FISCALÍA GENERAL DE LA REPÚBLICA FISCAL GENERAL EL SALVADOR, C.A.

GOBIERNO DE EL SALVADOR

MINISTERIO DE EDUCACIÓN CIENCIA Y TECNOLOGÍA

CONTRATO No. MINEDUCYT – 336/2021 – GOES

RESOLUCIÓN DE ADJUDICACIÓN No. MINEDUCYT– 27/2021

LICITACIÓN ABIERTA DR-CAFTA LA/ADACA-UE No. 128/2021 – MINEDUCYT–GOES/GOES 7239/FANTEL

"ADQUISICIÓN DE EQUIPO INFORMÁTICO PARA DIFERENTES UNIDADES DEL MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA AÑO 2021"

FINANCIAMIENTO: FONDOS DEL GOBIERNO DE EL SALVADOR

NOSOTROS, RODOLFO ANTONIO DELGADO MONTES, mayor de edad, [redacted] del domicilio de [redacted] departamento de [redacted] portador del Documento Único de Identidad número: [redacted] actuando en nombre y representación del Estado y Gobierno de El Salvador, específicamente del Ministerio de Educación, Ciencia y Tecnología, con Número de Identificación Tributaria: [redacted] en carácter de Fiscal General de la República, y que en el transcurso de este instrumento me denominaré "la Institución Contratante o MINEDUCYT", y ALEJANDRO JOSÉ MORA ZEPEDA, mayor de edad, [redacted] del domicilio de [redacted] departamento de San Salvador, portador del Documento Único de Identidad número: [redacted] con Número de Identificación Tributaria: cero seiscientos [redacted] actuando en mi carácter de Administrador Único Propietario y por tanto Representante Legal de la Sociedad "AM TECHNOLOGY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE", que se abrevia "AM TECHNOLOGY, S.A. DE C.V.", del domicilio de [redacted], departamento de [redacted] con Número de Identificación Tributaria: [redacted] y que en lo sucesivo del presente instrumento me denominaré "la contratista". CONVENIMOS: En celebrar el presente contrato de "ADQUISICIÓN DE EQUIPO INFORMÁTICO PARA DIFERENTES UNIDADES DEL MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA AÑO 2021", conforme a las cláusulas que a continuación se especifican: **I. OBJETO DEL CONTRATO.** La contratista se compromete a brindar a satisfacción de la Institución Contratante el suministro de EQUIPO INFORMÁTICO PARA DIFERENTES UNIDADES DEL

CAROLINA MÁRMOL SEGURA NOTARIO REPÚBLICA DE EL SALVADOR

00002090

MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA AÑO 2021, de acuerdo al siguiente detalle:

No. ÍTEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO (US$)	PRECIO TOTAL (US$)
1	ACCESS POINTS	60	900.00	54,000.00
TOTAL CONTRATADO (IVA INCLUIDO)				US$ 54,000.00

Con las especificaciones técnicas siguientes:

Ítem No.1	ACCESS POINTS	Cantidad: 60
ESPECIFICACIONES TECNICAS PUNTO DE ACCESO FORTINET MODELO: FAP-231F-N MODELO FG-600E		
	Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico;	
	Soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;	
	Identificar automáticamente el controlador inalámbrico al que se conectará;	
	Permitir administrarse remotamente a través de links WAN;	
	Poseer capacidad dual-band con radios 2.4GHz y 5GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;	
	El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico;	
	Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	
	Permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;	
	Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;	
	En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;	
	Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora	
	Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs;	
	En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);	
	En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;	
	En conjunto con el controlador inalámbrico, debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	
	En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;	
	Admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	

	Implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;
	Se impartirá una inducción técnica de al menos 40 horas para la utilización de la plataforma, la capacitación debe ser impartida en las instalaciones del proveedor quien debe tener las instalaciones adecuadas y/o acreditadas para este tipo de capacitación técnica o arquitecturas tecnológicas. La inducción técnicas será dirigida a seis (6) técnicos puesto el MINEDUCYT
	Se realizara la configuración inicial e instalación de la plataforma debe ser realizada por el proveedor, por lo que se solicita que el equipo técnico local cuente con certificaciones relacionadas a redes inalámbricas y de diseño de redes inalámbricas. Certificaciones vigentes no diplomas cursos.
	1 carta demostrando la experiencia implementando este tipo de plataforma WLC y la línea o serie de Access points.
	Como parte de la solución requerida para dicho dimensionamiento, se deberá anexar un reporte que incluya toda la justificación técnica de cobertura y rendimiento de la solución inalámbrica, con el fin de garantizar diferentes aspectos técnicos (Área de coberturas, cantidad de usuarios en los diferentes salones) que permitan justificar los alcances de toda la solución, y así brindar un nivel de servicio para los usuarios de la red inalámbrica de la institución.
Consideraciones necesarias para adquisición	1- El fabricante de la solución debe de estar en el cuadrante leader de Gartner en la solución de Wireless y LAN en el último año
	2- Levantamiento inicial de información acerca de la infraestructura tecnológica actual con el fin de detectar aspectos de mejora, si existiesen.
	3- Instalar e implementar, configurar solución ofertada.
	4- La solución ofertada deberá integrarse de manera transparente a la infraestructura de TI del MINEDUCYT, incluyendo, pero no limitado a: Active directory, LDAP, DNS, DHCP, etc.
	5- La solución ofertada deberá incluir la configuración y puesta en producción de un servicio wifi para visitantes, captive portal nativo de la solución, para la generación de Tickets de navegación controlada, por el tiempo que la institución considere necesario.
	6- Se deberá poder configurar redes (SSIDs) para eventos específicos las cuales podrá apagarse tan pronto como se termine el evento.
	7- Se deberá poder programar horarios de funcionamiento de algunas o todas las redes (SSIDs) Wifi de la institución según la demanda del servicio.
	8- Roaming entre los dispositivos inalámbricos para garantizar conectividad estable para los usuarios en todos los puntos de cobertura.
	9- Proporcionar 2 técnicos certificados de la marca a ofertar.
	10- La empresa adjudicada tiene que dar los insumos necesarios para la instalación e implementación de la solución.
ESTUDIO DE COBERTURA, ANALISIS Y JUSTIFICACION TECNICA DE LA SOLUCION.	Se proveerá el plano de los diferentes sitios en donde se instalara la solución inalámbrica con los siguientes detalles:
	Se proveerá los diagramas de calor que muestren detalles de intensidad de señal, dicho calculo deberá ser basado en 3D, es decir, se deberá poder incrustar dentro del plano cualquier objeto con una densidad específica, que posea características de atenuación propias del material del objeto, con su la altura del objeto desde el suelo, ancho y profundidad. Mostrando así la atenuación y los diferentes niveles de la intensidad de la señal en el mismo.
	Los cálculos de la intensidad de señal en los planos, deberán ser basados con los siguientes límites: Intensidad de señal Efectiva o requerida: se considerará como intensidad de señal efectiva, los niveles óptimos aceptables para las aplicaciones específicas a utilizar en la institución, nivel aceptado: -45dbm. Intensidad de corte: se considerará como la intensidad de señal mínima aceptable para las aplicaciones específicas a utilizar en la institución, nivel aceptado mínimo: -75dbm. Intensidad baja: se considerará como intensidad baja a los niveles de señal por debajo de la señal de corte, se deberá especificar qué áreas están fuera de la cobertura solicitada, límite de intensidad baja: -80dbm. Límite inferior: se deberá mostrar el límite en el cual ya no existe ninguna cobertura, se deberá mostrar a -90dbm.
	Incluir en el reporte estadísticas de intensidad de señal, en la que se pueda determinar los porcentajes de áreas cubiertas en los siguientes intervalos: -45dbm o superior -48dbm a - 45dbm -51dbm a – 48dbm -54dbm a -51dbm -57dbm a -54dbm -60dbm a -57dbm

	-63dbm a -60dbm
	Se proveerá diagramas de calor, en los que se proveerá información de relación intensidad de la señal versus ruido (SNR), basado en el nivel de ruido medido por el adaptador WiFi usado en los cálculos o por la interferencia co-canal calculada.
	Los cálculos de (SNR) (Signal to Noise Ratio) en los planos, deberán ser basados con los siguientes límites: Nivel SNR aceptado: 10dbm.
	Incluir en el reporte estadísticas de SNR, en la que se pueda determinar los porcentajes de áreas con mayor ruido que señal en los siguientes intervalos: 40dbm o superior 35dbm a 40dbm 30dbm a 35dbm 25dbm a 30dbm 20dbm a 25dbm 15dbm a 20dbm 10dbm a 15dbm
	Se incluirá un gráfico con la visualización de la predicción de asociación de un cliente o dispositivo con cada Access Point, dicha visualización se deberá diferenciar con una paleta de colores para distinguir las áreas en donde cada AP tendrá una típica participación de cobertura, dicho calculo podrá proporcionar información para reconsiderar áreas en dondo podría mover APs para mejorar balanceo de carga.
	Se proporcionará diagramas de calor que muestren la cobertura de señal por canal, y por banda utilizada. Dicha cobertura deberá distinguirse con una paleta de colores que permita visualizar las áreas cubiertas por canal específico.
	Se proporcionara una estadística dondo se pueda determinar los porcentajes de áreas cubiertas por cada canal y por cada banda.
	Se proporcionara un diagrama de calor mostrando solapamiento de canales (Channel Overlap), dicha grafica deberá mostrar mediante una paleta de colores la adyacencia de canales entre uno o varios Access Point, la posición, la distribución de canales por cada AP, deberá sor un cálculo basado en un criterio técnico, por el algoritmo del software de estudio de cobertura o site survey, permitiendo mostrar áreas en las cuales no exista este solapamiento, se requiere un nivel do cálculo basado en 4 Access Point adyacentes.
	Se proporcionara una estadística donde se pueda determinar los porcentajes de áreas compartidas por cada canal.
	Se proporcionará un diagrama de calor mostrando algún problema detectado por los diferentes parámetros incluidos en los cálculos del diseño, en el cual se pueda apreciar deficiencias tales como: Deficiencias en base de solapamiento de canalos. Deficiencias por señal pobre. Deficiencias por APs fuera do cobertura. Cada una de estas deficiencias deberá ser mostrada mediante una palota de colores en la cual pueda tomarse una acción proactiva que mejore la cobertura, previo al análisis mostrado y si fuese requerido por la institución.
	Se deberá incluir una estadística grafica porcentual de cada problema detoctado (Network Issues)
	El harán los puntos de red para cada uno de los equipos con sus respectivas certificaciones por cada punto.
CONTROLADORA	1
App Control	Los dispositivos de protección de red deben tener la capacidad do reconocer las aplicaciones, indopendiontomonte del puerto y protocolo;
App Control	Detección de miles de aplicaciones en 18 categorías, 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;
App Control	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;
App Control	Identificar el uso de tácticas evasivas, os 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;
App Control	Para trafico 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;

App Control	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
App Control	Actualización de la base de firmas de la aplicación de forma automática;
App Control	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;
App Control	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
App Control	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;
App Control	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
App Control	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/regias para el mismo;
App Control	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
App Control	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
App Control	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
App Control	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);
App Control	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
App Control	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
App Control	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
User Identity	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;
User Identity	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;
User Identity	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;
User Identity	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;
User Identity	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;
User Identity	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);
User Identity	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;
User Identity	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
User Identity	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
User Identity	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;
QoS & Shaping	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;
QoS & Shaping	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
QoS & Shaping	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
QoS & Shaping	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
QoS & Shaping	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
QoS & Shaping	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
QoS & Shaping	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
QoS & Shaping	En QoS debe permitir la definición de tráfico con máximo ancho de banda;

QoS & Shaping	En QoS debe permitir la definición de colas de prioridad;
QoS & Shaping	Soportar marcación de paquetes DiffServ, incluso por aplicación;
QoS & Shaping	Soportar la modificación de los valores de DSCP para Diffserv;
QoS & Shaping	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
QoS & Shaping	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;
Wireless Controller	Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);
Wireless Controller	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;
Wireless Controller	Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;
Wireless Controller	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;
Wireless Controller	El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;
Wireless Controller	La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;
Wireless Controller	Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;
Wireless Controller	El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;
Wireless Controller	Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;
Wireless Controller	Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;
Wireless Controller	Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;
Wireless Controller	La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;
Wireless Controller	La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;
Wireless Controller	La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;
Wireless Controller	La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;
Wireless Controller	La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;
Wireless Controller	La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;
Wireless Controller	La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;
Wireless Controller	La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;

Wireless Controller	La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;
Wireless Controller	La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;
Wireless Controller	La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;
Wireless Controller	La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;
Wireless Controller	La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;
Wireless Controller	Permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;
Wireless Controller	La solución debe implementar el estándar IEEE 802.11 r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;
Wireless Controller	La solución debe implementar el estándar IEEE 802.11 k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;
Wireless Controller	La solución debe implementar el estándar IEEE 802.11 v para permitir que la red influya en las decisiones de roaming del cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;
Wireless Controller	La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;
Wireless Controller	La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;
Wireless Controller	La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;
Wireless Controller	La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado , Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;
Wireless Controller	Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;
Wireless Controller	La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4 y 5GHz y los estándares 802.11 a / b / g / n / ac;
Wireless Controller	La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;
Wireless Controller	La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;
Wireless Controller	La solución debe permitir la configuración del valor de Short Guard Interval para 802.11 n y 802.11 ac en 5GHz;
Wireless Controller	La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;
Wireless Controller	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;
Wireless Controller	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;
Wireless Controller	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

00002087

	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;
Wireless Controller	La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;
Wireless Controller	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;
Wireless Controller	La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;
Wireless Controller	La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados: - Ataques de flood contra el protocolo EAPOL (EAPOL Flooding); - Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast Deauthentication y Spoofed Deauthentication; -ASLEAP; - Null Probe Response/ Null SSID Probe Response; - Long Duration; - Ataques contra Wireless Bridges; -WeakWEP; - Invalid MAC OUI.
Wireless Controller	La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de deauthentication
Wireless Controller	La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;
Wireless Controller	La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos;
Wireless Controller	Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;
Wireless Controller	Debe implementar la autenticación administrativa a través del protocolo RADIUS;
Wireless Controller	En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
Wireless Controller	En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;
Wireless Controller	La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;
Wireless Controller	Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;
Wireless Controller	La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;
Wireless Controller	La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;
Wireless Controller	La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
Wireless Controller	La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;
Wireless Controller	La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;
Wireless Controller	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;
Wireless Controller	La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;
Wireless Controller	La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;
Wireless Controller	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;

Wireless Controller	La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;
Wireless Controller	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;
Wireless Controller	Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;
Wireless Controller	La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;
Wireless Controller	La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;
Wireless Controller	La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;
Wireless Controller	La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;
Wireless Controller	La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;
Wireless Controller	La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;
Wireless Controller	La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;
Wireless Controller	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;
Wireless Controller	La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;
Wireless Controller	La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);
Wireless Controller	La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;
Wireless Controller	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;
Wireless Controller	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;
Wireless Controller	La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;
Wireless Controller	La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;
Wireless Controller	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;
Wireless Controller	La solución debe tener herramientas de diagnóstico y depuración;
Wireless Controller	La solución debe soportar la comunicación con elementos externos a través de las API;
Wireless Controller	La solución deberá ser compatible y administrar los puntos de acceso de este proceso;
Generales	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;
Generales	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
Generales	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
Generales	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
Generales	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
Generales	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
Generales	Los dispositivos de protección de red deben soportar DHCP Relay;
Generales	Los dispositivos de protección de red deben soportar DHCP Server;
Generales	Los dispositivos de protección de red deben soportar Jumbo Frames;
Generales	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;

Generales	Debe ser compatible con NAT dinámica (varios-a-1);
Generales	Debe ser compatible con NAT dinámica (muchos-a-muchos);
Generales	Debe soportar NAT estática (1-a-1);
Generales	Debe admitir NAT estática (muchos-a-muchos);
Generales	Debe ser compatible con NAT estático bidireccional 1-a-1;
Generales	Debe ser compatible con la traducción de puertos (PAT);
Generales	Debe ser compatible con NAT Origen;
Generales	Debe ser compatible con NAT de destino;
Generales	Debe soportar NAT de origen y NAT de destino de forma simultánea;
Generales	Debe soportar NAT de origen y NAT de destino en la misma política
Generales	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
Generales	Debe ser compatible con NAT64 y NAT46;
Generales	Debe implementar el protocolo ECMP;
Generales	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;
Generales	Enviar logs a sistemas de gestión externos simultáneamente;
Generales	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
Generales	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
Generales	Implementar la optimización del tráfico entre dos dispositivos;
Generales	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
Generales	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
Generales	Soportar OSPF graceful restart;
Generales	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
Generales	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
Generales	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
Generales	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
Generales	Soportar la configuración de alta disponibilidad activo/ pasivo y activo/ activo: En modo transparente;
Generales	Soportar la configuración de alta disponibilidad activo/ pasivo y activo/ activo: En capa 3;
Generales	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
Generales	La configuración de alta disponibilidad debe sincronizar: Sesiones;
Generales	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
Generales	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
Generales	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
Generales	Debe soportar la creación de sistemas virtuales en el mismo equipo;
Generales	Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
Generales	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;
Generales	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;
Generales	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);
Generales	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;
Generales	La consola de administración debe soportar como mínimo, ingles, Español y Portugues.
Generales	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.

Generales	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
Generales	Debe soportar controles de zona de seguridad;
Generales	Debe contar con políticas de control por puerto y protocolo;
Generales	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;
Generales	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
Generales	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall
Rendimiento	El dispositivo deberá contar con 8 interfaces RJ45 Gigabit Ethernet
Rendimiento	El dispositivo deberá contar con 8 interfaces (slots) SFP Gigabit Ethernet
Rendimiento	El dispositivo deberá contar con 2 interfaces (slots) SFP+ (10 Gigabit Ethernet)
Rendimiento	El dispositivo deberá contar con un puerto USB
Rendimiento	El dispositivo deberá contar con un puerto de consola
Rendimiento	El dispositivo deberá soportar un mínimo de 512 access points
Rendimiento	El dispositivo deberá contar con un rendimiento de CAPWAP de 18Gbps (HTTP 64K)
Rendimiento	El dispositivo deberá contar con un rendimiento de CAPWAP de 18Gbps (HTTP 64K)
Garantía	3 Años en toda la solución implementada

II. PRECIO Y FORMA DE PAGO. El precio total por los bienes objeto del presente contrato, asciende a la suma de CINCUENTA Y CUATRO MIL DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA (US$ 54,000.00), IVA INCLUIDO, a dicho precio se le harán las retenciones de ley aplicables; asimismo, siendo el Ministerio de Educación, Ciencia y Tecnología Agente de Retención del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, designado por el Ministerio de Hacienda, según Resolución Número: 12301-NEX-2141-2007, de fecha 03 de Diciembre de 2007, en aplicación al Art. 162 del Código Tributario, retendrá el uno por ciento (1%) como anticipo al pago que causa este impuesto, en toda factura igual ó mayor a Cien Dólares de los Estados Unidos de América. El monto anteriormente mencionado, será pagado por la Institución contratante de la siguiente manera: PAGO TOTAL: Corresponderá al CIEN POR CIENTO (100%) del monto del contrato, el cual, se gestionará cuando se hayan recibido la totalidad de los bienes objeto de este contrato, a través del Administrador del presente contrato. Los documentos a presentar, para efectos de gestión de pago por parte de la contratista son: I) Factura de Consumidor Final a nombre del MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA, en la que se indique una descripción, la cantidad, el precio unitario y el monto total de los bienes; y II) Acta de Recepción debidamente firmada y sellada, por el Administrador del presente contrato, de haber recibido los bienes objeto del contrato. **III. PLAZO.** El plazo máximo de entrega para los bienes objeto de este contrato, será de NOVENTA DÍAS CALENDARIOS, contados a partir de la fecha indicada en la Orden de Pedido emitida por el Administrador de Contrato. **IV. FORMA DE ENTREGA Y RECEPCIÓN.** De conformidad al artículo cuarenta y cuatro literal j), de la Ley de Adquisiciones y Contrataciones de la Administración Pública (en adelante LACAP), la contratista garantiza que entregará los bienes objeto de este contrato en una sola entrega con las mismas condiciones y especificaciones ofertadas de acuerdo a lo establecido en las Bases de Licitación, todo a satisfacción del Ministerio de Educación, Ciencia y Tecnología. El lugar de entrega para los bienes objeto de esta contratación será en las instalaciones de la Bodega del Ministerio de Educación, Ciencia y Tecnología en Colonia Ouezaltepec, Santa Tecla, La Libertad. **V. OBLIGACIONES DE LA INSTITUCIÓN CONTRATANTE.** El pago de los bienes será financiado con Fondos del GOBIERNO DE EL SALVADOR, por un monto total de CINCUENTA Y CUATRO MIL DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA (US$

54,000.00), IVA INCLUIDO. **VI. SUPERVISIÓN Y CONTROL.** Según Acuerdo número QUINCE – UN MIL DOSCIENTOS CUARENTA Y TRES, emitido en esta misma fecha, por la Ministra de Educación, Ciencia y Tecnología, la administración de este contrato será ejercida por Elmer Alexander Melara, Analista Informático de la Gerencia de Tecnologías de Información y Comunicaciones Institucionales de la Dirección de Planificación del Ministerio de Educación, Ciencia y Tecnología; quien será la persona encargada de administrar la ejecución de este contrato y tendrá el derecho a inspeccionar a fin de verificar su conformidad con las especificaciones del contrato. Cuando los bienes inspeccionados no se sujeten a los términos contractuales, la institución contratante podrá rechazarlos previo informe del Administrador del Contrato, y la contratista deberá, sin cargo para la institución contratante, reemplazarlos o hacer todas las modificaciones necesarias para que ellas cumplan con las especificaciones del contrato. **VII. CESIÓN.** Queda expresamente prohibido a la contratista, traspasar o ceder a cualquier título los derechos y obligaciones que emanan del presente contrato. La Transgresión de esta disposición dará lugar a la caducidad del contrato. **VIII. GARANTÍA.** Para garantizar el cumplimiento de las obligaciones emanadas del presente contrato, la contratista deberá rendir a satisfacción del MINEDUCYT, dentro del plazo de cinco días hábiles posteriores a la notificación que el contrato está debidamente legalizado, la garantía siguiente: GARANTÍA DE CUMPLIMIENTO DE CONTRATO, a favor del Ministerio de Educación, Ciencia y Tecnología, por un monto de SEIS MIL CUATROCIENTOS OCHENTA DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA (US$ 6,480.00), equivalente al doce por ciento (12%) del valor del contrato. Dicha garantía tendrá una vigencia de cuatro meses, a partir de la fecha de suscripción del contrato. **IX. INCUMPLIMIENTO.** En caso de mora en el cumplimiento por parte de la contratista, de las obligaciones, emanadas del presente contrato, se aplicarán las multas establecidas en el artículo ochenta y cinco de la LACAP. La contratista expresamente se somete a las sanciones que emanan de la ley o del presente contrato las que serán impuestas por la Institución contratante, a cuya competencia se somete a efectos de la imposición. Además, será causa de caducidad del presente contrato según lo establecido en el artículo noventa y cuatro de la LACAP. **X. PLAZO DE RECLAMOS.** A partir de la suscripción del contrato, la Institución contratante tendrá un plazo de cuatro meses de acuerdo a la garantía de cumplimiento de contrato, para efectuar cualquier reclamo respecto de alguna inconformidad sobre los bienes contratados. **XI. MODIFICACIONES, PRÓRROGAS Y PROHIBICIONES.** La Institución Contratante podrá modificar el contrato en ejecución, de común acuerdo entre las partes, respecto del objeto, monto y plazo del mismo, siguiendo el procedimiento establecido en la LACAP. Para ello, la Institución Contratante autorizará la modificativa mediante resolución razonada; y la correspondiente modificativa que se genere será firmada por el Fiscal General de la República y por la contratista, debiendo estar conforme a las condiciones establecidas en el artículo ochenta y tres guion "A" de la LACAP y artículo veintitrés literal "k" del Reglamento de la Ley de Adquisiciones y Contrataciones de la Administración Pública (en adelante RELACAP). Si en cualquier momento durante la ejecución del contrato la contratista encontrase impedimentos para la entrega del suministro, notificará con prontitud y por escrito a la Institución Contratante, e indicará la naturaleza de la demora, sus causas y su posible duración, tan pronto como sea posible. Después de recibir la notificación la Institución Contratante evaluará la situación y podrá prorrogar el plazo de la entrega. En este caso, la prórroga del plazo se hará mediante modificación al contrato, la cual será autorizada por la Institución Contratante mediante resolución razonada; y la modificativa será firmada por el Fiscal General de la República y la contratista, de conformidad a lo establecido en los artículos

ochenta y seis y noventa y dos inciso segundo de la LACAP, así como con los artículos setenta y seis y ochenta y tres del RELACAP. Por otra parte, el contrato podrá prorrogarse una sola vez, por un período igual o menor al pactado inicialmente, para lo cual deberá seguirse lo establecido en el artículo ochenta y tres de la LACAP, así como con el artículo setenta y cinco del RELACAP; dicha prórroga será autorizada mediante resolución razonada por la Institución Contratante; y la prórroga del contrato será firmada por el Fiscal General de la República y la contratista. Respecto a las prohibiciones, se estará a lo dispuesto en el artículo ochenta y tres guion "B" LACAP. De común acuerdo, el presente contrato podrá ser modificado. En tal caso, la institución contratante emitirá la correspondiente resolución, la cual se relacionará en el instrumento modificatorio, y para que surta efecto legal, esta modificativa debe ser firmada por el Fiscal General de la República y la Contratista. **XII. DOCUMENTOS CONTRACTUALES.** Forman parte integral del presente contrato los siguientes documentos, si los hubiere: a) Bases de Licitación, b) Adendas, c) Aclaraciones, d) Enmiendas, e) Consultas, f) Documentos de petición de suministro, g) Interpretaciones e instrucciones sobre la forma de cumplir las prestaciones formuladas por la institución contratante, h) Garantías, i) La oferta, j) La resolución de adjudicación, k) La rectificación a la resolución de adjudicación, l) Resoluciones modificativas, y m) Otros documentos que emanaren del presente contrato. En caso de controversia entre estos documentos y el contrato, prevalecerá este último. **XIII. INTERPRETACIÓN DEL CONTRATO.** De conformidad al Artículo ochenta y cuatro incisos primero y segundo de la LACAP, la institución contratante se reserva la facultad de interpretar el presente contrato, de conformidad a la Constitución de la República, la LACAP, demás legislación aplicable y los Principios Generales del Derecho Administrativo y de la forma que más convenga al interés público que se pretende satisfacer de forma directa o indirecta con la prestación, objeto del presente instrumento, pudiendo en tal caso girar las instrucciones por escrito que al respecto considere convenientes. La contratista expresamente acepta tal disposición y se obliga a dar estricto cumplimiento a las instrucciones que al respecto dicte la institución contratante las cuales le serán comunicadas por medio del Administrador de este Contrato. En caso de haber dudas ó contradicciones en la interpretación de los conceptos expresados entre el presente contrato y las Bases de Licitación o documentos anexos, que forman parte de este contrato, prevalecerán los conceptos expresados en el contrato. **XIV MODIFICACIÓN UNILATERAL.** Queda convenido por ambas partes que cuando el interés público lo hiciera necesario, sea por necesidades nuevas, causas imprevistas u otras circunstancias, la institución contratante podrá modificar de forma unilateral el presente contrato, emitiendo al efecto la resolución correspondiente, la que formará parte integrante del presente contrató. **XV. CASO FORTUITO Y FUERZA MAYOR.** En situaciones de caso fortuito o fuerza mayor y de conformidad al artículo ochenta y seis de la LACAP, la contratista, previa justificación y entrega de la garantía cuando proceda, podrá solicitar una prórroga del plazo de cumplimiento de las obligaciones objeto del presente contrato. En todo caso, y aparte de la facultad de la institución contratante para otorgar tal prórroga, la misma se concederá por medio de resolución razonada que formará parte integrante del presente contrato. **XVI. SOLUCIONES DE CONFLICTOS.** Para resolver las diferencias o conflictos que surgieren durante la ejecución del presente contrato se estará a lo dispuesto en el Título VIII, Capítulo I, de la LACAP, y la Ley de Mediación, Conciliación y Arbitraje. **XVII. TERMINACIÓN BILATERAL.** Las partes contratantes podrán de conformidad al artículo noventa y cinco de la LACAP, dar por terminado bilateralmente la relación jurídica que emana del presente contrato, debiendo en tal caso emitirse la resolución correspondiente y otorgarse el instrumento de resciliación en un plazo no mayor de ocho días hábiles de notificada tal

00002084

resolución. **XVIII. JURISDICCIÓN Y LEGISLACIÓN APLICABLE.** Para los efectos jurisdiccionales de este contrato las partes se someten a la legislación vigente de la República de El Salvador cuya aplicación se realizará de conformidad a lo establecido en el Artículo cinco de la LACAP. Asimismo, señalan como domicilio especial el de esta ciudad a la competencia de cuyos tribunales se someten. **XIX. NOTIFICACIÓN.** 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 señalan como lugar para recibir notificaciones los siguientes: Para el MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGIA. Dirección: Centro de Gobierno, Plan Maestro, Ministerio de Educación, Ciencia y Tecnología, Gerencia de Adquisiciones y Contrataciones Institucional, Edificio A-1, segundo nivel, Teléfono: 2592-3031. Fax: 2592-3046. Para el Contratista: AM TECHNOLOGY, S.A. DE C.V [redacted]

XX. RESPONSABILIDAD SOCIAL PARA LA PREVENCIÓN Y ERRADICACIÓN DEL TRABAJO INFANTIL. Si durante la ejecución del contrato se comprobare por la Dirección General de Inspección de Trabajo del Ministerio de Trabajo y Previsión Social, incumplimiento por parte de la contratista a la normativa que prohíbe el trabajo infantil y de protección de la persona adolescente trabajadora, se deberá tramitar el procedimiento sancionatorio que dispone el artículo 160 de la LACAP para determinar el cometimiento o no durante la ejecución del contrato de la conducta tipificada como causal de inhabilitación en el artículo 158 romano V literal b) de la LACAP, relativa a la invocación de hechos falsos para obtener la adjudicación de la contratación. Se entenderá por comprobado el incumplimiento a la normativa por parte de la Dirección General de Inspección de Trabajo, si durante el trámite de re inspección se determina que hubo subsanación por haber cometido una infracción, o por el contrario si se remitiere a procedimiento sancionatorio, y en éste último caso deberá finalizar el procedimiento para conocer la resolución final. **XXI. VIGENCIA DEL CONTRATO.** El presente contrato entrará en vigencia a partir de la fecha de su firma, hasta el treinta y uno de mayo de dos mil veintidós. **XXII. IDIOMA.** El idioma oficial del contrato será el castellano. Así nos expresamos los comparecientes quienes, enterados y conscientes de los términos y efectos legales del presente contrato por convenir así a los intereses de nuestros representados, ratificamos su contenido. En fe de lo cual firmamos en la ciudad de San Salvador, el día diecinueve de noviembre de dos mil veintiuno.

[redacted]

RODOLFO ANTONIO DELGADO MONTES
FISCAL GENERAL DE LA REPÚBLICA
CONTRATANTE

[redacted]

ALEJANDRO JOSE MORA ZEPEDA
Administrador Único Propietario y Representante Legal de
AM TECHNOLOGY, S.A. DE C.V.
CONTRATISTA

En

NOTARIO

REPUBLICA DE EL SALVADOR

la ciudad de San Salvador, a las diez horas con cincuenta y dos minutos del día diecinueve de noviembre de dos mil veintiuno. Ante mí, ZILA CAROLINA MARMOL SEGURA, Notaria, de este domicilio, COMPARECE: El señor RODOLFO ANTONIO DELGADO MONTES, de [redacted] años de edad, [redacted] del domicilio de [redacted] departamento de [redacted] persona a quien por el presente acto conozco e identifico por medio del Documento Único de Identidad número: [redacted] actuando en nombre y representación del Estado y Gobierno de El Salvador, específicamente del Ministerio de Educación, Ciencia y Tecnología, con Número de Identificación Tributaria: [redacted] en carácter de Fiscal General de la República, personería que doy fe de ser legitima y suficiente por haber tenido a la vista el Decreto Legislativo Número Cinco, emitido por la Asamblea Legislativa el día dos de mayo de dos mil veintiuno, publicado en el Diario Oficial Número Ochenta y Dos, Tomo Número Cuatrocientos Treinta y Uno, de esa misma fecha; mediante el cual la Asamblea Legislativa eligió en el cargo de Fiscal General de la República, al Abogado Rodolfo Antonio Delgado Montes, para el período de ocho meses y tres días, que inició a partir del día dos de mayo del año dos mil veintiuno y concluye el cinco de enero del año dos mil veintidós, en sustitución del Abogado Raúl Ernesto Melara Morán, y quien actúa sobre la base de lo dispuesto en los artículos Ciento Noventa y Tres, Ordinal Quinto de la Constitución de la República; Dieciocho literal "i" de la Ley Orgánica de La Fiscalía General de la República; y Dieciocho, Inciso Cuarto de la Ley de Adquisiciones y Contrataciones de la Administración Pública, los cuales le conceden facultades para celebrar contratos como el presente; y que en el transcurso de este instrumento se denominará "la Institución Contratante o MINEDUCYT"; y el señor ALEJANDRO JOSÉ MORA ZEPEDA, de [redacted] años de edad, [redacted] del domicilio de [redacted] departamento de [redacted] persona a quien por el presente acto conozco e identifico por medio del Documento Único de Identidad número: [redacted]

00002083

D7

[redacted] con Número de Identificación Tributaria: [redacted] quien actúa en su carácter de Administrador Único Propietario y por tanto Representante Legal de la Sociedad "AM TECHNOLOGY, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE", que se abrevia "AM TECHNOLOGY, S.A. DE C.V.", del domicilio de [redacted], departamento de [redacted], con Número de Identificación Tributaria: [redacted]; de cuya Personería Jurídica Doy Fe de ser legitima y suficiente por haber tenido a la vista el siguiente documento: Fotocopia Certificada por Notario del Testimonio de Escritura Pública de Modificación al Pacto Social de la Sociedad, otorgada en la ciudad de San Salvador, a las catorce horas del día once de septiembre del año dos mil diecisiete, ante los oficios Notariales de NADY PATRICIA MARROQUIN REYES, e inscrita en el Registro de Comercio bajo el número OCHENTA del Libro Número TRES MIL OCHOCIENTOS CUATRO del Registro de Sociedades, el día doce de octubre de dos mil diecisiete; la cual contiene las nuevas cláusulas que regirán el pacto social de la sociedad, de las que en lo medular, se establece que la naturaleza de la sociedad es Anónima sujeta al régimen de Capital Variable, de nacionalidad Salvadoreña, girará con la denominación social de "AM TECHNOLOGY, SOCIEDAD ANONIMA DE CAPITAL VARIABLE", que se abrevia "AM TECHNOLOGY, S.A. DE C.V."; su domicilio será el de la ciudad de [redacted]; la Sociedad tendrá entre otras, la finalidad de brindar servicios de asesoría, consultoría, estudios y mantenimiento en materia informática; las Juntas Generales de Accionistas constituirán la suprema autoridad de la sociedad, pero la administración de la sociedad estará confiada a un Administrador Único Propietario y su respectivo suplente, quienes durarán en sus funciones cinco años, pudiendo ser reelectos; y corresponderá al Administrador Único Propietario la representación judicial y extrajudicial de la sociedad y el uso de la firma social. En dicha escritura se encuentra el nombramiento del señor ALEJANDRO JOSE MORA ZEPEDA, como Administrador Único Propietario, por un plazo

de cinco años; por lo que, el compareciente está ampliamente facultado para realizar actos como el presente, y que en el transcurso del presente instrumento se denominará "la Contratista"; Y ME DICEN: a) Que para efecto de darle valor de instrumento público me presentan el instrumento privado que antecede; y b) Que las firmas que anteceden son suyas y que como tales las reconocen por haber sido puestas de su puño y letra, al pie del instrumento que antecede, otorgado en esta ciudad, este mismo día; escrito en siete hojas de papel simple; así mismo reconocen y ratifican todos los términos y condiciones que en el mismo se otorgan, el cual se refiere al CONTRATO NÚMERO MINEDUCYT – TRESCIENTOS TREINTA Y SEIS/ DOS MIL VEINTIUNO – GOES, con RESOLUCIÓN DE ADJUDICACIÓN NÚMERO MINEDUCYT – VEINTISIETE/ DOS MIL VEINTIUNO, del proceso de LICITACIÓN ABIERTA DR - CAFTA LA / ADACA - UE NUMERO CIENTO VEINTIOCHO / DOS MIL VEINTIUNO – MINEDUCYT – GOES / GOES SIETE MIL DOSCIENTOS TREINTA Y NUEVE / FANTEL, referente a la "ADQUISICIÓN DE EQUIPO INFORMÁTICO PARA DIFERENTES UNIDADES DEL MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA AÑO DOS MIL VEINTIUNO", financiado con fondos del GOBIERNO DE EL SALVADOR; cuyas cláusulas más relevantes son las siguientes: Cláusula Primera. OBJETO DEL CONTRATO. La contratista se compromete a entregar los bienes detallados en la cláusula primera del contrato que antecede. Cláusula Segunda. PRECIO Y FORMA DE PAGO. El precio total por los bienes objeto del presente contrato, asciende a la suma máxima de CINCUENTA Y CUATRO MIL DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA, IVA INCLUIDO, a dicho precio se le harán las retenciones de ley aplicables; asimismo, siendo el Ministerio de Educación, Ciencia y Tecnología Agente de Retención del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios, designado por el Ministerio de Hacienda, según Resolución Número: DOCE MIL TRESCIENTOS UNO – NEX - DOS MIL CIENTO CUARENTA Y UNO – DOS MIL SIETE, de fecha tres de Diciembre de dos mil siete, en aplicación al Artículo Ciento Sesenta y Dos del Código Tributario, retendrá el uno por

00002082

ciento como anticipo al pago que causa este impuesto, en toda factura igual o mayor a Cien Dólares de los Estados Unidos de América. El monto anteriormente mencionado, será pagado por la Institución contratante de la siguiente manera: PAGO TOTAL: Corresponderá al CIEN POR CIENTO del monto del contrato, el cual, se gestionará cuando se hayan recibido la totalidad de los bienes objeto de este contrato, a través del Administrador del presente contrato. Los documentos a presentar, para efectos de gestión de pago por parte de la contratista son: Primero) Factura de Consumidor Final a nombre del MINISTERIO DE EDUCACIÓN, CIENCIA Y TECNOLOGÍA, en la que se indique una descripción, la cantidad, el precio unitario y el monto total de los bienes; y Segundo) Acta de Recepción debidamente firmada y sellada, por el Administrador del presente contrato, de haber recibido los bienes objeto del contrato. Cláusula Tercera. PLAZO. El plazo máximo de entrega para los bienes objeto de este contrato, será de NOVENTA DIAS CALENDARIO, contados a partir de la fecha indicada en la Orden de Pedido emitida por el MINEDUCYT. Cláusula Cuarta. FORMA DE ENTREGA Y RECEPCIÓN. De conformidad al artículo cuarenta y cuatro literal j), de la Ley de Adquisiciones y Contrataciones de la Administración Pública (en adelante LACAP), la contratista garantiza que entregará los bienes objeto de este contrato en una sola entrega con las mismas condiciones y especificaciones ofertadas de acuerdo a lo establecido en las Bases de Licitación, todo a satisfacción del Ministerio de Educación, Ciencia y Tecnología. El lugar de entrega para los bienes objeto de esta contratación será en las instalaciones de la Bodega del Ministerio de Educación, Ciencia y Tecnología en Colonia Quezaltepec, Santa Tecla, La Libertad. Cláusula Octava. GARANTÍA. Para garantizar el cumplimiento de las obligaciones emanadas del presente contrato, la contratista deberá rendir a satisfacción del MINEDUCYT, dentro del plazo de cinco días hábiles posteriores a la notificación que el contrato está debidamente legalizado, la garantía siguiente: GARANTÍA DE CUMPLIMIENTO DE CONTRATO, a favor del Ministerio de Educación, Ciencia y Tecnología, por un monto de SEIS MIL CUATROCIENTOS OCHENTA

DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA, equivalente al doce por ciento del valor del contrato. Dicha garantía tendrá una vigencia de cuatro meses, a partir de la fecha de suscripción del contrato. Cláusula Vigésima Primera. VIGENCIA DEL CONTRATO. El presente contrato entrará en vigencia a partir de la fecha de su firma, hasta el treinta y uno de mayo de dos mil veintidós. Así se expresaron los comparecientes a quienes expliqué los efectos legales de la presenta Acta Notarial que consta de cuatro hojas de papel simple, y leído que se las hube, íntegramente en un solo acto sin interrupción, ratifican su contenido y firmamos. DOY FE.-

[redacted]

[redacted]

[redacted]

00002081

Versión Pública