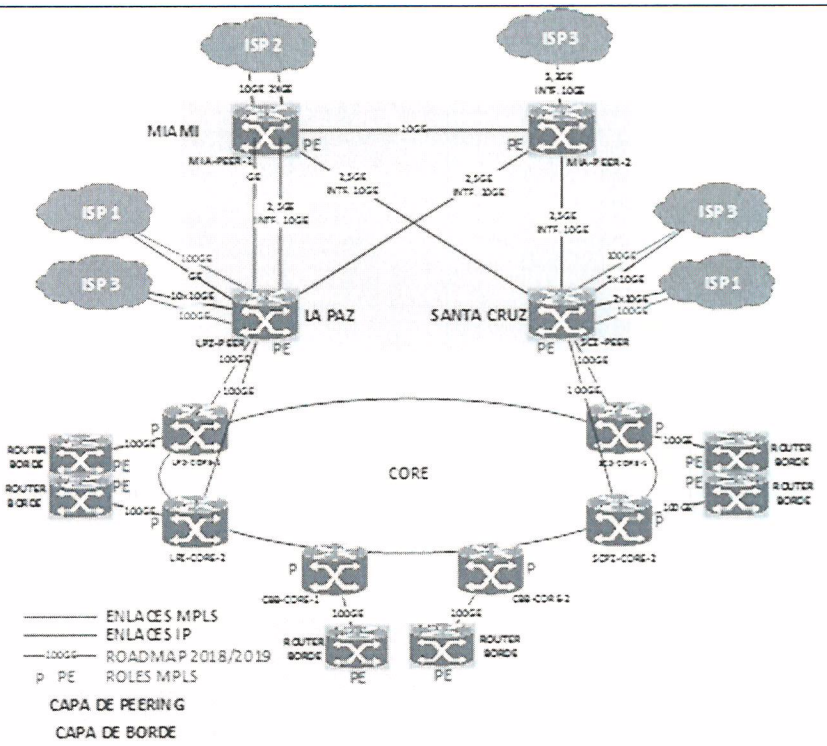
CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
Telecomunicaciones a nivel global incluidos los Tier 1 es la de seleccionar un fabricante para el Monitoreo/Detección de Ataques y otro diferente para la MItigación de los Ataques DoS/DDoS, permitiendo de esa manera a las instituciones adquirir la mejor tecnología para cada componente de la estrategia de detección y limpieza de ataques de denegación de servicios. **Consulta.-** Para garantizar una sana competencia, se solicita se considere como opcional el requisito referenciado y se acepten propuestas en las que se usen sistemas de gestión diferentes para el Monitoreo/Detección y para la Mitigación/Limpieza de Ataques"	
12.- En la Pagina 19, Numeral 3.22 se indica: "Debe contar con estadísticas gráficas detalladas de tráfico permitido y mitigado a nivel de cliente, grupo de clientes y sistema, en rangos de tiempo de 5 minutos, 1 hora, 24 horas, 7 días o intervalos personalizados. Se debe contar con un histórico mínimo de un mes" **Consulta.-** Se solicita se considere como opcional el requisito referenciado y se acepten propuestas con sistemas de reportes y gestión que posean las siguientes características: - Dashboard de Seguridad - Ancho de Banda, Conexiones por Segundo, Paquetes por Segundo - Detalles por evento de Seguridad : Mostrar Tráfico de Ataques, Firmas en tiempo real, Gráfico de Ataques, Paquetes Por segundo y Throughput asociado al ataque deberá incluir como mínimo los siguientes reportes de seguridad: - Ataques permitidos y denegados - Ataques permitidos por Fuente y Destino - Ataques por Destino y Puerto - Ataques por Categoría de Amenaza - Ataques Críticos - Principales Fuentes de Ataques - Principales Aplicaciones Atacadas - Principales Destinos Atacados - Principales Atacantes por Hora del Día - Principales Ataques por Protocolo - Principales Ataques por Fuente - Categorías de Ataques por Ancho de Banda - Ataques por VLAN - Ataques por política de seguridad de red - Ancho de banda por Categoría de Amenaza por Hora del Día - Principales Ataques por Ancho de Banda - Principales Ataques por Duración"	Se considera que lo solicitado, es una medida de la operación fundamental del sistema, es decir la cantidad de tráfico permitido y mitigado. Es posible aceptar la propuesta siempre que exista la posibilidad de verificar lo solicitado y en los rangos de tiempo especificados.
13.- En la Pagina 19, Numeral 3.34 se indica: "Sobre todo el tráfico monitoreado y mitigado, se debe mostrar a detalle y gráficamente: tráfico total, tráfico total permitido y bloqueado, número de hosts bloqueados, estadísticas sobre cada tipo de prevención, tráfico por URL, tráfico por dominio, información de ubicación IP, distribución de protocolos, distribución de servicios y estadísticas principales de hosts bloqueados" **Consulta.-** se solicita se considere como opcional el requisito referenciado y se acepten propuestas con sistemas de reportes y gestión que posean las siguientes características:	Los indicadores son mandatorios, se aceptarán los reportes propuestos.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
- Dashboard de Seguridad - Ancho de Banda, Conexiones por Segundo, Paquetes por Segundo - Detalles por evento de Seguridad : Mostrar Tráfico de Ataques, Firmas en tiempo real, Gráfico de Ataques, Paquetes Por segundo y Throughput asociado al ataque deberá incluir como mínimo los siguientes reportes de seguridad: - Ataques permitidos y denegados - Ataques permitidos por Fuente y Destino - Ataques por Destino y Puerto - Ataques por Categoría de Amenaza - Ataques Críticos - Principales Fuentes de Ataques - Principales Aplicaciones Atacadas - Principales Destinos Atacados - Principales Atacantes por Hora del Día - Principales Ataques por Protocolo - Principales Ataques por Fuente - Categorías de Ataques por Ancho de Banda - Ataques por VLAN - Ataques por política de seguridad de red - Ancho de banda por Categoría de Amenaza por Hora del Día - Principales Ataques por Ancho de Banda - Principales Ataques por Duración"	

Point 3.8 Funcionalities Point. 3.9 • El equipamiento podrá disponerse en las ciudades del eje troncal y opcionalmente en Miami. • Se debe soportar la cantidad de interfaces actual. Para fines de crecimiento, en los enlaces de Peering hacia los ISP se debe considerar la siguiente cantidad de puertos GE/10GE (intercambiables por SFP): 24 puertos La Paz, 24 puertos Santa Cruz y 12 puertos Miami, adicionalmente se debe incluir los interfaces en roadmap. **Consulta.-** Por favor confirmar si se tiene que proveer el equipmaiento en Miami con un ítem adicional o mandatorio en la propuesta técnica y comercial, ya que hay varios costos asociados al no tratarse de suelo Boliviano como provisión, desaduanización, instalación, soporte que deben ser dimensionadionados correctamente.	Si la solución planteada requiere la provisión e implementación de equipos en Miami, ésta puede ser realizada directamente en este sitio.
Point 3.8 Funcionalities Point. 3.9 • El equipamiento podrá disponerse en las ciudades del eje troncal y opcionalmente en Miami. Se debe soportar la cantidad de interfaces actual. Para fines de crecimiento, en los enlaces de Peering hacia los ISP se debe considerar la siguiente cantidad de puertos GE/10GE (intercambiables por SFP): 24 puertos La Paz, 24 puertos Santa Cruz y 12 puertos	Si la solución planteada requiere la provisión e implementación de equipos en Miami, ésta puede ser realizada directamente en este sitio.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
Miami, adicionalmente se debe incluir los interfaces en roadmap **Consulta.-** Por favor confirmar alcance de los trabajos y provision de equipos en Miami para realizar el dimensionamiento correct.	
REQUERIMIENTOS GENERALES 3.1 Se debe proveer e implementar un Sistema de Seguridad Anti DDoS (Distributed Denial of Service) que se integre de forma transparente a la Red de Internet de ENTEL S.A. y actúe sobre las capas de Peering y Borde detalladas a continuación, permitiendo analizar y monitorear el tráfico de Red de modo que se pueda detectar patrones de ataque o tráfico malicioso del tipo DDoS, así como la mitigación de los mismos de forma automatizada, rápida y efectiva. Consulta.- De acuerdo a la topología, los equipos deben soportar 100Gbps o 40Gbps para conectarse a través de Router de Borde PE con el fin de mitigar los ataques DDoS. Por favor aclarar el requerimiento.	En el presente documento TBC se especifica los interfaces mínimos requeridos para la integración. Sin embargo, de acuerdo a la solución específica del proveedor, se debe proveer todos los interfaces que se consideren necesarios para que la misma sea puesta en producción.

DADO EL SIGUIENTE GRÁFICO	El entendimiento es correcto.

CONSULTAS	ACLARACIÓN/ MODIFICACIÓN
 ¿Dado el gráfico anterior se debe entender que la solución debe abarcar 4 equipos de Peering y 6 equipos de Borde? Esto para dimensionar el Licenciamiento adecuado requerido para la solución.	
¿Dado el punto 3.9 que indica "El equipamiento podrá disponerse en las ciudades del eje troncal y opcionalmente en Miami." Se debe considerar que ENTEL S.A. puede disponer una instalación de equipos en MIAMI?	Es correcto, ENTEL S.A. cuenta con un nodo de Telecomunicaciones en la ciudad de Miami USA.
En el punto 3.42 indica que se deberá contar con equipos "repuesto" estos deben estar en oficinas de ENTEL SA o en almacenes del Proveedor para poder Mantener los SLA del pliego.	Deberán estar en oficinas de ENTEL S.A.
Toda la solución debe ser de la misma marca o ENTEL S.A permitiría la convergencia de herramientas de terceros para realizar la detección y/o mitigación?	Debe ser de la misma marca, sin embargo es posible aceptar integraciones con equipos existentes en ENTEL.
Con la consulta No 1 de todos los equipos considerados para el licenciamiento. ENTEL S.A puede proveer Marca Modelo y versión de Sistema Operativo de estos equipos?	Peering: Marca Cisco, Modelo ASR9010, Versión 6.1.4 Borde: Marca Cisco, Modelo ASR9904/9010, Versión 5.1.3
Considerando que se trata de una solución de misión crítica, que debe operar de forma transparente, Entel debería solicitar experiencia demostrable del fabricante de instalaciones similares en Service Providers tanto en Bolivia como de la región. Podría ser incluido como mandatorio/calificable?	No es posible realizar esta modificación.
¿ENTEL S.A. Requiere Gente certificada que radique en Bolivia?	Es lo requerido durante el tiempo de implementación.
Para poder dimensionar los costos del cableado estructurado, solicitamos realizar una visita técnica de los sitios donde se instalarán los equipos.	No es posible realizar el survey en esta instancia del proceso.