INDICE

"CONTRATO DE ADQUISICION DE SISTEMA CORE SWITCH PARA LA OFICINA PRINCIPAL DE TEGUCIGALPA Y OFICINAREGIONAL DE SAN PEDRO SULA DEL IPM, SEGUN LICITACIÓN PÚBLICA 12-2021"

Nosotros, **INSTITUTO DE PREVISIÓN MILITAR (IPM),** identificada con Registro Tributario Nacional número 08019003238214 y representada en este acto por el Señor **ALFREDO FABRICIO ERAZO PUERTO**, mayor de edad, Coronel de Seguridad de Instalaciones DEMA, casado, hondureño, con Tarjeta de Identidad número 0101-1966-01501, actuando en mi condición de Gerente y Representante Legal del **INSTITUTO DE PREVISIÓN MILITAR** (I.P.M.) Organismo con Personalidad Jurídica y Patrimonio Propio, según Decreto Número Ciento Sesenta y Siete guión Dos Mil Seis (167-2006) emitido por el Soberano Congreso Nacional el Veintisiete (27) de Noviembre del año Dos Mil Seis (2006), con facultades suficientes para celebrar este contrato, nombrado por la Junta Directiva del Instituto de Previsión Militar, en Sesión Extraordinaria Número Ciento Cincuenta y Uno (151) mediante Resolución Número Cuatro Mil Novecientos Ochenta y Tres (4983) de fecha Nueve (09) de Marzo del año dos mil veinte (2020) y el Poder General de Representación y Administración otorgado mediante Instrumento Público número Cincuenta y Ocho (58) autorizado en esta ciudad ante los oficios de la Notario David Alfonso Velásquez el Doce (12) de Marzo del año Dos Mil Veintiuno (2021), e inscrito bajo el Número Cuarenta y tres (43) del Tomo Trescientos Cinco (305) del Registro Especial de Poderes del Registro de la Propiedad del Departamento de Francisco Morazán y quien en lo sucesivo y para efectos del presente contrato me denominaré como **EL INSTITUTO** y **OVIDIO ANTONIO NÚÑEZ,** mayor de edad, hondureño, casado, de este domicilio; con tarjeta de identidad No. **0801-1957-02524**, RTN número **08011957025249** actuando en mi condición de Representante Legal de la Sociedad **GBM DE HONDURAS S. A.,** Sociedad con RTN No. 08019002278467 y constituida en escritura pública No. 32 de fecha seis (06) de Diciembre de mil novecientos cincuenta y dos (1952) autorizada por el Notario Carlos Zelaya Galindo, inscrita bajo asiento No. 49, folios 128 al 136, Tomo 13 del Registro Mercantil de Francisco Morazán, cuya denominación social fue modificada en testimonio de escritura pública No. 10 de fecha treinta (30) de octubre de mil novecientos noventa y uno (1991) autorizada mediante los oficios del notario Tomas Moncada Fornero, debidamente inscrita bajo el No. 2 del Tomo 258 del Registro de Comerciantes Sociales del Registro de la propiedad Mercantil de Francisco Morazán, con facultades suficientes para la suscripción del presente contrato según Poder de Administración otorgado en instrumento público No. 85 de fecha 10 de octubre de 2019, por el Notario Rafael Roger Ordoñez, inscrito con numero 56946 matricula 70482 del Registro del Registro de la propiedad Mercantil de Francisco Morazán de la Cámara de Comercio Asociado IP, de la ciudad de Tegucigalpa, y para efectos de este contrato me denominaré como **EL PROVEEDOR**, hemos convenido en celebrar el presente "CONTRATO DE ADQUISICION DE SISTEMA CORE SWITCH PARA LA OFICINA PRINCIPAL DE TEGUCIGALPA Y OFICINAREGIONAL DE SAN PEDRO SULA DEL IPM", Según Acta No. 37-2021 del comité de compras y licitaciones de fecha 29 de septiembre de 2021, el que se regirá por las cláusulas y condiciones siguientes: PRIMERA: **OBJETO DEL CONTRATO**: El presente contrato tiene como objeto la adquisición de CORE SWITCH de comunicaciones del Data Center de Tegucigalpa por ciclo y obsolescencia tecnológica e instalar un switch de altas capacidades para la oficina regional de san pedro sula, las actividades son las siguientes: **I) Switch CORE de comunicaciones para uso del IPM: 1) ESPECIFICACIONES GENERALES MINIMAS: 1.1)** El switch propuesto deberá ser de arquitectura tipo Chasis modular, con al menos 07 slots o ranuras para tarjetas de línea y tarjetas supervisoras. **1.2)** El switch propuesto debe tener redundancia 1+1 para tarjetas supervisoras. Incluir al menos 1 supervisora.**1.3)** El switch propuesto debe tener redundancia N+1 ó N+N para ventiladores. **1.4)** El switch propuesto debe tener redundancia N+1 ó N+N para fuentes de poder. Incluir al menos 2 fuentes AC. **1.5)** El switch propuesto debe contar con, al menos, las tecnologías de siguiente generación que se listan a continuación: ASICs que soporten un Pipeline programable Y Asignación configurable basada en plantillas de: forwarding en capas 2 y 3, ACLs (Access Control Lists) y QoS (Quality of Service). **1.6)** El switch propuesto debe tener al menos una CPU x86 con 16 (diez y seis) GB de memoria RAM y 10 GB de memoria Flash o SSD. La memoria flash o SSD especificada debe estar

embebida en el equipo. 1.7) El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal. 1.8) El switch propuesto debe contar con un puerto USB como opción para cargar el sistema operativo y configuraciones. 1.9) El switch propuesto debe soportar la ejecución de scripts usando Python directamente desde el switch (on-box Python). De esta manera los scripts de Python pueden aprovechar la conexión directa con el dispositivo. 1.10) El switch propuesto debe contar con, al menos, 1 tarjetas de línea con 24 puertos basados en SFP cada una. Además de 2 tarjetas de 48-Port UPOE+ 10/100/1000 (RJ-45). 1.11) El chasis del switch propuesto debe proporcionar un ancho de banda por slot de 450 Gbps. 1.12) El switch propuesto debe ofrecer, al menos, el siguiente rendimiento: Capacidad de conmutación: 120 (ciento veinte) Gbps por slot, Capacidad de transmisión: 900 (novecientos) Mpps. 1.13) El switch propuesto debe poder manejar, al menos, 4000 (cuatro mil) identificadores de VLANs. 1.14) El switch propuesto debe poder manejar jumbo frames con un tamaño mínimo de 9000 bytes. 1.15) El switch propuesto debe tener, al menos, 2 (dos) fuentes de poder. Estas fuentes deben poder ser reemplazadas en caliente. 1.16) El switch propuesto debe contar con, al menos, los siguientes mecanismos de QoS: 802.1p CoS (Class of Service), Clasificación DSCP (Differentiated Services Code Point), Planificación SRR (Shaped Round Robin), CIR (Committed Information Rate), Class Based weighted fair queuing (CBWFQ), QoS Jerárquico (H-QoS), Weighted Random Early Detection (WRED), Manejo de prioridad a nivel de colas, ocho colas de salida por puerto basado en hardware, Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y numero de puertos TCP y UDP Y Configuración automática de QoS. 1.17) El switch propuesto debe poder enrutar el tráfico mediante cualquiera de los siguientes protocolos estándar: OSPF, BGP, Policy based routing, PIM, VRRP (Virtual router redundancy protocol), IP SLA (service level agreement) Y VRF. 1.18) El switch ofertado debe soportar APIs REST que puedan interactuar directamente con el sistema operativo del switch. 1.19) El switch propuesto debe soportar Spanning Tree IEEE 802.1d así como las mejoras tales como convergencia rápida (RSTP 802.1w) y múltiples instancias (MSTP 802.1s). 1.20) Los puertos del switch propuesto deben poder operar en half y full dúplex. 1.21) El switch propuesto debe soportar NTP e IGMP. 1.22) El switch propuesto debe soportar Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad. 1.23) El switch propuesto debe contar con los siguientes puertos para administración: puerto de consola: RJ45 y puerto ethernet dedicado para administración fuera de banda. 1.24) El switch propuesto debe soportar syslog. 1.25) El switch propuesto debe soportar administración vía web. 1.26) El switch propuesto debe soportar múltiples niveles de privilegios de acceso (mínimo 4) por puerto de consola o Telnet para administración. 1.27) Para asegurar una óptima seguridad en la gestión, el switch propuesto debe soportar la configuración de filtros de acceso que sólo permitan el acceso a determinadas IP en los puertos de gestión.1.28) El switch debe soportar procesos de debug para análisis en caso de fallas. 1.29) El switch propuesto debe tener la capacidad de limitar la cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.1.30) El switch propuesto Debe soportar mecanismos para evitar ataques tipo MITM, basados en STP y DHCP, así como "VLAN Hopping", "DHCP Rogue Server". 1.31) El switch propuesto debe soportar filtros aplicables por puerto, filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP. 1.32) El switch propuesto debe soportar de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL). 1.33) El switch propuesto debe soportar control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x. 1.34) El switch propuesto debe soportar movilidad de MAC en esquemas de 802.1x detrás de un teléfono, permitiendo que al ser autenticado el usuario conectado a un teléfono y luego de su desconexión, el switch pueda recibir información de la desconexión a pesar de no estar usuario físicamente conectado al switch, evitando el spoofing de la MAC. 1.35) El switch propuesto debe soportar de 802.1x, autenticación por MAC (MAB) y Web Authentication de manera dinámica para usuarios que se conectan detrás de un teléfono IP. 1.36) El switch propuesto debe soportar análisis de tráfico usando protocolos tipo Netflow o similares. El análisis de tráfico debe de ser tanto en el downlink como en el uplink. 1.37) El switch propuesto debe soportar de "port mirroring"

por puerto y por VLAN. **1.38)** El switch propuesto debe soportar múltiples sesiones de "port mirroring" así como "port mirroring" remoto.**1.39)** El software del switch deberá estar firmado criptográficamente; cuando el equipo inicia, las firmas del sistema operativo son verificadas. Se deberá ofercer información pública con los procedimientos para garantizar la autenticidad del software. **1.40)** El switch propuesto debe soportar boot seguro a prueba de manipulaciones, para asegurar que solamente el sistema operativo del fabricante pueda ser ejecutado en el hardware del mismo haciendo verificaciones procesador, memoria y ROM de arranque. **1.41)** El switch propuesto debe contar con un chip, con criptografía robusta, el cual provee garantía de autenticidad del hardware. **2) ESCALABILIDAD: 2.1)** El switch propuesto debe tener una memoria buffer para paquetes de, al menos, 16 (dieciséis) MB. **2.2)** El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware. **2.3)** El switch propuesto debe soportar dual-stack IPv4/IPv6 para facilitar la migración de IPv4 a IPv6. **2.4)** El switch propuesto debe tener posibilidad de crecer en puertos de 1Gbps, 10Gbps y 40 Gbps ya sea a través de puertos embebidos o tarjetas modulares adicionales. **3) SEGURIDAD: 3.1)** El switch propuesto debe soportar cifrado MACSEC (802.1AE) en todos los puertos y a todas las velocidades. **3.2)** Se debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, con el objetivo de detectar potenciales amenazas de seguridad. Esto deberá hacerse con tecnologías propias de los switches propuestos y software adicional; o a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis. **3.3)** La precisión a la hora de detectar malware en tráfico cifrado HTTPS debe ser de, al menos, el 99 (noventa y nueve) %. **3.4)** Los falsos positivos a la hora de detectar malware en tráfico cifrado HTTPS debe ser, como mucho, del 1 (uno)%. **3.5)** a solución propuesta debe permitir identificar los distintos mecanismos de encriptación que se están usando en la red. **3.6)** La solución propuesta debe permitir detectar: ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS) incluyendo inundaciones de todo tipo (ICMP, UDP, TCP SYN, TCP NULL, IP NULL, etc), presencia de botnets en la red, suplantación DNS, exploits de día cero, malware auto modificador, ataques en el tráfico cifrado o mal uso de recursos o configuración incorrecta de los dispositivos de comunicación (como por ejemplo errores de configuración en la segmentación de las VLANs). **3.7)** En caso de usar IPFIX, Netflow o protocolos similares para realizar la detección de anomalías de seguridad descrita en esta sección, los switches deben tener la capacidad de generar de forma conjunta como mínimo 200 (doscientos) flujos por segundo mediante la utilización de protocolos Netflow o similares. Estos flujos deberán ser usados para detectar anomalías en el tráfico tal como lo describe este apartado (apartado 6: seguridad). **4) AUTOMATIZACION: 4.1)** El switch propuesto debe soportar la automatización de las siguientes funciones, mediante el uso de un software con interfaz gráfica, el cual se debe incluir en la solución: El switch debe poder ser dado de alta automáticamente. Esto es aprovisionamiento "zero-touch", Plantillas de configuración, Obtención de información de inventario de los equipos, Administración de versiones de software: estandarización de imágenes de software, verificaciones antes y después de realizar el despliegue de nuevas versiones de software en los switches, Generación de grupos de dispositivos para simplificar tareas administrativas, Despliegue de políticas de Calidad de Servicio (QoS), Políticas de control de acceso, Segmentación automatizada basada en políticas de usuarios, dispositivos y cosas usando un overlay o fabric de red automatizado. La segmentación de usuarios debe poder hacerse en base a sus respectivos roles en la organización. La configuración de estas políticas debe poder hacerse en un entorno gráfico, de manera centralizada y debe estar preparado para tener una misma política en redes cableadas e inalámbricas. **5) MONITOREO Y ASEGURAMIENTO DE SERVICIOS: 5.1)** El switch propuesto debe soportar la automatización de las siguientes funciones, mediante el uso de un software con interfaz gráfica, el cual se debe incluir en la solución: Analíticos de la salud general de los dispositivos de infraestructura de red, Analíticos de conectividad de los dispositivos finales conectándose a la red, mediante la recolección de información con respecto a DHCP, estado de los puertos, autenticación, etc, Y Funcionalidad de búsqueda de dispositivos de infraestructura de red y usuarios. **6) REQUERIMIENTOS ESPECIFICOS: OPERATIVOS: 6.1)** El switch propuesto debe poder operar en un entorno físico cuya temperatura oscile entre los 0 (cero) y los 40 (cuarenta)

grados Celsius. **6.2)** El switch propuesto debe poder operar en un entorno físico cuya humedad relativa esté entre el 10 (diez) y el 95 (noventa y cinco) por ciento. **6.3)** El switch propuesto debe tener al menos, un MTBF de 300,000 (tres cientos mil) horas para la tarjeta supervisora del sistema y al menos un MTBF de 270,000 (dos cientos setenta mil) horas para las tarjetas de línea.**7) CONTROL DE ACCESO: 7.1)** Se debe incluir un software de control de acceso de red que soporte las siguientes funcionalidades para 200 dispositivos: Perfilar (identificar) el tipo de dispositivo que se conecta a la red, Poder registrar dispositivos personales en la red de SEDAPAL (BYOD), Autenticación, autorización y registro (AAA) Y Administración de cuentas de invitado. **8) SOPORTE: 8.1)** El equipo propuesto debe contar con una suscripción por, al menos, 3 (tres) años que incluya lo siguiente: Soporte y acceso a las actualizaciones del software del switch durante los 3 (tres) años de validez de la suscripción Y Apertura de casos con el oferente adjudicado o el fabricante de la solución para la resolución de problemas. **9) GARANTÍAS: 9.1)** Los equipos deben ser nuevos, no remanufacturados y garantizados contra defectos de fabricación. **9.2)** La solución propuesta debe contar con soporte técnico avalado por el fabricante durante 3 (tres) años. **9.3)** El soporte avalado por el fabricante debe brindar los siguientes beneficios durante su vigencia: Reemplazo del equipo y/o sus partes bajo modalidad 24x7x4 (24 horas laborables al día, 7 días laborables de la semana y reemplazo en sitio al en 4 hrs una vez que el fabricante ha confirmado el daño del equipo y/o sus partes), Acceso a actualizaciones del sistema operativo y parches de seguridad del switch Y Apertura de casos con el oferente adjudicado o el fabricante de la solución para la resolución de problemas. **10) INSTALACION: 10.1)** Instalación física en los racks propios del Instituto de previsión militar. **10.2)** Migración de configuración actual de Cisco 4507 hacia al nuevo Hardware. **10.3)** Conexiones hacia equipos existentes SG300. **II) Switch de acceso LAN de 48 Puertos para uso del IPM-SPS:** 1) Se deberá de incluir todo lo necesario para la correcta operación del equipo. 2) Todo el software deberá residir y ejecutarse con recursos propios del equipo propuesto. 3) Soporte de un puerto 10/100 para administración fuera de banda. 4) Se deberá de incluir todo lo necesario para la correcta instalación y operación del equipo. 5) Capacidad de apilamiento por medio tecnología dedicada para la creación de pilas y velocidad de 320 Gbps por cada miembro de la pila. 6) Capacidad administración y apilamiento de hasta 8 switches con una dirección IP. 7) Contar con puerto serial de consola y puerto USB 2.0 para respaldo de archivos. 8) Soporte de 48 puertos multigigabit ethernet. 9) Debe soportar los protocolos L3, Advanced IP unicast routing protocols (including Full [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], Border Gateway Protocol Version 4 [BGPv4], and Intermediate System-to-Intermediate System Version 4 [IS-ISv4]) are supported for load balancing and for constructing scalable LANs. IPv6 routing (using OSPFv3 and BGPv6) is supported in hardware for maximum performance. 10) Soporte de fuente de poder redundante interna. 11) Soporte de Listas de control de acceso, de QoS, de Seguridad y de seguridad de IPv6. 12) Soporte de IPv6 en hardware. 13) Soporte de IPv6 forwarding wire-rate en todos sus puertos. 14) Debe poseer un 176 Gbps de backplane. 15) Debe soportar un forwarding rate de al menos 130 Mbps para la versión de 48 puertos. 16) Debe soportar Nonstop Forwarding with Stateful switchover (NSF/SSO). 17) Debe soportar las tecnologias Ethernet, Fast Ethernet, Gigabit Ethernet, 10G Ethernet. 18) Deberá incluir 8 puertos sfp+, no incluir los módulos. 19) Debe manejar un mínimo de 8 colas de egreso por puerto. 20) Debe hacer el descubrimiento de dispositivos de transmisión half-duplex o full-duplex con selección automática de velocidad 10/100/1000 BaseT por puerto. 21) Debera.hacer Snooping para IPv4 y para IPv6. 22) Debe contar con el soporte de Jumbo Frames de 9198 bytes. 23) Debe permitir hasta 4000 VLANs y soporte del protocolo 802.1Q 24) Debe permitir Rapid Spanning Tree por VLAN. 25) Debe implementar un mecanismo centralizado para la adición, substracción, y cambio de nombres de VLANS, divulgando los cambios a la base de datos para todos los demás equipos en la red. 26) Debe ser capaz de implementar NTP (Network Time Protocol). 27) Deberá de incluir mecanismos que permitan la configuración de políticas de uso de puertos para ahorro de energía, se podrá utilizar protocolos como LLDP ó LLDP-Med para ello o el mecanismo que ofrezca el licitante. 28) Deberá de incluir la característica de autoconfiguración de puertos en base al tipo de servicio (Teléfono, Access Point, PC, etc) que se conecte al switch con el objeto de aplicar políticas de seguridad y de Calidad de Servicio por medio de plantillas ó similar; cabe señalar que el descubrimiento de dispositivos se podrá realizar en base a dirección

MAC ó por medio de Protocolo LLDP ó LLDP-MED. 29) Deberá de soportar control de flujo es decir deberá de tener mecanismos para hacer más eficiente la transmisión de datos a través de Gigabit Ethernet. 30) El equipo propuesto deberá permitir la administración centralizada para la creación, modificación y eliminación de VLANs a través de interfaz gráfica ó línea de comandos. En caso de ésta se pueda realizar a través de un interfaz gráfica, ésta deberá de incluirse; así mismo esta funcionalidad deberá estar protegida para evitar que equipos terceros no administrados por la convocante puedan modificar de manera no autorizada la base de datos de VLANs en cada uno de los switches de la infraestructura de la convocante. 31) El sistema Operativo deberá de incluir scripts que permitan la automatización de tareas en base a eventos ocurridos en el equipo; tales como la Detección de cambios en una interfaz ó puerto; generación de eventos en base a autenticaciones fallidas (802.1x), Eventos relacionados a la memoria del switch (umbrales de utilización), eventos en base al descubrimiento de otros dispositivos conectados a la red (utilizando LLDP) y eventos basados en el flujo de tráfico de datos (basado en Netflow). 32) El switch deberá contar con mecanismos para contar con visibilidad de tráfico alámbrico e inalámbrico que circula por el switch (o por el stack) monitoreando cada flujo. 33) El switch deberá contar con ASIC programables que permitan el desarrollo de APIs para agregar funcionalidades tanto a la red alámbrica como inalámbrica, soportándo la tendencia de la industria conocida como "Software Defined Networks (SDN)". 34) Debe soportar una arquitectura de acceso definido por software que permita simplificar la administración, unificar redes cableadas e inalámbricas, generar políticas basadas en grupos y analíticos basados en contexto. 35) Debe permitir capturar al menos 64,000 flujos de Flexible Netflow. 36) Debe soportar Encripted Traffic Analysis. 37) Debe soportar AES-256. 38) Debe soportar al menos 32,000 rutas en IPv4. 39) Debe soportar al menos 16,000 rutas en IPv6. 40) El equipo deberá contar con un tag RFID que permita su inventario y localización. 41) El equipo deberá incluir elementos para su montaje de un rack de 19 pulgadas. **ALTA DISPONIBILIDAD 42)** Deberá soportar que cuando se apilen dos o más switches entre sí, deberán de tener la capacidad de hacer "stacking", lo cual permite apilar por medio de interconexiones dedicadas entre dos switches o más, de tal manera que, para el resto de la red, parezca un solo switch; estas interconexiones deberán de tener un rendimiento (throughput) de al menos 480 Gbps y deberá de soportarse al menos 9 switches en stack. No deberá confundirse con el término "cascadeo", no aceptará soluciones con equipos cascadeados. 43) Debe soportar agrupación de interfases Ethernet en un solo enlace lógico. 44) Debe soportar Spanning Tree Protocol (STP) por VLAN de forma independiente. 45) Debe soportar Spanning Tree Protocol estándares: 802.1d, 802.1w, y 802.1s. **SEGURIDAD 46)** Encrypted Traffic Analytics (ETA). Se beneficia del poder del aprendizaje automático para identificar y tomar medidas contra amenazas o anomalías en su red, incluida la detección de malware en el tráfico cifrado (sin descifrado) y la detección de anomalías distribuidas. 47) El equipo deberá tener la capacidad de proteger el protocolo DHCP para evitar que en la infraestructura de redes puedan operar servidores DHCP no administrados por la solicitante. La funcionalidad deberá identificar intentos de consumir el(los) scope(s) de direcciones administradas por el o los servidores DHCP de CONAMP. Este mecanismo deberá utilizar el campo CHADDR del protocolo DHCP y no solamente la dirección mac address origen de la solicitud DHCP. 48) Protección de Protocolo ARP (Address Resolution Protocol) para ataques de ARP Poisoning. 49) El equipo debe tener la capacidad de evitar que dos dispositivos conectados en la misma VLAN traten de utilizar una dirección IP que está siendo utilizada por otro dispositivo en la misma VLAN, con el fin de evitar que equipos terceros intenten utilizar direcciones IPs de servicios críticos en la VLAN en donde el tercero no autorizado pueda encontrarse conectado (i.e. que intente utilizar la dirección IP del Gateway por defecto). 50) El equipo propuesto deberá tener la capacidad de limitar el número direcciones MAC que puede tener asociadas a un mismo puerto físico. El equipo propuesto también deberá tener la capacidad de permitir el acceso al puerto físico del switch dependiendo de la dirección MAC del dispositivo que busca el acceso. 51) El equipo propuesto deberá permitir el acceso a la red mediante previa autorización mediante el protocolo 802.1x. 52) El equipo propuesto deberá tener la capacidad de evitar que BPDUs del protocolo spanning tree puedan ingresar por un puerto que está identificado como puerto de acceso. Cuando el equipo propuesto detecte que existe un intento de introducir un BPDU por un puerto de acceso, el puerto de acceso deberá inhabilitarse. 53) El equipo propuesto deberá tener la

capacidad de evitar que BPDUs del protocolo spanning tree puedan ingresar por un puerto que está identificado como puerto de acceso. Cuando el equipo propuesto detecte que existe un intento de introducir un BPDU deberá evitar que este paquete ingrese a la red y dejar que el resto del tráfico pueda seguir transitando. 54) El equipo propuesto deberá tener la capacidad de evitar que ciertos puertos físicos del switch puedan resultar electos como puertos root de spanning tree. Cuando el recálculo de la topología spanning tree de como resultado que un puerto físico del switch sea elegido como root de spanning tree y este sea un puerto que la convocante no quiere que sea designado como root de spanning tree el dispositivo deberá deshabilitar este puerto. 55) El equipo propuesto deberá ser capaz mediante 802.1x de asignar la VLAN a la cual pertenece puerto del switch en donde se conecta el cliente en base a las credenciales que el usuario presenta ante la infraestructura de red. 56) El equipo propuesto deberá tener la capacidad de poder configurar puertos de acceso para replicar el tráfico de otros puertos o de otras VLANs en el mismo switch físico o en switches que se encuentre físicamente separado del switch en donde se encuentra configurado este puerto espejo. 57) El equipo deberá tener la capacidad de segmentar dominios de capa dos (VLANs) sin necesidad de segmentar en capa tres. 58) Debe desempeñar 802.1x. 59) Debe soportar autenticación RADIUS o TACACS+ permitiendo un control centralizado del equipamiento y evitando que usuarios no autorizados alteren la configuración del dispositivo. 60) MAC de al menos 32,000 direcciones. 61) Debe soportar SSHv2 y SNMPv3. 62) IEEE 802.1x suplicant. 63) Bypass de autenticación basada en dirección MAC. 64) DHCP snooping . 65) Listas de control de acceso para interfaces de L2. 66) Deberá proteger puertos de acceso y de troncal en base a direcciones MAC. 67) Capaz de usar puertos para análisis. 68) Notificación de direcciones MAC. 69) Deberá proteger puertos en los que se conecte el switch en base a direcciones MAC. 70) IGMP para IPv4 y para IPv6. **CALIDAD DEL SERVICIO 71)** Debe implementar colas de prioridades por puerto permitiendo priorizar el tráfico y la interoperación de voz, video y data mediante el protocolo IEEE 802.1P CoS ("Class of Service"). 72) Debe de manejar la detección automática de teléfonos IP sin requerir políticas de 802.1x. 73) Debe detectar y clasificar paquetes con CoS y DSCP. 74) Debe asegurar priorización diferencial. **ADMINISTRACION 75)** Debe soportar configuración vía línea de comando y conexión SSH v2. 76) Debe poder ser administrado ("in-band") por el protocolo SNMP v3. 77) Debe poder ser administrado vía puerto de consola ("out-of-band"). 78) Debe soportar los siguientes grupos de RMON: históricos, estadísticas, alarmas y eventos. 79) El equipo deberá ser capaz de configurar puertos de monitoreo para análisis de tráfico por puerto o por vlan en el switch local o en cualquier otro switch dentro de la misma red. 80) Debe tener capacidad de implementar Syslog. 81) Proveer los beneficios de balanceo de carga de Layer 2. **NORMAS QUE DEBE CUMPLIR EL EQUIPO 82)** IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1X-Rev, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.3af, IEEE 802.3at. **PROTOCOLOS 83)** Ethernet IEEE 802.3, 10BASE-T. Fast Ethernet IEEE 802.3u, 100BASE-TX, 100BASE-FX (SFP). Gigabit Ethernet 1000BASE-SX (SFP), 1000BASE-LX/LH (SFP). 10 Gigabit Ethernet 10GBASE-X (SFP+). 40 Gigabit Ethernet 40GBASE-X (QSFP+). **PUERTOS 84)** 48 puertos 10/100/1000 RJ45 8 puertos sfp+. ACCESORIOS 85) Equipado con software y licencias correspondientes para su operación, Debe incluir juego de manuales en idioma español o inglés. **GARANTIA 86)** Los equipos deben ser nuevos, no re manufacturados y garantizados contra defectos de fabricación, La solución propuesta debe contar con soporte técnico avalado por el fabricante durante 3 (tres) años, El soporte avalado por el fabricante debe brindar los siguientes beneficios durante su vigencia: (Reemplazo del Equipo y/o sus partes modalidad 24x7x4 (24 horas laborables al día, 7 días laborables de la semana y reemplazo en sitio al menos en 4 horas una vez el fabricante ha confirmado el daño del equipo y/o sus partes): Acceso a actualizaciones del sistema operativo y parches de seguridad de los switches Y Apertura de casos con el oferente adjudicado o el fabricante de la solución para la resolución de problemas. INSTALACION 87) instalación física del dispositivo en los Racks del IPM, Migracion de configuración actual de switches dell y cisco hacia el nuevo hardware, Verificacion de buen funcionamiento en la nueva plataforma. **SEGUNDA: MONTO DEL CONTRATO:** El monto total del presente contrato es por la cantidad de **OCHOCIENTOS SESENTA Y NUEVE MILNOVENTA Y SIETE LEMPIRAS CON 69/100 (L.869,097.69). TERCERA: FORMA DE PAGO: EL INSTITUTO**, pagará a **EL PROVEEDOR** un

único pago para lo cual deberá de presentarse un acta de recepción del trabajo realizado con el visto bueno de la Division de Tecnología y Procesos del Instituto de Previsión Militar.- CUARTO: GARANTÍA: **EL PROVEEDOR**, se compromete a entregar: 1) **UNA GARANTÍA DE CUMPLIMIEMTO DE CONTRATO** equivalente al quince por ciento (15%) del monto total del contrato, por un valor de **CIENTO TREINTA MIL TRESCIENTOS SESENTA Y CUATRO LEMPIRAS CON 65/100 (L. 130,364.65)** esta garantía deberá ser emitida por una Institución Bancaría o entidad Aseguradora establecida legalmente en el País.- QUINTO: **EL PROVEEDOR se compromete a facilitar cualquier tipo de información a los Auditores Externos contratados por el INSTITUTO, referente a los montos y ejecución del presente contrato.** SEXTO: CAUSAS DE DISOLUCIÓN DEL CONTRATO: Las partes contratantes podrán invocar cualesquiera de las causas de disolución del contrato tales como: 1) El grave o reiterado incumplimiento de las cláusulas convenidas, 2) La declaración de quiebra o de suspensión de pagos del **PROVEEDOR**, o su comprobada incapacidad financiera; 3) Los motivos de interés públicos o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor sobreviviente a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución; 4) El incumplimiento de las obligaciones de pago más allá del plazo previsto en el contrato; 5) El mutuo acuerdo de las partes; y, 6) Las demás que establezca expresamente este contrato y las Leyes vigentes en la República. SÉPTIMO: MULTAS: Por cada día de retraso de la entrega del proyecto y por causas atribuidas a **EL CONTRATISTA, EL INSTITUTO**, cobrará el **0.36%** del monto que falte por pagar al momento del incumplimiento.- SEPTIMO: SOLUCIÓN DE CONFLICTOS Si existiera alguna desavenencia con motivo o en ocasión de la ejecución e interpretación de este contrato, y las misma no fuera solucionada por el buen entendimiento extrajudicial, o la conciliación de ambas partes, ambas nos sometemos a la jurisdicción y competencia del Juzgado de Letras Civil de Francisco Morazán. Para todo lo no previsto en el presente contrato, se aplicarán las disposiciones legales del ordenamiento jurídico vigente de la República de Honduras que le sean aplicables. Este contrato no se regirá con las normas contenidas en la legislación laboral, ya que su carácter es de naturaleza enteramente civil. OCTAVO: VIGENCIA DEL CONTRATO: Será de un (1) año a partir de la orden de inicio, girada por escrito por la Division de Tecnología y Procesos.- NOVENO: CLAUSULA DE INTEGRIDAD: 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, ABSTENIÉNDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LAS MISMAS.** 2. Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado tales como: Transparencia, igualdad y libre competencia. 3. Que durante la ejecución del contrato ninguna persona que actué debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado autorizado o no, realizará a) **Prácticas Corruptivas:** entendiendo estas como aquellas en las que se ofrece dar, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) Prácticas Colusorias: entendiendo estas como aquellas en las que denoten, surgieran 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 y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de 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 por el Tribunal competente y sin perjuicio de la responsabilidad civil o penal, en la que incurra. 7. Denunciar en forma oportuna ante las autoridades correspondientes, cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende al sub-contratista, con los cuales el contratista o consultor contrate así como los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar a: De parte del contratista o consultor: i. A la inhabilitación para contratar con el Estado, sin prejuicio de las responsabilidades que pudieren deducírsele a. La aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral, en su caso entablar las acciones legales que correspondan. b. De parte del contratante a la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o 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. ii. A la aplicación del empleado o funcionario infractor de las sanciones que correspondan según Código de conducta Ética del servidor público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar.

En fe de lo cual firmamos el presente contrato, manifestando nuestra conformidad con todas y cada una de las cláusulas, condiciones y disposiciones incluidas y nos obligamos a su fiel cumplimiento. Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los veinticinco (25) días del mes de octubre del año Dos Mil veintiuno (2021).

CORONEL DE SEGURIDAD DE INSTALACIONES

ALFREDO FABRICIO ERAZO PUERTO
EL INSTITUTO

An IBM Alliance Company

OVIDIO ANTONIO NÚÑEZ
EL PROVEEDOR

"CONTRATO DE COMPRA DE MOBILIARIO, EQUIPO DE OFICINA Y GIMNASIO PARA EL INSTITUTO DE PREVISIÓN MILITAR SEGÚN, LICITACIÓN PÚBLICA NO. 10-2021".

Nosotros, **ALFREDO FABRICIO ERAZO PUERTO**, mayor de edad, Coronel de Seguridad de Instalaciones DEMA, casado, hondureño, con Tarjeta de Identidad número 0101-1966-01501, actuando en mi condición de Gerente y Representante Legal del **INSTITUTO DE PREVISIÓN MILITAR** (I.P.M.) Organismo con Personalidad Jurídica y Patrimonio Propio, según Decreto Número Ciento Sesenta y Siete guión Dos Mil Seis (167-2006) emitido por el Soberano Congreso Nacional el Veintisiete (27) de Noviembre del año Dos Mil Seis (2006), con facultades suficientes para celebrar este contrato, nombrado por la Junta Directiva del Instituto de Previsión Militar, en Sesión Extraordinaria Número Ciento Cincuenta y Uno (151) mediante Resolución Número Cuatro Mil Novecientos Ochenta y Tres (4983) de fecha Nueve (09) de Marzo del año dos mil veinte (2020) y el Poder General de Representación y Administración otorgado mediante Instrumento Público número Cincuenta y Ocho (58) autorizado en esta ciudad ante los oficios del Notario David Alfonso Velásquez el Doce (12) de Marzo del año Dos Mil Veintiuno (2021), e inscrito bajo el Número Cuarenta y tres (43) del Tomo Trescientos Cinco (305) del Registro Especial de Poderes del Registro de la Propiedad del Departamento de Francisco Morazán y quien en lo sucesivo y para efectos del presente contrato me denominaré como **EL INSTITUTO** y **ROBERTO SALVADOR PANAYOTTI MARTIN,** mayor de edad, hondureño, casado, Licenciado en Administración de Empresas, con Identidad No. 0101-1963-01366, con RTN número 01011963013665, con domicilio en la Ciudad de Tegucigalpa, Municipio del Distrito Central, actuando en mi condición de Representante de la Sociedad **INDUSTRIAS PANAVISIÓN S.A. DE C.V.**, con RTN No. 05019995136860 y constituida en escritura pública No. 169 de fecha once (11) de Julio de mil novecientos setenta y nueve (1979) autorizada por el Notario SERGIO ZAVALA LEIVA, inscrita bajo el número 93, Tomo 6 del Registro Mercantil de San Pedro Sula, cuya denominación social fue modificada en testimonio de escritura pública No. 75 de fecha veintidós (22) de marzo de mil novecientos ochenta y cinco (1985) autorizada mediante los oficios del notario NAPOLEON HUMBERTO ZAVALA VALLADARES , debidamente inscrita bajo el número 90, Tomo 51 del Registro Mercantil de San Pedro Sula, debidamente inscrita y con facultades suficientes para este acto según Poder General de Administración otorgado mediante instrumento público No. 506 de fecha uno (1) de agosto de dos mil dieciocho (2018) autorizado en la Ciudad de San Pedro Sula por el Notario RAMON EDGARDO IRULA RODRIGUEZ, inscrito bajo matricula No. 75099 del Registro Mercantil de San Pedro Sula Centro Asociado del Registro Mercantil de San Pedro Sula y que para efectos de este contrato me denominaré como **EL PROVEEDOR**, en el cual hemos convenido en celebrar el presente **"CONTRATO DE COMPRA DE MOBILIARIO, EQUIPO DE OFICINA Y GIMNASIO PARA EL INSTITUTO DE PREVISIÓN MILITAR SEGÚN, LICITACIÓN PÚBLICA NO. 10-2021",** Aprobado en Comité de Compras y

Licitaciones No. 35-2021 del 17 de septiembre de 2021 y Resolución de Gerencia de fecha 30 de septiembre de 2021, el cual se regirá por las cláusulas y condiciones siguientes: **PRIMERA: OBJETO DEL CONTRATO**: El presente contrato tiene como objeto la compra de: **LOTE 1:** un (1) escritorio ejecutivo, catorce (14) escritorios semi ejecutivos, Diez (10) escritorios secretariales. **LOTE 2:** Cincuenta (50) sillas ejecutivas, Cincuenta y Seis (56) sillas Semi-ejecutivas, una (1) sillas Semi-ejecutiva Ergonómica, Treinta y cinco (35) sillas de Visita con Brazos, EXCEPTUANDO EL ITEN B. **LOTE 3:** Doce (12) Armario de persiana vertical alto (Leitz), Seis (6) Armario de persiana vertical alto (pendaflex), Ocho (8) armarios de persianas vertical (medio), un (1) Mueble de Cocina, Ocho (8) archivadores metálico de cuatro gavetas, Tres (3) Locker de 3 compuertas, Dos (2) Locker de 2 compuertas, Diecinueve (19) Gavetero con Rodos, Tres (3) Mesa con rodos pequeña, Dos (2) Mesa con Rodo para impresora, Dos (2) Mesa de Noche, Dos (2) Mesa de Conferencia 8 personas, Tres (3) Closet con espejo, Un (1) Mesa Redonda 1.5m diámetro. **LOTE 4:** Veinticuatro (24) Estaciones de Trabajo L 60.00cmX135.00X120.00cm, Siete (7) Estaciones de Trabajo L 140.00cmX60.00X120.00cm, Once (11) Estaciones de Trabajo L 120.00cmX60.00X120.00cm. El mobiliario y equipo antes descrito debe reunir todas las especificaciones técnicas establecidas en las bases de licitación; las que forman parte integra del presente Contrato- **SEGUNDA: MONTO DEL CONTRATO:** El monto total del presente contrato es por la cantidad de **DOS MILLONES TRESCIENTOS TREINTA Y SIETE MIL SEISCIENTOS OCHENTA LEMPIRAS CON 68/00 (L. 2,337,680.68)** Oferta que incluye el Impuesto sobre ventas. **TERCERA: FORMA DE PAGO: EL INSTITUTO** pagará a **EL PROVEEDOR** un pago único, previo a informe de satisfacción y verificación del total de los productos entregados, emitido por el supervisor de la División de Bienes y Seguridad Institucional del IPM.- **CUARTA: SUPERVISIÓN POR PARTE DEL INSTITUTO**: **EL INSTITUTO** nombrará un supervisor de la División de Bienes y Seguridad Institucional, quien se encargará de verificar y dar fé de la calidad de los productos entregados y el cumplimiento del contrato por parte de **EL PROVEEDOR.- QUINTA: GARANTÍAS DEL PROVEEDOR: 1) UNA GARANTÍA DE CUMPLIMIENTO DE CONTRATO** por la cantidad de **TRESCIENTOS CINCUENTA MIL SEISCIENTOS CINCUENTA Y DOS LEMPIRAS CON 10/100 (L. 350,652.10)** en concepto del quince por ciento (15%) del monto total del Contrato, la cual tendrá una vigencia de seis (6) meses, contados a partir de la fecha en que se firme el presente contrato, **(2) UNA GARANTÍA DE CALIDAD:** por la cantidad de **CIENTO DIECISEIS MIL OCHOCIENTOS OCHENTA Y CUATRO LEMPIRAS CON 03/100 (L. 116,884.03)** en concepto del cinco por ciento (5%) del monto total del Contrato, con vigencia de un (1) año a partir de la entrega de los bienes; ambas garantías deberán ser emitidas por una Institución Bancaría o Entidad Aseguradora establecida legalmente en el País, de reconocida experiencia y capacidad, y ser aceptada por **EL INSTITUTO.- SEXTA: EL CONTRATISTA se compromete a facilitar cualquier tipo de información a los Auditores Externos contratados por el INSTITUTO, referente a los montos y ejecución del presente contrato. SEPTIMA: INCUMPLIMIENTO DEL CONTRATO:** En caso de incumplimiento comprobado por parte del **PROVEEDOR** en

las cláusulas convenidas y en el objeto del presente contrato, **EL INSTITUTO** hará efectiva la Garantía de Cumplimiento de Contrato, con previa notificación a **EL PROVEEDOR**. De igual forma el Proveedor pagará la indemnización que conforme a Ley corresponda.- **OCTAVA: CAUSAS DE DISOLUCIÓN DEL CONTRATO:** Las partes contratantes podrán invocar cualesquiera de las causales de disolución del contrato tales como: **1)** El grave o reiterado incumplimiento de las cláusulas convenidas, **2)** La falta de constitución de las garantías a cargo del **PROVEEDOR** dentro de los plazos correspondientes; **3)** En caso de muerte de **EL PROVEEDOR** y sus sucesores no pudieren concluir el Contrato; **4)** La declaración de quiebra o suspensión de pagos del **PROVEEDOR,** o su comprobada insolvencia financiera; **5)** Los motivos de interés públicos o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor que surjan a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución; **6)** El incumplimiento de las obligaciones de pago más allá del plazo previsto en el contrato; **7)** El mutuo acuerdo de las partes; **8)** Las demás que establezca expresamente este contrato, las especificaciones técnicas y las Leyes vigentes en la República; y, **9)** En caso de existir alguna orden de cambio y/o modificación no aprobada por la División de Bienes y Seguridad Institucional del IPM o alguna modificación no contemplada por el **INSTITUTO**.- **NOVENA: CESIÓN, SUB CONTRATACIÓN, TRASPASO DEL CONTRATO: EL PROVEEDOR** no podrá ceder, subcontratar o traspasar lo estipulado en el presente contrato sin previo consentimiento por escrito del **INSTITUTO.** La aprobación de cualquier subcontratación no eximirá a **EL PROVEEDOR** de ninguna responsabilidad u obligación bajo los términos de este contrato. **EL PROVEEDOR** no podrá ceder su derecho a recibir pago conforme a lo estipulado en el presente contrato, sin previo consentimiento por escrito del **INSTITUTO. - DECIMA: SOLUCIÓN DE CONFLICTOS:** Si existiera alguna desavenencia en la interpretación y ejecución de este contrato y la misma no fuera solucionada por el buen entendimiento extrajudicial o la conciliación, ambas partes nos sometemos a la jurisdicción y competencia del Juzgado de Letras Civil de Francisco Morazán. Para todo lo no previsto en el presente contrato, se aplicarán las disposiciones legales del ordenamiento jurídico vigente de la República de Honduras que le sean aplicables. **DECIMA PRIMERA: MULTAS:** Por cada día de retraso de la entrega y por causas atribuidas a **EL PROVEEDOR, EL INSTITUTO**, cobrará el **0.36%** del monto del contrato o que no cubran con lo especificado en el contrato y las bases de licitación.- **DÉCIMA SEGUNDA: CLAUSULA DE INTEGRIDAD:** 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, ABSTENIÉNDONOS DE**

DAR DECLARACIONES PÚBLICAS SOBRE LAS MISMAS. 2.) Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado tales como: Transparencia, igualdad y libre competencia. 3.) Que durante la ejecución del contrato ninguna persona que actué debidamente autorizada en nuestro nombre y representación, empleado o trabajador, socio o asociado autorizado o no, realizar a) **Prácticas Corruptivas:** entendiendo estas como aquellas en las que se ofrece dar, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) Prácticas Colusorias: entendiendo estas como aquellas en las que denoten, surgieran 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 y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de 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 por el Tribunal competente y sin perjuicio de la responsabilidad civil o penal, en la que incurra. 7.) Denunciar en forma oportuna ante las autoridades correspondientes, cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende al sub-contratista, con los cuales el contratista o consultor contrate así como los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar: a) De parte del contratista o consultor: i) A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudieren deducírsele la aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral, en su caso entablar las acciones legales que correspondan. b) De parte del contratante: A la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o 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. ii) A la aplicación del empleado o funcionario infractor de las sanciones que correspondan según Código de conducta Ética del servidor público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar. **DÉCIMA TERCERA: RESPONSABILIDADES:** El PROVEEDOR se hace responsable por cualquier accidente de trabajo y pago de planilla de sus empleados. Además asume todas las responsabilidades legales, sociales y laborales

prescritas en todas las leyes que se mantengan en vigencia en el país y que se deriven de las relaciones obreras patronales que mantengan con todos los trabajadores que presten el servicio objeto del presente contrato de Servicios, obligaciones que correrán por cuenta de EL PROVEEDOR.- **DÉCIMA CUARTA: VIGENCIA DEL CONTRATO:** La vigencia del presente contrato es de cuarenta y cinco (45) días hábiles a partir de la firma del mismo. En fé de lo cual firmamos el presente contrato, manifestando nuestra conformidad con todas y cada una de las cláusulas, condiciones y disposiciones incluidas y nos obligamos a su fiel cumplimiento. Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los un (01) días del mes de octubre del año Dos Mil Veintiuno (2021).

CORONEL DE SEGURIDAD DE INSTALACIONES DEMA

ALFREDO FABRICIO ERAZO PUERTO
EL INSTITUTO

LICENCIADO EN ADMINISTRACIÓN DE EMPRESAS

25/11/21

ROBERTO SALVADOR PANAYOTTI MARTIN
EL PROVEEDOR