* * * * *

CONTRATO PRIVADO DE ADQUISICIÓN DE EQUIPO DE COMUNICACIÓN DE RED Y SOFTWARE DE GESTIÓN DEL BANCO HONDUREÑO PARA LA PRODUCCIÓN Y LA VIVIENDA (BANHPROVI) SUSCRITO ENTRE EL BANHPROVI Y LA EMPRESA PRODUCTIVE BUSINESS SOLUTION HONDURAS (PBS HONDURAS) DEL LOTE NO 2 DE LA LICITACIÓN PÚBLICA NACIONAL 008/2020.

Nosotros **MAYRA ROXANA LUISA FALCK REYES**, mayor de edad, casada, licenciada en Economía, hondureña y de este domicilio con número de identidad 0801-1959-03287, actuando en mi condición de Presidenta Ejecutiva y representante legal del BANCO HONDUREÑO PARA LA PRODUCCIÓN Y LA VIVIENDA (BANHPROVI), Institución creada originalmente como "FONDO NACIONAL PARA LA PRODUCCIÓN Y LA VIVIENDA" (FONAPROVI), según Decreto No. 53-97, de fecha ocho (8) de mayo del año mil novecientos noventa y siete (1997), publicado en el Diario Oficial la Gaceta el treinta (30) de mayo de mil novecientos noventa y siete (1997) y transformada mediante Decreto Legislativo No.6-2005, de fecha veintiséis (26) de Enero del dos mil cinco (2005), que contiene la Ley del "BANCO HONDUREÑO PARA LA PRODUCCIÓN Y LA VIVIENDA" que también se identifica con la sigla (BANHPROVI), publicado en el Diario Oficial La Gaceta No.30,659, el uno (01) de Abril del dos mil cinco (2005) y reformado mediante Decreto Legislativo No. 358-2014, de fecha veinte (20) de enero del año dos mil catorce (2014), publicado en el Diario Oficial la Gaceta No. 33,431 el veinte (20) de mayo del año dos mil catorce (2014); dicho Decreto fue rectificado a Decreto Legislativo No. 358-2013, mediante Fe de Errata publicada en el Diario Oficial La Gaceta No. 33530, el doce (12) de septiembre del año dos mil catorce (2014); acredita su representación, mediante Certificación del Acuerdo número 28-2018 por nombramiento hecho por el Presidente de la Republica, de fecha veintinueve (29) de enero del año dos mil dieciocho (2018) y conforme al artículo 28 numeral 2, de la Ley Constitutiva del BANHPROVI, en donde constan facultades suficientes para el otorgamiento de actos y contratos como los contenidos en el presente Contrato, denominado en adelante también como **"BANHPROVI"**, con dirección en la ciudad de Tegucigalpa, M.D.C. en el Boulevard Juan Pablo II, contiguo a Plaza COLPROSUMAH, con el número de teléfono (504) 2232-5500; y los señores: Miriam Luz Santamaria Zschocher con tarjeta de identidad 0902-1963-00050 y Juan Carlos Fonseca Meza con tarjeta de identidad 0801-1982-04878 actuando en condición de Representantes Legales de **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS**

HONDURAS) del domicilio de la ciudad de Tegucigalpa, con Registro Tributario Nacional 05019010314509, quien en el transcurso de este instrumento se denominará **"EL PROVEEDOR"**, y en las calidades antes expresadas **MANIFESTAMOS:** Que hemos acordado otorgar y en efecto otorgamos el presente **CONTRATO PRIVADO DE ADQUISICIÓN DE EQUIPO DE COMUNICACIÓN DE RED Y SOFTWARE DE GESTIÓN". DEL BANCO HONDUREÑO PARA LA PRODUCCIÓN Y LA VIVIENDA (BANHPROVI) SUSCRITO ENTRE EL BANHPROVI Y LA EMPRESA PRODUCTIVE BUSINESS SOLUTION HONDURAS (PBS HONDURAS) DEL LOTE NO 2 DE LA LICITACIÓN PÚBLICA NACIONAL 008/2020** el cual se regirá por las cláusulas siguientes:

CLÁUSULA PRIMERA
OBJETO DEL CONTRATO

El Objeto del presente contrato es:

a. Modernizar la infraestructura de comunicaciones para poder asegurar 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 Por lo que, para poder alcanzar dichos objetivos es necesarios 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.

CLÁUSULA SEGUNDA
ESPECIFICACIONES TÉCNICAS

El Banco Hondureño de Producción y Vivienda (BANHPROVI) requiere contar con el **DE "ADQUISICIÓN DE EQUIPO DE COMUNICACIÓN DE RED Y SOFTWARE DE GESTIÓN"**

SWITCHES: CARACTERÍSTICAS GENERALES

Funcionalidades de Administración

1. El switch deberá poder aceptar acutalizaciones de firmware desde una interface de tipo GUI

2. Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la funcion de PoE
3. Deberá soportar detección y notificación de conflictos de direcciones IP
4. Deberá soportar administración en la nube
5. Deberá soportar administración por IPv4 e IPv6
6. Deberá soportar Telnet / SSH para acceso a la consola
7. Deberá soportar HTTP / HTTPS
8. Deberá soportar SNMP v1/v2c/v3
9. Deberá poder configurar su reloj mediante un NTP Server
10. Deberá contar con una linea de comandos estándar y con interface para configurar via Web
11. Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
12. Deberá soportar HTTP REST APIs para Configuracion y monitoreo

Funcionalidad de Alta Disponibilidad

13. Deberá soportar Multi-Chassis LAG (MCLAG)
14. Deberá soportar STP sobre Multi-Chassis LAG (MCLAG)

Funcionalidades de Calidad de Servicio

15. Deberá soportar priorización de tráfico basada en 802.1p
16. Deberá soportar priorización de tráfico basada en IP TOS/DSCP
17. Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP

Funcionalidades de Capa 2

18. Deberá soportar Link Aggregation estático
19. Deberá soportar LACP
20. Deberá soportar Spanning Tree
21. Deberá soportar Jumbo Frames
22. Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex
23. Deberá soportar el estandar IEEE 802.1D MAC Bridging/STP
24. Deberá soportar el estandar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
25. Deberá soportar el estandar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
26. Deberá soportar la funcionalidad STP Root Guard
27. Deberá soportar STP BPDU Guard
28. Deberá soportar Edge Port / Port Fast
29. Deberá soportar el estandar IEEE 802.1Q VLAN Tagging

30. Deberá soportar Private VLAN
31. Deberá soportar el estandar IEEE 802.3ad Link Aggregation con LACP
32. Deberá poder balancear trafico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
33. Deberá soportar el estandar IEEE 802.1AX Link Aggregation
34. Deberá soportar instancias de Spanning Tree (MSTP/CST)
35. Deberá soportar el estandar IEEE 802.3x Flow Control con Back-pressure
36. Deberá soportar el estandar IEEE 802.3 10Base-T
37. Deberá soportar el estandar IEEE 802.3u 100Base-TX
38. Deberá soportar el estandar IEEE 802.3z 1000Base-SX/LX
39. Deberá soportar el estandar IEEE 802.3ab 1000Base-T
40. Deberá soportar el estandar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa fisica
41. Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
42. Deberá soportar la creacion de VLANs por MAC, IP y Ethertype-based
43. Deberá soportar la funcionalidad de Virtual-Wire
44. Deberá soportar Time-Domain Reflectometer (TDR)
45. Deberá soportar 4094 VLANs simultáneas
46. Deberá soportar IGMP Snooping
47. Deberá soportar IGMP proxy y querier
48. Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED
49. Deberá permitir la negociación de POE en LLDP-MED
50. Deberá permitir limitar la cantidad de MACs aprendidas por puerto
51. Deberá permitir un mínimo de 15 instancias de MSTP
52. Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
53. Deberá soportar un mecanismo de detección y prevención de loops
54. Deberá soportar VLAN Stacking (QinQ)
55. Deberá soportar SPAN
56. Deberá soportar RSPAN y ERSPAN
57. Deberá soportar ruteo estático
58. Deberá soportar RIP v2
59. Deberá soportar OSPF v2
60. Deberá soportar VRRP

61. Deberá soportar IS-IS
62. Deberá soportar BGP
63. Deberá soportar protocolos de ruteo multicast
64. Deberá soportar Equal Cost Multipath Routing (ECMP)
65. Deberá soportar Bidirectional Forwarding Detection (BFD)
66. Deberá soportar DHCP Relay
67. Deberá soportar DHCP Server

Funciones de Capa 3

68. Deberá soportar el RFC 2571 Architecture for Describing SNMP
69. Deberá soportar DHCP Client
70. Deberá soportar el RFC 854 Telnet Server
71. Deberá soportar el RFC 2865 RADIUS
72. Deberá soportar el RFC 1643 Ethernet-like Interface MIB
73. Deberá soportar el RFC 1213 MIB-II
74. Deberá soportar el RFC 1354 IP Forwarding Table MIB
75. Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching
76. Deberá soportar el RFC 1573 SNMP MIB II
77. Deberá soportar el RFC 1157 SNMPv1/v2c
78. Deberá soportar el RFC 2030 SNTP
79. Deberá soportar Port Mirroring
80. Deberá soportar Admin Authentication Via RFC 2865 RADIUS
81. Deberá soportar el estándar IEEE 802.1x authentication Port-based
82. Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
83. Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
84. Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
85. Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
86. Deberá soportar Radius CoA (Change of Authority)
87. Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
88. Deberá soportar el estándar IEEE 802.1ab LLDP-MED
89. Deberá soportar Radius Accounting
90. Deberá soportar EAP pass-through
91. Deberá soportar detección de dispositivos
92. Deberá soportar MAC-IP binding

93. Deberá soportar sFlow
94. Deberá soportar Flow Export
95. Deberá soportar ACLs
96. Deberá soportar múltiples ACLs de ingreso
97. Deberá soportar scheduling de ACLs
98. Deberá soportar DHCP Snooping
99. Deberá soportar listas de servidores DHCP permitidos
100. Deberá soportar bloqueo de DHCP
101. Deberá permitir Dynamic ARP Inspection (DAI)
102. Deberá permitir Access VLANs
103. Deberá permitir tagging de tráfico con VLAN ID mediante ACLs

Funciones de Seguridad

104. Deberá soportar Syslog
105. Debe contar con un sensor de temperatura interno
106. Debe permitir monitorear la temperatura del dispositivo
107. Debe soportar QSFP+ low-power mode
108. Debe soportar Energy-Efficient Ethernet (EEE)
109. Debe soportar QSFP+ low-power mode
110. Debe soportar Energy-Efficient Ethernet (EEE)

Equipo de comunicación de tipo 1

111. Mínimo de 48 interfaces de 10Gbps según estándar IEEE 802.3ae
112. Mínimo de 6 interfaces de 40Gbps
113. Tener 1 puerto de gestión dedicado
114. Tener interfaz de consola RJ-45
115. Form Factor del tipo 1 RU
116. Capacidad de switching de 1020 Gbps
117. Soportar 1518 Mpps
118. MAC address storage minima de 144K
119. Soportar protocolos de enrutamiento dinémico , BGP, IS-IS, PIM-SM/SSM
120. Soportar Link Aggregation con hasta 48 elementos
121. Packet buffers de al menos 12 MB
122. Memoria DRAM de al menos 8 GB
123. Flash (NAND) de al menos 128 MB
124. Fuente redundante del tipo Interna (HotSwap)

125. Deberá soportar Split Port (QSFP+ breakout to 4xSFP+)

Equipos de Comunicación Tipo 2

126. Mínimo de 24 interfaces de 1Gbps RJ-45
127. Mínimo de 2 interfaces de 10Gbps según estandar IEEE 802.3ae
128. Mínimo de 24 interfaces PoE de 1Gbps RJ-45
129. Minimo de 421 W Watts de PoE Budget
130. Tener 1 puerto de gestión dedicado
131. Tener interfaz de consola RJ-45
132. Form Factor del tipo 1 RU
133. Capacidad de switching de 128 Gbps
134. Soportar 204 Mpps
135. MAC address storage mínimo de 16K
136. VLANs soportadas 4K entradas
137. Soportar Link Aggregation con hasta 8 elementos
138. Packet buffers de al menos 2 MB
139. Memoria DRAM de al menos 1 GB
140. Flash de al menos 256 MB

FIREWALLS:

1. 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
2. Throughput de por lo menos 10 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6
3. Soporte a por lo menos 1.5M sesiones concurrentes
4. Soporte a por lo menos 56 K nuevas sesiones por segundo
5. Throughput de al menos 11.5 Gbps de VPN IPSec
6. Estar licenciado para, o soportar sin necesidad de licencia, 2.5K túneles de VPN IPSec site-to-site simultáneos
7. Estar licenciado para, o soportar sin necesidad de licencia, 16K túneles de clientes VPN IPSec simultáneos
8. Throughput de al menos 1Gbps de VPN SSL
9. Soportar al menos 500 clientes de VPN SSL simultáneos
10. Soportar al menos 2.6 Gbps de throughput de IPS

11. Soportar al menos 1 Gbps de throughput de Inspección SSL
12. Soportar al menos 2.2 Gbps de throughput de Application Control
13. Soportar al menos 1.6 Gbps de throughput de NGFW
14. Soportar al menos 1 Gbps de throughput de Threat Protection
15. Permitir gestionar al menos 24 Switches
16. Tener al menos 12 interfaces 1Gbps BASE-T
17. Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance
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.;
19. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
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;
21. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
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;
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;
24. Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
25. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
26. Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
27. Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
28. Los dispositivos de protección de red deben soportar DHCP Relay;
29. Los dispositivos de protección de red deben soportar DHCP Server;
30. Los dispositivos de protección de red deben soportar sFlow;
31. Los dispositivos de protección de red deben soportar Jumbo Frames;

32. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
33. Debe ser compatible con NAT dinámica (varios-a-1);
34. Debe ser compatible con NAT dinámica (muchos-a-muchos);
35. Debe soportar NAT estática (1-a-1);
36. Debe admitir NAT estática (muchos-a-muchos);
37. Debe ser compatible con NAT estático bidireccional 1-a-1;
38. Debe ser compatible con la traducción de puertos (PAT);
39. Debe ser compatible con NAT Origen;
40. Debe ser compatible con NAT de destino;
41. Debe soportar NAT de origen y NAT de destino de forma simultánea;
42. Debe soportar NAT de origen y NAT de destino en la misma política
43. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
44. Debe ser compatible con NAT64 y NAT46;
45. Debe implementar el protocolo ECMP;
46. Debe soportar SD-WAN de forma nativa
47. Debe soportar el balanceo de enlace hash por IP de origen;
48. Debe soportar el balanceo de enlace por hash de IP de origen y destino;
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;
50. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
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;
52. Enviar logs a sistemas de gestión externos simultáneamente;
53. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
54. Debe soporta protección contra la suplantación de identidad (anti-spoofing);
55. Implementar la optimización del tráfico entre dos dispositivos;
56. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

57. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
58. Soportar OSPF graceful restart;
59. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
60. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
61. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
62. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
63. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
64. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 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;
66. La configuración de alta disponibilidad debe sincronizar: Sesiones;
67. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando. políticas de Firewalls, NAT, QoS y objetos de la red;
68. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
69. La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
70. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
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;
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;
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);

74. Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
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;
76. La consola de administración debe soportar como mínimo, ingles y Español.
77. La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad
78. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
79. Debe soportar controles de zona de seguridad;
80. Debe contar con políticas de control por puerto y protocolo;
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;
82. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
83. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
84. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
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.
86. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
87. Debe soportar el protocolo estándar de la industria VXLAN;
88. La solución debe permitir la implementación sin asistencia de SD-WAN
89. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;

90. la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.
91. Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
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;
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;
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;
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;
96. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
97. Actualización de la base de firmas de la aplicación de forma automática;
98. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
99. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
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;
101. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
102. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

103. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
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;
105. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
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);
107. Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
108. Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
109. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
110. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
111. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
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;
113. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
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;
115. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
116. Debe incluir la protección contra ataques de denegación de servicio;
117. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;

118. Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
119. Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
120. Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
121. Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
122. Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
123. Detectar y bloquear los escaneos de puertos de origen;
124. Bloquear ataques realizados por gusanos (worms) conocidos;
125. Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
126. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
127. Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
128. Identificar y bloquear la comunicación con redes de bots;
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;
130. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
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;
132. Los eventos deben identificar el país que origino la amenaza;
133. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
134. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
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;

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;
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);
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);
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;
140. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
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;
142. Tener por lo menos 75 categorías de URL;
143. Debe tener la funcionalidad de exclusión de URLs por categoría;
144. Permitir página de bloqueo personalizada;
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);
146. Además del Explicit Web Proxy, soportar proxy web transparente;
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;
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;

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;
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;
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;
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);
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;
154. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
155. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
156. Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;
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;
158. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

159. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
160. Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
161. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
162. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
163. En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
164. En QoS debe permitir la definición de tráfico con máximo ancho de banda;
165. En QoS debe permitir la definición de colas de prioridad;
166. Soportar marcación de paquetes DiffServ, incluso por aplicación;
167. Soportar la modificación de los valores de DSCP para Diffserv;
168. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
169. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;
170. Permite la creación de filtros para archivos y datos predefinidos;
171. Los archivos deben ser identificados por tamaño y tipo;
172. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
173. Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
174. Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
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;
176. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
177. Debe permitir la visualización de los países de origen y destino en los registros de acceso;
178. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;
179. Soporte VPN de sitio-a-sitio y cliente-a-sitio;

180. Soportar VPN IPSec;

181. Soportar VPN SSL;

182. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512

183. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;

184. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

185. La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

186. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

187. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;

188. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;

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;

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;

191. Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

192. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

193. Deberá mantener una conexión segura con el portal durante la sesión;

194. El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

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;

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;

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;

198. La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;

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;

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;

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;

202. La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;

203. La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;

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;

205. La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;

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;

207. Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;

208. La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;

209. La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;
210. La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;
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;
212. La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;
213. La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);
214. La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;
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;
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;
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;

HERRAMIENTA DE ADMINISTRACIÓN CENTRALIZADA Y HERRAMIENTA DE ANÁLISIS Y GESTIÓN DE EVENTOS DE LOS EQUIPOS DE COMUNICACIÓN.

Requerimiento mínimo de la máquina Virtual

1. La solución no deberá tener límites en cuanto a la cantidad de vCPU si la solución es virtual
2. 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
3. La solución deberá contemplar la administración de al menos 100 dispositivos, entiéndase firewall, switches, y aps.
4. La solución no deberá tener límites en cuanto a la cantidad de memoria RAM si el aparto es virtual
5. Debe de soportar la recepción de volumen de logs diarios de al menos 1GB

6. Debe de soportar 500GB de capacidad de almacenamiento como mínimo
7. Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución
8. 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.
9. Debe permitir accesos concurrentes de administradores
10. Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores
11. Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
12. Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión;

Requerimiento mínimo Herramienta de Administración Centralizada

13. Debe tener la capacidad de permitir provisionar y monitorear configuración de SD-WAN de todos los dispositivos gestionados desde una sola consola.
14. 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.
15. Debe tener la capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola
16. 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.
17. La solución debe ser capaz de realizar respaldos automáticos de configuración hasta en 5 nodos, conteniendo updates de todos los dispositivos gestionados.
18. 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.
19. La solución debe permitir utilización de API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.
20. Permitir integración de intercambio y compartición de datos con terceros mediante pxGrid, OCI, Esxi .
21. 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

22. Debe tener interfaz basada en línea de comando para administración de la solución de gestión;
23. Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos;
24. Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones;
25. Generar alertas automáticas por Email
26. Generar alertas automáticas por SNMP
27. Generar alertas automáticas por Syslog
28. 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;
29. Debe ser permitido al administrador transferir los backups a un servidor FTP.
30. Debe ser permitido al administrador transferir los backups a un servidor SCP
31. Debe ser permitido al administrador transferir los backups a un servidor SFTP
32. Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante;
33. Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES
34. Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS+
35. Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP
36. Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS
37. Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI)
38. Debe soportar sincronización de reloj interno por protocolo NTP.
39. Debe registrar las acciones efectuadas por cualquier usuario:
40. 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);
41. 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;

42. La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización;
43. La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación;
44. La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware;
45. La gestión debe permitir la creación y administración de políticas de Filtro de URL;
46. Permitir buscar cuáles reglas un objeto está siendo utilizado;
47. Permitir la creación de reglas que permanezcan activas en horario definido;
48. 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
49. Debe tener capacidad de desplegar los resultados de auditoría de seguridad de los dispositivos gestionados
50. Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;
51. Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing);
52. Debe permitir la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas;
53. Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión;
54. 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;
55. La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos;
56. Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados;
57. 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;

58. Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de los mismos;
59. Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.
60. 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;
61. Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos;
62. Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración;
63. Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos;
64. Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión;
65. Permitir configurar y visualizar el manejo de SD-WAN de los dispositivos gestionados de forma centralizada;
66. Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos;
67. Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada;
68. Permitir la creación de reglas anti DoS de forma centralizada;
69. Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada;
70. 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;
71. Debe permitir el uso de DDNS en VPNs de manera centralizada
72. Debe permitir la gestión de Access Points propietarios de manera centralizada
73. Debe permitir la gestión de Switches propietarios de manera centralizada
74. Debe permitir la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada

Requerimientos mínimos Herramienta de Análisis y Gestión de eventos de los equipos de comunicación.

75. Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
76. Autenticación de usuarios de acceso a la plataforma via LDAP
77. Autenticación de usuarios de acceso a la plataforma via Radius
78. Autenticación de usuarios de acceso a la plataforma via TACACS+
79. Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
80. Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
81. Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
82. 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.
83. Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
84. Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
85. Contar con mecanismos de borrado automático de logs antiguos.
86. Permitir la importación y exportación de reportes
87. Debe contar con la capacidad de crear informes en formato HTML
88. Debe contar con la capacidad de crear informes en formato PDF
89. Debe contar con la capacidad de crear informes en formato XML
90. Debe contar con la capacidad de crear informes en formato CSV
91. Debe permitir exportar los logs en formato CSV
92. Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
93. 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.
94. La solución debe contar con reportes predefinidos
95. Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
96. Debe ser posible la duplicación de reportes existentes para su posterior edición.
97. Debe tener la capacidad de personalizar la portada de los reportes obtenidos.

98. 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.
99. 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.
100. Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
101. Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
102. Debe permitir descargar de la plataforma los archivos de logs para uso externo.
103. Tener la capacidad de generar y enviar reportes periódicos automáticamente.
104. Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
105. Permitir el envío por email de manera automática de reportes.
106. Debe permitir que el reporte a enviar por email sea al destinatario específico.
107. Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
108. Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
109. Debe permitir el uso de filtros en los reportes.
110. Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
111. Permitir especificar el idioma de los reportes creados
112. Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
113. Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
114. 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.
115. 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.

116. 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.
117. 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.
118. Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
119. Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
120. Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
121. Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
122. Debe permitir visualizar en tiempo real los logs recibidos.
123. Debe permitir el reenvío de logs en formato syslog.
124. Debe permitir el reenvío de logs en formato CEF (Common Event Format).
125. Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
126. Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
127. Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
128. Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
129. Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
130. Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
131. Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
132. Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs

133. Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
134. Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
135. Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
136. Debe permitir generar alertas de eventos a partir de logs recibidos
137. Debe permitir crear incidentes a partir de alertas de eventos para endpoint
138. Debe permitir la integración al sistema de tickets ServiceNow
139. 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.
140. Debe permitir respaldar logs en nube publica de Microsoft Azure
141. Debe soportar el estándar SAML para autenticación de usuarios administradores

SERVICIOS CONEXOS

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, Esta capacitación (workshop) se brindara de manera virtual.
2. Instalación e implementación de todos los servicios adjudicados
3. Servicio de Garantía
4. Garantía, 3 años como mínimo
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.
6. Deberá incluir el soporte y actualización de sistema operativo durante el tiempo de garantía
7. Carta del fabricante que indique que el oferente es distribuidor de la marca
8. Cronograma detallado de las actividades a realizar, en dicho cronograma deberá además especificarse los tiempos de entrega de cada producto como ser licencias,

hardware, transferencia de conocimiento o cualquier otro que la solución oferta disponga.

9. El oferente deberá hacer entrega de todas las licencias que aseguren el correcto funcionamiento de la solución, para el caso que el licenciamiento entregado por correo electrónico, el oferente deberá hacer entrega de comprobante en papel membretado, indicando las especificaciones de esta, numero de parte y/o serie en caso de tenerlo.
10. La empresa que brinda el soporte debe ser centro autorizado de soporte de al menos dos marcas Americanas (USA).
11. El oferente como producto final para pago deberá hacer entrega de un informe que contenga la documentación técnica relacionada al proyecto de implementación. Indicando a detalle las configuraciones realizadas en los equipos.

CLÁUSULA TERCERA
RELACIÓN DE DOCUMENTOS

Forman parte del presente contrato los pliegos de condiciones, modificaciones, enmiendas, aclaraciones y toda correspondencia intercambiada a partir de la publicación de los pliegos de condiciones, la RESOLUCIÓN CD-58/2020 del 23 de diciembre del 2020 del Consejo Directivo de BANHPROVI, oferta Técnica y Económica presentada por PRODUCTIVE BUSINESS SOLUTION HONDURAS S.A. DE C.V. (PBS HONDURAS).

CLÁUSULA CUARTA
PLAZO DEL CONTRATO

El plazo de los servicios del presente contrato es de vigencia de noventa (90) días a partir de la de suscripción del contrato distribuidos de la siguiente manera sesenta (60) días para entrega de equipo y treinta (30) días de implementación.

CLÁUSULA QUINTA
PRÓRROGA DE LOS PLAZOS

Si la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** en cualquier momento durante la ejecución del Contrato, o en sus Subcontratistas encontrasen condiciones que impidiesen la entrega oportuna de los bienes o el cumplimiento de los Servicios conexos, informará prontamente y por escrito al BANHPROVI sobre la demora y posible duración y la causa en un período no mayor de cinco días hábiles, tan pronto como sea posible. Después de recibir la comunicación de la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS) El BANHPROVI** evaluará la situación y a su discreción podrá prorrogar el plazo de cumplimiento de la **PRODUCTIVE BUSINESS SOLUTIONS**

HONDURAS S.A. DE C.V (PBS HONDURAS) En caso de ocurrir dicha circunstancia, ambas partes ratificarán la prórroga mediante un Adendum al Contrato.

CLÁUSULA SEXTA
PRECIO Y FORMA DE PAGO

BANHPROVI se compromete a cancelar la cantidad de **DOS MILLONES CUATROCIENTOS SETENTA Y NUEVE MIL TRESCIENTOS CINCUENTA Y OCHO LEMPIRAS CON OCHENTA Y OCHO CENTAVOS (L2,479,358.88)** que incluye el monto **DE TRESCIENTOS VEINTITRÉS MIL TRESCIENTOS NOVENTA Y CUATRO LEMPIRAS CON SESENTA Y TRES CENTAVOS (L323,394.63)**. El pago se realizará mediante un (1) pago después de recibido a satisfacción y se cancelarán en lempiras en un plazo no mayor de treinta (30) días calendario, posteriores a la fecha en que se reciba el recibo correspondiente, en el cual se detalle el valor a cancelar correspondiente objeto de la presente licitación, debiendo contener la factura el visto bueno del Departamento de Informática; el cual incluye el Impuesto Sobre Ventas y deberá cancelarse en un solo pago el cien por ciento (100%) del valor del contrato. Las facturas de cobro deberán cumplir con el Reglamento del Régimen de Facturación, Otros Documentos Fiscales y Registro Fiscal de Imprenta.

CLÁUSULA SÉPTIMA
IMPUESTOS Y DERECHOS

La empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** será totalmente responsable por todos los impuestos, gravámenes, timbres, comisiones por licencias, y otros cargos similares incurridos hasta la entrega de los Servicios contratados por El BANHPROVI.

CLÁUSULA OCTAVA
GARANTÍA DE CUMPLIMIENTO

LA EMPRESA, PRODUCTIVE BUSSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS) dentro de los siguientes treinta (30) días siguientes al recibo de la notificación de adjudicación por pate de BANHPROVI, el proveedor deberá presentar la Garantía de Cumplimiento de Contrato otorgado por una institución Bancaria o de Compañía de Seguros extendida a favor de EL BANHPROVI por el monto equivalente al quince por ciento (15%) del valor del Contrato, garantizando el fiel cumplimiento de todas las obligaciones que la Empresa a **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** sume en los documentos del Contrato. Los recursos de la Garantía de Cumplimiento serán pagaderos al comprador como indemnización por cualquier pérdida que le pudiera ocasionar el incumplimiento de las obligaciones del Proveedor en virtud del Contrato. La vigencia de dicha Garantía deberá

ser por tiempo de duración del Contrato más tres meses después del plazo, conforme al establecido en la Ley de Contratación del Estado y su Reglamento.

CLÁUSULA NOVENA
IDIOMA

Toda correspondencia y documentos relativos al Contrato intercambiados entre la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** El BANHPROVI, deberán ser escritos en español. Los documentos de sustento y material impreso que formen parte del Contrato pueden estar en otro idioma siempre que los mismos estén acompañados de una traducción fidedigna de los apartes pertinentes al español y, en tal caso, dicha traducción prevalecerá para efectos de interpretación del Contrato. 2. la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** será responsable de todos los costos de la traducción al idioma que rige, así como de todos los riesgos derivados de la exactitud de dicha traducción de los documentos proporcionados por la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS).**

CLÁUSULA DÉCIMA
CONSORCIO

Si la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)**, es un Consorcio, todas las partes que lo conforman deberán ser mancomunada y solidariamente responsables frente a El BANHPROVI por el cumplimiento de las disposiciones del Contrato y deberán designar a una de ellas para que actúe como representante con autoridad para comprometer al Consorcio. La composición o constitución del Consorcio no podrá ser alterada sin el previo consentimiento del BANHPROVI.

CLÁUSULA DÉCIMA PRIMERA
SEGUNDA NOTIFICACIONES

Todas las notificaciones referentes a la ejecución de este contrato, serán válidas solamente cuando sean hechas por escrito a las direcciones de las partes contratantes, para cuyos efectos las partes señalamos como lugar para recibir notificaciones las siguientes direcciones: Todas las notificaciones entre las partes en virtud de este Contrato deberán ser por escrito y dirigidas: (Atención Licenciado Edwin Noé García Amador, Secretario del Comité de Licitaciones y Compras y Jefe de la División de Administración / Banco Hondureño para la Producción y la Vivienda, Primer piso del Edificio Principal del Banco Hondureño para la Producción y la Vivienda (BANHPROVI), al final del boulevard Centroamérica y prolongación al boulevard Juan Pablo II, Tegucigalpa,

Honduras, Teléfono (504) 2232-5500 extensión 102, correo electrónico edwin.garcia@banhprovi.gob.hn, y El Proveedor: **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS),** Colonia Izaguirre, Complejo Industrial San Miguel, Ofibodega #9.

CLÁUSULA DÉCIMA SEGUNDA
FRAUDE Y CORRUPCIÓN

El Estado Hondureño exige a todos los organismos ejecutores y organismos contratantes, al igual que a todas las firmas, entidades o personas oferentes por participar o participando en procedimientos de contratación, incluyendo, entre otros, solicitantes, oferentes, contratistas, consultores y concesionarios (incluyendo sus respectivos funcionarios, empleados y representantes), observar los más altos niveles éticos durante el proceso de selección y las negociaciones o la ejecución de un contrato. Los Actos de Fraude y Corrupción están prohibidos. 1. El BANHPROVI, así como cualquier instancia de control del Estado Hondureño tendrán el derecho revisar a los Adjudicados, proveedores, contratistas, subcontratistas, consultores y concesionarios sus cuentas y registros y cualesquiera otros documentos relacionados con el cumplimiento del contrato y someterlos a una auditoría por auditores designados por el BANHPROVI, o la respectiva instancia de control del Estado Hondureño. Para estos efectos, de la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** sus subcontratistas deberán: (i) conserven todos los documentos y registros relacionados con este Contrato por un período de cinco (5) años luego de terminado el trabajo contemplado en el Contrato; y (ii) entreguen todo documento necesario para la investigación de denuncias de fraude o corrupción, y pongan a la disposición del BANHPROVI o la respectiva instancia de control del Estado Hondureño, los empleados o agentes de la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** a y sus subcontratistas que tengan conocimiento del Contrato para responder las consultas provenientes de personal del BANHPROVI o la respectiva instancia de control del Estado Hondureño o de cualquier investigador, agente, auditor o consultor apropiadamente designado para la revisión o auditoría de los documentos. **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)**cualquiera de sus subcontratistas incumple el requerimiento del BANHPROVI o la respectiva instancia de control del Estado Hondureño, o de cualquier otra forma obstaculiza la revisión del asunto por éstos, el BANHPROVI o la respectiva instancia de control del Estado Hondureño bajo su sola discreción, podrá tomar medidas apropiadas contra la empresa **LA**

EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS) o subcontratista para asegurar el cumplimiento de esta obligación. 2. Los actos de fraude y corrupción son sancionados por la Ley de Contratación del Estado, sin perjuicio de la responsabilidad en que se pudiera incurrir conforme al Código Penal.

CLÁUSULA DÉCIMA TERCERA
JURISDICCIÓN Y LEGISLACIÓN APLICABLE

El presente Contrato se regirá y se interpretará según lo que estipule el presente Contrato, Los pliegos de Condiciones, Ley de Contratación del Estado y su Reglamento, y demás leyes vigentes en el país.

CLÁUSULA DÉCIMA CUARTA
SOLUCIÓN DE CONTROVERSIAS

El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) y la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** harán todo lo posible para resolver amigablemente mediante negociaciones directas informales, cualquier desacuerdo o controversia que se haya suscitado entre ellos en virtud o en referencia al Contrato. Cualquier divergencia que se presente sobre un asunto que no se resuelva mediante un arreglo entre la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** y El Banco Hondureño para la Producción y la Vivienda (BANHPROVI), deberá ser resuelto por éste, quien previo estudio del caso dictará su resolución y la comunicará al reclamante. Contra la resolución del Comprador quedará expedita la vía judicial ante la jurisdicción de los tribunales de lo Contencioso Administrativo del Departamento de Francisco Morazán.

CLÁUSULA DÉCIMA QUINTA
SUBCONTRATACIÓN

LA EMPRESA PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS), informará a EL BANHPROVI por escrito de todos los subcontratos que adjudique en virtud del Contrato si no los hubiera especificado en su oferta. Dichas notificaciones, en la oferta original o posterior, no eximirán al Proveedor de sus obligaciones, deberes y compromisos o responsabilidades contraídas en virtud del Contrato.

CLÁUSULA DÉCIMA SEXTA
MULTAS Y SANCIONES PECUNIARIAS POR INCUMPLIMIENTO

EL Banco Hondureño para la Producción y la Vivienda (BANHPROVI) en estricto cumplimiento al Artículo 76 de las Disposiciones Generales de Presupuesto General de Ingresos y Egresos de la República para el Ejercicio Fiscal del año 2020 y para garantizar

el fiel cumplimiento de las obligaciones de la empresa **LA EMPRESA, PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** deberá pagar al Banco Hondureño para la Producción y la Vivienda (BANHPROVI) una la multa diaria aplicable de cero puntos treinta y seis por ciento (0.36%), en relación con el monto total del saldo del Contrato por incumplimiento del plazo de entrega. **UNA DEMORA NO JUSTIFICADA DEL PLAZO DE ENTREGA** dará origen **A LA APLICACIÓN** DE UNA MULTA ACUMULADA EQUIVALENTE AL DIEZ por ciento (10%) del valor del Contrato, El BANHPROVI podrá considerar la resolución total del mismo y hacer efectiva la Garantía de Cumplimiento.

CLÁUSULA DÉCIMA SÉPTIMA
INDEMNIZACIÓN POR DERECHOS DE PATENTE

La empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** indemnizará y librará de toda responsabilidad a El BANHPROVI y sus empleados y funcionarios de esta, en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que El BANHPROVI tenga que incurrir como resultado de transgresión o supuesta transgresión de derechos de patente, uso de modelo, diseño registrado, marca registrada, derecho de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del Contrato.

CLÁUSULA DÉCIMA OCTAVA
CONFIDENCIALIDAD DE LA INFORMACION

Las partes, en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y Acceso a la Información Pública (LTAIP), y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del Estado de Derecho, nos comprometemos libre y voluntariamente a: **1)** Mantener el más alto nivel de conducta ética, moral y de respeto a las leyes de la República, así como los valores de **INTEGRIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRECIÓN CON LA INFORMACIÓN CONFIDENCIAL QUE MANEJAMOS, ABSTENIENDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LA MISMA. 2)** Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidas en la Ley de Contratación del Estado, tales como: Transparencia, Igualdad y Libre Competencia; **3)** Que durante la

ejecución del Contrato de Privado entre la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** y el Banco Hondureño para la Producción y la Vivienda BANHPROVI ninguna persona que actúe debidamente autorizada en nuestro nombre y representación y que ningún funcionario o empleado autorizado a no realizar **a) Prácticas Corruptivas:** Entendiendo éstas como aquellas en la que se ofrece, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; **b) Prácticas Colusorias:** Entendiendo éstas como aquellas en las que denoten, sugieran o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de alcanzar un propósito inadecuado, incluyendo influenciar en forma inapropiada las acciones de la otra parte. **4)** Revisar y verificar toda la información que deba ser presentada a través de terceros a la otra parte, para efectos del Contrato Privado entre el Banco Hondureño para la Producción y la Vivienda BANHPROVI, y dejamos manifestado que, durante el proceso de esta consultoría, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de la información inconsistente, imprecisa o que no corresponda a la realidad, para efectos de este contrato. **5)** Mantener la debida confidencialidad sobre toda la información a la que se tenga acceso por razón del contrato, y no proporcionarla ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos. **6)** Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta cláusula Tribunal competente, y sin perjuicio de la responsabilidad Civil, Administrativa o Penal en la que se incurra. **7)** Denunciar en forma oportuna ante las autoridades correspondientes cualquier hecho o acto irregular cometido por nuestros funcionarios o empleados, del cual tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad Civil, Administrativo o Penal. Lo anterior se extiende a la empresa PRODUCTIVE **BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** El Incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar: **a) De Parte de la empresa PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** 1) A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudieren deducírsele. **2)** A la aplicación al funcionario o empleado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral y en su caso entablar las acciones legales que correspondan. **b) De Parte del BANHPROVI: 1)** A la eliminación definitiva de la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** que

pudiendo hacerlo no denunciaron la irregularidad de su registro de proveedores y contratistas que al efecto llevare para no ser sujeto de elegibilidad futura en procesos de contratación. **2)** A la aplicación al funcionario o empleado infractor, de las sanciones que correspondan según el Código de Conducta Ética del Servidor Público, sin perjuicio de exigir la responsabilidad Administrativa Civil o Penal a los que hubiere lugar. En fe de lo anterior, las partes manifiestan la aceptación de los compromisos adoptados en el presente documento bajo el entendido que esta Declaración de Integridad forma parte del Contrato, firmado voluntariamente para constancia.

CLÁUSULA DÉCIMA NOVENA
RENUNCIA

La omisión de cualquiera de las partes en insistir ante una o más instancias, en el cumplimiento estricto de las obligaciones incluidas en el presente contrato o en el ejercicio de cualquier opción contemplada en este contrato, no se interpretará como una renuncia o abandono para el futuro de dichas obligaciones u opciones, sino que se mantendrán y preservarán con plena vigencia y efecto.

CLÁUSULA VIGÉSIMA
LIMITACIONES DE RESPONSABILIDAD

Excepto en casos de negligencia grave o actuación de mala fe: a la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** no tendrá ninguna responsabilidad contractual, de agravio o de otra índole frente al Banco Hondureño para la Producción y la Vivienda (BANHPROVI) por pérdidas o daños indirectos o consiguientes, pérdidas de utilización, pérdidas de producción, o pérdidas de ganancias o por costo de intereses, estipulándose que esta exclusión no se aplicará a ninguna de las obligaciones de la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** de pagar al Banco Hondureño para la Producción y la Vivienda (BANHPROVI) los daños y perjuicios previstos en el Contrato, y (b) la responsabilidad total de la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** ente al Banco Hondureño para la Producción y la Vivienda (BANHPROVI), ya sea contractual, de agravio o de otra índole, no podrá exceder el Precio del Contrato, entendiéndose que tal limitación de responsabilidad no se aplicará a los costos provenientes de la reparación o reemplazo de equipo defectuoso, ni afecta la obligación de la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** de indemnizar al Banco Hondureño para la Producción y la Vivienda (BANHPROVI) por las transgresiones de patente.

CLÁUSULA VIGÉSIMA PRIMERA

FUERZA MAYOR O CASO FORTUITO

El incumplimiento Parcial o total sobre las obligaciones que le corresponden a la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** de acuerdo con los requerimientos de esta Contratación y el Contrato firmado, no será considerado como tal, si a juicio del BANHPROVI se atribuye a fuerza mayor o caso fortuito debidamente justificado. Se entenderá por fuerza mayor o caso fortuito, todo acontecimiento que no ha podido preverse o que previsto, no ha podido resistirse; y que impide el exacto cumplimiento de las obligaciones contractuales, tales como fenómenos naturales, accidentes, huelgas, guerras, revoluciones o sediciones, naufragio e incendios. Si se presentara un evento de fuerza mayor o caso Fortuito, la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** notificará por escrito a El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) a la máxima brevedad posible sobre dicha condición y causa. A menos que el Banco Hondureño para la Producción y la Vivienda (BANHPROVI) disponga otra cosa por escrito en un plazo no mayor de cinco (5) días hábiles, la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** continuará cumpliendo con sus obligaciones en virtud del Contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de Fuerza Mayor o Caso Fortuito existente.

CLÁUSULA VIGÉSIMA SEGUNDA
TERMINACIÓN DEL CONTRATO

terminación por Incumplimiento: (a) El Banco Hondureño para la Producción y la Vivienda (BANHPROVI), sin perjuicio de otros recursos a su haber en caso de incumplimiento del Contrato, podrá terminar el mismo en su totalidad o en parte mediante una comunicación de incumplimiento por escrito a la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** en cualquiera de las siguientes circunstancias: (i) Si La Empresa no entrega parte o ninguno de los Servicios dentro del período establecido en el Contrato, o dentro de alguna prórroga otorgada por El Banco Hondureño para la Producción y la Vivienda (BANHPROVI), de conformidad con lo que estipula la Cláusula sexta de este Contrato. - (ii) Si la empresa. **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** no cumple con cualquier otra obligación en virtud del Contrato; o.- (iii) Si La Empresa a juicio del El Banco Hondureño para la Producción y la Vivienda (BANHPROVI), durante el proceso de licitación o de ejecución del Contrato, ha participado en actos de fraude y corrupción, según se define en la Cláusula Décimo

Séptima de este Contrato; o (iv) La disolución de la Sociedad Mercantil Proveedora, salvo en los casos de fusión de sociedades y siempre que solicite de manera expresa a El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) su autorización para la continuación de la ejecución del contrato, dentro de los diez días hábiles siguientes a la fecha en que tal fusión ocurra. El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) podrá aceptar o denegar dicha solicitud, sin que, en este último caso, haya derecho a indemnización alguna; o (v) La falta de Constitución de la Garantía de Cumplimiento del Contrato o de las demás Garantías a cargo de la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** dentro de los plazos correspondientes; (b) En caso de que El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) termine el Contrato en su totalidad o en parte, de conformidad con la Cláusula Décimo Cuarta Numeral 1 de este Contrato, éste podrá adquirir, bajo términos y condiciones que considere apropiadas, Bienes o Servicios Conexos similares a los no suministrados o prestados. En estos casos, la Empresa deberá pagar a El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) los costos adicionales resultantes de dicha adquisición. Sin embargo, seguirá estando obligado a completar la ejecución de aquellas obligaciones en la medida que hubiesen quedado sin concluir. 2. Terminación por Insolvencia: (a) El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) podrá rescindir el Contrato en cualquier momento mediante comunicación por escrito a la empresa de la declaración de quiebra o de suspensión de pagos o su comprobada incapacidad financiera. 3. Terminación por Conveniencia: (a) El Banco Hondureño para la Producción y la Vivienda (BANHPROVI), mediante comunicación enviada a la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** en podrá terminar el Contrato total o parcialmente, en cualquier momento por razones de conveniencia. La comunicación de terminación deberá indicar que la terminación es por conveniencia del Banco Hondureño para la Producción y la Vivienda (BANHPROVI), el alcance de la terminación de las responsabilidades de Empresa en virtud del Contrato y la fecha de efectividad de dicha terminación. b) Los bienes que ya estén fabricados y listos para embarcar dentro de los veintiocho (28) días siguientes al recibo por la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** de la notificación de terminación del Banco Hondureño para la Producción y la Vivienda (BANHPROVI) deberán ser aceptados por EL BANHPROVI de acuerdo con los términos y precios establecidos en el Contrato. En cuanto al resto de los Bienes, El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) podrá

elegir entre las siguientes opciones: (i) que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del Contrato; y/o. (ii) que se cancele el balance restante y se pague a la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** una suma convenida por aquellos Bienes o Servicios Conexos que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por La Empresa. 4. la empresa **PRODUCTIVE BUSINESS SOLUTIONS HONDURAS S.A. DE C.V (PBS HONDURAS)** y el Banco Hondureño para la Producción y la Vivienda (BANHPROVI) podrá terminar el Contrato también en caso de muerte del Proveedor individual, salvo que los herederos ofrezcan concluir con el mismo con sujeción a todas sus estipulaciones; la aceptación de esta circunstancia será potestativa de El Banco Hondureño para la Producción y la Vivienda (BANHPROVI) sin que los herederos tengan derecho a indemnización alguna en caso contrario. 5. El Contrato también podrá ser terminado por el mutuo acuerdo de las partes o por cualquiera de las causas establecidas en los artículos 126 y 127 de la Ley de Contratación del Estado.

CLÁUSULA VIGÉSIMA TERCERA
ACEPTACIÓN

Ambas partes declaran que aceptan para sus representadas las condiciones y términos estipulados en y se obligan a cumplirlos fielmente. Las partes manifestamos estar de acuerdo en todas y cada una de las cláusulas establecidas en el presente Contrato y nos comprometemos al fiel cumplimiento de estas, para Garantía de las partes, firmamos el presente contrato en dos ejemplares del mismo texto, en la ciudad de Tegucigalpa M.D.C. Departamento de Francisco Morazán, a los cinco (5) del mes de febrero del año dos mil veintiunos (2021).

POR BANHPROVI:

MAYRA ROXANA LUISA FALCK REYES
Presidenta Ejecutiva y representante legal del
BANCO HONDUREÑO PARA LA PRODUCCIÓN Y LA VIVIENDA
(BANHPROVI),
ID N° 0801-1959-03287

POR EL PROVEEDOR:

JUAN CARLOS FONSECA MEZA
REPRESENTANTE LEGAL
PRODUCTIVE BUSINESS SOLUTION
(PBS HONDURAS)
ID N° 0801-1982-04878

MIRIAM LUZ SANTAMARIA ZCHOCHER
REPRESENTANTE LEGAL
PRODUCTIVE BUSINESS SOLUTION
(PBS HONDURAS)
ID N°0902-1963-0005