Proyecto Sistema Hiperconvergente BANHPROVI

Antecedentes

Durante los años 2011 y 2013, el BANHPROVI adquirió una infraestructura de servidores tipo "blade" para el sitio principal y sitio alterno, con el objetivo de contar con una infraestructura sólida para soportar la operación del core bancario ABANKS, incluyendo una estrategia de recuperación en caso de desastres. Si bien la operación del core ya se migró a una nueva plataforma, dicha infraestructura aún se encuentra en funcionamiento y sobre ella corren servicios críticos para la operación del BANHPROVI, como ser:

a. Active Directory
b. Servidores de WebService, que cada día cobran más importancia al tercerizar ciertas herramientas.
c. Servidores de bases de datos SQL para los sistemas:
    i. Planilla
    ii. Activo fijo
    iii. Históricos de contabilidad
    iv. Históricos de sistemas de cartera
d. Servidor de consola de antivirus
e. Servidores de Archivos (FileServer)
f. Sistemas de Digitalización (LaserFiche)

En la actualidad, los equipos que componen la infraestructura virtualizada con VMWare se encuentra fuera de servicio de soporte, debido a que por la obsolescencia de los mismo dicha renovación es de un costo muy elevado. Esto nos coloca en una posición de riesgo elevado, pues se trata de servidores que se aproximan a los 10 años de operación y que ya presentan fallas de algunos de sus componentes, sin que tengamos la posibilidad de repararlos.

Objetivos

1. Renovar la infraestructura de servidores que soporta las aplicaciones secundarias, y que ya presenta signos de deterioro.
2. Contar con una plataforma adecuada para el desarrollo de futuras aplicaciones que requieran las distintas áreas del Banco.
3. Reducir el riesgo tecnológico del BANHPROVI, colocando las aplicaciones "secundarias" (pero críticas para la operación) en infraestructura adecuada.
4. Rehabilitar la alta disponibilidad y resiliencia frente a fallas en ambos centros de datos.
5. Proteger la información crítica del BANHPROVI implementando tecnologías como RAID 1 y herramientas de y respaldo y replicación
6. Realizar Disaster Recovery del sitio principal al alterno, con el propósito de asegurar la continuidad de las operaciones
7. Implementar una herramienta para monitorear los equipos desde una consola centralizada, para prevenir fallas
8. Reducir los puntos de fallas de las aplicaciones y equipos que requieran contratos de soporte
9. Establecer la capacidad para interconectar a nubes públicas o híbridas, ahora o en un futuro

Especificaciones Técnicas

La solución tecnológica requerida por el BANHPROVI debe de incluir lo siguiente:

	Características Generales	
	Sistema Hiperconvergente deberá de incluir 2 dispositivos (appliances) como mínimo por sitio, a ser instalados bajo la modalidad llave en mano en el sitio principal y el sitio alterno respectivamente, en configuraciones similares, los cuales se utilizarán en modo activo-pasivo entre sitios.	
	El Fabricante del Sistema Hiperconvergente deberá estar ubicado en el cuadrante de líderes, en el último Cuadrante Mágico de Gartner para infraestructura hiperconvergente disponible a la fecha de publicación del proceso.	
	El soporte del Sistema Hiperconvergente debe ser entregado en forma unificada: hardware de los Nodos, virtualización de cómputo, virtualización de almacenamiento y sistemas de gestión a través de un servicio de soporte integral y unificado.	
	El Hardware debe ser soportado y certificado por el fabricante de Hiperconvergencia como sistema hiperconvergente.	
	Los componentes ofertados deben ser nuevos de fábrica, no remanufacturados, ni reparados, ni reacondicionados en ninguna de sus partes.	
	Las actualizaciones de software, firmware, parches/fixes deben ser certificadas para cada uno de los elementos del sistema de hiperconvergencia como ser: Virtualización Cómputo, Virtualización Almacenamiento y Sistema de Gestión. El fabricante debe entregar los detalles de parches soportados y su procedimiento de aplicación mientras se encuentre vigente el contrato soporte.	
	El oferente deberá ofrecer y certificar un esquema de atención directa de llamadas y problemas que deberá ser provisto desde un centro de soporte unificado, desde donde deberán asistirse todos los problemas asociados a los componentes de red, computo, almacenamiento y virtualización.	
	El sistema debe contar con una aplicación de soporte que reporte el estado del equipo al fabricante en forma automática, para diagnóstico, monitoreo remoto y call home.	
	El soporte a la solución tanto a nivel de software como de hardware deberá ser en un horario 24x7x365, por un periodo de 60 meses, en idioma español y con la posibilidad de escalar a fabrica. El oferente deberá de brindar la documentación necesaria para la comunicación en el caso de requerirse el soporte.	
	El proveedor deberá de presentar documentación de parte del fabricante que compruebe que posee piezas de reemplazo en el territorio nacional, con la capacidad de entregar las piezas de remplazo en 4 horas 24x7x365, tanto en Tegucigalpa como en San Pedro Sula.	
	Se requiere que la solución de infraestructura de software siga el concepto de **SDDC** (Software Defined Data Center) y constituya el primer paso para migrar a un servicio de nube pública, mediante herramientas nativas a la solución de virtualización.	
	Deberán ofrecer una interfaz gráfica y amigable al usuario para realizar las tareas administrativas de toda la solución tanto del sitio principal como sitio alterno	
	Debe poder escalar los recursos informáticos y de almacenamiento de al menos 32 servidores (nodos) administrados de forma unificada	
	La solución deberá tener la característica de soportar la instalación de actualizaciones, sin que se requiera dar de baja ningún servicio en	

	producción, con el objetivo de no producir interrupciones en los servicios informáticos del BANCO	
	La solución deberá de incluir al menos dos (2) servidores físicos (nodos) del tipo rack por sitio con su respectivo almacenamiento y de configuración flexible.	
	El proveedor debe considerar en su oferta cualquier hardware o software adicional que sea requerido o necesario para brindar la protección de fallos en caso de que uno de los equipos de la solución de cada sitio presente algún problema, el otro pueda seguir funcionando	
	La solución deberá de contener todo el cableado tanto eléctrico como de comunicación necesario para el correcto funcionamiento y conexión del storage que el BANCO ya posee, los oferentes deberán de realizar las visitas correspondientes para validar estas conexiones.	
	El soporte a la solución debe tanto a nivel de software como de hardware objeto de esta licitación deberá ser en un horario 24x7 por un periodo de 60 meses en idioma español con la posibilidad de escalar a fabrica. **El oferente deberá de brindar la documentación necesaria para la comunicación en el caso de requerirse el soporte.** Además, el proveedor deberá de presentar una carta de parte del fabricante que asegure que posee piezas de reemplazo en el territorio nacional (presentar copia de la carta)	
	La solución ofertada deberá de prever crecimientos futuros, los cuales deberán ser independientes de la plataforma de hardware ofertada, esto significa que se podrá a futuro agregar nodos de un segundo fabricante de hardware con nodos similares	
	La solución deberá de permitir el crecimiento de manera vertical (agregar más discos, memoria) a cada uno de los nodos, o de manera horizontal (agregar mas nodos completos), con lo que se busca contribuir al almacenamiento compartido	
	Para procurar la mayor compatibilidad con la infraestructura actual y la migración más transparente posible se debe incluir el software de virtualización VMware como hipervisor debido a que este es el software actualmente utilizado. Se requiere al menos contar con licenciamiento vSphere Standard y vCenter foundation para cada sitio	
	La solución deberá de ser capaz de incrementar mas memoria y discos sin incrementar el costo de soporte ni el licenciamiento de software de toda la solución	
	No se aceptará soluciones que requieran almacenamiento externo a los servidores (nodos)	
	El proveedor deberá de tener un centro de soporte con atención 24/7 en caso de que el BANCO requiera solución a cualquier problema con la infraestructura ofertada	
	Toda la solución propuesta deberá de tener al menos 60 meses de licenciamiento y soporte	

Especificaciones Técnicas de Cada Servidor que Integra la Solución.

	La solución ofertada deberá tener al menos un (1) procesador igual o superior al Intel Xeon 6230R	
	Deberán de manejar al menos 26 cores totales	
	Deberán de manejar al menos 52 threads totales	
	Un mínimo de 256 GB RAM de tipo DDR4 RDIMM ECC de 2933Mhz	
	Deberán de tener la capacidad mínima de crecimiento en cada nodo de al menos 1024GB de memoria RAM sin cambiar DIMM	

	La memoria RAM de los equipos debe de estar instalada y certificada, por lo que se les indica a los participantes que no se admitirá memorias genéricas o que no sea certificadas por el fabricante	
	Deberá de poseer (equipado) un expansor de la tarjeta de red con puertos duales de 8GB de fibra canal.	
	Deberá de poseer (equipado) dos (2) expansores de la tarjeta de red con puertos duales de 10GbE de manera que cada servidor de la solución cuente con al menos 4 interfaces de 10GbE	
	Deberá de contar con una tarjeta de red de administración de al menos de 1GB para el acceso remoto a la solución	
	Deberá soportar el acceso mediante una solución de KVM remota y el protocolo SSH	
	Los equipos que componen la solución deberán soportar el arranque (boot) desde una tarjeta USB o M2 flash para inicio del sistema	
	La solución ofertada deberá de soportar el concepto de almacenamiento basado en software o hiperconvergencia de almacenamiento	
	Deberá soportar al menos los siguientes sistemas operativos: Vmware vSphere 6.7 o superior Microsoft Windows Server 2019 o la más reciente al momento de esta licitación La solución deberá de soportar las nuevas versiones de sistemas operativos y/o sus respetivas actualizaciones que vayan saliendo durante el periodo de la garantía	
	La solución deberá de ser capaz de asignar políticas de protección a las máquinas virtuales en términos de número de tolerancia a fallos (FTT - Failures to tolerate). Esto es, desde ninguna tolerancia hasta tolerancias de 1 o más fallas.	
	Virtualización de cómputo (Hipervisor)	
	El proveedor del Sistema Hiperconvergente debe proveer el soporte integrado de la capa de virtualización de cómputo, ósea deberá de proveer el soporte como un todo.	
	El Hipervisor debe incluir switches virtuales distribuidos de modo de manejar las configuraciones de estos como una sola entidad.	
	Los switches virtuales deberán estar distribuidos entre los nodos del Cluster de la solución de hiperconvergencia.	
	El Hipervisor debe proveer una funcionalidad de registro o LOG integrada de modo de proveer una visión de los eventos de hardware y software.	
	El Hipervisor debe disponer de funcionalidades de alta disponibilidad automática, distribución automática de recursos y migración de almacenamiento en caliente.	
	Para procurar la mayor compatibilidad con la infraestructura actual y la migración más transparente posible se debe incluir el software de virtualización VMware como hipervisor debido a que este es el software actualmente utilizado. Se requiere al menos contar con licenciamiento vSphere Standard y vCenter foundation para cada sitio.	

Especificaciones Técnica del Almacenamiento de la Solución Propuesta

El almacenamiento de los servidores debe ser de la siguiente manera:

	El almacenamiento ofrecido en los servidores deberá ser de tipo SSD para todos los servidores que compongan la solución ofertada	
	Capacidad de almacenamiento total presentado de 20TB por sitio, con la siguiente configuración:	

	Almacenamiento efectivo presentado por la solución deberá ser de al menos 20TB efectivos, sin compresión ni de-duplicación, no debe de considerar el almacenamiento presentado en cache y debe excluir los requerimientos para mecanismos de rebalanceo	
	Al menos 960GB SSD para cache.	
	El sistema de virtualización de almacenamiento debe poder configurarse en uno de dos modos: - All flash: donde todos los discos del sistema son del tipo SSD. - Híbrido: donde se mezclan discos SSD y discos SAS o SATA. En ambos casos uno de los discos SSD debe cumplir las funciones de caché de escritura y debe ser del tipo “High Endurance”.	
	La distribución del espacio se realizará al momento de la implementación	
	Deberá de soportar la inserción y remoción en caliente (hot-swap) de los discos duros	
	Debe adoptar la arquitectura de almacenamiento distribuido en escalamiento horizontal con el propósito de admitir la migración automática de datos y el equilibrio durante la expansión y/o reducción de la capacidad, todo lo anterior en relación en los casos que se requiera más recursos tanto de computación y almacenamiento	
	El almacenamiento ofertado deberá de permitir tener configuración de tipo RAID 1	
	El Acceso al almacenamiento irá directamente al kernel de la solución de virtualización	
	Virtualización de almacenamiento	
	El sistema de hiperconvergencia debe soportar la arquitectura para almacenamiento de vSAN.	
	El sistema hiperconvergente debe incluir un software integrado de virtualización de almacenamiento (vSAN).	
	No se aceptarán soluciones basadas en Virtual Storage Appliance (VSA) que corran como una máquina virtual tipo *guest* en cada nodo.	
	El fabricante del Sistema Hiperconvergente debe proveer el soporte integrado de la capa de virtualización de almacenamiento.	
	La capa de virtualización de almacenamiento debe correr en el mismo Kernel del hipervisor a fin de optimizar el uso de los recursos y asegurar performance.	
	La solución integrada de almacenamiento del sistema hiperconvergente debe permitir la creación de un pool de almacenamiento distribuido con capacidad de crecer mediante scale up (adicionando discos individuales) y scale out (añadiendo nodos con discos internos).	
	La organización local de los discos de cada nodo del cluster debe ser en disk groups.	
	Cada disk group del nodo debe soportar por lo menos de un disco de estado sólido configurado como caché.	
	La administración de la virtualización de almacenamiento debe ser integrada a la administración de servidores virtuales y no ser una consola independiente.	
	Los requerimientos de almacenamiento deberán ser manejados a través de definición de políticas que contengan elementos como: - Desempeño - Nivel de protección - Calidad de Servicio Estas características deben tener la granularidad de disco virtual y podrán ser modificadas dinámicamente. Los objetos y componentes de las máquinas virtuales deberán estar distribuidos entre todos los disks groups del cluster.	

	El sistema de hiperconvergencia deberá contar con la capacidad de establecer límites superiores de IOPs que una máquina virtual pueda desempeñar.	
	El sistema propuesto deberá contar con la capacidad futura de poder crear una configuración de Cluster distribuido entre nodos ubicados en diferentes centros de datos.	

Especificaciones Técnicas del Software de Gestión y Administración

	Deberá proporcionar puertos de administración y control remotos independientes y GUI para la supervisión remota a fin de implementar control remoto completo sobre los servidores, independientemente del tipo de sistema operativo. El control remoto completo deberá incluir entre otras cosas inicio, apagado y restablecimiento remoto, y virtualización de USB y CD-DVD	
	Debe de poseer la opción de reiniciar automáticamente los servidores	
	Deberá de tener la opción de controlar los módulos de ventiladores, fuentes de alimentación y control de temperatura	
	Debe de permitir la gestión remota de cada uno de los nodos	
	Debe de ser capaz desde la misma herramienta realizar las actualizaciones del firmware local	
	Debe de llevar un control de todos los eventos	
	Las funciones de administración de cómputo y de almacenamiento virtualizado deben ser integradas en una sola consola.	
	Debe proveerse una consola integrada tipo GUI para realizar funciones de gestión. Al menos debe contar con todas las siguientes: - Aprovisionamiento de nodos nuevos - Actualización de parches de software del sistema - Visualizar la utilización de los recursos - Visualizar el estado de salud del sistema	
	Debe proveer capacidad de monitoreo remoto (call home) para diagnóstico y reparación.	

Especificaciones Técnicas Software de Replicación y copias de respaldo

El BANHPROVI requiere una solución capaz de enviar réplicas de las máquinas virtuales del sitio principal al sitio alterno, para lo cual consideramos que el software debe de contar con las siguientes características

	Debe ser capaz de realizar copias de seguridad basadas en imágenes y con reconocimiento de aplicaciones	
	Debe ser capaz de realizar copias de respaldo completas	
	Deberá ser capaz de administrar los archivos de copias de seguridad de las máquinas virtuales	
	Deberá ser capaz de replicar cada una de las máquinas virtuales basada en imágenes	
	Deberá de poseer un mecanismo de **Failover para recuperación asistida**	
	Deberá ser capaz de realizar copias de respaldo desde un respaldo existente	
	Deberá ser capaz de realizar conmutación por error planeados, o entrar en modo Failover a solicitud del usuario	
	Capaz de recuperar máquinas virtuales completas	
	Deberá ser capaz de recuperar archivos de máquinas y discos virtuales	

Servicio Conexos

	El proveedor en su propuesta el deberá de considerar la interconexión de la SAN que actualmente posee el banco tanto para el sitio principal como para el sitio de contingencias.	
	El oferente deberá de considerar en su oferta la migración de al menos 10 maquinas virtuales de la infraestructura actual, cabe aclarar que son maquinas virtualizadas en vmware.	
	El oferente deberá de considerar en su oferta una capacitación certificada para al menos 3 colaboradores del BANHPROVI sobre el uso de la plataforma de software ofertada incluyendo los componentes de cómputo, virtualización del almacenamiento y software de replicación y copias de seguridad.	

Proyecto de Comunicación de red BANHPROVI

Antecedentes

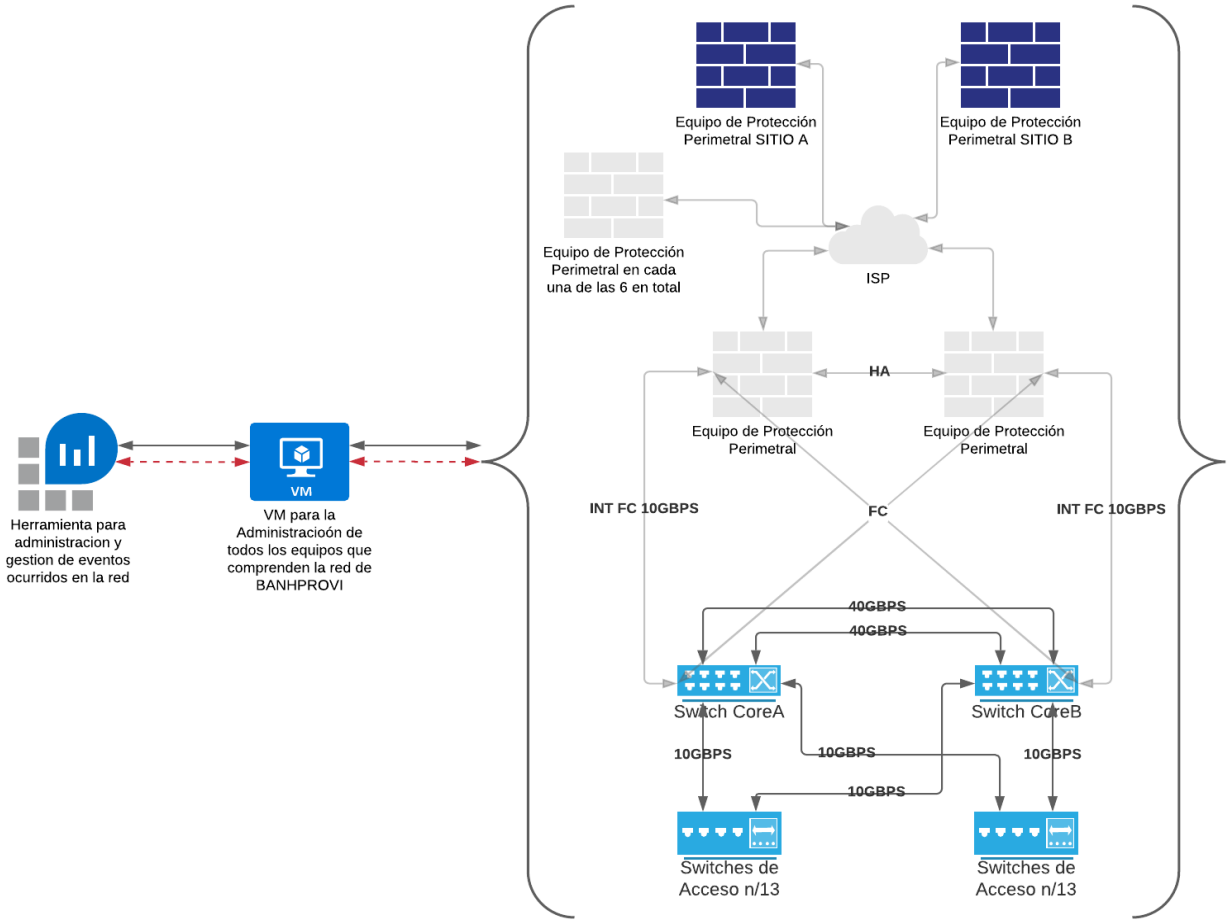
Durante el año 2015, el Banco adquirió equipos de comunicación, con el propósito de sustituir otros que databan del 2005 y que presentaban un grado de obsolescencia alto. Sin embargo, con los pasos acelerados que ha dado el BANHPROVI, tanto en número de colaboradores como en todos los servicios digitales que se prestan, se requiere fortalecer dicha infraestructura de comunicación para afrontar exitosamente los nuevos retos que el BANHPROVI se esta imponiendo, con el objetivo de ser un banco con altos niveles de servicio y productos bancarios.

Objetivos

a. Modernizar la infraestructura de comunicaciones para poder asegurar una comunicaciones segura y confiable entre los colaboradores y los servicios tecnológicos
b. Crear una consola de control de incidentes, para dar soluciones a temas relacionados con comunicaciones.
c. Aumentar las velocidades comunicación dentro de la red del BANHPROVI
d. Llevar un control de los incidentes de seguridad de la información.
e. Crear sistemas de encriptación de enlaces de datos entre las oficinas y los centros de datos.
f. Centralizar la administración de todos los equipos de comunicación del BANCO, para poder dar soporte y responder a problemas de manera más rápida y certera.

Para poder alcanzar dichos objetivos, es necesario realizar una reestructuración a nivel de equipos de comunicación. En el punto 1 de esta sección Términos de Referencia se establece un diagrama de comunicación el cual se considera apto para soportar la transferencia de datos.

1. Diagrama Propuesto



2. Switches

ítem	Descripción	Cumple	
		SI	NO
Características Generales			
2.1	**Funcionalidades de Administración**	**---**	
2.1.01	El switch deberá poder aceptar acutalizaciones de firmware desde una interface de tipo GUI		
2.1.02	Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la funcion de PoE		
2.1.03	Deberá soportar detección y notificación de conflictos de direcciones IP		
2.1.04	Deberá soportar administración en la nube		
2.1.05	Deberá soportar administración por IPv4 e IPv6		
2.1.06	Deberá soportar Telnet / SSH para acceso a la consola		
2.1.07	Deberá soportar HTTP / HTTPS		
2.1.08	Deberá soportar SNMP v1/v2c/v3		

2.1.09	Deberá poder configurar su reloj mediante un NTP Server		
2.1.10	Deberá contar con una linea de comandos estándar y con interface para configurar via Web		
2.1.11	Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI		
2.1.12	Deberá soportar HTTP REST APIs para Configuracion y monitoreo		
2.2	**Funcionalidad de Alta Disponibilidad**	**---**	
2.2.01	Deberá soportar Multi-Chassis LAG (MCLAG)		
2.2.02	Deberá soportar STP sobre Multi-Chassis LAG (MCLAG)		
2.3	**Funcionalidades de Calidad de Servicio**	**---**	
2.3.01	Deberá soportar priorización de tráfico basada en 802.1p		
2.3.02	Deberá soportar priorización de tráfico basada en IP TOS/DSCP		
2.3.03	Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP		
2.4	**Funcionalidades de Capa 2**	**---**	
2.4.01	Deberá soportar Link Aggregation estático		
2.4.02	Deberá soportar LACP		
2.4.03	Deberá soportar Spanning Tree		
2.4.04	Deberá soportar Jumbo Frames		
2.4.05	Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex		
2.4.06	Deberá soportar el estandar IEEE 802.1D MAC Bridging/STP		
2.4.07	Deberá soportar el estandar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)		
2.4.08	Deberá soportar el estandar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
2.4.09	Deberá soportar la funcionalidad STP Root Guard		
2.4.10	Deberá soportar STP BPDU Guard		
2.4.11	Deberá soportar Edge Port / Port Fast		
2.4.12	Deberá soportar el estandar IEEE 802.1Q VLAN Tagging		
2.4.13	Deberá soportar Private VLAN		
2.4.14	Deberá soportar el estandar IEEE 802.3ad Link Aggregation con LACP		
2.4.15	Deberá poder balancear trafico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)		
2.4.16	Deberá soportar el estandar IEEE 802.1AX Link Aggregation		
2.4.17	Deberá soportar instancias de Spanning Tree (MSTP/CST)		
2.4.18	Deberá soportar el estandar IEEE 802.3x Flow Control con Back-pressure		
2.4.19	Deberá soportar el estandar IEEE 802.3 10Base-T		
2.4.20	Deberá soportar el estandar IEEE 802.3u 100Base-TX		
2.4.21	Deberá soportar el estandar IEEE 802.3z 1000Base-SX/LX		
2.4.22	Deberá soportar el estandar IEEE 802.3ab 1000Base-T		
2.4.23	Deberá soportar el estandar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física		
2.4.24	Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)		
2.4.25	Deberá soportar la creacion de VLANs por MAC, IP y Ethertype-based		
2.4.26	Deberá soportar la funcionalidad de Virtual-Wire		
2.4.27	Deberá soportar Time-Domain Reflectometer (TDR)		
2.4.28	Deberá soportar 4094 VLANs simultáneas		
2.4.29	Deberá soportar IGMP Snooping		

2.4.30	Deberá soportar IGMP proxy y querier		
2.4.31	Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED		
2.4.32	Deberá permitir la negociación de POE en LLDP-MED		
2.4.33	Deberá permitir limitar la cantidad de MACs aprendidas por puerto		
2.4.34	Deberá permitir un mínimo de 15 instancias de MSTP		
2.4.35	Deberá permitir controlar tormentas de broadcast independientemente en cada puerto		
2.4.36	Deberá soportar un mecanismo de detección y prevención de loops		
2.4.37	Deberá soportar VLAN Stacking (QinQ)		
2.4.38	Deberá soportar SPAN		
2.4.39	Deberá soportar RSPAN y ERSPAN		
2.4.40	Deberá soportar ruteo estático		
2.4.41	Deberá soportar RIP v2		
2.4.42	Deberá soportar OSPF v2		
2.4.43	Deberá soportar VRRP		
2.4.44	Deberá soportar IS-IS		
2.4.45	Deberá soportar BGP		
2.4.46	Deberá soportar protocolos de ruteo multicast		
2.4.47	Deberá soportar Equal Cost Multipath Routing (ECMP)		
2.4.48	Deberá soportar Bidirectional Forwarding Detection (BFD)		
2.4.49	Deberá soportar DHCP Relay		
2.4.50	Deberá soportar DHCP Server		
2.5	**Funciones de Capa 3**	**---**	
2.5.01	Deberá soportar el RFC 2571 Architecture for Describing SNMP		
2.5.02	Deberá soportar DHCP Client		
2.5.03	Deberá soportar el RFC 854 Telnet Server		
2.5.04	Deberá soportar el RFC 2865 RADIUS		
2.5.05	Deberá soportar el RFC 1643 Ethernet-like Interface MIB		
2.5.06	Deberá soportar el RFC 1213 MIB-II		
2.5.07	Deberá soportar el RFC 1354 IP Forwarding Table MIB		
2.5.08	Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching		
2.5.09	Deberá soportar el RFC 1573 SNMP MIB II		
2.5.10	Deberá soportar el RFC 1157 SNMPv1/v2c		
2.5.11	Deberá soportar el RFC 2030 SNTP		
2.5.12	Deberá soportar Port Mirroring		
2.5.13	Deberá soportar Admin Authentication Via RFC 2865 RADIUS		
2.5.14	Deberá soportar el estándar IEEE 802.1x authentication Port-based		
2.5.15	Deberá soportar el estándar IEEE 802.1x Authentication MAC-based		
2.5.16	Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN		
2.5.17	Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)		
2.5.18	Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment		
2.5.19	Deberá soportar Radius CoA (Change of Authority)		
2.5.20	Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)		
2.5.21	Deberá soportar el estándar IEEE 802.1ab LLDP-MED		

2.5.22	Deberá soportar Radius Accounting		
2.5.23	Deberá soportar EAP pass-through		
2.5.24	Deberá soportar detección de dispositivos		
2.5.25	Deberá soportar MAC-IP binding		
2.5.26	Deberá soportar sFlow		
2.5.27	Deberá soportar Flow Export		
2.5.28	Deberá soportar ACLs		
2.5.29	Deberá soportar múltiples ACLs de ingreso		
2.5.30	Deberá soportar scheduling de ACLs		
2.5.31	Deberá soportar DHCP Snooping		
2.5.32	Deberá soportar listas de servidores DHCP permitidos		
2.5.33	Deberá soportar bloqueo de DHCP		
2.5.34	Deberá permitir Dynamic ARP Inspection (DAI)		
2.5.35	Deberá permitir Access VLANs		
2.5.36	Deberá permitir tagging de tráfico con VLAN ID mediante ACLs		
2.6	**Funciones de Seguridad**	**---**	
2.6.01	Deberá soportar Syslog		
2.6.02	Debe contar con un sensor de temperatura interno		
2.6.03	Debe permitir monitorear la temperatura del dispositivo		
2.6.04	Debe soportar QSFP+ low-power mode		
2.6.05	Debe soportar Energy-Efficient Ethernet (EEE)		
2.6.06	Debe soportar QSFP+ low-power mode		
2.6.07	Debe soportar Energy-Efficient Ethernet (EEE)		
Características Especificas			
2.7	**Equipo de comunicación de tipo 1**	**2**	
2.7.01	Mínimo de 48 interfaces de 10Gbps según estándar IEEE 802.3ae		
2.7.02	Mínimo de 6 interfaces de 40Gbps		
2.7.03	Tener 1 puerto de gestión dedicado		
2.7.04	Tener interfaz de consola RJ-45		
2.7.05	Form Factor del tipo 1 RU		
2.7.06	Capacidad de switching de 1020 Gbps		
2.7.07	Soportar 1518 Mpps		
2.7.08	MAC address storage minima de 144K		
2.7.09	Soportar protocolos de enrutamiento dinémico , BGP, IS-IS, PIM-SM/SSM		
2.7.10	Soportar Link Aggregation con hasta 48 elementos		
2.7.11	Packet buffers de al menos 12 MB		
2.7.12	Memoria DRAM de al menos 8 GB		
2.7.13	Flash (NAND) de al menos 128 MB		
2.7.14	Fuente redundante del tipo Interna (HotSwap)		
2.7.15	Deberá soportar Split Port (QSFP+ breakout to 4xSFP+)		
2.8	**Equipos de Comunicación Tipo 2**	**13**	
2.8.01	Mínimo de 24 interfaces de 1Gbps RJ-45		
2.8.02	Mínimo de 2 interfaces de 10Gbps según estandar IEEE 802.3ae		

2.8.03	Mínimo de 24 interfaces PoE de 1Gbps RJ-45		
2.8.04	Minimo de 421 W Watts de PoE Budget		
2.8.05	Tener 1 puerto de gestión dedicado		
2.8.06	Tener interfaz de consola RJ-45		
2.8.07	Form Factor del tipo 1 RU		
2.8.08	Capacidad de switching de 128 Gbps		
2.8.09	Soportar 204 Mpps		
2.8.10	MAC address storage mínimo de 16K		
2.8.11	VLANs soportadas 4K entradas		
2.8.12	Soportar Link Aggregation con hasta 8 elementos		
2.8.13	Packet buffers de al menos 2 MB		
2.8.14	Memoria DRAM de al menos 1 GB		
2.8.15	Flash de al menos 256 MB		

3. Firewalls.

ítem	Descripción	Cumple	
		SI	NO
3.01	Banhprovi para su proyecto de comunicaciones necesitara la instalación y configuración de dos equipos firewall de nueva generación (NGF), ubicados uno en su sitio principal y otro en su sitio alterno haciendo en total dos **(2)** dispositivos		
3.02	Throughput de por lo menos 10 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6		
3.03	Soporte a por lo menos 1.5M sesiones concurrentes		
3.04	Soporte a por lo menos 56 K nuevas sesiones por segundo		
3.05	Throughput de al menos 11.5 Gbps de VPN IPSec		
3.06	Estar licenciado para, o soportar sin necesidad de licencia, 2.5K túneles de VPN IPSec site-to-site simultáneos		
3.07	Estar licenciado para, o soportar sin necesidad de licencia, 16K túneles de clientes VPN IPSec simultáneos		
3.08	Throughput de al menos 1Gbps de VPN SSL		
3.09	Soportar al menos 500 clientes de VPN SSL simultáneos		
3.10	Soportar al menos 2.6 Gbps de throughput de IPS		
3.11	Soportar al menos 1 Gbps de throughput de Inspección SSL		
3.12	Soportar al menos 2.2 Gbps de throughput de Application Control		
3.13	Soportar al menos 1.6 Gbps de throughput de NGFW		
3.14	Soportar al menos 1 Gbps de throughput de Threat Protection		
3.15	Permitir gestionar al menos 24 Switches		
3.16	Tener al menos 12 interfaces 1Gbps BASE-T		
3.17	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance		

3.18	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;		
3.19	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;		
3.20	Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;		
3.21	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;		
3.22	Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;		
3.23	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;		
3.24	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;		
3.25	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;		
3.26	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;		
3.27	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);		
3.28	Los dispositivos de protección de red deben soportar DHCP Relay;		
3.29	Los dispositivos de protección de red deben soportar DHCP Server;		
3.30	Los dispositivos de protección de red deben soportar sFlow;		
3.31	Los dispositivos de protección de red deben soportar Jumbo Frames;		
3.32	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;		
3.33	Debe ser compatible con NAT dinámica (varios-a-1);		
3.34	Debe ser compatible con NAT dinámica (muchos-a-muchos);		
3.35	Debe soportar NAT estática (1-a-1);		
3.36	Debe admitir NAT estática (muchos-a-muchos);		
3.37	Debe ser compatible con NAT estático bidireccional 1-a-1;		
3.38	Debe ser compatible con la traducción de puertos (PAT);		
3.39	Debe ser compatible con NAT Origen;		
3.40	Debe ser compatible con NAT de destino;		
3.41	Debe soportar NAT de origen y NAT de destino de forma simultánea;		
3.42	Debe soportar NAT de origen y NAT de destino en la misma política		
3.43	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;		
3.44	Debe ser compatible con NAT64 y NAT46;		
3.45	Debe implementar el protocolo ECMP;		
3.46	Debe soportar SD-WAN de forma nativa		
3.47	Debe soportar el balanceo de enlace hash por IP de origen;		
3.48	Debe soportar el balanceo de enlace por hash de IP de origen y destino;		
3.49	Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;		

3.50	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;		
3.51	Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;		
3.52	Enviar logs a sistemas de gestión externos simultáneamente;		
3.53	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;		
3.54	Debe soporta protección contra la suplantación de identidad (anti-spoofing);		
3.55	Implementar la optimización del tráfico entre dos dispositivos;		
3.56	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);		
3.57	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);		
3.58	Soportar OSPF graceful restart;		
3.59	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;		
3.60	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;		
3.61	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;		
3.62	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;		
3.63	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;		
3.64	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;		
3.65	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;		
3.66	La configuración de alta disponibilidad debe sincronizar: Sesiones;		
3.67	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;		
3.68	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;		
3.69	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;		
3.70	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;		
3.71	Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;		
3.72	La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;		
3.73	Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);		
3.74	Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;		
3.75	El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;		

3.76	La consola de administración debe soportar como mínimo, ingles y Español.		
3.77	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad		
3.78	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.		
3.79	Debe soportar controles de zona de seguridad;		
3.80	Debe contar con políticas de control por puerto y protocolo;		
3.81	Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;		
3.82	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;		
3.83	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;		
3.84	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;		
3.85	Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.		
3.86	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);		
3.87	Debe soportar el protocolo estándar de la industria VXLAN;		
3.88	La solución debe permitir la implementación sin asistencia de SD-WAN		
3.89	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;		
3.90	la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.		
3.91	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;		
3.92	Detección de miles de aplicaciones en 18 categorias, 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;		
3.93	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;		
3.94	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;		
3.95	Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;		
3.96	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;		
3.97	Actualización de la base de firmas de la aplicación de forma automática;		
3.98	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;		

3.99	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;		
3.100	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;		
3.101	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;		
3.102	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;		
3.103	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;		
3.104	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;		
3.105	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;		
3.106	Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);		
3.107	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;		
3.108	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;		
3.109	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente		
3.110	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;		
3.111	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);		
3.112	Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;		
3.113	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;		
3.114	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;		
3.115	Deber permitir el bloqueo de vulnerabilidades y exploits conocidos		
3.116	Debe incluir la protección contra ataques de denegación de servicio;		
3.117	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;		
3.118	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;		
3.119	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;		
3.120	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;		
3.121	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);		
3.122	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;		
3.123	Detectar y bloquear los escaneos de puertos de origen;		
3.124	Bloquear ataques realizados por gusanos (worms) conocidos;		
3.125	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;		

3.126	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);		
3.127	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;		
3.128	Identificar y bloquear la comunicación con redes de bots;		
3.129	Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;		
3.130	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;		
3.131	Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;		
3.132	Los eventos deben identificar el país que origino la amenaza;		
3.133	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);		
3.134	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;		
3.135	Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;		
3.136	En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;		
3.137	Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);		
3.138	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);		
3.139	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;		
3.140	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;		
3.141	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;		
3.142	Tener por lo menos 75 categorías de URL;		
3.143	Debe tener la funcionalidad de exclusión de URLs por categoría;		
3.144	Permitir página de bloqueo personalizada;		
3.145	Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);		
3.146	Además del Explicit Web Proxy, soportar proxy web transparente;		
3.147	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;		

3.148	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;		
3.149	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;		
3.150	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;		
3.151	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios;		
3.152	Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);		
3.153	Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;		
3.154	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;		
3.155	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;		
3.156	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;		
3.157	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;		
3.158	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;		
3.159	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;		
3.160	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;		
3.161	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;		
3.162	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;		
3.163	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;		
3.164	En QoS debe permitir la definición de tráfico con máximo ancho de banda;		
3.165	En QoS debe permitir la definición de colas de prioridad;		
3.166	Soportar marcación de paquetes DiffServ, incluso por aplicación;		
3.167	Soportar la modificación de los valores de DSCP para Diffserv;		
3.168	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);		
3.169	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;		
3.170	Permite la creación de filtros para archivos y datos predefinidos;		

3.171	Los archivos deben ser identificados por tamaño y tipo;		
3.172	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;		
3.173	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;		
3.174	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;		
3.175	Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;		
3.176	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;		
3.177	Debe permitir la visualización de los países de origen y destino en los registros de acceso;		
3.178	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;		
3.179	Soporte VPN de sitio-a-sitio y cliente-a-sitio;		
3.180	Soportar VPN IPSec;		
3.181	Soportar VPN SSL;		
3.182	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512		
3.183	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;		
3.184	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);		
3.185	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);		
3.186	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;		
3.187	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;		
3.188	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;		
3.189	Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;		
3.190	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;		
3.191	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;		
3.192	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;		
3.193	Deberá mantener una conexión segura con el portal durante la sesión;		
3.194	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.		
3.195	La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;		
3.196	La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;		
3.197	La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e		

	implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;		
3.198	La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;		
3.199	La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps ou Bps) para las aplicaciones reconocidas a través de la técnica de DPI;		
3.200	La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;		
3.201	La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;		
3.202	La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;		
3.203	La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;		
3.204	La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;		
3.205	La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;		
3.206	La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;		
3.207	Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;		
3.208	La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;		
3.209	La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;		
3.210	La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;		
3.211	La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;		
3.212	La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;		
3.213	La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);		
3.214	La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;		
3.215	La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;		
3.216	La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;		
3.217	La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;		

4. Herramienta de Administración Centralizada y Herramienta de Análisis y Gestión de eventos de los equipos de comunicación.

ítem	Descripción	Cumple	
		SI	NO
Características Generales			
4.1	Requerimiento mínimo de la máquina Virtual		
4.1.01	La solución no deberá tener límites en cuanto a la cantidad de vCPU si la solución es virtual		
4.1.02	Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 2.5.0/2.5.1/2.5.5/6.0/6.5/6.7		
4.1.03	La solución deberá contemplar la administración de al menos 100 dispositivos, entiéndase firewall, switches, y aps.		
4.1.04	La solución no deberá tener límites en cuanto a la cantidad de memoria RAM si el aparto es virtual		
4.1.05	Debe de soportar la recepción de volumen de logs diarios de al menos 1GB		
4.1.06	Debe de soportar 500GB de capacidad de almacenamiento como mínimo		
4.1.07	Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución		
4.1.08	Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.		
4.1.09	Debe permitir accesos concurrentes de administradores		
4.1.10	Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores		
4.1.11	Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.		
4.1.12	Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión;		
Características Especificas			
4.2	Requerimiento mínimo Herramienta de Administración Centralizada		
4.2.01	Debe tener la capacidad de permitir provisionar y monitorear configuración de SD-WAN de todos los dispositivos gestionados desde una sola consola.		
4.2.02	Como parte de la visibilidad SD-WAN de los dispositivos gestionados centralmente, la solución debe contar con visibilidad de estado de enlace, desempeño de aplicación, utilización de ancho de banda y cumplimiento de SLA objetivo.		
4.2.03	Debe tener la capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola		
4.2.04	La solución debe tener la capacidad Multi-tenancy para separar los datos de gestión de infraestructura de manera lógica o geográfica y permitir despliegue zerotouch para un aprovisionamiento masivo rápido.		
4.2.05	La solución debe ser capaz de realizar respaldos automáticos de configuración hasta en 5 nodos, conteniendo updates de todos los dispositivos gestionados.		
4.2.06	Debe tener la capacidad de permitir provisionar comunidades VPN y monitorear conexiones VPN de todos los dispositivos gestionados desde una sola consola y mostrar su geolocalización en un mapa.		
4.2.07	La solución debe permitir utilización de API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.		
4.2.08	Permitir integración de intercambio y compartición de datos con terceros mediante pxGrid, OCI, Esxi .		

4.2.09	En la fecha de la propuesta, ninguno de los modelos de la oferta puede estar en el sitio del fabricante en listados de end-of-life o end-of-sales		
4.2.10	Debe tener interfaz basada en línea de comando para administración de la solución de gestión;		
4.2.11	Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;		
4.2.12	Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones;		
4.2.13	Generar alertas automáticas por Email		
4.2.14	Generar alertas automáticas por SNMP		
4.2.15	Generar alertas automáticas por Syslog		
4.2.16	Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario;		
4.2.17	Debe ser permitido al administrador transferir los backups a un servidor FTP.		
4.2.18	Debe ser permitido al administrador transferir los backups a un servidor SCP		
4.2.19	Debe ser permitido al administrador transferir los backups a un servidor SFTP		
4.2.20	Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante;		
4.2.21	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES		
4.2.22	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS+		
4.2.23	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP		
4.2.24	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS		
4.2.25	Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI)		
4.2.26	Debe soportar sincronización de reloj interno por protocolo NTP.		
4.2.27	Debe registrar las acciones efectuadas por cualquier usuario;		
4.2.28	Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Web Services (API);		
4.2.29	Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado;		
4.2.30	La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización;		
4.2.31	La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación;		
4.2.32	La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware;		
4.2.33	La gestión debe permitir la creación y administración de políticas de Filtro de URL;		
4.2.34	Permitir buscar cuáles reglas un objeto está siendo utilizado;		
4.2.35	Permitir la creación de reglas que permanezcan activas en horario definido;		
4.2.36	La solución debe permitir ser repositorio de firmas de antivirus, IPS, Web Filtering, email filtering, para optimizar la velocidad y descarga centralizada a los dispositivos gestionados		
4.2.37	Debe tener capacidad de desplegar los resultados de auditoría de seguridad de los dispositivos gestionados		
4.2.38	Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;		
4.2.39	Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing);		

4.2.40	Debe permitir la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas;		
4.2.41	Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión;		
4.2.42	La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta;		
4.2.43	La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos;		
4.2.44	Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados;		
4.2.45	Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador;		
4.2.46	Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos;		
4.2.47	Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.		
4.2.48	Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware;		
4.2.49	Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos;		
4.2.50	Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración;		
4.2.51	Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos;		
4.2.52	Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión;		
4.2.53	Permitir configurar y visualizar el manejo de SD-WAN de los dispositivos gestionados de forma centralizada;		
4.2.54	Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos;		
4.2.55	Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada;		
4.2.56	Permitir la creación de reglas anti DoS de forma centralizada;		
4.2.57	Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada;		
4.2.58	Debe permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topologia (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía;		
4.2.59	Debe permitir el uso de DDNS en VPNs de manera centralizada		
4.2.60	Debe permitir la gestión de Access Points propietarios de manera centralizada		
4.2.61	Debe permitir la gestión de Switches propietarios de manera centralizada		
4.2.62	Debe permitir la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada		
4.3	Requerimientos mínimos Herramienta de Análisis y Gestión de eventos de los equipos de comunicación.		
4.3.01	Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH		
4.3.02	Autenticación de usuarios de acceso a la plataforma via LDAP		
4.3.03	Autenticación de usuarios de acceso a la plataforma via Radius		
4.3.04	Autenticación de usuarios de acceso a la plataforma via TACACS+		
4.3.05	Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos		

4.3.06	Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.		
4.3.07	Generación de informes en tiempo real de tráfico, en formato de gráfica tabla		
4.3.08	Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.		
4.3.09	Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.		
4.3.10	Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado		
4.3.11	Contar con mecanismos de borrado automático de logs antiguos.		
4.3.12	Permitir la importación y exportación de reportes		
4.3.13	Debe contar con la capacidad de crear informes en formato HTML		
4.3.14	Debe contar con la capacidad de crear informes en formato PDF		
4.3.15	Debe contar con la capacidad de crear informes en formato XML		
4.3.16	Debe contar con la capacidad de crear informes en formato CSV		
4.3.17	Debe permitir exportar los logs en formato CSV		
4.3.18	Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.		
4.3.19	Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.		
4.3.20	La solución debe contar con reportes predefinidos		
4.3.21	Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución		
4.3.22	Debe ser posible la duplicación de reportes existentes para su posterior edición.		
4.3.23	Debe tener la capacidad de personalizar la portada de los reportes obtenidos.		
4.3.24	Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.		
4.3.25	Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.		
4.3.26	Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas		
4.3.27	Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.		
4.3.28	Debe permitir descargar de la plataforma los archivos de logs para uso externo.		
4.3.29	Tener la capacidad de generar y enviar reportes periódicos automáticamente.		
4.3.30	Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.		
4.3.31	Permitir el envío por email de manera automática de reportes.		
4.3.32	Debe permitir que el reporte a enviar por email sea al destinatario específico.		
4.3.33	Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.		
4.3.34	Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.		
4.3.35	Debe permitir el uso de filtros en los reportes.		

4.3.36	Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.		
4.3.37	Permitir especificar el idioma de los reportes creados		
4.3.38	Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.		
4.3.39	Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.		
4.3.40	Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.		
4.3.41	Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.		
4.3.42	Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.		
4.3.43	Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.		
4.3.44	Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.		
4.3.45	Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.		
4.3.46	Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.		
4.3.47	Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos		
4.3.48	Debe permitir visualizar en tiempo real los logs recibidos.		
4.3.49	Debe permitir el reenvío de logs en formato syslog.		
4.3.50	Debe permitir el reenvío de logs en formato CEF (Common Event Format).		
4.3.51	Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red		
4.3.52	Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.		
4.3.53	Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.		
4.3.54	Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red		
4.3.55	Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).		
4.3.56	Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.		
4.3.57	Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.		
4.3.58	Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs		
4.3.59	Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)		
4.3.60	Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC		
4.3.61	Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3		
4.3.62	Debe permitir generar alertas de eventos a partir de logs recibidos		
4.3.63	Debe permitir crear incidentes a partir de alertas de eventos para endpoint		
4.3.64	Debe permitir la integración al sistema de tickets ServiceNow		

4.3.65	Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.		
4.3.66	Debe permitir respaldar logs en nube publica de Microsoft Azure		
4.3.67	Debe soportar el estándar SAML para autenticación de usuarios administradores		

5. Servicios Conexos

ítem	Descripción	Cumple	
		SI	NO
5.1	Capacitación para la configuración, Mantenimiento y operatividad del producto ofertado, esta debe ser impartida por una entidad que se dedique al rubro de la educación certificada. Se proveerá para al menos 4 Participantes, y debe incluir todos los costos que se requieran para recibir dicha capacitación. el horario y la fecha se definirá con BANHPROVI		
5.2	Instalación e implementación de todos los servicios adjudicados		
5.3	Servicio de Garantía		
5.4	Garantía, 3 años como mínimo		
5.5	La garantía deberá incluir el cambio de partes/equipo completo. El tiempo máximo de respuesta o solución será de 1 semana después de reportada la falla.		
5.6	Deberá incluir el soporte y actualización de sistema operativo durante el tiempo de garantía		
5.7	El oferente deberá ser centro autorizado de servicios, para lo cual deberá de incluir una carta por parte de la marca representada indicando lo mismo		