UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

CONVOCATORIA NACIONAL

La Universidad de Guadalajara, a través del Sistema de Educación Media Superior, en cumplimiento a las disposiciones establecidas en el artículo 88 fracción III de la Ley Orgánica de la Universidad de Guadalajara y de los artículos 16, 19, 20, 44, 45 y 47 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, de la Universidad de Guadalajara, mediante la Coordinación de Servicios Generales del Sistema de Educación Media Superior.

CONVOCA

A las personas físicas o morales nacionales debidamente constituidas en posibilidad de suministrar equipos descritas a continuación y que deseen participar en las licitaciones para la adjudicación de los contratos correspondientes:

LICITACIONES DE ADQUISICIONES:

LICITACIÓN	DESCRIPCIÓN DE LOS BIENES Y/O SERVICIOS	FECHA LIMITE DE INSCRIPCIÓN	JUNTA DE ACLARACIONES	PRESENTACIÓN Y APERTURA DE PROPUESTAS	ACTA DE LECTURA DE FALLO
LI-SEMS-009-2021	Adquisición de puntos de acceso inalámbricos y nodos de red, para el Sistema de Educación Media Superior de la Universidad de Guadalajara	28 de septiembre de 2021	06 de octubre de 2021 11:00 horas	13 de octubre de 2021 11:00 horas	29 de octubre de 2021 11:00 horas
LI-SEMS-010-2021	Adquisición de equipo de solución de seguridad UTM/NGFW, para el Sistema de Educación Media Superior de la Universidad de Guadalajara.	28 de septiembre de 2021	06 de octubre de 2021 13:00 horas	13 de octubre de 2021 13:00 horas	29 de octubre de 2021 13:00 horas

LOS INTERESADOS A PARTICIPAR EN LA PRESENTE LICITACIÓN DEBERÁN:
Solicitar su inscripción, requisito previo para poder adquirir las bases de la licitación a partir de la fecha de esta publicación, en días hábiles y hasta **28 de septiembre de 2021**, de las **10:00 a 14:00 horas**, ante la Coordinación de Servicios Generales del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicada en Liceo #496 4to. Piso, colonia Centro, en la ciudad de Guadalajara, Jalisco; asimismo, deberán obtener las bases de la licitación, previa aceptación de su registro, las cuales serán entregadas el día **29 de septiembre de 2021** de **10:00 a 14:00 horas.**
Cumplir con los requisitos establecidos en la presente convocatoria y realizar el pago no rembolsable, de $2,500.00 (Dos mil quinientos pesos 00/100 M. N.) I.V.A. incluido, mediante depósito bancario en la cuenta institucional que se indique en la orden de pago.

LA JUNTA DE ACLARACIONES, CON CARÁCTER DE OBLIGATORIA, SERÁ:
LI-SEMS-009-2021 06 de octubre de 2021 a las 11:00 horas.
LI-SEMS-010-2021 06 de octubre de 2021 a las 13:00 horas.
En la Sala de Juntas (ala derecha) anexa al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco.

DEL ACTO DE ENTREGA Y APERTURA DE PROPUESTAS:
LI-SEMS-009-2021 13 de octubre de 2021 a las 11:00 horas.
LI-SEMS-010-2021 13 de octubre de 2021 a las 13:00 horas.
En la Sala de Juntas (Ala derecha) anexa al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco.
Dicho acto se realizará en sesión pública al que podrán asistir los participantes de esta licitación. La presentación de las propuestas deberá estar estructurada, conforme se establece en las bases de la licitación.
Fuente de los recursos corresponden a los recursos del Tus prioridades - Internet en escuelas F-1.3.13.3.

REQUISITOS QUE DEBEN CUMPLIR LOS INTERESADOS:
1. Solicitud por escrito dirigida al Ing. Fernando Calvillo Vargas, en papel membretado de la empresa (original y copia fotostática), firmada por el Representante Legal y/o persona física participante), donde expresen su interés en participar en la licitación, indicando el número y la descripción de ésta.
2. Acta constitutiva y sus modificaciones, que incluya la constancia ante el Registro Público de la Propiedad y de Comercio o en el caso de persona física, acta de nacimiento (copia fotostática simple).

aymundo Riva Palacio
apalacio@ejecentral.com.mx
tter: @rivapa

STRICTAMENTE ERSONAL

El ataque

sión contra los científicos solicitada el 24 de agosto pasado al juez de Distrito en El Altiplano, Gregorio Salazar Hernández, que revela sevicia y despropósito.

En esa reveladora solicitud señaló que los investigadores y académicos -muchos de ellos reconocidos internacionalmente-, tenían una conducta criminal, que de acuerdo con sus investigaciones, por las "enormes cantidades de dinero" y "capacidad económica obtenida de forma ilícita, podrían realizar actos de corrupción en algún centro con medidas de seguridad bajas o media

de peculado y uso ilícito de atribuciones y facultades, escaló a manejo de operaciones con recursos de origen de procedencia ilícita y delincuencia organizada, crímenes federales donde se ingresa a la cárcel sin posibilidad de defensa en libertad. Las penas que pidió en contra de los principales científicos imputados fueron de hasta 40 años de prisión.

Gertz Manero actuó de forma expedita. Nueve días antes de solicitar la orden de aprehensión, el 15 de agosto, recibió documentación y constancias de la Secretaría de Hacienda para

con lo cual, al presentarle como "suplente", dejó en Ramírez de la O la carga de la denuncia, deslindándose, para efectos prácticos, de ella. La Secretaría de Hacienda, sin embargo, actuó en consecuencia con la demanda del Conacyt y una moción, sin saberse hasta este momento de dónde, para presentar la denuncia ante la Fiscalía General, y darle así los elementos para fincar los delitos de delincuencia organizada.

Las constancias que entregó Hacienda no explican en qué se sustentan las operaciones con recursos de procedencia ilícita, si la de- ficar o tomar distancia de las acusaciones por delincuencia organizada, respondió que "el que nada debe, nada teme".

El juez Salazar Hernández rechazó esta semana la segunda solicitud de orden de aprehensión contra los científicos, y antes de que terminara el día, la Fiscalía General, volvió a acometer contra ese grupo con una tercera petición para que los detengan. Se han eliminado, cuando menos por ahora, los delitos relacionados con delincuencia organizada, pero la embestida va para adelante y no va a terminar. Gertz Manero, con el apoyo presidencial, irá más allá de los límites, y hasta donde le permiten llegar.

Carlos Loret de Mola A.
carlosloret@yahoo.com.mx

HISTORIAS DE REPORTERO

El medio abrazo de sonrisas forzadas AMLO-

Bases de la Licitación Pública LI-SEMS-009-2021

ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA

SEPTIEMBRE 2021

ÍNDICE

SECCIÓN I
INSTRUCCIONES A LOS LICITANTES

A. Introducción

1. Fuente de los recursos

1.1 Los recursos corresponden a: Proyecto 259928 TUS PRIORIDADES - INTERNET EN ESCUELAS, EQUIPAM. T (F-1.3.13.3) (AÑO: 2021).

1.2 La presente licitación quedará sujeta a la disponibilidad presupuestal, por lo que sus efectos estarán condicionados a la existencia de los recursos financieros correspondientes, sin que la no realización de la presente origine responsabilidad para la contratante.

2. Licitantes elegibles

2.1 Esta convocatoria se hace a todas las personas físicas o morales nacionales, debidamente constituidas, con actividad empresarial, con domicilio en territorio nacional, que estén en posibilidad de suministrar e instalar quipos de puntos de acceso y nodos de red.

3. Costo de la licitación

3.1 El licitante sufragará todos los costos relacionados con la preparación y presentación de su propuesta y la Universidad de Guadalajara no será responsable, en ningún caso por dichos costos, cualquiera que sea la forma en que se realice la licitación o su resultado.

4. Restricciones

4.1 Las personas que se encuentren en alguno de los supuestos establecidos en el artículo 29 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, no podrán participar en la licitación.

B. Documentos de la Licitación

5. Información contenida en los documentos de la licitación

5.1 Las condiciones contractuales, además de la convocatoria, los documentos de la licitación incluyen:

I. Instrucciones a los licitantes,
II. Condiciones generales,
III. Catálogo de Conceptos,

IV. Carta de seriedad de la propuesta,
V. Carta compromiso.

5.2 El licitante deberá examinar todas las instrucciones, condiciones y especificaciones que figuren en los documentos de la licitación. Si el licitante "**no**" incluye toda la información requerida en la convocatoria y las bases de la licitación presenta una propuesta que no se ajusta sustancialmente y en todos sus aspectos a esos documentos, el resultado será el "**rechazo de su oferta"**.

6. Aclaración de las Bases de la Licitación.

6.1 Cualquier licitante inscrito puede solicitar aclaraciones sobre las bases de la licitación, para lo cual se llevará a cabo una **junta de aclaraciones, con carácter de obligatoria,** misma que se celebrará el día **6 de octubre de 2021, a las 11:00 horas**, en la Sala de Juntas anexa (ala derecha) al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco.

6.2 Para llevar a cabo esta reunión, los participantes deberán enviar sus preguntas por correo electrónico, en archivo de Word, a más tardar a las **16:00 horas del día 30 de septiembre de 2021**, a las **2 (dos)** siguientes direcciones:

Rosaura.rodriguez@sems.udg.mx

fcalvillo@sems.udg.mx

6.3 Cualquier modificación a las bases de la licitación, derivada del resultado de la junta de aclaraciones, será considerada como parte integrante de las propias bases de la licitación.

6.4 Al participante que no asista a la junta de aclaraciones en la **fecha y hora exacta estipulada en las bases de la licitación**, por sí o su representante, no obstante haber adquirido las bases de la licitación, le será desechada su propuesta.

7. Modificación de los documentos de la Licitación

7.1 El Sistema de Educación Media Superior podrá, por cualquier causa y en cualquier momento, antes de que venza el plazo para la presentación de propuestas, modificar las bases de la licitación mediante enmienda, ya sea por iniciativa propia o en atención a una aclaración solicitada por un licitante interesado.

7.2 Las enmiendas serán notificadas por escrito a los licitantes registrados, pudiendo entregarse el aviso mediante correo electrónico y serán obligatorias para ellos.

7.3 El Sistema de Educación Media Superior podrá, a su discreción, prorrogar el plazo para la presentación de ofertas a fin de dar a los posibles licitantes tiempo razonable para tomar en cuenta en la preparación de sus ofertas por las enmiendas hechas a las bases de la licitación. De

la misma forma se podrá prorrogar fecha de la lectura de fallo, dentro del plazo de la vigencia de las propuestas, la cual les será notificada por correo electrónico a todos los licitantes participantes.

C. Preparación de las Propuestas

8. Idioma

8.1 La propuesta que prepare el licitante y toda la correspondencia y documentos relativos a ella que intercambien el licitante y el Sistema de Educación Media Superior, deberá redactarse en español; en todo caso, cualquier material impreso que proporcione el ofertante en otro idioma, deberá ser acompañado de una traducción al español de las partes pertinentes de dicho material impreso, la cual prevalecerá a los efectos de interpretación de la propuesta.

9. Descripción de los bienes a adquirir

9.1 El licitante elaborará su propuesta en papel membretado de la empresa, en la cual describirá los bienes a suministrar, de acuerdo con el catálogo de conceptos de la **Sección III** de las presentes bases.

9.2 Los bienes a adquirir se adjudicarán por bloque, los licitantes deberán cotizar todas las partidas, **ya que la evaluación y la adjudicación de las propuestas se realizará por bloque.**

10. Requisitos para el proveedor

10.1 Los licitantes deberán ser compañías legalmente establecidas en territorio nacional, que se dediquen preponderantemente al suministro e instalación quipos de puntos de acceso y nodos de red.

10.2 Adicionalmente los licitantes presentarán documentación que describa las características, capacidad y cobertura de la infraestructura que le permite ofertar los bienes objeto de la presente licitación.

10.3 En caso de no apegarse a cualquiera de los requisitos solicitados en la convocatoria, las presentes bases y el acta de la junta de aclaraciones, **será motivo de descalificación de la propuesta.**

10.4 Cabe mencionar que en el contrato de compra que se suscriba entre las partes se incorporarán a los requisitos y demás condiciones planteadas en este documento.

10.5 El número de artículos a adquirir podrá variar en razón del monto de las propuestas que se presenten y de la disponibilidad presupuestal con que se cuenta.

11. Precios y vigencia

11.1 El licitante indicará los precios unitarios y totales de su propuesta de acuerdo al catálogo de conceptos de la presente licitación.

11.2 Precio fijo. Los precios cotizados por el ofertante serán fijos y no estarán sujetos a variación por ningún motivo. No se considerarán las ofertas presentadas con cotizaciones de precios variables por no ajustarse a los documentos de la licitación y en consecuencia, serán rechazadas.

11.3 La facturación de las partidas adjudicadas serán con cargo al Proyecto 259928

11.4 Las cantidades solicitadas **podrán disminuir o aumentar** de acuerdo al recurso disponible con el que cuenta la convocante para cada una de las partidas.

12. Moneda en la que se expresará la propuesta

12.1 El licitante deberá cotizar en moneda nacional.

13. Documentos que establezcan la elegibilidad y calificación del licitante.

13.1 El licitante presentará todos los documentos solicitados en convocatoria y en las presentes bases como acreditación que es elegible y calificable para participar en la licitación.

14. Garantías

14.1 La circunstancia de que el licitante adjudicado no cumpla con la suscripción del contrato o lo dispuesto en las cláusulas del mismo, constituirá causa suficiente para la anulación de la adjudicación, en cuyo caso el Sistema de Educación Media Superior podrá adjudicar el contrato al licitante cuya oferta fue la siguiente mejor evaluada, o convocar a una nueva Licitación.

14.2 El licitante deberá garantizar la seriedad de su propuesta, mediante carta original en papel membretado de la empresa, firmada por el representante legal, conforme al modelo que se adjunta en la Sección IV de estas bases, la cual deberá apegarse estrictamente al contenido de la misma.

14.3 El licitante adjudicado deberá contratar a favor de la Universidad de Guadalajara una fianza, correspondiente al 10% del monto total adjudicado en el contrato respectivo, para asegurar su debido cumplimiento, mismo que se establece en la sección V de las bases de la licitación.

14.4 El licitante deberá especificar claramente el tiempo de garantía en su propuesta económica de todos los bienes ofertados, misma que se deberá ofertar por el licitante participante.

14.5 En caso de que el concursante adjudicado requiera **anticipo el cual será por un máximo del (30%)**, **deberá garantizar previo a su entrega, el 100% del importe total del anticipo otorgado, incluido el impuesto al valor agregado (IVA),** mediante constitución de fianza en original por una institución legalmente autorizada, a favor de la Universidad de Guadalajara, mismo que se establece en la sección V de las bases de la licitación.

14.6 Las fianzas que presente el licitante adjudicado deberán contener el número y nombre de la licitación, tal como se especifica en las presentes bases.

15. Período de validez de la propuesta

15.1 El participante deberá de especificar la vigencia o el periodo de validez de su propuesta. Se adjunta modelo de carta en la **Sección V** de estas bases, la cual se deberá apegar estrictamente al contenido de la misma y presentar original en papel membretado de la empresa, firmada por el representante legal.

16. Formato y firma de la propuesta

16.1 El paquete original de la propuesta deberá estar firmado con tinta indeleble, por el representante legal, en todas las hojas que lo integran, así como los documentos anexos al mismo y organizado en un recopilador, marcando cada sección con separadores de la siguiente manera:

A) Propuesta técnica:

A.1 Especificaciones técnicas, folletos, manuales, características de cada una de las partidas, capacidad y cobertura de la infraestructura que le permite al licitante suministrar los bienes o prestar los servicios requeridos.

A.2 Bases y anexos de la licitación completos, firmados en todas sus hojas por el representante legal de la empresa en señal de aceptación de las mismas, incluyendo el acta de la junta de aclaraciones.

B) Propuesta económica:

B.1 Propuesta económica firmada en todas sus hojas, con base en la descripción de los equipos a adquirir del punto 9.1.

B.2 Carta de seriedad de la propuesta.

B.3 Carta compromiso.

16.2 El licitante presentará un ejemplar original de la propuesta, la cual no deberá contener textos entre líneas, borrones, tachaduras ni enmendaduras.

D. Presentación de Propuestas

17. Sellado y marca de propuesta

17.1 La oferta será colocada dentro de un sobre que el licitante deberá cerrar y marcar respectivamente.

17.2 El sobre:

a) Estará rotulado con la siguiente dirección:

Sistema de Educación Media Superior de la Universidad de Guadalajara

Domicilio: Liceo 496 Esq. Juan Álvarez

Atención: Mtro. Jesús Alberto Jiménez Herrera

Secretario Ejecutivo del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior

b) **Indicará:** Propuesta para la Licitación Pública **LI-SEMS-009-2021** denominada ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA., **fecha de la convocatoria y la frase "NO ABRIR ANTES DE LAS 11:00 HORAS DEL 13 DE OCTUBRE DE 2021".**

c) Si el sobre no fuese sellado y marcado siguiendo las instrucciones establecidas en estas bases, el Sistema de Educación Media Superior, no asumirá responsabilidad alguna en caso de que la oferta sea traspapelada o abierta prematuramente.

18. Plazo para la presentación de ofertas.

18.1 **Las ofertas deberán ser presentadas en** la Sala de Juntas anexa **(ala derecha)** al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) **piso ala derecha** del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco; antes de las **11:00 HORAS DEL 13 DE OCTUBRE DE 2021".**

18.2 El Sistema de Educación Media Superior podrá, a su discreción, prorrogar el plazo para la presentación de propuestas, mediante la enmienda de los documentos de la licitación, en cuyo caso todos los derechos y obligaciones de la Universidad de Guadalajara y de los licitantes anteriormente sujetos a plazo original quedarán en adelante sujetos a los nuevos plazos que al efecto se establezcan.

19. Propuestas tardías

19.1 Toda propuesta que se presente después del plazo y hora exacta fijada para su recepción no será considerada y se devolverá sin abrir al licitante.

20. Modificación, sustitución y retiro de propuestas

20.1 Una vez presentadas las propuestas, ninguna de ellas, podrá ser modificada, sustituida, retirada o negociada.

20.2 Todos los documentos presentados dentro del sobre serán conservados por el Sistema de Educación Media Superior como constancia de su participación en la licitación.

E. Apertura y evaluación de propuestas

21. Apertura de propuestas

21.1 El Sistema de Educación Media Superior, abrirá las propuestas en sesión pública exactamente a las **11:00 HORAS DEL 13 DE OCTUBRE DE 2021.**, en la Sala de Juntas anexa **(ala derecha)** al Auditorio del Sistema de Educación Media Superior de la Universidad de Guadalajara situada en el 1er, (primer) piso del edificio "Valentín Gómez Farías" del Sistema de Educación Media Superior de la Universidad de Guadalajara, ubicado en la calle Liceo No. 496, Colonia Centro, Guadalajara, Jalisco.

21.2 El Sistema de Educación Media Superior, elaborará el acta de presentación y apertura de las propuestas, en la que se hará constar las ofertas recibidas, la falta de cualquier documento de la licitación, así como las que hubieren sido rechazadas y las causas que lo motivaron, la cual deberá ser firmada por los asistentes, entregándoles copia de la misma. La falta de firma de algún licitante no invalidará su contenido y efectos, poniéndose a partir de esa fecha a disposición de los que no hayan asistido, para efecto de su notificación.

22. Aclaración de propuestas

22.1 A fin de facilitar la revisión, evaluación y comparación de propuestas, el Sistema de Educación Media Superior podrá, a su discreción, solicitar a cualquier licitante las aclaraciones de su oferta.

23. Revisión, evaluación y comparación de las propuestas

23.1 El Sistema de Educación Media Superior examinará las propuestas para determinar si están completas, si contienen errores de cálculo, si los documentos han sido debidamente firmados y si, en general, las propuestas cumplen con los requisitos establecidos en las presentes bases y en la convocatoria de la licitación.

23.2 Los errores aritméticos serán ratificados de la siguiente manera: si existiera una discrepancia entre un precio unitario y el precio total que resulte de multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido. Si existiera una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras. Si el licitante no aceptara la corrección, su propuesta será rechazada.

23.3 La comparación de las propuestas, se hará tomando en cuenta el cumplimiento de la convocatoria, las bases, el acta de la junta de aclaraciones, los antecedentes del suministro de bienes o prestación de servicios anteriormente prestados, los tiempos de entrega, así como los precios propuestos por cada licitante, los cuales incluirán todos los costos, comisiones y los derechos e impuestos aplicables.

24. Comunicaciones con la Universidad de Guadalajara

24.1 Ningún licitante se comunicará con el Sistema de Educación Media Superior sobre ningún aspecto de su propuesta a partir del momento en el que se le entreguen las bases y hasta el momento de la adjudicación.

24.2 Cualquier intento, por parte de un licitante, de ejercer influencia sobre las decisiones del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior, en la evaluación y comparación de ofertas, podrá dar lugar al rechazo de su propuesta. Los casos en que se considere que ha existido influencia estarán determinados por el criterio del Sistema de Educación Media Superior.

F. Adjudicación del Contrato

25. Criterios para la adjudicación.

25.1 El Sistema de Educación Media Superior, adjudicará la adquisición al licitante cuya oferta se ajuste sustancialmente a los documentos de la licitación y haya sido evaluada como la mejor, a condición que, además se haya determinado que esté calificado para cumplir satisfactoriamente con la adjudicación.

26. Derecho del Sistema de Educación Media Superior de aceptar cualquier propuesta y rechazar cualquiera (todas las) propuesta (s).

26.1 El Sistema de Educación Media Superior, se reserva el derecho de aceptar o rechazar cualquier propuesta, así como el de declarar desierta la licitación y rechazar todas las propuestas en cualquier momento, con anterioridad a la adjudicación, sin que por ello incurra en responsabilidad alguna respecto al licitante o los licitantes afectados por esta decisión y/o tenga la obligación de comunicar al licitante o los licitantes afectados los motivos de la acción del Sistema de Educación Media Superior.

26.2 Los acuerdos, disposiciones y decisiones tomadas por los miembros del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior con respecto al resolutivo de la licitación, serán inapelables.

26.3 El Comité de Compras y Adquisiciones del Sistema de Educación Media Superior tendrá la facultad de decidir sobre cualquier controversia que pudiera presentarse durante el desarrollo de la licitación y de aplicar la normatividad de la Universidad de Guadalajara.

27. Notificación de la adjudicación

27.1 Antes de la expiración del período de validez de la oferta el Sistema de Educación Media Superior, notificará a los licitantes, a través del acta de lectura de fallo, el fallo emitido por el Comité de Compras y Adquisiciones del Sistema de Educación Media Superior.

27.2 El contrato se entenderá perfeccionado hasta el momento en que sea suscrito el mismo por los representantes legales de las partes.

27.3 A partir de la misma fecha del acta de lectura de fallo, la misma estará disponible en el Sistema de Educación Media Superior, para los licitantes que no hubieran asistido al acto de la lectura del fallo.

28. Firma del contrato

28.1 Desde el momento en que reciba el formulario de contrato, el licitante adjudicado tendrá **48 horas** después de su notificación para pasar a firmarlo al Sistema de Educación Media Superior.

G. Motivos por las que puede ser desechada la propuesta

29. Causas por las que puede ser desechada la propuesta

Se considerará como suficiente para desechar una propuesta, cualquiera de las siguientes causas:

A) El incumplimiento de alguno de los requisitos establecidos en las presentes Bases de la licitación y sus anexos.

B) Que se encuentre en cualquiera de los supuestos del Artículo 29 del Reglamento de Adquisiciones, Arrendamientos, y Contratación de Servicios de la Universidad de Guadalajara.

C) Que el licitante no presente su propuesta con tinta indeleble.

D) La falta de alguno de los requisitos o esté diferente a lo solicitado o incumpla lo acordado en el acta de la junta aclaratoria, en su caso.

E) La falta de la firma autógrafa con tinta indeleble del Representante Legal en alguna de las hojas de la propuesta.

F) Si presenta alguno de los documentos solicitados elaborados a lápiz o si lo presenta con tachaduras o enmendaduras.

G) Cuando no satisfagan cualquiera de los requisitos determinados en estas bases y sus anexos, y que no hayan sido detectados en el acto de presentación y apertura de propuestas.

H) Cuando los precios de los bienes ofertados por el licitante, se encuentren fuera de los precios de mercado o sean elevados de acuerdo al precio de referencia con los que cuente la convocante.

I) Si el licitante no especifica claramente el tiempo de garantía en su propuesta económica de todos los bienes ofertados, misma que se deberá ofertar por el licitante participante.

J) Si el licitante no especifica claramente dentro de la propuesta económica las condiciones de pago.

K) Si el licitante solicita en su propuesta anticipo superior al máximo establecido en las presentes bases.

L) Si el licitante no especifica la marca y modelo del bien (es) cotizado (s) en su propuesta económica

M) Si el licitante establece su propuesta económica con un costo variable o negociable de los bienes ofertados.

N) Si el licitante no especifica claramente dentro de la propuesta económica el tiempo de entrega de los bienes ofertados.

O) Si el licitante no especifica claramente dentro de la propuesta la **vigencia de la cotización mínima requerida por la convocante** en la propuesta ofertada.

P) Si el licitante establece en su propuesta alguna de las condiciones generales de dos maneras diferentes.

Q) Si el licitante no se presenta al acto de junta aclaratoria en la fecha y hora exacta establecidas en las bases de la licitación.

R) Si el licitante no presenta su propuesta en el acto de presentación y apertura de propuestas en la fecha y hora exacta establecidas en la bases de la licitación.

S) Si el licitante no se apega estrictamente al contenido de la carta de seriedad de la propuesta, establecida en la **sección IV**, de las bases de la licitación.

T) Si el licitante no se apega estrictamente al contenido de la carta compromiso, establecida en la **sección V**, de las bases de la licitación.

U) Si el licitante establece en su propuesta alguna sanción o penalización en contra de la convocante por cualquier motivo.

Sección II.
CONDICIONES GENERALES

1. Entrega y documentos

1.1 El Licitante deberá de especificar claramente en su propuesta el tiempo de entrega.

1.2 El licitante **suministrará los bienes y servicios** de acuerdo a lo dispuesto por el Sistema de Educación Media Superior, en los siguientes lugares que a continuación se indican:

DEPENDENCIA	PARTIDA 1	PARTIDA 2	PARTIDA 3
	CANTIDAD	CANTIDAD/MTRS	CANTIDAD
ESC PREP REG SAN JOSE DEL VALLE Ubicación: Av. Concepción S/N, San José del Valle, Tlajomulco de Zúñiga, Jalisco **Teléfono(s):** 33 1099 0008 y 33 1099 0394	**18**	**19**	**1**
ESCUELA PREPARATORIA REGIONAL DE TEPATITLÁN NUEVA SEDE Ubicación: Av. González Gallo No. 205, Tepatitlán de Morelos, Jalisco, C.P. 47600 Teléfono(s): 378 782 0965, fax 378 781 0282	**16**	**19**	**3**
ESC PREP REG DE TOLUQUILLA Ubicación: Camino al Canal No. 17, Delegación Toluquilla, San Pedro Tlaquepaque, Jalisco, C.P. 45610 **Teléfono(s):** 33 3601 4208 y 33 3601 4209	**15**	**16**	**1**
ESC PREP METROP NO. 20 (EL FORTIN) Ubicación: Av. Paseos del Bosque S/N, Col. El Fortín, Zapopan, Jalisco C.P. 45066 **Teléfono(s):** 33 1654 2700	**17**	**19**	**2**
ESC PREP METROP NO. 17 Ubicación: Av. Emiliano Zapata No. 2568 F-2, Col. Las Pintas, El Salto, Jalisco. **Teléfono(s):** 33 3695 5723	**17**	**18**	**1**
ESC PREP REG CIUDAD GUZMAN Ubicación: Av. Juan José Arreola No. 850, Col. Las Américas, Ciudad Guzmán, Jalisco, C.P. 49000 **Teléfono(s):** 341 410 6262, 341 410 6303	**15**	**17**	**2**
MÓDULO IXTLAHUACAN DE LOS MEMBRILLOS Ubicación: Circuito Real del Lago Sur No. 475, Fraccionamiento Real del Lago, (Antiguo Camino a la Capilla-Atequiza) Ixtlahuacán de los Membrillos, Jalisco, C. P. 45877 **Teléfono(s):** 333 801 3652	**7**	**7**	**N/A**
ESC PREP REG DE JALOSTOTITLAN Ubicación: Ramón Corona No. 174, Jalostotitlán, Jalisco C.P.	**6**	**7**	**1**

47120 **Teléfono (s):** 431 746 1382			
ESC PREP TONALA NORTE Ubicación: Av. Juan Gil Preciado esq. Antonio Caso, Col. Basilio Vadillo, Tonalá, Jalisco. C.P. 45409. **Teléfono(s):** 33 1187 0718 y 33 3602 1044	**19**	**21**	**2**
ESC PREP METROP NO. 19 (VISTAS DE TESISTAN) Ubicación: Paseo del Almendro S/N esq. Lucio Blanco, Fracc. Vistas de Tesistán, Zapopan, Jalisco. C.P. 45200 **Teléfono(s):** 33 1561 9097	**19**	**20**	**1**
ESCUELA PREPARATORIA REGIONAL DE PUERTO VALLARTA (EL PITILLAL) Ubicación: 21 de Marzo No. 500, Col. Loma Bonita, Puerto Vallarta, Jalisco, C.P. 48290 **Teléfono(s):** 322 299 2050 fax: 322 299 2040	**13**	**14**	**1**
ESC PREP METROP NO. 13 Ubicación: Isla Pianosa No. 4575, Col. El Sauz, Guadalajara, Jalisco. C.P. 45080 **Teléfono(s):** 33 3663 7087, 33 3663 7215	**20**	**21**	**1**
ESC PREP METROP NO. 02 Ubicación: Emilio Rabaza y Álvarez del Castillo No. 760, Guadalajara, Jalisco. C.P. 44370 **Teléfono(s):** 33 3649 2185, 33 3655 7020, 33 3665 6328, fax: 33 3649 2185	**21**	**25**	**4**
TOTAL	**203**	**223**	**20**

Nota:

Se anexan **URL** de la página oficial del Sistema de Educación Media Superior que contiene las direcciones y teléfonos de las dependencias antes mencionadas:

Escuelas Preparatorias Metropolitanas

http://www.sems.udg.mx/escuelas-metropolitanas

Escuelas Preparatorias Regionales

http://www.sems.udg.mx/preparatorias-regionales

1.3 El licitante que requiera parte o la totalidad de la información de carácter comercial presentada en virtud de este procedimiento se clasifique con carácter de confidencial, deberá de presentar la carta correspondiente en la que se especifique tal situación, de conformidad con la Ley de Información Pública del Estado de Jalisco y sus Municipios.

2. Pago

2.1 El pago al proveedor se realizará con un máximo de 30% anticipo y pagos contra avance de los equipos entregados e instalados en su totalidad y este será en moneda nacional, contra la entrega de las facturas originales que cumplan todos los requisitos fiscales en vigor, de acuerdo a los tiempos establecidos en su propuesta.

2.2 El participante deberá de especificar en su propuesta las condiciones de pago

2.3 En caso de que el concursante adjudicado requiera un máximo de **anticipo de (30%)**, **deberá garantizar previo a su entrega, el 100% del importe total del anticipo otorgado, incluido el impuesto al valor agregado (IVA),** mediante constitución de fianza en original por una institución legalmente autorizada, a favor de la Universidad de Guadalajara.

3. Precios y vigencia

3.1 Los precios facturados por el licitante, no serán mayores a los que haya cotizado en su propuesta.

3.2 El Sistema de Educación Media Superior requiere una **vigencia de cotización**

4. Modificaciones al contrato

4.1 Toda variación o modificación de los términos del contrato deberá efectuarse mediante adendum o convenio modificatorio firmado por las partes.

5. Resolución por incumplimiento

5.1 El Sistema de Educación Media Superior podrá, sin perjuicio de los demás recursos que tenga en caso de incumplimiento del contrato por el licitante, terminar el contrato en todo o en parte mediante notificación escrita al licitante, si:

a) El licitante no entrega los bienes, de conformidad con el contrato.

b) Se considera incumplimiento si el licitante no cumple cualquier otra de sus obligaciones establecidas en el contrato.

c) En caso de incumplimiento por causa imputable al licitante, se obligará al pago de una pena del 1%, por cada día que transcurra, hasta el 10%, misma que se establecerá en el contrato respectivo.

5.2 El licitante será sancionado de acuerdo al Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara y a lo estipulado en el Código Civil vigente en el Estado de Jalisco, por incumplimiento del contrato, así como el pago de los daños y perjuicios que estos ocasionen al Sistema de Educación Media Superior.

6. Resolución por insolvencia

6.1 El Sistema de Educación Media Superior, podrá terminar anticipadamente el contrato con el licitante en cualquier momento mediante notificación por escrito, sin indemnización alguna a la misma, si ésta fuese declarada en concurso mercantil o insolvente siempre que dicha terminación no perjudique o afecte derecho alguno a acción o recurso, que tenga o pudiera tener la Universidad de Guadalajara.

7. Revocación por conveniencia

7.1 El Sistema de Educación Media Superior, podrá en cualquier momento terminar total o parcialmente el contrato por razones de conveniencia, mediante notificación escrita a la licitante. La notificación indicará que la terminación se debe a conveniencia de la Universidad de

7.2 Guadalajara, el alcance del suministro que se haya completado y la fecha a partir de la cual la terminación entrará en vigor.

8. Idioma

8.1 El contrato se redactará en idioma español.

9. Leyes aplicables

9.1 La interpretación del contrato se hará de conformidad con las leyes vigentes del Estado de Jalisco.

10. Notificaciones

10.1 Toda notificación entre las partes, de conformidad con el contrato se harán por escrito a la dirección especificada para tal fin en las condiciones especiales del contrato, que en su caso se establezcan.

Contratante:

Secretario Ejecutivo del Comité de Compras y Adjudicaciones del Sistema de Educación Media Superior.

Liceo 496, Col centro, Guadalajara, Jalisco.

La notificación entrará en vigor en el momento de su entrega o en la fecha de entrada en vigor que se especifique en la notificación, si dicha fecha fuese posterior.

Sección III

CATÁLOGO DE CONCEPTOS

Descripción de los bienes y servicios requeridos por el Sistema de Educación Media Superior, conforme a la siguiente tabla:

PARTIDA	CANTIDAD	DESCRIPCIÓN	C.U.	TOTAL
1	203	**PUNTO DE ACCESO INALÁMBRICO "TIPO A"** El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, deberá ser una solución basada en el estándar IEEE 802.11ax para 5Ghz y 2.4Ghz que permita habilitar el acceso de red para los usuarios en general paradispositivos móviles (tablets, smartphones, laptops), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, deberán contemplarse como mínimo las siguientes funcionalidades: • Operación de banda dual en 2.4 y 5Ghz, concurrente • Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet • Conexión a la red alámbrica en 1000BaseT • Firewall para bloqueo de tráfico capa 3 y capa 7 a nivel del punto de acceso, con la capacidad de identificar aplicaciones específicas • Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio. • Prevención de Intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación medianteun tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para el servicio de los clientes inalámbricos. Capacidad de integrarse al servicio de Umbrella para protección inalámbrica a nivel de DNS que prevenga el acceso a sitios y dominios maliciosos, al igual que la capacidad de filtrar contenido basado en categorías (Requierelicencia de Umbrella). **Administración** • Gestión centralizada desde una consola de administración basada en Web, desde la cual se deberá poder acceder, configurar y monitorear todos los equipos de LAN o WLAN considerados en esta licitación • De igual manera, desde la misma consola de administración basada en Web, se deberán poder generar los reportes de operación correspondientes a todos los equipos de LAN o WLAN objeto de esta licitación • La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la Universidad de Guadalajara, soportando cualquier navegador moderno de Internet disponible • Deberá de haber mecanismos que limiten el acceso a la consola, basado en la definición de direcciones IP públicas autorizadas • El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación • El acceso a la consola de gestión deberá soportar la integración con repositorios de identidad externos via SAML para un Single Sign On (SSO). • El acceso a la consola de gestión deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet • La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola • La consola reportará sobre intentos de logins al sistema, mostrando qué cuenta intentó entrar, dirección IP, locación, estatus del intento y la hora y fecha del intento • El sistema de gestión centralizado deberá dar la opción de empujar nuevo firmware a los AP's, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad • El nivel jerárquico de los administradores de la consola deberá ser los siguientes: o Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todos los contenedores (colección de dispositivos de red) dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura. o El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece: • Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización • Resetear contraseñas • Crear, editar y borrar redes • Agregar nuevos dispositivos a las redes de la organización o Administrador de Contenedor: Tendrá visibilidad en aquellas contenedores de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de contenedor podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca: • Crear, editar y borrar otras cuentas de administrador dentro del contenedor • Crear, editar y borrar contenedores para las cuales cuente con privilegios **Características físicas y eléctricas de los equipos Puntos de acceso de red inalámbrica** • Antenas integradas al interior del equipo del tipo omnidireccional		

		• Alimentación PoE de 37 – 57 V, compatible con IEEE 802.3af ó IEEE 802.3at, asegurando que la alimentación requerida por el equipo, asegure su operación a carga máxima • Soporte de alimentación con eliminador de DC externo • Consumo máximo de potencia de 15W • Capacidad para energizarse via eliminador de corriente directa • Debe incluir tornillo de seguridad, así como bahía para candado Kensington • Placa para montaje en pared **Servicios de Red** El equipo propuesto debe contar con los siguientes servicios de red: • Interfaz de Radio Frecuencia: o Un radio a 2.4GHz 802.11b/g/n/ax y uno a 5GHz 802.11a/n/ac/ax o Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas o Que incluya embebido o agregado al AP un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades de monitoreo de entrada y salida de dispositivos que emitan beacons, mandando alertas de estos eventos. o Soporte de Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350Ghz (UNII- 2), 5.470-5.600, 5.660-5.725 (UNII-2e) y 5.725-5.825GHz (UNII-3) o Arreglo de Antenas integradas al chasis del tipo omnidireccional con ganancia de 5.4dBi@2.4GHz y 6dBi@5GHz o Arreglo MU-MIMO 2x2 con dos tramas espaciales (spatial streams) o La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:CCC Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz 5GHz únicamente Ambas bandas pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada o Ancho de banda de canales de 20, 40MHz y 80MHz o Tasa de datos combinada de 1.7Gbps o Certificado para especificación 802.11ax DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, 1024-QAM o Soporte de Maximal Ratio Combining (MRC) o Formación de haz (beamforming) o Agregación de paquetes o Soporte a Cyclic Shift Diversity (CSD) • Interfaz alámbrica de red: o Una interfaz 10/100/1000Base-T Ethernet (RJ-45) con soporte de 802.3at para PoE o VLAN tagging basado en IEEE802.1q o Cada Access Point deberá soportar los siguientes esquemas de direccionamiento IP: Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP Modo Bridge, donde el Access Point relevan los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN Roaming de capa 3 (L3), que permita al usuario mantener la misma dirección IP en caso de cambio de segmento de red, manteniendo la sesión activa todo el tiempo Túnel VPN con IPSEC hacia un concentrador central, para el caso en que se requiera habilitar esquemas de trabajador remoto y oficina remota como si se encontraran en la oficina principal • Calidad de Servicio: o Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e o Soporte de DSCP 802.1p o Modelado de tráfico a nivel de capa 7 (L7) Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se debe soportar la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema. La asignación de ancho de banda mediante el modelado de tráfico, deberá poderse definir mediante dos mecanismos: • Manual o Rangos CIDR/IP o hostname (URL) o Puertos UDP/TCP o Combinación de Red,Subnet y puerto o Red local (subredes y redes de clase completa en la LAN) • Mediante categorías de tráfico o Blogging o Email o Compartición de archivos o Juegos o Noticias o Respaldo en línea o Peer-to-peer o Redes sociales y compartición de fotos o Actualizaciones de programas y antivirus o Deportes o VoIP y videoconferencia o Compartición de archivos vía web • La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios • De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz) **Servicios de seguridad** La solución de Red Inalámbrica debe de incluir las siguientes funcionalidades de seguridad: a) Firewall a. La solución inalámbrica de red deberá soportar la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.		

i. Mediante las reglas de capa 3, se definirán políticas de acceso por:
1. Protocolo (UDP o TCP)
2. Host, subred o red origen
3. Puerto TCP o UDP origen
4. Host, subred o red destino
5. Puerto TCP o UDP destino
ii. Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
1. Blogging
2. Email
3. Compartición de archivos
4. Juegos
5. Noticias
6. Respaldo en línea
7. Peer-to-peer
8. Redes sociales y compartición de fotos
9. Actualizaciones de programas y antivirus
10. Deportes
11. VoIP y videoconferencia
12. Compartición de archivos vía web
b. Políticas basadas en identidad
i. La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de Radius de la [INSTITUCIÓN]
c. Políticas basadas en grupos
i. Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
ii. Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna
d. Control de acceso a la red inalámbrica: La solución deberá soportar la creación de 15 SSIDs como máximo, permitiendo para cada uno los siguientes métodos de acceso:
i. Abierta y sin encripción para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo
ii. Llave compartida con anterioridad (Pre-Shared key) con WPA2, WPA3-Transition Mode y WPA3-Personal
iii. Control de acceso basado en dirección MAC mediante autenticación Radius
iv. WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
1. Un servidor RADIUS incluido en la misma solución
2. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
v. WPA3-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
1. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
2. El servidor de RADIUS debe utilizar uno de los siguientes tipos de cifrado EAP
a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
vi. Capacidad para definir hasta 50 claves pre-compartidas de identidad (IPSK) para autenticar usuarios con servicios diferenciados dentro de una misma SSID sin tener que depender de un servidor de RADIUS o autenticación 802.1X
vii. Acceso vía portal cautivo (splash page), que permita habilitar los siguientes métodos de autenticación, conforme lo requiera la Universidad de Guadalajara
1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario

2. Portal “Click-through”, donde el usuario debe ver un portal de bienvenida y dar “click” a un botón para continuar su acceso
3. Portal captivo tipo “sign-on”, donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
a. Un servidor RADIUS interno a la solución propuesta
b. Un servidor RADIUS externo hosteado en alguna localidad de la Universidad de Guadalajara
c. Autenticación hacia una base de datos de Directorio Activo de la Universidad de Guadalajara
d. Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página oficial de la Universidad de Guadalajara en dicha red social
viii. Con excepción de la autenticación portal captivo deberá ser personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.
ix. De igual manera, se deberá contar con la funcionalidad de Walled Garden, que permita el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente
x. De acuerdo a lo que requiera la Universidad de Guadalajara, la solución deberá permitir o bloquear el tráfico no-HTTP
b) Control de acceso a la red (Network Access Control)
a. La solución deberá contar con la opción de verificación de la presencia de un software para la detección de antivirus actualizado en el dispositivo de usuario, previo a su autenticación a la red
c) Asignación de políticas de acceso por tipo de dispositivo
a. De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso

d) Filtrado de Contenido
a. La solución deberá incluir en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos, sin requerir para tal efecto añadir una solución de seguridad externa
e) Detección y Prevención de Intrusos en el Canal Inalámbrico
a. La solución de red inalámbrica, deberá contar con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:
i. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz
ii. Deberá descargar desde la consola central las últimas actualizaciones en firmas de ataques
iii. Deberá habilitar políticas de detección y remediación granulares sobre la misma consola de gestión de la solución
iv. El WIPS deberá estar basado en un motor heurístico que permita detectar los ataques más sofisticados, mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de desasociación e identificar las variantes a partir del comportamiento normal
v. Deberá identificar y organizar las siguientes categorías de ataques como mínimo:
1. SSIDs no autorizados
2. Intentos de robo de identidad (spoofs) del AP
3. Inundación de paquetes que tengan como finalidad generar eventos de negación de servicio (DoS)
vi. Para efectos de remediar los ataques, la solución deberá permitir la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID
vii. Deberá notificar de eventos de seguridad a los administradores de la red por medio de correo electrónico
Reportes y monitoreo
• Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución deberá incluir dentro de la misma consola de gestión un inventario de equipo tanto operativo como desconectado, accesible para los administradores de la red
• Se deberá poder cargar los planos de las ubicaciones en donde se desplieguen los AP, así como la alineación a Google Maps, con el propósito de tener la ubicación de cada AP bien definido.
• La solución deberá de contar con una aplicación móvil que facilite el monitoreo de los AP's desplegados, así como la capacidad de tomar fotos de cada AP montado para que se refleje en la plataforma de gestión fija.
• La solución deberá poder mostrar diagnósticos de salud desde el punto de vista del cliente, permitiendo hacer "drill-down" en un cliente específico y obtener información sobre la salud del mismo
o Indicación gráfica de la salud de la conexión entre el cliente y su Access Point, con la tasa de transferencia negociada y la tasa de datos en transferencia en ese instante de tiempo
o Indicación gráfica de la salud del Access Point, con desglose de utilización de canal, carga actual de clientes y utlización en el canal actual del cliente

o Capacidad de lanzar una captura de paquetes filtrada para el cliente desde ese Access Point
o Indicación de la calidad de la conexión de ese Access Point a su switch de acceso, mostrando el estatus del puerto, problemas de conectividad, exceso de broadcast/multicast/unknown unicast, y problemas de negociación
o Indicación de problemas de salud en el switch de acceso, desglosados por problemas de DNS, RADIUS, OSPF o host capa 3
o Pestaña de Conexiones de cliente con las estadísticas y el desglose de los problemas de conectividad inalámbrica experimentados por el cliente desglosados en las etapas de Asociación, Autenticación, DHCP y DNS
o Rendimiento del cliente representado de forma gráfica que permita obtener métricas de rendimiento del mismo desglosadas en
 Gráfico de utilización histórica por aplicación, superpuesta con eventos de conexión del cliente como asociaciones, autenticaciones por RADIUS/802.1X, o roaming
 Gráfico de calidad de señal histórica percibida por el cliente, superpuesta con los eventos de conectividad del mismo
 Gráfico de latencia promedio histórica experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
 Gráfico de utilización de canal experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
 Gráfico de utilización del Access Point al que el cliente está asociado, superpuesta con los eventos de conectividad del mismo
 Gráfico de cantidad de clientes asociados al Access Point en el que se encuentra el cliente, superpuesto con los eventos de conectividad del mismo
 Gráfico de tasas de datos del cliente negociadas con cada uno de los Access Points por los que se ha movido
o Historial de conectividad del cliente que desglose todos los movimientos del mismo y que sea filtrable por SSID, Access Point, Banda, Etapa de Fallo, Severidad de Fallo
 La herramienta podrá aportar sugerencias de cómo solucionar ciertos problemas encontrados por el cliente y su posible causa raíz
• La solución deberá mostrar diagnósticos de salud desde el punto de vista del Access Point ofreciendo
o Información de salud de resumen desde el punto de vista del Access Point, indicando porcentualmente la cantidad de conexiones exitosas, fallidas y problemáticas, y desglosando las fallas en problemas de Asociación, Autenticación, DHCP y DNS
o Historial de rendimiento del Access Point, desglosado en
 Gráfico de utilización superpuesto con eventos de cambio de canal e intensidad de potencia
 Gráfico de cantidad de clientes asociados superpuesto con eventos de cambio de canal e intensidad de potencia
 Calidad de señal histórica promedio superpuesta con eventos de cambio de canal e intensidad de potencia
 Latencia inalámbrica promedio superpuesta con eventos de cambio de canal e intensidad de potencia
• La solución deberá poder mostrar información de diagnósticos globales sobre el rendimiento de la red inalámbrica ofreciendo los siguientes reportes de manera gráfica
o Salud por Access Point, indicando con código de colores de semáforo (verde, amarillo, rojo) los Access Points en un mapa para ilustrar gráficamente problemas de salud
o Listado de Access Points con mayor porcentaje de problemas de conectividad
o Desglose de salud por tipo de dispositivo, indicando por sistema operativo los problemas de conectividad observados en la red
o Conexiones fallidas desglosadas por porcentaje y tipo de fallo
 Fallos en Asociación
 Fallos en Autenticación
 Fallos en DHCP
 Fallos en DNS

		o Capacidad de hacer “drill-down” por tipo de fallo para ver todos los eventos relacionados al tipo de fallo por SSID, por Access Point y por Red o Desglose de latencia de paquetes por tipo de tráfico, ofreciendo las métricas de rendimiento histórico para o Tráfico de Voz o Tráfico de Vídeo o Tráfico Best Effort o Tráfico Background o Capacidad para extraer toda esta información por medio de APIs para graficar en Dashboards personalizados • La solución deberá generar sobre demanda un reporte ejecutivo por la último día, la última semana, el último mes y sobre un período específico de monitoreo, incluyendo los siguientes parámetros: o Utilización total de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos durante el tiempo especificado o Los Top 50 Access Points del sistema por utilización o Los SSID’s con mayor consumo o Conteo individual de clientes durante el período seleccionado y por día o Los Top 50 usuarios por utilización o Las Top 50 aplicaciones con mayor presencia en la red o Los Top 50 dispositivos por fabricante o Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red • Deberá proporcionar a los administradores con una lista de bitácoras de eventos y de cambios en la configuración. • Deberá contarse de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación. • Finalmente, la solución deberá contabilizar y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo: o Dispositivos que pasaron dentro del área de cobertura pero permanecieron un intervalo de tiempo pequeño o Dispositivos que aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura o Dispositivos que finalmente se conectaron a la red o Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente o Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales **Analíticos de ubicación de dispositivos** • La solución inalámbrica de red debe de estar equipada con la habilidad de detectar la presencia del dispositivo de usuario, basado en la información contenida en los mensajes de “probe request” generados por los radios WiFi encendidos en smartphones, laptops y tabletas. • Con la información recabada, la controladora en la nube deberá consolidar analíticos históricos de los dispositivos WiFi, con gráficas intuitivas y personalizables, facilitando la interpretación de tendencias tales como: o Flujo de paseantes por día y hora o Lealtad de usuarios basado en visitantes nuevos y repetidos o Tiempo de permanencia de visitantes en la zona de cobertura • La información de presencia, deberá estar disponible para su exportación a un sistema externo, que incluya: o Dirección MAC del AP que reporta o Dirección MAC del dispositivo de usuario o Intensidad de señal recibida (RSSI) con la cual fue escuchado el dispositivo o Estampa de tiempo o Coordenadas X y Y de la ubicación del dispositivo, de acuerdo a la información entregada por todos los APs del sistema **Inyector de Energía a través de cable Ethernet (PoE)** Los puntos de acceso tipo A, deberán incluir un inyector de energía a través de cable Ethernet (PoE) que debe operar con un voltaje de entrada de entre 100 a 240 Volts de corriente alterna, proporcionar un voltaje de salida de 55V de corriente directa, potencia de salida de 30W acorde al estandar IEEE 802.3at y debe ser compatible con Ethernet 10/100/1000 Mbits/s full duplex. **Licenciamiento, Garantías y soporte** • Deberá incluir todo el licenciamiento necesario para su correcto funcionamiento por lo menos durante 7 años. • Garantía de por vida en hardware de interiores. • Soporte técnico telefónico en español 24x7x365. • Tickets de soporte podrán ser abierto mediante la misma plataforma de gestión. • Reemplazo de partes de siguiente día hábil. • Esta garantía y soporte estará vigente por 7 años.		
2	**223**	**NODO DE RED CAT6 60 MTS** Suministro e instalación de nodo de red de 60 metros con las siguientes características: Certificación del fabricante con una garantía de 25 años mínimo en el desempeño de la instalación de Cableado Estructurado, dicha garantía debe estar detallada en un contrato en español y bajo leyes mexicanas, donde incluye mano de obra y producto. Los servicios de datos se instalarán con cable de par trenzado sin blindaje (UTP), Categoría 6, U/UTP, CM, Ignífugo, (PVC) Diámetro exterior nominal del cable (In.)0.225 Diámetro exterior nominal del cable (mm)5.7 Radio de plegado (mm)22, Número de pares 4, Conductor Material Cobre, Tipo de conductor Sólido, Medidor conductor (AWG)23 Estándares cumplidos Supera ISO 11801 Clase E y ANSI / TIA568.2-D Categoría 6 con garantía de espacio libre de canal, IEC 61156-5, UL 1685, cumple con IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt para aplicaciones PoE; Cumple con RoHS; Jack Categoría 6 en lado panel, estilo TP, ABS, en bronce fosforado chapado, esquema de cableado T568A/T568B, sin blindar, Jack plug en lado usuario enchufe modular terminable de campo Longitud total (mm) 46.2 Sin blindar (UTP), Ancho total (mm) 13.5, Altura total (mm) 15.8, Medidor de alambre compatible (AWG) 22-26, Supera los requisitos de rendimiento del canal ANSI/TIA 568-C.2 Categoría 6A e ISO 11801 Clase EA con hasta dos enchufes de canal de término de campo. Cumple o excede los requisitos propuestos de TIA Modular Plug Terminated Link con hasta dos enchufes de término de campo en el enlace, cumple con ANSI / TIA-1096-A (anteriormente FCC Parte 68), IEC 60603-7, IEC 60529 (IP 20), admite IEEE 802.3af / 802.3at (PoE / PoE +) y propone aplicaciones 802.3bt tipo 3 y tipo 4 (PoE ++). Soporta Power over HDBaseT hasta 100 vatios, compatible con RoHS Todos los componentes del cableado y accesorios deberán ser de la misma marca y categoría ya que se deberán de considerar paneles de parcheo modulares de 24 o 48 puertos, siendo utilizados solo los modulos necesarios, patch cords de 5 pies, face		

		plate, etiquetas para identificación en ambos extremos, organizadores horizontales, soportes de pared de 6 unidades de rack, charolas de 19 pulgadas rackeables, cinchos, velcro y todo lo necesario para su correcta instalación. Si el edificio cuenta con infraestructura que se centralice en un IDF, deberá centralizarse los ductos y cableado al rack existente. Se deberá considerar la canalización galvanizada para exteriores en pared gruesa que corresponda para cada nodo de datos incluyendo soporteria, accesorios de unión, cruces en losa o muro con los respectivos resanes y reparaciones de acuerdo con las mejores prácticas de instalación y cumpliendo con los siguientes estándares: ANSI/TIA/EIA–568B Comercial Building Wiring Standard, que permite la planeación e instalación de un sistema de Cableado Estructurado que soporta independientemente del proveedor y sin conocimiento previo, los servicios y dispositivos de telecomunicaciones que serán instalados durante la vida útil del edificio. EIA/TIA-568-B.1 (Requerimientos Generales) EIA/TIA-568-B.2-1 (Componentes de Cableado – Categoría 6 Par Trenzado balanceado) ANSI/TIA/EIA-569-B Commercial Building Standard for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos. ANSI/EIA/TIA-606A Administration Standard for the Telecomunications Commercial Building dura of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado. J-STD-607A Commercial Building Grounding (Earthing) and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio. UL 5A Estándar de UL para Canaletas Superficiales no Metálicas y sus Accesorios que analiza la resistencia física del material con que está hecha la canaleta. UL es el único Laboratorio reconocido por la ANSI/TIA/EIA 569A para prueba de materiales. UL 94 Estándar de UL que Prueba la Resistencia a la Propagación de la Flama en los productos.		
3	20	**PUNTO DE ACCESO INALÁMBRICO "TIPO B"** El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, deberá ser una solución basada en el estándar IEEE 802.11ax para 5Ghz y 2.4Ghz que permita habilitar el acceso de red para los usuarios en general para dispositivos móviles (tabletas, smartphones, laptops), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, deberán contemplarse como mínimo las siguientes funcionalidades: • Operación de banda dual en 2.4 y 5Ghz, concurrente • Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet • Conexión a la red alámbrica en 1000BaseT • Firewall para bloqueo de tráfico capa 3 y capa 7 a nivel del punto de acceso, con la capacidad de identificar aplicaciones específicas • Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio. • Prevención de Intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación mediante un tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para el servicio de los clientes inalámbricos. • Capacidad de integrarse al servicio de Umbrella para protección inalámbrica a nivel de DNS que prevenga el acceso a sitios y dominios maliciosos, al igual que la capacidad de filtrar contenido basado en categorías (Requiere licencia de Umbrella) **Administración** • Gestión centralizada desde una consola de administración basada en Web, desde la cual se deberá poder acceder, configurar y monitorear todos los equipos de LAN o WLAN considerados en esta licitación • De igual manera, desde la misma consola de administración basada en Web, se deberán poder generar los reportes de operación correspondientes a todos los equipos de LAN o WLAN objeto de esta licitación • La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la Universidad de Guadalajara, soportando cualquier navegador moderno de Internet disponible • Deberá de haber mecanismos que limiten el acceso a la consola, basado en la definición de direcciones IP públicas autorizadas • El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación • El acceso a la consola de gestión deberá soportar la integración con repositorios de identidad externos via SAML para un Single Sign On (SSO). • El acceso a la consola de gestión deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet • La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola • La consola reportará sobre intentos de logins al sistema, mostrando qué cuenta intentó entrar, dirección IP, locación, estatus del intento y la hora y fecha del intento • El sistema de gestión centralizado deberá dar la opción de empujar nuevo firmware a los AP's, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad • El nivel jerárquico de los administradores de la consola deberá ser los siguientes: o Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todos los contenedores (colección de dispositivos de red) dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura. ▪ El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:		

- Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
- Resetear contraseñas
- Crear, editar y borrar redes
- Agregar nuevos dispositivos a las redes de la organización

- Administrador de Contenedor: Tendrá visibilidad en aquellos contenedores de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de contenedor podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
  - Crear, editar y borrar otras cuentas de administrador dentro del contenedor
  - Crear, editar y borrar contenedores para las cuales cuente con privilegios

Características físicas y eléctricas de los equipos Puntos de acceso de red inalámbrica

- Conectores externos para antenas del tipo N
- Calificación ambiental IP67 (sellado contra el agua y el polvo)
- Temperatura de operación de -40 a 55 °C
- Alimentación compatible con IEEE 802.3at
- Debe incluir tornillos de seguridad, así como bahía para candado Kensington
- Placa para montaje en pared

Servicios de Red

El equipo propuesto debe contar con los siguientes servicios de red:

- Interfaz de Radio Frecuencia:
  - Un radio a 2.4GHz 802.11b/g/n/ax y uno a 5GHz 802.11a/n/ac/ax
  - Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas.
  - Que incluya embebido o agregado al AP un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades de monitoreo de entrada y salida de dispositivos que emitan beacons, mandando alertas de estos eventos.
  - Soporte de Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350Ghz (UNII-2), 5.470-5.600, 5.660-5.725 (UNII-2e) y 5.725-5.825GHz (UNII-3).
  - Antena exterior con conector N, que permita conectar antenas omnidireccionales (4dBi@2.4GHz y 7dBi@5GHz) ó en caso de requerirse por la [INSTITUCIÓN]antenas sectoriales (11dBi@2.4Ghz ó 13dBi@5GHz) o de parche (8dBi@2.4Ghz y 6.5dBi@5GHz)
  - Arreglo MU-MIMO 4x4 con cuatro tramas espaciales (spatial streams)
  - La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:
    - Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz
    - 5GHz únicamente
    - Ambas bandas, pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada
  - Ancho de banda de canales de 20, 40MHz y 80MHz
  - Tasa de datos combinada de 3.55Gbps
  - Certificado para especificación 802.11ax DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, 1024-QAM
  - Soporte de Maximal Ratio Combining (MRC)
  - Formación de haz (beamforming)
  - Agregación de paquetes
  - Soporte a Cyclic Shift Diversity (CSD)

- Interfaz alámbrica de red:
  - Una interfaz 100/1000/2.5GBase-T Ethernet (RJ-45) con soporte de 802.3at para PoE
  - VLAN tagging basado en IEEE802.1q
  - Cada Access Point deberá soportar los siguientes esquemas de direccionamiento IP:
    - Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP
    - Modo Bridge, donde el Access Point relevan los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN
    - Roaming de capa 3 (L3), que permita al usuario mantener la misma dirección IP en caso de cambio de segmento de red, manteniendo la sesión activa todo el tiempo
    - Túnel VPN con IPSEC hacia un concentrador central, para el caso en que se requiera habilitar esquemas de trabajador y oficina remotos como si se encontraran en la oficina principal
- Calidad de Servicio:
  - Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
  - Soporte de DSCP 802.1p
  - Modelado de tráfico a nivel de capa 7 (L7)
    - Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se debe soportar la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.
    - La asignación de ancho de banda mediante el modelado de tráfico deberá poderse definir mediante dos mecanismos:
      - Manual
        - Rangos CIDR/IP
        - hostname (URL)

- Puertos UDP/TCP
- Combinación de Red,Subnet y puerto
- Red local (subredes y redes de clase completa en la LAN)

- Mediante categorías de tráfico
  - Blogging
  - Email
  - Compartición de archivos
  - Juegos
  - Noticias
  - Respaldo en línea
  - Peer-to-peer
  - Redes sociales y compartición de fotos
  - Actualizaciones de programas y antivirus
  - Deportes
  - VoIP y videoconferencia
  - Compartición de archivos vía web
- La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios
- De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz).

Servicios de seguridad

La solución de Red Inalámbrica debe de incluir las siguientes funcionalidades de seguridad:

a) Firewall

a. La solución inalámbrica de red deberá soportar la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.
   i. Mediante las reglas de capa 3, se definirán políticas de acceso por:
      1. Protocolo (UDP o TCP)
      2. Host, subred o red origen
      3. Puerto TCP o UDP origen
      4. Host, subred o red destino
      5. Puerto TCP o UDP destino
   ii. Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
      1. Blogging
      2. Email
      3. Compartición de archivos
      4. Juegos
      5. Noticias
      6. Respaldo en línea
      7. Peer-to-peer
      8. Redes sociales y compartición de fotos
      9. Actualizaciones de programas y antivirus
      10. Deportes
      11. VoIP y videoconferencia
      12. Compartición de archivos vía web

b. Políticas basadas en identidad
   i. La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de Radius de la [INSTITUCIÓN]

c. Políticas basadas en grupos
   i. Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
   ii. Las políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna

d. Control de acceso a la red inalámbrica: La solución deberá soportar la creación de 15 SSIDs como máximo, permitiendo para cada uno los siguientes métodos de acceso:
   i. Abierta y sin encriptación para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo
   ii. Llave compartida con anterioridad (Pre-Shared key) con WPA2, WPA3-Transition Mode y WPA3-Personal
   iii. Control de acceso basado en dirección MAC mediante autenticación Radius
   iv. WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
      1. Un servidor RADIUS incluido en la misma solución
      2. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
      3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
   v. WPA3-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:

1. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
2. El servidor de RADIUS debe utilizar uno de los siguientes tipos de cifrado EAP
    a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales

vi. Capacidad para definir hasta 50 claves pre-compartidas de identidad (IPSK) para autenticar usuarios con servicios diferenciados dentro de una misma SSID sin tener que depender de un servidor de RADIUS o autenticación 802.1X

vii. Acceso vía portal cautivo (splash page), que permita habilitar los siguientes métodos de autenticación, conforme lo requiera la Universidad de Guadalajara

1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario
2. Portal "Click-through", donde el usuario debe ver un portal de bienvenida y dar "click" a un botón para continuar su acceso
3. Portal captivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
    a. Un servidor RADIUS interno a la solución propuesta
    b. Un servidor RADIUS externo hosteado en alguna localidad de la Universidad de Guadalajara
    c. Autenticación hacia una base de datos de Directorio Activo de la Universidad de Guadalajara la Universidad de Guadalajara Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página oficial de la Universidad de Guadalajara en dicha red social

viii. Con excepción de la autenticación portal captivo deberá ser personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.

ix. De igual manera, se deberá contar con la funcionalidad de Walled Garden, que permita el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente

x. De acuerdo a lo que requiera la Universidad de Guadalajara la solución deberá permitir o bloquear el tráfico no-HTTP

b) Control de acceso a la red (Network Access Control)
    a. La solución deberá contar con la opción de verificación de la presencia de un software para la detección de antivirus actualizado en el dispositivo de usuario, previo a su autenticación a la red

c) Asignación de políticas de acceso por tipo de dispositivo
    a. De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso

d) Filtrado de Contenido
    a. La solución deberá incluir en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos, sin requerir para tal efecto añadir una solución de seguridad externa

e) Detección y Prevención de Intrusos en el Canal Inalámbrico
    a. La solución de red inalámbrica deberá contar con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:
        i. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz
        ii. Deberá descargar desde la consola central las últimas actualizaciones en firmas de ataques
        iii. Deberá habilitar políticas de detección y remediación granulares sobre la misma consola de gestión de la solución
        iv. El WIPS deberá estar basado en un motor heurístico que permita detectar los ataques más sofisticados, mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de de asociación e identificar las variantes a partir del comportamiento normal
        v. Deberá identificar y organizar las siguientes categorías de ataques como mínimo:
            1. SSIDs no autorizados
            2. Intentos de robo de identidad (spoofs) del AP
            3. Inundación de paquetes que tengan como finalidad generar eventos de negación de servicio (DoS)
        vi. Para efectos de remediar los ataques, la solución deberá permitir la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID
        vii. Deberá notificar de eventos de seguridad a los administradores de la red por medio de correo electrónico

Reportes y monitoreo

- Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución deberá incluir dentro de la misma consola de gestión un inventario de equipo tanto operativo como desconectado, accesible para los administradores de la red
- Se deberá poder cargar los planos de las ubicaciones en donde se desplieguen los AP, así como la alineación a Google Maps, con el propósito de tener la ubicación de cada AP bien definido.

- La solución deberá de contar con una aplicación móvil que facilite el monitoreo de los AP's desplegados, así como la capacidad de tomar fotos de cada AP montado para que se refleje en la plataforma de gestión fija.
- La solución deberá poder mostrar diagnósticos de salud desde el punto de vista del cliente, permitiendo hacer "drill-down" en un cliente específico y obtener información sobre la salud del mismo
    - Indicación gráfica de la salud de la conexión entre el cliente y su Access Point, con la tasa de transferencia negociada y la tasa de datos en transferencia en ese instante de tiempo
    - Indicación gráfica de la salud del Access Point, con desglose de utilización de canal, carga actual de clientes y utlización en el canal actual del cliente
    - Capacidad de lanzar una captura de paquetes filtrada para el cliente desde ese Access Point
    - Indicación de la calidad de la conexión de ese Access Point a su switch de acceso, mostrando el estatus del puerto, problemas de conectividad, exceso de broadcast/multicast/unknown unicast, y problemas de negociación
    - Indicación de problemas de salud en el switch de acceso, desglosados por problemas de DNS, RADIUS, OSPF o host capa 3
    - Pestaña de Conexiones de cliente con las estadísticas y el desglose de los problemas de conectividad inalámbrica experimentados por el cliente desglosados en las etapas de Asociación, Autenticación, DHCP y DNS
    - Rendimiento del cliente representado de forma gráfica que permita obtener métricas de rendimiento del mismo desglosadas en
        - Gráfico de utilización histórica por aplicación, superpuesta con eventos de conexión del cliente como asociaciones, autenticaciones por RADIUS/802.1X, o roaming
        - Gráfico de calidad de señal histórica percibida por el cliente, superpuesta con los eventos de conectividad del mismo
        - Gráfico de latencia promedio histórica experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
        - Gráfico de utilización de canal experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
        - Gráfico de utilización del Access Point al que el cliente está asociado, superpuesta con los eventos de conectividad del mismo
        - Gráfico de cantidad de clientes asociados al Access Point en el que se encuentra el cliente, superpuesto con los eventos de conectividad del mismo
        - Gráfico de tasas de datos del cliente negociadas con cada uno de los Access Points por los que se ha movido
    - Historial de conectividad del cliente que desglose todos los movimientos del mismo y que sea filtrable por SSID, Access Point, Banda, Etapa de Fallo, Severidad de Fallo
        - La herramienta podrá aportar sugerencias de cómo solucionar ciertos problemas encontrados por el cliente y su posible causa raíz
- La solución deberá mostrar diagnósticos de salud desde el punto de vista del Access Point ofreciendo
    - Información de salud de resumen desde el punto de vista del Access Point, indicando porcentualmente la cantidad de conexiones exitosas, fallidas y problemáticas, y desglosando las fallas en problemas de Asociación, Autenticación, DHCP y DNS
    - Historial de rendimiento del Access Point, desglosado en
        - Gráfico de utilización superpuesto con eventos de cambio de canal e intensidad de potencia
        - Gráfico de cantidad de clientes asociados superpuesto con eventos de cambio de canal e intensidad de potencia
        - Calidad de señal histórica promedio superpuesto con eventos de cambio de canal e intensidad de potencia
        - Latencia inalámbrica promedio superpuesta con eventos de cambio de canal e intensidad de potencia
- La solución deberá poder mostrar información de diagnósticos globales sobre el rendimiento de la red inalámbrica ofreciendo los siguientes reportes de manera gráfica
    - Salud por Access Point, indicando con código de colores de semáforo (verde, amarillo, rojo) los Access Points en un mapa para ilustrar gráficamente problemas de salud
    - Listado de Access Points con mayor porcentaje de problemas de conectividad
    - Desglose de salud por tipo de dispositivo, indicando por sistema operativo los problemas de conectividad observados en la red
    - Conexiones fallidas desglosadas por porcentaje y tipo de fallo
        - Fallos en Asociación
        - Fallos en Autenticación
        - Fallos en DHCP
        - Fallos en DNS
    - Capacidad de hacer "drill-down" por tipo de fallo para ver todos los eventos relacionados al tipo de fallo por SSID, por Access Point y por Red
    - Desglose de latencia de paquetes por tipo de tráfico, ofreciendo las métricas de rendimiento histórico para
        - Tráfico de Voz
        - Tráfico de Vídeo
        - Tráfico Best Effort
        - Tráfico Background
    - Capacidad para extraer toda esta información por medio de APIs para graficar en Dashboards personalizados
- La solución deberá generar sobre demanda un reporte ejecutivo por el último día, la última semana, el último mes y sobre un período específico de monitoreo, incluyendo los siguientes parámetros:
    - Utilización total de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos durante el tiempo especificado
    - Los Top 50 Access Points del sistema por utilización
    - Los SSID's con mayor consumo
    - Conteo individual de clientes durante el período seleccionado y por día
    - Los Top 50 usuarios por utilización
    - Las Top 50 aplicaciones con mayor presencia en la red
    - Los Top 50 dispositivos por fabricante
    - Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red
- Deberá proporcionar a los administradores con una lista de bitácoras de eventos y de cambios en la configuración.

		• Deberá contarse de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación. • Finalmente, la solución deberá contabilizar y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo: o Dispositivos que pasaron dentro del área de cobertura, pero permanecieron un intervalo de tiempo pequeño o Dispositivos que, aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura o Dispositivos que finalmente se conectaron a la red o Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente o Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales **Analíticos de ubicación de dispositivos** • La solución inalámbrica de red debe de estar equipada con la habilidad de detectar la presencia del dispositivo de usuario, basado en la información contenida en los mensajes de "probe request" generados por los radios WiFi-encendidos en smartphones, laptops y tabletas. • Con la información recabada, la controladora en la nube deberá consolidar analíticos históricos de los dispositivos WiFi, con gráficas intuitivas y personalizables, facilitando la interpretación de tendencias tales como: o Flujo de paseantes por día y hora o Lealtad de usuarios basado en visitantes nuevos y repetidos o Tiempo de permanencia de visitantes en la zona de cobertura • La información de presencia deberá estar disponible para su exportación a un sistema externo, que incluya: o Dirección MAC del AP que reporta o Dirección MAC del dispositivo de usuario o Intensidad de señal recibida (RSSI) con la cual fue escuchado el dispositivo o Estampa de tiempo o Coordenadas X y Y de la ubicación del dispositivo, de acuerdo a la información entregada por todos los APs del sistema **Antenas** Los puntos de acceso tipo C, deberán incluir 2 antenas externas de banda dual MIMO tipo Sector ganancia de 9 dBi a 2.4 GHz, ganancia de 12 dBi a 5 GHz **Inyector de Energía a través de cable Ethernet (PoE)** Los puntos de acceso tipo C, deberán incluir un inyector de energía a través de cable Ethernet (PoE) que debe operar con un voltaje de entrada de entre 100 a 240 Volts de corriente alterna, proporcionar un voltaje de salida de 55V de corriente directa, potencia de salida de 30W acorde al estándar IEEE 802.3at y debe ser compatible con Ethernet 10/100/1000 Mbits/s full duplex. • Deberá incluir todo el licenciamiento necesario para su correcto funcionamiento por lo menos durante 7 años. • Garantía de por vida en hardware de interiores. • Soporte técnico telefónico en español 24x7x365. • Tickets de soporte podrán ser abierto mediante la misma plataforma de gestión. • Reemplazo de partes de siguiente día hábil. Esta garantía y soporte estará vigente por 7 años.			
		SUBTOTAL			
		I.V.A			
		TOTAL			

Condiciones de pago:
Tiempo de garantía que otorga el licitante concursante de los bienes ofertados:
Tiempo de entrega:
Vigencia de la cotización:

Notas:

- **Los equipos ofertados de cada partida deberán ser de marca.**
- **Se deberá especificar la marca y modelo del equipo ofertado en cada partida.**
- **Se deberán especificar en su propuesta económica el tiempo de garantía de todas las partidas, misma que deberá ser ofertado por la empresa licitante**
- **En los precios ofertados deberá de considerarse el costo de flete para la entrega a cada dependencia beneficiada.**

A T E N T A M E N T E

_____, Jalisco; a _____de _____ 2021

_____
NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

ANEXOS PROPUESTA ECONÓMICA

1. El participante deberá presentar el datasheet del equipo ofertado, con link de la página oficial, en el cual se pueda corroborar la información de acuerdo a su propuesta técnica.

2. El participante deberá presentar carta original emitida por el fabricante, donde se avale como distribuidor autorizado de sus productos en México.

3. Para garantizar que los productos que distribuye son nuevos, no remanufacturados y cuentan con garantía, el participante deberá presentar una carta original emitida por el fabricante, que es un partner autorizado, mínimo de nivel premier.

4. El participante deberá presentar también una carta original emitida por el fabricante, donde demuestre que ha trabajado en conjunto la solución, y que cuenta con la experiencia y conocimiento técnico para dar cumplimiento a los requisitos del presente proyecto.

5. El participante deberá presentar una carta original emitida por el fabricante, donde señale que el producto cuenta con servicio de soporte proporcionado directamente por el fabricante.

6. El participante deberá presentar certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration)

7. El participante deberá presentar copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

8. El participante deberá presentar copia de un certificado vigente de Project Manangement Professional (PMP), así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

9. El licitante deberá contar con un centro de soporte que brinde atención las 24 horas del día, los 365 días del año, atendiendo solicitudes por teléfono y por correo electrónico, manifestado en una carta bajo protesta de decir la verdad.

10. El participante deberá incluir en su propuesta una matriz de escalación donde indique los tiempos de respuesta, responsables y números de contacto, así como el procedimiento para el levantamiento y la atención de reportes

FORMATO PARA PROPUESTA TÉCNICA

PARTIDA	CANTIDAD	DESCRIPCIÓN TÉCNICA COTIZADA EN PROPUESTA ECONÓMICA
1	**203**	
2	**223**	
3	**20**	

Nota:

Se deberán anexar folletos y/o manuales que ilustren su propuesta

A T E N T A M E N T E

_____, Jalisco; a _____de _____ 2021

_____
NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

SECCION IV

CARTA DE SERIEDAD DE LA PROPUESTA

Licitación Pública No. LI-SEMS-009-2021

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media Superior
Universidad de Guadalajara.
Presente.

En referencia a la convocatoria publicada el 24 de septiembre 2021, mediante la cual se invita a participar en la Licitación Pública arriba indicada, relativa a la ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA., y como representante legal de la empresa _____, manifiesto a usted que se cumplió en tiempo y forma con el registro señalado en dicha convocatoria y se adquirieron las bases y los anexos relativos a la licitación mencionada. También le informo que estamos enterados del contenido de las bases y las hemos aceptado íntegramente. Para tal efecto he tomado la debida nota a que nos sujetamos y se devuelven debidamente firmados.

Por otra parte manifiesto a usted, que se han tomado en cuenta las aclaraciones a las dudas de los licitantes participantes y declaro que mi representada posee y conoce toda la información adicional proporcionada por el Sistema de Educación Media Superior como complemento de la documentación inicial que se recibió y que se anexa a nuestra proposición.

Igualmente le informo que la empresa a la que represento se compromete a acatar las instrucciones señaladas en las bases de la licitación y garantizamos respetar nuestra oferta hasta la fecha límite de vigencia.

A T E N T A M E N T E

_____, Jalisco; a _____de _____ 2021

_____
NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

Sección V

CARTA COMPROMISO

Licitación Pública No. LI-SEMS-009-2021

Secretario Ejecutivo del Comité de Compras
y Adquisiciones del Sistema de Educación Media Superior
Universidad de Guadalajara.
Presente.

Luego de haber examinado los documentos de la licitación, de los cuales confirmamos recibo por la presente, los suscritos ofrecemos ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA., de conformidad con dichos documentos, por la suma de $ ---------- (monto total de la oferta en palabras), con I.V.A. incluido, de acuerdo a la propuesta económica que se adjunta a la presente oferta y que forma parte integrante de ella.

Si nuestra oferta es aceptada, contrataremos a favor de la Universidad de Guadalajara una fianza, ante una institución legalmente autorizada para emitirla, correspondiente al 10% del monto total adjudicado en el contrato respectivo, para asegurar su debido cumplimiento.

Si nuestra oferta es aceptada, contrataremos a favor de la Universidad de Guadalajara una fianza, ante una institución legalmente autorizada para emitirla, correspondiente al 100% del monto total que se reciba por concepto de anticipo, para garantizar la correcta aplicación de los recursos del anticipo. (Anticipo máximo 30%).

Convenimos en mantener esta oferta por un período de ____ días naturales a partir de la fecha fijada para la apertura de las propuestas, la cual nos obligará y podrá ser aceptada en cualquier momento antes de que expire el período indicado. Ésta, junto con el acta de lectura de fallo de adjudicación, constituirá un contrato obligatorio hasta que se prepare y firme el Contrato formal.

Entendemos que ustedes no están obligados a aceptar la más baja, ni ninguna otra de las ofertas que reciban.

A T E N T A M E N T E

Guadalajara, Jalisco; a_____de_____de 2021

_____

NOMBRE Y FIRMA
REPRESENTANTE LEGAL DE LA EMPRESA O PERSONA FÍSICA

UNIVERSIDAD DE GUADALAJARA
Sistema de Educación Media Superior
Secretaría Administrativa
Coordinación de Cómputo e Informática

SEMS/CCEI/0098/21
ASUNTO: Administrativas

Ing. Fernando Calvillo Vargas
Coordinador de Servicios Generales del SEMS
Presente.

Por medio del presente le envío un cordial saludo, asimismo y en respuesta a su oficio fechado el día 13 de octubre 2021, anexo dictamen técnico de las propuestas de las empresas que se presentaron en el concurso No. LI-SEMS-009-2021 denominado "ADQUISICIÓN DE PUNTOS DE ACCESO INALAMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDICACION MEDA SUPERIOR DE LA UNIVERSIDAD DE GUADADALAJARA."

Sin más por el momento, me despido reiterándoles mis más distinguidas consideraciones.

Atentamente
"Piensa y Trabaja"
"Año del legado de Fray Antonio Alcalde en Guadalajara"
Guadalajara, Jalisco; 14 de octubre de 2021

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO

Ing. María Esmeralda Olmos de la Cruz
Coordinación de Cómputo e Informática

Ocmej/mmm

DICTAMEN TÉCNICO

Fecha 14 de octubre de 2021.

LICITACIÓN: LI-SEMS-009-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.
1.- Relación de las proposiciones declaradas solventes, porque cumplen con todos los requisitos técnicos solicitados:

EMPRESAS
REDEFONIA, S.A. DE C.V.
SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.

PARTIDA 1

PUNTO DE ACCESO INALÁMBRICO "TIPO A"

El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, deberá ser una solución basada en el estándar IEEE 802.11ax para 5Ghz y 2.4Ghz que permita habilitar el acceso de red para los usuarios en general paradispositivos móviles (tablets, smartphones, laptops), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, deberán contemplarse como mínimo las siguientes funcionalidades:

- Operación de banda dual en 2.4 y 5Ghz, concurrente
- Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso alnternet
- Conexión a la red alámbrica en 1000BaseT
- Firewall para bloqueo de tráfico capa 3 y capa 7 a nivel del punto de acceso, con la capacidad de identificar aplicaciones específicas
- Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio.
- Prevención de Intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación medianteun tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para el servicio de los clientes inalámbricos.

Capacidad de integrarse al servicio de Umbrella para protección inalámbrica a nivel de DNS que prevenga el acceso a sitios y dominios maliciosos, al igual que la capacidad de filtrar contenido basado en categorías (Requierelicencia de Umbrella).

Administración

- Gestión centralizada desde una consola de administración basada en Web, desde la cual se deberá poder acceder, configurar y monitorear todos los equipos de LAN o WLAN considerados en esta licitación
- De igual manera, desde la misma consola de administración basada en Web, se deberán poder generar los reportes de operación correspondientes a todos los equipos de LAN o WLAN objeto de esta licitación
- La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la Universidad de Guadalajara, soportando cualquier navegador moderno de Internet disponible
- Deberá de haber mecanismos que limiten el acceso a la consola, basado en la definición de direcciones IP públicas autorizadas
- El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola de gestión deberá soportar la integración con repositorios de identidad externos via SAML para un Single Sign On (SSO).
- El acceso a la consola de gestión deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet
- La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola
- La consola reportará sobre intentos de logins al sistema, mostrando qué cuenta intentó entrar, dirección IP, locación, estatus del intento y la hora y fecha del intento
- El sistema de gestión centralizado deberá dar la opción de empujar nuevo firmware a los AP's, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad
- El nivel jerárquico de los administradores de la consola deberá ser los siguientes:
  - Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todos los contenedores (colección de dispositivos de red) dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura.
  - El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:
    - Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
    - Resetear contraseñas
    - Crear, editar y borrar redes
    - Agregar nuevos dispositivos a las redes de la organización

- Administrador de Contenedor: Tendrá visibilidad en aquellas contenedores de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de contenedor podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
  - Crear, editar y borrar otras cuentas de administrador dentro del contenedor
  - Crear, editar y borrar contenedores para las cuales cuente con privilegios

Características físicas y eléctricas de los equipos Puntos de acceso de red inalámbrica

- Antenas integradas al interior del equipo del tipo omnidireccional
- Alimentación PoE de 37 – 57 V, compatible con IEEE 802.3af ó IEEE 802.3at, asegurando que la alimentación requerida por el equipo, asegure su operación a carga máxima
- Soporte de alimentación con eliminador de DC externo
- Consumo máximo de potencia de 15W
- Capacidad para energizarse via eliminador de corriente directa
- Debe incluir tornillo de seguridad, así como bahía para candado Kensington
- Placa para montaje en pared

Servicios de Red

El equipo propuesto debe contar con los siguientes servicios de red:

- Interfaz de Radio Frecuencia:
  - Un radio a 2.4GHz 802.11b/g/n/ax y uno a 5GHz 802.11a/n/ac/ax
  - Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas
  - Que incluya embebido o agregado al AP un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades de monitoreo de entrada y salida de dispositivos que emitan beacons, mandando alertas de estos eventos.
  - Soporte de Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350Ghz (UNII- 2), 5.470-5.600, 5.660-5.725 (UNII-2e) y 5.725-5.825GHz (UNII-3)
  - Arreglo de Antenas integradas al chasis del tipo omnidireccional con ganancia de 5.4dBi@2.4GHz y 6dBi@5GHz
  - Arreglo MU-MIMO 2x2 con dos tramas espaciales (spatial streams)
  - La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:CCC
    - Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz
    - 5GHz únicamente
    - Ambas bandas pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada
  - Ancho de banda de canales de 20, 40MHz y 80MHz
  - Tasa de datos combinada de 1.7Gbps
  - Certificado para especificación 802.11ax DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, 1024-QAM
  - Soporte de Maximal Ratio Combining (MRC)
  - Formación de haz (beamforming)
  - Agregación de paquetes
  - Soporte a Cyclic Shift Diversity (CSD)
- Interfaz alámbrica de red:
  - Una interfaz 10/100/1000Base-T Ethernet (RJ-45) con soporte de 802.3at para PoE
  - VLAN tagging basado en IEEE802.1q
  - Cada Access Point deberá soportar los siguientes esquemas de direccionamiento IP:
    - Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP
    - Modo Bridge, donde el Access Point relevan los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN
    - Roaming de capa 3 (L3), que permita al usuario mantener la misma dirección IP en caso de cambio de segmento de red, manteniendo la sesión activa todo el tiempo
    - Túnel VPN con IPSEC hacia un concentrador central, para el caso en que se requiera habilitar esquemas de trabajador remoto y oficina remota como si se encontraran en la oficina principal
- Calidad de Servicio:
  - Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
  - Soporte de DSCP 802.1p
  - Modelado de tráfico a nivel de capa 7 (L7)
    - Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se debe soportar la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.
    - La asignación de ancho de banda mediante el modelado de tráfico, deberá poderse definir mediante dos mecanismos:
- Manual
  - Rangos CIDR/IP
  - hostname (URL)
  - Puertos UDP/TCP
  - Combinación de Red,Subnet y puerto
  - Red local (subredes y redes de clase completa en la LAN)
- Mediante categorías de tráfico
  - Blogging
  - Email
  - Compartición de archivos
  - Juegos
  - Noticias
  - Respaldo en línea
  - Peer-to-peer
  - Redes sociales y compartición de fotos
  - Actualizaciones de programas y antivirus
  - Deportes
  - VoIP y videoconferencia
  - Compartición de archivos vía web
- La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios
- De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz)

Servicios de seguridad

La solución de Red Inalámbrica debe de incluir las siguientes funcionalidades de seguridad:

a) Firewall

a. La solución inalámbrica de red deberá soportar la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

vi. Para efectos de remediar los ataques, la solución deberá permitir la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID
vii. Deberá notificar de eventos de seguridad a los administradores de la red por medio de correo electrónico

Reportes y monitoreo

- Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución deberá incluir dentro de la misma consola de gestión un inventario de equipo tanto operativo como desconectado, accesible para los administradores de la red
- Se deberá poder cargar los planos de las ubicaciones en donde se desplieguen los AP, así como la alineación a Google Maps, con el propósito de tener la ubicación de cada AP bien definido.
- La solución deberá de contar con una aplicación móvil que facilite el monitoreo de los AP's desplegados, así como la capacidad de tomar fotos de cada AP montado para que se refleje en la plataforma de gestión fija.
- La solución deberá poder mostrar diagnósticos de salud desde el punto de vista del cliente, permitiendo hacer "drill-down" en un cliente específico y obtener información sobre la salud del mismo
  - Indicación gráfica de la salud de la conexión entre el cliente y su Access Point, con la tasa de transferencia negociada y la tasa de datos en transferencia en ese instante de tiempo
  - Indicación gráfica de la salud del Access Point, con desglose de utilización de canal, carga actual de clientes y utlización en el canal actual del cliente
  - Capacidad de lanzar una captura de paquetes filtrada para el cliente desde ese Access Point
  - Indicación de la calidad de la conexión de ese Access Point a su switch de acceso, mostrando el estatus del puerto, problemas de conectividad, exceso de broadcast/multicast/unknown unicast, y problemas de negociación
  - Indicación de problemas de salud en el switch de acceso, desglosados por problemas de DNS, RADIUS, OSPF o host capa 3
  - Pestaña de Conexiones de cliente con las estadísticas y el desglose de los problemas de conectividad inalámbrica experimentados por el cliente desglosados en las etapas de Asociación, Autenticación, DHCP y DNS
  - Rendimiento del cliente representado de forma gráfica que permita obtener métricas de rendimiento del mismo desglosadas en
    - Gráfico de utilización histórica por aplicación, superpuesta con eventos de conexión del cliente como asociaciones, autenticaciones por RADIUS/802.1X, o roaming
    - Gráfico de calidad de señal histórica percibida por el cliente, superpuesta con los eventos de conectividad del mismo
    - Gráfico de latencia promedio histórica experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
    - Gráfico de utilización de canal experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
    - Gráfico de utilización del Access Point al que el cliente está asociado, superpuesta con los eventos de conectividad del mismo
    - Gráfico de cantidad de clientes asociados al Access Point en el que se encuentra el cliente, superpuesto con los eventos de conectividad del mismo
    - Gráfico de tasas de datos del cliente negociadas con cada uno de los Access Points por los que se ha movido
  - Historial de conectividad del cliente que desglose todos los movimientos del mismo y que sea filtrable por SSID, Access Point, Banda, Etapa de Fallo, Severidad de Fallo
    - La herramienta podrá aportar sugerencias de cómo solucionar ciertos problemas encontrados por el cliente y su posible causa raíz
- La solución deberá mostrar diagnósticos de salud desde el punto de vista del Access Point ofreciendo
  - Información de salud de resumen desde el punto de vista del Access Point, indicando porcentualmente la cantidad de conexiones exitosas, fallidas y problemáticas, y desglosando las fallas en problemas de Asociación, Autenticación, DHCP y DNS
  - Historial de rendimiento del Access Point, desglosado en
    - Gráfico de utilización superpuesto con eventos de cambio de canal e intensidad de potencia
    - Gráfico de cantidad de clientes asociados superpuesto con eventos de cambio de canal e intensidad de potencia
    - Calidad de señal histórica promedio superpuesta con eventos de cambio de canal e intensidad de potencia
    - Latencia inalámbrica promedio superpuesta con eventos de cambio de canal e intensidad de potencia
- La solución deberá poder mostrar información de diagnósticos globales sobre el rendimiento de la red inalámbrica ofreciendo los siguientes reportes de manera gráfica
  - Salud por Access Point, indicando con código de colores de semáforo (verde, amarillo, rojo) los Access Points en un mapa para ilustrar gráficamente problemas de salud
  - Listado de Access Points con mayor porcentaje de problemas de conectividad
  - Desglose de salud por tipo de dispositivo, indicando por sistema operativo los problemas de conectividad observados en la red
  - Conexiones fallidas desglosadas por porcentaje y tipo de fallo
    - Fallos en Asociación
    - Fallos en Autenticación
    - Fallos en DHCP
    - Fallos en DNS
  - Capacidad de hacer "drill-down" por tipo de fallo para ver todos los eventos relacionados al tipo de fallo por SSID, por Access Point y por Red
  - Desglose de latencia de paquetes por tipo de tráfico, ofreciendo las métricas de rendimiento histórico para
    - Tráfico de Voz
    - Tráfico de Vídeo
    - Tráfico Best Effort
    - Tráfico Background
  - Capacidad para extraer toda esta información por medio de APIs para graficar en Dashboards personalizados
- La solución deberá generar sobre demanda un reporte ejecutivo por la último día, la última semana, el último mes y sobre un período específico de monitoreo, incluyendo los siguientes parámetros:
  - Utilización total de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos durante el tiempo especificado
  - Los Top 50 Access Points del sistema por utilización
  - Los SSID's con mayor consumo
  - Conteo individual de clientes durante el período seleccionado y por día
  - Los Top 50 usuarios por utilización
  - Las Top 50 aplicaciones con mayor presencia en la red
  - Los Top 50 dispositivos por fabricante
  - Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red
- Deberá proporcionar a los administradores con una lista de bitácoras de eventos y de cambios en la configuración.
- Deberá contarse de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación.
- Finalmente, la solución deberá contabilizar y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo:
  - Dispositivos que pasaron dentro del área de cobertura pero permanecieron un intervalo de tiempo pequeño
  - Dispositivos que aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura
  - Dispositivos que finalmente se conectaron a la red
  - Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente
  - Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales

Analíticos de ubicación de dispositivos

- La solución inalámbrica de red debe de estar equipada con la habilidad de detectar la presencia del dispositivo de usuario, basado en la información contenida en los mensajes de "probe request" generados por los radios WiFi encendidos en smartphones, laptops y tabletas.

i. Mediante las reglas de capa 3, se definirán políticas de acceso por:
1. Protocolo (UDP o TCP)
2. Host, subred o red origen
3. Puerto TCP o UDP origen
4. Host, subred o red destino
5. Puerto TCP o UDP destino
ii. Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
1. Blogging
2. Email
3. Compartición de archivos
4. Juegos
5. Noticias
6. Respaldo en línea
7. Peer-to-peer
8. Redes sociales y compartición de fotos
9. Actualizaciones de programas y antivirus
10. Deportes
11. VoIP y videoconferencia
12. Compartición de archivos vía web
b. Políticas basadas en identidad
i. La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de Radius de la [INSTITUCIÓN]
c. Políticas basadas en grupos
i. Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
ii. Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna
d. Control de acceso a la red inalámbrica: La solución deberá soportar la creación de 15 SSIDs como máximo, permitiendo para cada uno los siguientes métodos de acceso:
i. Abierta y sin encripción para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo
ii. Llave compartida con anterioridad (Pre-Shared key) con WPA2, WPA3-Transition Mode y WPA3-Personal
iii. Control de acceso basado en dirección MAC mediante autenticación Radius
iv. WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
1. Un servidor RADIUS incluido en la misma solución
2. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
v. WPA3-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
1. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
2. El servidor de RADIUS debe utilizar uno de los siguientes tipos de cifrado EAP
a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
vi. Capacidad para definir hasta 50 claves pre-compartidas de identidad (IPSK) para autenticar usuarios con servicios diferenciados dentro de una misma SSID sin tener que depender de un servidor de RADIUS o autenticación 802.1X
vii. Acceso vía portal cautivo (splash page), que permita habilitar los siguientes métodos de autenticación, conforme lo requiera la Universidad de Guadalajara
1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario
2. Portal "Click-through", donde el usuario debe ver un portal de bienvenida y dar "click" a un botón para continuar su acceso
3. Portal captivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
a. Un servidor RADIUS interno a la solución propuesta
b. Un servidor RADIUS externo hosteado en alguna localidad de la Universidad de Guadalajara
c. Autenticación hacia una base de datos de Directorio Activo de la Universidad de Guadalajara
d. Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página oficial de la Universidad de Guadalajara en dicha red social
viii. Con excepción de la autenticación portal captivo deberá ser personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.
ix. De igual manera, se deberá contar con la funcionalidad de Walled Garden, que permita el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente
x. De acuerdo a lo que requiera la Universidad de Guadalajara, la solución deberá permitir o bloquear el tráfico no-HTTP
b) Control de acceso a la red (Network Access Control)
a. La solución deberá contar con la opción de verificación de la presencia de un software para la detección de antivirus actualizado en el dispositivo de usuario, previo a su autenticación a la red
c) Asignación de políticas de acceso por tipo de dispositivo
a. De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso
d) Filtrado de Contenido
a. La solución deberá incluir en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos, sin requerir para tal efecto añadir una solución de seguridad externa
e) Detección y Prevención de Intrusos en el Canal Inalámbrico
a. La solución de red inalámbrica, deberá contar con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:
i. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz
ii. Deberá descargar desde la consola central las últimas actualizaciones en firmas de ataques
iii. Deberá habilitar políticas de detección y remediación granulares sobre la misma consola de gestión de la solución
iv. El WIPS deberá estar basado en un motor heurístico que permita detectar los ataques más sofisticados, mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de desasociación e identificar las variantes a partir del comportamiento normal
v. Deberá identificar y organizar las siguientes categorías de ataques como mínimo:
1. SSIDs no autorizados
2. Intentos de robo de identidad (spoofs) del AP
3. Inundación de paquetes que tengan como finalidad generar eventos de negación de servicio (DoS)

- Con la información recabada, la controladora en la nube deberá consolidar analíticos históricos de los dispositivos WiFi, con gráficas intuitivas y personalizables, facilitando la interpretación de tendencias tales como:
  - Flujo de paseantes por día y hora
  - Lealtad de usuarios basado en visitantes nuevos y repetidos
  - Tiempo de permanencia de visitantes en la zona de cobertura
- La información de presencia, deberá estar disponible para su exportación a un sistema externo, que incluya:
  - Dirección MAC del AP que reporta
  - Dirección MAC del dispositivo de usuario
  - Intensidad de señal recibida (RSSI) con la cual fue escuchado el dispositivo
  - Estampa de tiempo
  - Coordenadas X y Y de la ubicación del dispositivo, de acuerdo a la información entregada por todos los APs del sistema

Inyector de Energía a través de cable Ethernet (PoE)
Los puntos de acceso tipo A, deberán incluir un inyector de energía a través de cable Ethernet (PoE) que debe operar con un voltaje de entrada de entre 100 a 240 Volts de corriente alterna, proporcionar un voltaje de salida de 55V de corriente directa, potencia de salida de 30W acorde al estandar IEEE 802.3at y debe ser compatible con Ethernet 10/100/1000 Mbits/s full duplex.

Licenciamiento, Garantías y soporte

- Deberá incluir todo el licenciamiento necesario para su correcto funcionamiento por lo menos durante 7 años.
- Garantía de por vida en hardware de interiores.
- Soporte técnico telefónico en español 24x7x365.
- Tickets de soporte podrán ser abierto mediante la misma plataforma de gestión.
- Reemplazo de partes de siguiente día hábil.
- Esta garantía y soporte estará vigente por 7 años.

REDEFONIA, S.A. DE C.V.	SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.
CUMPLE	CUMPLE

PARTIDA 2

NODO DE RED CAT6 60 MTS
Suministro e instalación de nodo de red de 60 metros con las siguientes características:

Certificación del fabricante con una garantía de 25 años mínimo en el desempeño de la instalación de Cableado Estructurado, dicha garantía debe estar detallada en un contrato en español y bajo leyes mexicanas, donde incluye mano de obra y producto. Los servicios de datos se instalarán con cable de par trenzado sin blindaje (UTP), Categoría 6, U/UTP, CM, Ignífugo, (PVC) Diámetro exterior nominal del cable (In.)0.225 Diámetro exterior nominal del cable (mm)5.7 Radio de plegado (mm)22, Número de pares 4, Conductor Material Cobre, Tipo de conductor Sólido, Medidor conductor (AWG)23 Estándares cumplidos Supera ISO 11801 Clase E y ANSI / TIA568.2-D Categoría 6 con garantía de espacio libre de canal, IEC 61156-5, UL 1685, cumple con IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt para aplicaciones PoE; Cumple con RoHS; Jack Categoría 6 en lado panel, estilo TP, ABS, en bronce fosforado chapado, esquema de cableado T568A/T568B, sin blindar, Jack plug en lado usuario enchufe modular terminable de campo Longitud total (mm) 46.2 Sin blindar (UTP), Ancho total (mm) 13.5, Altura total (mm) 15.8, Medidor de alambre compatible (AWG) 22-26, Supera los requisitos de rendimiento del canal ANSI/TIA 568-C.2 Categoría 6A e ISO 11801 Clase EA con hasta dos enchufes de canal de término de campo. Cumple o excede los requisitos propuestos de TIA Modular Plug Terminated Link con hasta dos enchufes de término de campo en el enlace, cumple con ANSI / TIA-1096-A (anteriormente FCC Parte 68), IEC 60603-7, IEC 60529 (IP 20), admite IEEE 802.3af / 802.3at (PoE / PoE +) y propone aplicaciones 802.3bt tipo 3 y tipo 4 (PoE ++). Soporta Power over HDBaseT hasta 100 vatios, compatible con RoHS

Todos los componentes del cableado y accesorios deberán ser de la misma marca y categoría ya que se deberán de considerar paneles de parcheo modulares de 24 o 48 puertos, siendo utilizados solo los modulos necesarios, patch cords de 5 pies, face plate, etiquetas para identificación en ambos extremos, organizadores horizontales, soportes de pared de 6 unidades de rack, charolas de 19 pulgadas rackeables, cinchos, velcro y todo lo necesario para su correcta instalación.

Si el edificio cuenta con infraestructura que se centralice en un IDF, deberá centralizarse los ductos y cableado al rack existente.

Se deberá considerar la canalización galvanizada para exteriores en pared gruesa que corresponda para cada nodo de datos incluyendo soportería, accesorios de unión, cruces en losa o muro con los respectivos resanes y reparaciones de acuerdo con las mejores prácticas de instalación y cumpliendo con los siguientes estándares:

ANSI/TIA/EIA-568B Comercial Building Wiring Standard, que permite la planeación e instalación de un sistema de Cableado Estructurado que soporta independientemente del proveedor y sin conocimiento previo, los servicios y dispositivos de telecomunicaciones que serán instalados durante la vida útil del edificio.
EIA/TIA-568-B.1 (Requerimientos Generales)
EIA/TIA-568-B.2-1 (Componentes de Cableado – Categoría 6 Par Trenzado balanceado)
ANSI/TIA/EIA-569-B Commercial Building Standard for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos.
ANSI/EIA/TIA-606A Administration Standard for the Telecomunications Commercial Building dura of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado.

J-STD-607A Commercial Building Grounding (Earthing) and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio.

UL 5A Estándar de UL para Canaletas Superficiales no Metálicas y sus Accesorios que analiza la resistencia física del material con que está hecha la canaleta. UL es el único Laboratorio reconocido por la ANSI/TIA/EIA 569A para prueba de materiales.

UL 94 Estándar de UL que Prueba la Resistencia a la Propagación de la Flama en los productos.

REDEFONIA, S.A. DE C.V.	SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.
CUMPLE	CUMPLE

PARTIDA 3

PUNTO DE ACCESO INALÁMBRICO "TIPO B"

El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, deberá ser una solución basada en el estándar IEEE 802.11ax para 5Ghz y 2.4Ghz que permita habilitar el acceso de red para los usuarios en general para dispositivos móviles (tabletas, smartphones, laptops), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, deberán contemplarse como mínimo las siguientes funcionalidades:

- Operación de banda dual en 2.4 y 5Ghz, concurrente
- Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet
- Conexión a la red alámbrica en 1000BaseT
- Firewall para bloqueo de tráfico capa 3 y capa 7 a nivel del punto de acceso, con la capacidad de identificar aplicaciones específicas
- Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio.
- Prevención de Intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación mediante un tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para el servicio de los clientes inalámbricos.
- Capacidad de integrarse al servicio de Umbrella para protección inalámbrica a nivel de DNS que prevenga el acceso a sitios y dominios maliciosos, al igual que la capacidad de filtrar contenido basado en categorías (Requiere licencia de Umbrella)

Administración

- Gestión centralizada desde una consola de administración basada en Web, desde la cual se deberá poder acceder, configurar y monitorear todos los equipos de LAN o WLAN considerados en esta licitación
- De igual manera, desde la misma consola de administración basada en Web, se deberán poder generar los reportes de operación correspondientes a todos los equipos de LAN o WLAN objeto de esta licitación
- La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la Universidad de Guadalajara, soportando cualquier navegador moderno de Internet disponible
- Deberá de haber mecanismos que limiten el acceso a la consola, basado en la definición de direcciones IP públicas autorizadas
- El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola de gestión deberá soportar la integración con repositorios de identidad externos via SAML para un Single Sign On (SSO).
- El acceso a la consola de gestión deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet
- La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola
- La consola reportará sobre intentos de logins al sistema, mostrando qué cuenta intentó entrar, dirección IP, locación, estatus del intento y la hora y fecha del intento
- El sistema de gestión centralizado deberá dar la opción de empujar nuevo firmware a los AP's, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad
- El nivel jerárquico de los administradores de la consola deberá ser los siguientes:
    - Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todos los contenedores (colección de dispositivos de red) dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura.
        - El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:
            - Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
            - Resetear contraseñas
            - Crear, editar y borrar redes
            - Agregar nuevos dispositivos a las redes de la organización
    - Administrador de Contenedor: Tendrá visibilidad en aquellos contenedores de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de contenedor podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
        - Crear, editar y borrar otras cuentas de administrador dentro del contenedor
        - Crear, editar y borrar contenedores para las cuales cuente con privilegios

Características físicas y eléctricas de los equipos Puntos de acceso de red inalámbrica

- Conectores externos para antenas del tipo N
- Calificación ambiental IP67 (sellado contra el agua y el polvo)
- Temperatura de operación de -40 a 55 °C
- Alimentación compatible con IEEE 802.3at
- Debe incluir tornillos de seguridad, así como bahía para candado Kensington
- Placa para montaje en pared

Servicios de Red

El equipo propuesto debe contar con los siguientes servicios de red:

- Interfaz de Radio Frecuencia:
    - Un radio a 2.4GHz 802.11b/g/n/ax y uno a 5GHz 802.11a/n/ac/ax
    - Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas.
    - Que incluya embebido o agregado al AP un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades de monitoreo de entrada y salida de dispositivos que emitan beacons, mandando alertas de estos eventos.
    - Soporte de Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350Ghz (UNII-2), 5.470-5.600, 5.660-5.725 (UNII-2e) y 5.725-5.825GHz (UNII-3).
    - Antena exterior con conector N, que permita conectar antenas omnidireccionales (4dBi@2.4GHz y 7dBi@5GHz) ó en caso de requerirse por la [INSTITUCIÓN]antenas sectoriales (11dBi@2.4Ghz ó 13dBi@5GHz) o de parche (8dBi@2.4Ghz y 6.5dBi@5GHz)
    - Arreglo MU-MIMO 4x4 con cuatro tramas espaciales (spatial streams)
    - La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:
        - Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz

- 5GHz únicamente
- Ambas bandas, pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada

- Ancho de banda de canales de 20, 40MHz y 80MHz
- Tasa de datos combinada de 3.55Gbps
- Certificado para especificación 802.11ax DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, 1024-QAM
- Soporte de Maximal Ratio Combining (MRC)
- Formación de haz (beamforming)
- Agregación de paquetes
- Soporte a Cyclic Shift Diversity (CSD)

- Interfaz alámbrica de red:
  - Una interfaz 100/1000/2.5GBase-T Ethernet (RJ-45) con soporte de 802.3at para PoE
  - VLAN tagging basado en IEEE802.1q
  - Cada Access Point deberá soportar los siguientes esquemas de direccionamiento IP:
    - Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP
    - Modo Bridge, donde el Access Point relevan los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN
    - Roaming de capa 3 (L3), que permita al usuario mantener la misma dirección IP en caso de cambio de segmento de red, manteniendo la sesión activa todo el tiempo
    - Túnel VPN con IPSEC hacia un concentrador central, para el caso en que se requiera habilitar esquemas de trabajador y oficina remotos como si se encontraran en la oficina principal
- Calidad de Servicio:
  - Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
  - Soporte de DSCP 802.1p
  - Modelado de tráfico a nivel de capa 7 (L7)
    - Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se debe soportar la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.
    - La asignación de ancho de banda mediante el modelado de tráfico deberá poderse definir mediante dos mecanismos:
      - Manual
        - Rangos CIDR/IP
        - hostname (URL)
        - Puertos UDP/TCP
        - Combinación de Red,Subnet y puerto
        - Red local (subredes y redes de clase completa en la LAN)
      - Mediante categorías de tráfico
        - Blogging
        - Email
        - Compartición de archivos
        - Juegos
        - Noticias
        - Respaldo en línea
        - Peer-to-peer
        - Redes sociales y compartición de fotos
        - Actualizaciones de programas y antivirus
        - Deportes
        - VoIP y videoconferencia
        - Compartición de archivos vía web
      - La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios
      - De igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz).

Servicios de seguridad

La solución de Red Inalámbrica debe de incluir las siguientes funcionalidades de seguridad:

a) Firewall

a. La solución inalámbrica de red deberá soportar la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.
   i. Mediante las reglas de capa 3, se definirán políticas de acceso por:
      1. Protocolo (UDP o TCP)
      2. Host, subred o red origen
      3. Puerto TCP o UDP origen
      4. Host, subred o red destino
      5. Puerto TCP o UDP destino
   ii. Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
      1. Blogging
      2. Email
      3. Compartición de archivos
      4. Juegos
      5. Noticias
      6. Respaldo en línea
      7. Peer-to-peer
      8. Redes sociales y compartición de fotos
      9. Actualizaciones de programas y antivirus
      10. Deportes
      11. VoIP y videoconferencia
      12. Compartición de archivos vía web

b. Políticas basadas en identidad
   i. La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de Radius de la [INSTITUCIÓN]

c. Políticas basadas en grupos
   i. Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
   ii. Las políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna

d. Control de acceso a la red inalámbrica: La solución deberá soportar la creación de 15 SSIDs como máximo, permitiendo para cada uno los siguientes métodos de acceso:
   i. Abierta y sin encriptación para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo
   ii. Llave compartida con anterioridad (Pre-Shared key) con WPA2, WPA3-Transition Mode y WPA3-Personal
   iii. Control de acceso basado en dirección MAC mediante autenticación Radius
   iv. WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
      1. Un servidor RADIUS incluido en la misma solución
      2. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
      3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
   v. WPA3-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
      1. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
      2. El servidor de RADIUS debe utilizar uno de los siguientes tipos de cifrado EAP
         a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
         b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
         c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
      3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales
   vi. Capacidad para definir hasta 50 claves pre-compartidas de identidad (IPSK) para autenticar usuarios con servicios diferenciados dentro de una misma SSID sin tener que depender de un servidor de RADIUS o autenticación 802.1X
   vii. Acceso vía portal cautivo (splash page), que permita habilitar los siguientes métodos de autenticación, conforme lo requiera la Universidad de Guadalajara
      1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario
      2. Portal "Click-through", donde el usuario debe ver un portal de bienvenida y dar "click" a un botón para continuar su acceso
      3. Portal captivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
         a. Un servidor RADIUS interno a la solución propuesta
         b. Un servidor RADIUS externo hosteado en alguna localidad de la Universidad de Guadalajara
         c. Autenticación hacia una base de datos de Directorio Activo de la Universidad de Guadalajara la Universidad de Guadalajara Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página oficial de la Universidad de Guadalajara en dicha red social
   viii. Con excepción de la autenticación portal captivo deberá ser personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.
   ix. De igual manera, se deberá contar con la funcionalidad de Walled Garden, que permita el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente
   x. De acuerdo a lo que requiera la Universidad de Guadalajara la solución deberá permitir o bloquear el tráfico no-HTTP

b) Control de acceso a la red (Network Access Control)
   a. La solución deberá contar con la opción de verificación de la presencia de un software para la detección de antivirus actualizado en el dispositivo de usuario, previo a su autenticación a la red

c) Asignación de políticas de acceso por tipo de dispositivo
   a. De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso

d) Filtrado de Contenido
   a. La solución deberá incluir en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos, sin requerir para tal efecto añadir una solución de seguridad externa

e) Detección y Prevención de Intrusos en el Canal Inalámbrico
   a. La solución de red inalámbrica deberá contar con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:
      i. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz
      ii. Deberá descargar desde la consola central las últimas actualizaciones en firmas de ataques
      iii. Deberá habilitar políticas de detección y remediación granulares sobre la misma consola de gestión de la solución
      iv. El WIPS deberá estar basado en un motor heurístico que permita detectar los ataques más sofisticados, mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de de asociación e identificar las variantes a partir del comportamiento normal
      v. Deberá identificar y organizar las siguientes categorías de ataques como mínimo:
         1. SSIDs no autorizados
         2. Intentos de robo de identidad (spoofs) del AP
         3. Inundación de paquetes que tengan como finalidad generar eventos de negación de servicio (DoS)
      vi. Para efectos de remediar los ataques, la solución deberá permitir la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID
      vii. Deberá notificar de eventos de seguridad a los administradores de la red por medio de correo electrónico

Reportes y monitoreo

- Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución deberá incluir dentro de la misma consola de gestión un inventario de equipo tanto operativo como desconectado, accesible para los administradores de la red
- Se deberá poder cargar los planos de las ubicaciones en donde se despliegen los AP, así como la alineación a Google Maps, con el propósito de tener la ubicación de cada AP bien definido.
- La solución deberá de contar con una aplicación móvil que facilite el monitoreo de los AP's desplegados, así como la capacidad de tomar fotos de cada AP montado para que se refleje en la plataforma de gestión fija.
- La solución deberá poder mostrar diagnósticos de salud desde el punto de vista del cliente, permitiendo hacer "drill-down" en un cliente específico y obtener información sobre la salud del mismo
  - Indicación gráfica de la salud de la conexión entre el cliente y su Access Point, con la tasa de transferencia negociada y la tasa de datos en transferencia en ese instante de tiempo
  - Indicación gráfica de la salud del Access Point, con desglose de utilización de canal, carga actual de clientes y utlización en el canal actual del cliente
  - Capacidad de lanzar una captura de paquetes filtrada para el cliente desde ese Access Point
  - Indicación de la calidad de la conexión de ese Access Point a su switch de acceso, mostrando el estatus del puerto, problemas de conectividad, exceso de broadcast/multicast/unknown unicast, y problemas de negociación
  - Indicación de problemas de salud en el switch de acceso, desglosados por problemas de DNS, RADIUS, OSPF o host capa 3
  - Pestaña de Conexiones de cliente con las estadísticas y el desglose de los problemas de conectividad inalámbrica experimentados por el cliente desglosados en las etapas de Asociación, Autenticación, DHCP y DNS
  - Rendimiento del cliente representado de forma gráfica que permita obtener métricas de rendimiento del mismo desglosadas en

        - Gráfico de utilización histórica por aplicación, superpuesta con eventos de conexión del cliente como asociaciones, autenticaciones por RADIUS/802.1X, o roaming
        - Gráfico de calidad de señal histórica percibida por el cliente, superpuesta con los eventos de conectividad del mismo
        - Gráfico de latencia promedio histórica experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
        - Gráfico de utilización de canal experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
        - Gráfico de utilización del Access Point al que el cliente está asociado, superpuesta con los eventos de conectividad del mismo
        - Gráfico de cantidad de clientes asociados al Access Point en el que se encuentra el cliente, superpuesto con los eventos de conectividad del mismo
        - Gráfico de tasas de datos del cliente negociadas con cada uno de los Access Points por los que se ha movido
    - Historial de conectividad del cliente que desglose todos los movimientos del mismo y que sea filtrable por SSID, Access Point, Banda, Etapa de Fallo, Severidad de Fallo
        - La herramienta podrá aportar sugerencias de cómo solucionar ciertos problemas encontrados por el cliente y su posible causa raíz
- La solución deberá mostrar diagnósticos de salud desde el punto de vista del Access Point ofreciendo
    - Información de salud de resumen desde el punto de vista del Access Point, indicando porcentualmente la cantidad de conexiones exitosas, fallidas y problemáticas, y desglosando las fallas en problemas de Asociación, Autenticación, DHCP y DNS
    - Historial de rendimiento del Access Point, desglosado en
        - Gráfico de utilización superpuesto con eventos de cambio de canal e intensidad de potencia
        - Gráfico de cantidad de clientes asociados superpuesto con eventos de cambio de canal e intensidad de potencia
        - Calidad de señal histórica promedio superpuesto con eventos de cambio de canal e intensidad de potencia
        - Latencia inalámbrica promedio superpuesta con eventos de cambio de canal e intensidad de potencia
- La solución deberá poder mostrar información de diagnósticos globales sobre el rendimiento de la red inalámbrica ofreciendo los siguientes reportes de manera gráfica
    - Salud por Access Point, indicando con código de colores de semáforo (verde, amarillo, rojo) los Access Points en un mapa para ilustrar gráficamente problemas de salud
    - Listado de Access Points con mayor porcentaje de problemas de conectividad
    - Desglose de salud por tipo de dispositivo, indicando por sistema operativo los problemas de conectividad observados en la red
    - Conexiones fallidas desglosadas por porcentaje y tipo de fallo
        - Fallos en Asociación
        - Fallos en Autenticación
        - Fallos en DHCP
        - Fallos en DNS
    - Capacidad de hacer "drill-down" por tipo de fallo para ver todos los eventos relacionados al tipo de fallo por SSID, por Access Point y por Red
    - Desglose de latencia de paquetes por tipo de tráfico, ofreciendo las métricas de rendimiento histórico para
        - Tráfico de Voz
        - Tráfico de Vídeo
        - Tráfico Best Effort
        - Tráfico Background
    - Capacidad para extraer toda esta información por medio de APIs para graficar en Dashboards personalizados
- La solución deberá generar sobre demanda un reporte ejecutivo por el último día, la última semana, el último mes y sobre un período específico de monitoreo, incluyendo los siguientes parámetros:
    - Utilización total de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos durante el tiempo especificado
    - Los Top 50 Access Points del sistema por utilización
    - Los SSID's con mayor consumo
    - Conteo individual de clientes durante el período seleccionado y por día
    - Los Top 50 usuarios por utilización
    - Las Top 50 aplicaciones con mayor presencia en la red
    - Los Top 50 dispositivos por fabricante
    - Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red
- Deberá proporcionar a los administradores con una lista de bitácoras de eventos y de cambios en la configuración.
- Deberá contarse de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación.
- Finalmente, la solución deberá contabilizar y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo:
    - Dispositivos que pasaron dentro del área de cobertura, pero permanecieron un intervalo de tiempo pequeño
    - Dispositivos que, aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura
    - Dispositivos que finalmente se conectaron a la red
    - Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente
    - Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales

Analíticos de ubicación de dispositivos

- La solución inalámbrica de red debe de estar equipada con la habilidad de detectar la presencia del dispositivo de usuario, basado en la información contenida en los mensajes de "probe request" generados por los radios WiFi-encendidos en smartphones, laptops y tabletas.
- Con la información recabada, la controladora en la nube deberá consolidar analíticos históricos de los dispositivos WiFi, con gráficas intuitivas y personalizables, facilitando la interpretación de tendencias tales como:
    - Flujo de paseantes por día y hora
    - Lealtad de usuarios basado en visitantes nuevos y repetidos
    - Tiempo de permanencia de visitantes en la zona de cobertura
- La información de presencia deberá estar disponible para su exportación a un sistema externo, que incluya:
    - Dirección MAC del AP que reporta
    - Dirección MAC del dispositivo de usuario
    - Intensidad de señal recibida (RSSI) con la cual fue escuchado el dispositivo
    - Estampa de tiempo
    - Coordenadas X y Y de la ubicación del dispositivo, de acuerdo a la información entregada por todos los APs del sistema

Antenas

Los puntos de acceso tipo C, deberán incluir 2 antenas externas de banda dual MIMO tipo Sector ganancia de 9 dBi a 2.4 GHz, ganancia de 12 dBi a 5 GHz

Inyector de Energía a través de cable Ethernet (PoE)

Los puntos de acceso tipo C, deberán incluir un inyector de energía a través de cable Ethernet (PoE) que debe operar con un voltaje de entrada de entre 100 a 240 Volts de corriente alterna, proporcionar un voltaje de salida de 55V de corriente directa, potencia de salida de 30W acorde al estándar IEEE 802.3at y debe ser compatible con Ethernet 10/100/1000 Mbits/s full duplex.

- Deberá incluir todo el licenciamiento necesario para su correcto funcionamiento por lo menos durante 7 años.
- Garantía de por vida en hardware de interiores.
- Soporte técnico telefónico en español 24x7x365.
- Tickets de soporte podrán ser abierto mediante la misma plataforma de gestión.
- Reemplazo de partes de siguiente día hábil.

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

Esta garantía y soporte estará vigente por 7 años.

REDEFONIA, S.A. DE C.V.	SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.
CUMPLE	CUMPLE

Condiciones para el participante:

- El participante deberá presentar el datasheet del equipo ofertado, con link de la página oficial, en el cual se pueda corroborar la información de acuerdo a su propuesta técnica.
- El participante deberá presentar carta original emitida por el fabricante, donde se avale como distribuidor autorizado de sus productos en México.
- Para garantizar que los productos que distribuye son nuevos, no remanufacturados y cuentan con garantía, el participante deberá presentar una carta original emitida por el fabricante, que es un partner autorizado, mínimo de nivel premier.
- El participante deberá presentar también una carta original emitida por el fabricante, donde demuestre que ha trabajado en conjunto la solución, y que cuenta con la experiencia y conocimiento técnico para dar cumplimiento a los requisitos del presente proyecto.
- El participante deberá presentar una carta original emitida por el fabricante, donde señale que el producto cuenta con servicio de soporte proporcionado directamente por el fabricante.
- El participante deberá presentar certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration)
- El participante deberá presentar copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.
- El participante deberá presentar copia de un certificado vigente de Project Manangement Professional (PMP), así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.
- El licitante deberá contar con un centro de soporte que brinde atención las 24 horas del día, los 365 días del año, atendiendo solicitudes por teléfono y por correo electrónico, manifestado en una carta bajo protesta de decir la verdad.
- El participante deberá incluir en su propuesta una matriz de escalación donde indique los tiempos de respuesta, responsables y números de contacto, así como el procedimiento para el levantamiento y la atención de reportes

REDEFONIA, S.A. DE C.V.	SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.
NO CUMPLE	CUMPLE

La empresa REDEFONIA, S.A. DE C.V. no cumple, ya que según los documentos que recibimos por parte de la Coordinación de Servicios Generales, no anexan certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration). No presentan copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión y no presentan copia de un certificado vigente de Project Manangement Professional (PMP), así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

ELABORÓ

TSU Brian Valerio Flores
Jefe de la Unidad de Redes y Telecomunicaciones

AUTORIZÓ

SEMS
SECRETARÍA ADMINISTRATIVA
COORDINACIÓN DE CÓMPUTO E INFORMÁTICA

Ing. María Esmeralda Olmos de la Cruz
Coordinadora de Cómputo e Informática

DICTAMEN TÉCNICO

Guadalajara, Jalisco a 20 de octubre de 2020

LICITACION: LI-SEMS-009-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

1.- Relación de las proposiciones declaradas solventes, porque cumplen con todos los requisitos solicitados:

EMPRESAS	IMPORTE INCLUYE I.V.A
SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.	**$12´158,977.56**

2.- Criterios utilizados para la evaluación de las propuestas:

La Coordinación de Servicios Generales del Sistema de Educación Media Superior, para hacer la evaluación de las propuestas, realizaron lo siguiente:

Se revisaron las propuestas, de conformidad con lo estipulado en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, en sus artículos 24, 25, 45 y 47, en las bases de la licitación entregadas a los participantes, como se refleja en los siguientes puntos:

I) Se tomaron en cuenta sus antecedentes, su especialidad, su capacidad operativa.

II) Se consideraron los criterios de precio, calidad, tiempo de entrega, cumplimiento de requisitos técnicos, oportunidad y demás condiciones favorables a la Universidad de Guadalajara.

a) Que las propuestas contemplen todas y cada una de los requisitos solicitados en las bases de la licitación.

b) Que las mismas incluyan la información, documentos y requisitos solicitados.

c) Se verificó que las operaciones aritméticas se hayan ejecutado correctamente, en caso de que una o más tengan errores, se efectuaron las correcciones correspondientes, el monto correcto es el que se considera para el análisis comparativo de las proposiciones.

III) Criterios para la evaluación de las propuestas:

Se consideró la revisión del cumplimiento documental de las propuestas, que consistieron en lo siguiente:

- Verificación del cumplimiento de las especificaciones técnicas requeridas mediante dictamen técnico emitido por **Ing. Esmeralda Olmos De La Cruz Coordinadora de Cómputo e Informática del Sistema de Educación Media Superior**.
- Cumplimiento de los requisitos documentales para el concursante.
- Condiciones de pago.
- Precio.
- Vigencia de la cotización.
- Garantías.
- Tiempo de entrega.

3.-PROPUESTAS RECHAZADAS

3.1.-Se rechaza la propuesta de la empresa **REDEFONIA, S.A. DE C.V.,** debido a que se solicitan en la **SECCIÓN III** de las **BASES DE LA LICITACIÓN** los siguientes documentos:

6.-El participante deberá presentar certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration)

7.-El participante deberá presentar copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

8.-El participante deberá presentar copia de un certificado vigente de Project Manangement Professional (PMP), así como el currículum de la persona que lo poseea, quien deberá laborar para la empresa en cuestión.

Con base lo solicitado en las bases de la presente licitación, se observa que la empresa licitante de acuerdo a los documentos entregados, no presenta lo siguiente:

Los certificados vigentes de al menos 2 ingenieros CCNA (Cisco Certified Network Associate), 1 ingeniero CCDA (Cisco Certified Design Associate) y 1 ingeniero CCNP Collaboration (Cisco Certified Network Professional Collaboration). Asimismo, dentro de los documentos entregados no presentan copia de un certificado vigente de ITIL Foundation v3, así como el currículum de la empresa que lo posea, quien deberá laborar para la empresa en cuestión y no presenta copia de un certificado vigente de Project Manangement Profesisional (PMP), así como el currículum de la persona que lo posea, quien deberá laborar para la empresa en cuestión.

Con base a lo anterior, se rechaza la propuesta de la empresa **REDEFONIA, S.A. DE C.V.,** con base a lo establecido en la **SECCIÓN I "INSTRUCCIONES A LOS LICITANTES", inciso "G" Motivos por los que puede ser desechada la propuesta,** numeral **29 Causas por las que puede ser desechada la propuesta.**

Inciso "A"

El incumplimiento de alguno de los requisitos establecidos en las presentes Bases de la licitación y sus anexos.

Inciso "D"

La falta de alguno de los requisitos o esté diferente a lo solicitado o incumpla lo acordado en el acta de la junta aclaratoria, en su caso.

Inciso "G"

Cuando no satisfagan cualquiera de los requisitos determinados en estas bases y sus anexos, y que no hayan sido detectados en el acto

de presentación y apertura de propuestas.

4.- De conformidad con la revisión y evaluación de las propuestas, la Coordinación de Servicios Generales de Sistema de Educación Media Superior sugiere la adjudicación de la siguiente manera:

Partidas: **1, 2 y 3**

Empresa: **SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.**

Por un importe de **$12´158,977.56 (Doce millones ciento cincuenta y ocho mil novecientos setenta y siete pesos 56/100 m.n.) I.V.A. Incluido.**

En virtud de haber reunido las condiciones legales, técnicas y económicas para garantizar satisfactoriamente el cumplimiento de las obligaciones respectivas y haber presentado la propuesta solvente más baja en cada una de las partidas, en apego a lo establecido en los artículos 24, 25, 45 y 48., del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

ELABORÓ

MTRA. ROSAURA RODRIGUEZ RODRIGUEZ
JEFA DE LA UNIDAD DE ADQUISICIONES DEL SEMS

AUTORIZÓ

ING. FERNANDO CALVILLO VARGAS
COORDINADOR DE SERVICIOS GENERALES DEL SEMS

DICTAMEN TÉCNICO

Guadalajara, Jalisco a 18 de octubre de 2021

LICITACIÓN: LI-SEMS-010-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE EQUIPO DE SOLUCIÓN DE SEGURIDAD UTM/NGFW, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

1.- Relación de las proposiciones declaradas solventes, porque cumplen con todos los requisitos solicitados:

EMPRESAS	IMPORTE INCLUYE I.V.A
INITEL, S.A. DE C.V.	**$21,901,549.82**

2.- Criterios utilizados para la evaluación de las propuestas:

La Coordinación de Servicios Generales del Sistema de Educación Media Superior, para hacer la evaluación de las propuestas, realizaron lo siguiente:

Se revisaron las propuestas, de conformidad con lo estipulado en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, en sus artículos 24, 25, 45 y 47, en las condiciones generales entregadas a los participantes, como se refleja en los siguientes puntos:

I) Se tomaron en cuenta sus antecedentes, su especialidad, su capacidad operativa.

II) Se consideraron los criterios de precio, calidad, tiempo de entrega, cumplimiento de requisitos técnicos, oportunidad y demás condiciones favorables a la Universidad de Guadalajara.

a) Que las propuestas contemplen todas y cada una de los requisitos solicitados en las condiciones generales del concurso.

b) Que las mismas incluyan la información, documentos y requisitos solicitados.

c) Se verificó que las operaciones aritméticas se hayan ejecutado correctamente, en caso de que una o más tengan errores, se efectuaron las correcciones correspondientes, el monto correcto es el que se considera para el análisis comparativo de las proposiciones.

III) Criterios para la evaluación de las propuestas:

Se consideró la revisión del cumplimiento documental de las propuestas, que consistieron en lo siguiente:

- Verificación del cumplimiento de las especificaciones técnicas requeridas mediante dictamen técnico emitido por **Ing. Esmeralda Olmos De La Cruz Coordinadora de Cómputo e Informática del Sistema de Educación Media Superior**.
- Cumplimiento de los requisitos documentales para el concursante.
- Condiciones de pago.
- Precio.
- Vigencia de la cotización.
- Garantías.
- Tiempo de entrega.

3.-PROPUESTAS RECHAZADAS

3.1.-Se rechaza la propuesta de la empresa **SODENET, S. DE R.L. DE C.V.,** debido a que se solicitan en la **SECCIÓN III** de las **BASES DE LA LICITACIÓN** los siguientes documentos:

Condiciones para el participante:

1. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando su estado actual de revendedor autorizado con mínimo nivel advanced.

2. El participante deberá incluir en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert
a. Al menos 1 NSE4
b. Al menos 1 NSE5
c. Al Menos 1 NSE7

.

Con base lo solicitado en las bases de la presente licitación, se observa que la empresa licitante de acuerdo a los documentos entregados, no presenta lo siguiente:

Carta expedida por el fabricante constando su estado actual de revendedor autorizado como mínimo nivel advanced y tampoco incluye en su propuesta carta original expedida por el fabricante constatando el personal certificado Network Security Expert.
a. Al menos 1 NSE4
b. Al menos 1 NSE5
c. Al Menos 1 NSE7

Con base a lo anterior, se rechaza la propuesta de la empresa **SODENET, S. DE R.L. DE C.V.,** con base a lo establecido en la **SECCIÓN I "INSTRUCCIONES A LOS LICITANTES", inciso "G" Motivos por los que puede ser desechada la propuesta,** numeral **29 Causas por las que puede ser desechada la propuesta.**

Inciso "A"

El incumplimiento de alguno de los requisitos establecidos en las presentes Bases de la licitación y sus anexos.

Inciso "D"

La falta de alguno de los requisitos o esté diferente a lo solicitado o incumpla lo acordado en el acta de la junta aclaratoria, en su caso.

Inciso "G"

Cuando no satisfagan cualquiera de los requisitos determinados en estas bases y sus anexos, y que no hayan sido detectados en el acto de presentación y apertura de propuestas.

4.- De conformidad con la revisión y evaluación de las propuestas, la Coordinación de Servicios Generales de Sistema de Educación Media Superior sugiere que la adjudicación sea de la siguiente manera:

Partida. **1, 2, 3**
Empresa: **INITEL, S.A. DE C.V.**
Por un monto total de **$21,901,549.82 (Veintiún millones novecientos un mil quinientos cuarenta y nueve pesos 82/100 m.n.), I.V.A. incluido.**

En virtud de haber reunido las condiciones legales, técnicas y económicas para garantizar satisfactoriamente el cumplimiento de las obligaciones respectivas y haber presentado la propuesta solvente más baja y con las mejores condiciones generales en cada una de las partidas, en apego a lo establecido en los artículos 24, 25, 45 y 47 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

ELABORÓ

MTRA. ROSAURA RODRÍGUEZ RODRÍGUEZ
JEFA DE LA UNIDAD DE ADQUISICIONES
DEL SEMS

AUTORIZÓ

ING. FERNANDO CALVILLO VARGAS
COORDINADOR DE SERVICIOS
GENERALES DEL SEMS

ACTA DE FALLO

LICITACION: LI-SEMS-009-2021
DEPENDENCIA: SISTEMA DE EDUCACION MEDIA SUPERIOR
NOMBRE: ADQUISICIÓN DE PUNTOS DE ACCESO INALÁMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA.

En la Ciudad de Guadalajara, Jalisco siendo las **11:10 horas** del día **27 de octubre de 2021**, se reunieron en la sala de juntas de Dirección General del Sistema de Educación Media Superior, los integrantes del Comité de Adquisiciones para emitir el siguiente fallo.

El Lic. Jorge Navarro Peña, Presidente del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior con base en las atribuciones del Comité, contempladas en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, se llevó a cabo el análisis de los documentos presentados por la Coordinación de Servicios Generales del SEMS, e hizo saber que la adjudicación por Licitación Pública, corresponde a:

Partidas: **1, 2 y 3**
Empresa: **SOLUCIONES Y SERVICIOS INTEGRALES TELCO, S.A. DE C.V.**
Por un importe de **$12´158,977.56 (Doce millones ciento cincuenta y ocho mil novecientos setenta y siete pesos 56/100 m.n.) I.V.A. Incluido.**

En virtud de haber reunido las condiciones legales, técnicas y económicas para garantizar satisfactoriamente el cumplimiento de las obligaciones respectivas y haber presentado la propuesta solvente más baja en cada una de las partidas, en apego a lo establecido en los artículos 24, 25, 45 y 47., del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

Lic. Jorge Navarro Peña
Presidente del Comité de Compras
y Adquisiciones del SEMS

Mtro. Jesús Alberto Jiménez Herrera
Secretario Ejecutivo del Comité de Compras
y Adquisiciones SEMS

UNIVERSIDAD DE GUADALAJARA

Red Universitaria de Jalisco

CARATULA CONTRATO COMPRAVENTA

LAS PARTES

LA UNIVERSIDAD		EL VENDEDOR	
Nombre, denominación o razón social	Universidad de Guadalajara	**Nombre, denominación o razón social**	Soluciones y Servicios Integrales Telco, S.A. de C.V.
Representante	Mtra. María Guadalupe Cid Escobedo	**Acta Constitutiva**	Escritura pública No. 7,290 de fecha 26 de noviembre de 2007, ante la fe del Lic. Jorge Ramón Quiñones Ruiz, Notario Público Titular No. 18, de Zapopan, Jalisco.
Título	Apoderada	**Representante**	Oscar Alejandro Zetina Salazar
		Título	Administrador General Único
Documento que acredita las facultades	Escritura Pública No. 48,826 de fecha 12 de noviembre de 2019, otorgada ante la fe del Lic. Samuel Fernández Ávila, Notario Público No. 15 de Tlaquepaque, Jalisco	**Documento que acredita las facultades**	Escritura pública No. 103698 de fecha 02 de junio de 2020, ante la fe del Lic. Vidal González Durán Valencia, Notario Público No. 58, de Guadalajara, Jalisco.
		R.F.C.	SSI071203V58
		Clave Patronal I.M.S.S.	[redacted] 1
Domicilio	Avenida Juárez número 976, Zona Centro, Código Postal 44100, en Guadalajara, Jalisco	**Domicilio**	Calle Real Acueducto No. 240 Int. 61, Colonia Real Acueducto, Zapopan, Jalisco. C.P. 45116

OBJETO E IMPORTE

Denominación	Adquisición de puntos de acceso inalámbricos y nodos de red, para el Sistema de Educación Media Superior de la Universidad de Guadalajara.		
Clave	LI-SEMS-009-2021	**Procedimiento de Adjudicación**	Licitación
Dependencia responsable del seguimiento	Sistema de Educación Media Superior	**Dependencia o comité que adjudicó**	Comité de Compras y Adquisiciones del Sistema de Educación Media Superior
Cantidad a pagar	$12´158,977.56 IVA incluido	**Partidas**	1, 2 y 3
		Tipo de Recurso	☒ Estatal ☐ Federal
Forma de pago (periodicidad)	30% anticipo y 70% a contra entrega	**Fondo**	F-1.3.13.3, proyecto 259928, año 2021

PLAZO DE ENTREGA		INSTALACIÓN
Plazo de entrega	6 semanas naturales	☒ SI incluye instalación
A partir de	la firma del presente contrato	☐ NO incluye instalación

FIANZAS

☒	a) Fianza para garantizar la correcta aplicación de los recursos del anticipo, por el importe total de éste, la cual deberá ser cancelada solo con el consentimiento por escrito de LA UNIVERSIDAD, y que deberá ser entregada previo a la entrega de dicho anticipo.
☒	b) Fianza para garantizar el cabal cumplimiento de todas las obligaciones contenidas en el presente contrato, misma que se contratará por el 10% (diez por ciento) del valor total del presente, y que deberá ser entregada dentro de los tres días naturales siguientes a la firma del presente.
☐	c) Fianza para garantizar los defectos o vicios ocultos, la cual se contratará por la cantidad de 10% (diez por ciento) del valor total del presente contrato, la que contará con una duración de 1 (un) año a partir de la fecha en que LA UNIVERSIDAD reciba los bienes por escrito, y deberá ser cancelada solo con el consentimiento por escrito de LA UNIVERSIDAD, a la entrega del acta de recepción expedida por LA UNIVERSIDAD, y una vez entregada esta fianza, se procederá a la cancelación de las establecidas en los incisos a) y b), mediante el escrito que para tal efecto emita LA UNIVERSIDAD.
☐	d) Ninguna.

FIRMAS

Enteradas las partes del contenido y alcance, lo ratifican y firman en triplicado, de conformidad ante los testigos.

En la ciudad de Guadalajara, Jalisco		**Fecha**	29 de octubre de 2021
LA UNIVERSIDAD		**EL VENDEDOR**	
		[redacted] 2	
Representante	Mtra. María Guadalupe Cid Escobedo	**Representante**	Oscar Alejandro Zetina Salazar
Título	Apoderada	**Título**	Administrador General Único
TESTIGOS			
Nombre	Mtro. Jesús Alberto Jiménez Herrera	**Nombre**	Ing. Fernando Calvillo Vargas
Cargo	Secretario Administrativo del Sistema de Educación Media Superior	**Cargo**	Coordinador de Servicios Generales del Sistema de Educación Media Superior

CONTRATO DE COMPRAVENTA QUE CELEBRAN POR UNA PARTE **LA UNIVERSIDAD DE GUADALAJARA,** A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **LA UNIVERSIDAD,** Y POR LA OTRA PARTE, LA PERSONA CUYA DENOMINACIÓN APARECE EN LA CARATULA DEL PRESENTE CONTRATO, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **EL VENDEDOR,** DE ACUERDO A LAS SIGUIENTES:

DECLARACIONES:

Declara **LA UNIVERSIDAD**:

I. Que es un organismo público descentralizado del gobierno del Estado de Jalisco con autonomía, personalidad jurídica y patrimonio propios de conformidad con lo dispuesto en el artículo primero de su Ley Orgánica publicada por el Ejecutivo Estatal el día 15 de enero de 1994, en ejecución del Decreto número 15,319 del H. Congreso del Estado de Jalisco.

II. Que es atribución de la Universidad de Guadalajara, conforme a la fracción XI del artículo 6 de la Ley Orgánica, administrar su patrimonio.

III. Que el Rector General es la máxima autoridad ejecutiva de la Universidad, representante legal de la misma, de conformidad con el artículo 32 de la ley Orgánica de la Universidad.

IV. Que su representante cuenta con las facultades necesarias para suscribir el presente contrato, mismas que manifiesta no le han sido revocadas, modificadas o restringidas en sentido alguno.

Declara **EL VENDEDOR** bajo protesta de decir verdad:

I. Que tiene la capacidad jurídica para contratar y obligarse a suministrar los bienes adjudicados por **LA UNIVERSIDAD**.

II. Que conoce el contenido y los alcances del artículo29 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, y en su caso del artículo 50 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y que no se encuentra en alguno de los supuestos establecidos por el mismo.

Declaran las partes que han convenido celebrar el presente contrato, para lo cual se sujetan a lo establecido en las siguientes:

CLÁUSULAS:

PRIMERA.- Las partes acuerdan que el objeto del presente contrato es que **EL VENDEDOR** realice a favor de **LA UNIVERSIDAD** el suministro cuya denominación aparece en la carátula del mismo, y que se detalla en el documento que como Anexo "A" se acompaña al presente.

Al respecto **EL VENDEDOR** se sujetará conforme a las indicaciones que le dé **LA UNIVERSIDAD** y a lo establecido en el presente instrumento.

Todo aquello que **EL VENDEDOR** necesitará para lograr el cumplimiento de lo establecido en el presente, incluidos los costos de transportación de los bienes, será a su cargo exclusivamente, liberando en consecuencia a **LA UNIVERSIDAD** de cualquier reclamación que se intente en su contra por alguno de los conceptos antes señalados.

SEGUNDA.- LA UNIVERSIDAD se obliga a pagar a **EL VENDEDOR** por los conceptos amparados en el presente, la cantidad establecida en la carátula del presente.

LA UNIVERSIDAD pagará a **EL VENDEDOR** dicha cantidad conforme a lo establecido en la carátula del presente.

Por su parte **EL VENDEDOR** se compromete a entregar la factura correspondiente con los requisitos que las leyes fiscales establecen, y a su vez, asume cualquier obligación fiscal que se derive del presente contrato, sacando en paz y a salvo a **LA UNIVERSIDAD** de cualquier reclamación que al respecto se pudiera originar.

Adicionalmente las partes acuerdan que en el supuesto de que **EL VENDEDOR** no cumpla con alguna de sus obligaciones en los tiempos pactados o conforme a las características establecidas, el pago se verá retrasado en la misma proporción. Lo anterior independientemente de que **LA UNIVERSIDAD** decida continuar con el contrato o darlo por rescindido.

TERCERA.- EL VENDEDOR se obliga a realizar todas las gestiones necesarias y a tramitar a su cargo, todas las licencias, permisos, avisos, seguros aplicables, importaciones y demás autorizaciones en general que sean obligatorias y/o que se requieran, a fin de cumplir con lo establecido en el presente contrato.

EL VENDEDOR deberá pagar todas las multas debido a infracciones contempladas en las Leyes y/o Reglamentos aplicables al objeto del presente contrato, aún cuando no haya habido dolo o negligencia, liberando de cualquier responsabilidad a **LA UNIVERSIDAD**.

De igual forma **EL VENDEDOR** se obliga a tomar un seguro a su cargo y a favor de **LA UNIVERSIDAD**, para cubrir los riesgos derivados del presente, entre ellos los de responsabilidad civil, daños a terceros en sus bienes o personas etc., el cual deberá de estar vigente hasta el cumplimiento total de sus obligaciones plasmadas a su cargo en el presente, acordándose que en caso de no contar con dicho seguro, **EL VENDEDOR** será directamente responsable por dichos conceptos.

CUARTA.- EL VENDEDOR se compromete ante **LA UNIVERSIDAD** a entregar, y en su caso instalar, los bienes objeto del presente dentro del plazo señalado en la caratula del presente contrato, en la dependencia que **LA UNIVERSIDAD** designe. Al respecto queda establecido que **EL VENDEDOR** no podrá realizar entregas parciales y el plazo concedido es para realizar la entrega total de los bienes o servicios contratados.

En caso de retraso en el cumplimiento de lo establecido en el presente, por causas imputables a **EL VENDEDOR**, éste pagará a **LA UNIVERSIDAD** por concepto de pena el 1.5% de los bienes no entregados o instalados y de los servicios no realizados. Dicha cantidad se podrá deducir por **LA UNIVERSIDAD** de los pagos pendientes a su cargo y a favor de **EL VENDEDOR**.

Independientemente de la aplicación de la pena antes señalada **LA UNIVERSIDAD** podrá optar entre exigir el cumplimiento forzoso de las obligaciones del presente contrato, o darlo por rescindido.

Por causas justificadas y debidamente acreditadas a **LA UNIVERSIDAD**, la misma podrá, si lo considera conveniente, ampliar previa petición por escrito de **EL VENDEDOR**, el plazo de entrega contemplado en la presente cláusula y en cuyo caso deberá suscribirse un convenio modificatorio y deberá actualizarse la fianza correspondiente por parte de **EL VENDEDOR**, misma que se entregará a **LA UNIVERSIDAD** a la firma del convenio modificatorio.

QUINTA.- EL VENDEDOR queda obligado a realizar todo lo establecido en el presente de acuerdo a lo estipulado por las partes, para lo cual se responsabiliza hasta el cumplimiento de todas sus obligaciones.

SEXTA.- EL VENDEDOR dará aviso por escrito a **LA UNIVERSIDAD** cuando concluya con las obligaciones pactadas a su cargo en el presente, para que ésta última proceda a levantar un acta de entrega recepción por conducto de quien la misma señale.

SÉPTIMA.- Las partes acuerdan que **EL VENDEDOR** tiene prohibido:

a) Encomendar o subcontratar con otra persona la entrega o instalación de los bienes objeto del presente contrato, así como la cesión total o parcial de los derechos y obligaciones del mismo.
b) En su caso, hacer cambios estructurales en la o las instalaciones en donde se colocarán los bienes objeto del presente, sin la previa autorización por escrito de **LA UNIVERSIDAD,** estableciendo que en caso de no respetar lo antes señalado, **EL VENDEDOR** será responsable de los daños y perjuicios y la responsabilidad civil que dicho incumplimiento cause, lo anterior independientemente de la rescisión o cumplimiento forzoso del contrato.

OCTAVA.- EL VENDEDOR en tanto no se levante el acta de entrega recepción correspondiente, reconoce que **LA UNIVERSIDAD** no será responsable de la perdida (total o parcial), deterioro o maltrato de los bienes, materiales, herramientas o cualquier otro bien relacionado con el objeto del presente, ni aun en el supuesto de caso fortuito o fuerza mayor, ya que los mismos son responsabilidad directa de **EL VENDEDOR**, liberando a **LA UNIVERSIDAD** de cualquier responsabilidad que se pudiera derivar del presente concepto.

NOVENA.- Los servicios de entrega o, en su caso, de instalación de los bienes materia del presente contrato se ejecutarán durante días y horas hábiles de la o las dependencias universitarias en las cuales se entregarán los bienes materia del presente, acordando las partes que en caso de ser necesario realizar trabajos durante horas y días inhábiles, los mismos podrán llevarse a cabo, previa autorización por escrito que al efecto expida **LA UNIVERSIDAD**.

DÉCIMA.- La supervisión de lo establecido en el presente, estará a cargo de la Coordinación de Servicios Generales de la dependencia responsable o de la persona o las personas que esta última designe, quienes podrán inspeccionar en todo tiempo todo lo relacionado con los bienes, pudiendo en su caso, rechazar por escrito lo que no se ajuste a lo estipulado en el contrato y su Anexo "A".

Al respecto **EL VENDEDOR** se compromete a entregar los bienes nuevos y de primera calidad, según se establece en las especificaciones técnicas, siendo responsable de los daños y perjuicios, y la responsabilidad civil, que cause debido a la mala calidad de los mismos.

De existir inconformidad respecto a lo contemplado en esta cláusula, **LA UNIVERSIDAD** solicitará a **EL VENDEDOR** reemplazar a costa de esta última, los bienes defectuosos o no adecuados.

DÉCIMA PRIMERA.- EL VENDEDOR además de observar el cumplimiento de este contrato, estará obligado a lo siguiente:

a) Vigilar que el objeto del presente contrato sea de acuerdo a lo aprobado, y a las características especificaciones requeridas.
b) En su caso hacer la revisión detallada de la instalación de los bienes, rindiendo el informe correspondiente.
c) Tener en todo momento personal técnico capacitado para la dirección, supervisión e instalación y demás actividades relacionadas con el objeto materia de este contrato.
d) Estar al corriente de todas las contribuciones que se originen por el desempeño de su actividad.
e) Responder de la perdida, daño, robo o extravío de los bienes, hasta el momento en que se realice el acta de entrega recepción correspondiente, aún en el supuesto de que dichos bienes se encuentren en las instalaciones de **LA UNIVERSIDAD.**
f) Cumplir con todas las obligaciones derivadas de la ley, del presente y su Anexo "A".

DÉCIMA SEGUNDA.- LA UNIVERSIDAD podrá dar por terminado anticipadamente en cualquier momento el presente contrato, cuando concurran circunstancias imprevistas o razones de interés general, previa notificación por escrito a **EL VENDEDOR** con cuando menos 5 (cinco) días naturales de anticipación.

Adicionalmente, acuerdan las partes que **LA UNIVERSIDAD** podrá suspender los trabajos y/o pagos objeto del presente, en caso de que se presente alguno de los supuestos que a continuación se mencionan de manera enunciativa mas no limitativa:

a) En su caso cuando existan bienes y/o trabajos defectuosos o no adecuados, que no se reemplacen o corrijan, dentro de los 30 (treinta) días siguientes a la fecha en que **LA UNIVERSIDAD** lo haga del conocimiento de **EL VENDEDOR**.
b) Incumplimiento de **EL VENDEDOR** por no estar al corriente en el pago de las contribuciones que se generen por su operación o el pago de sus obligaciones directas e indirectas con su personal.

c) Por presentación de reclamación de cualquier naturaleza, si se llegara a formalizar, en contra de **LA UNIVERSIDAD** derivada del objeto del presente contrato.
d) Si **EL VENDEDOR** no entrega las fianzas a que se hace referencia en el presente contrato, dentro de los términos establecidos para tal efecto.
e) Si **EL VENDEDOR** cayera en insolvencia o se declara en concurso mercantil.
f) Por muerte o disolución de **EL VENDEDOR**, según corresponda.
g) En general por cualquier incumplimiento por parte de **EL VENDEDOR** a cualquiera de las obligaciones derivadas del presente contrato, su anexo o la ley.

A juicio de **LA UNIVERSIDAD** y una vez que se subsanen los problemas a que se refieren los incisos anteriores, se podrán reanudar los efectos y/o pagos o rescindir el presente contrato.

DÉCIMA TERCERA.- En caso de que se presente algún defecto o vicio oculto relacionado con el objeto del presente contrato, **EL VENDEDOR** será la responsable ante **LA UNIVERSIDAD** por los mismos.

DÉCIMA CUARTA.- La entrega, y en su caso instalación, de los bienes detallados en el presente contrato y su Anexo "A" deberá quedar terminada en el plazo que se consigna en la carátula del presente.

El plazo de terminación del presente instrumento solo podrá ser ampliado en caso de que haya modificaciones en lo establecido en el objeto del presente contrato, en caso fortuito o de fuerza mayor de conformidad a la ley o por mutuo acuerdo.

Para que el objeto del presente instrumento se pueda considerar como satisfecho se deberá haber cumplido con lo establecido en el contrato y su Anexo "A".

DÉCIMA QUINTA.- Las partes convienen en que **EL VENDEDOR** se compromete a cumplir con todas y cada una de las obligaciones derivadas de la relación laboral que imponen la Ley Federal del Trabajo, y demás ordenamientos legales aplicables a los patrones; por lo tanto **EL VENDEDOR** será el único responsable y obligado para con los trabajadores, ante todo tipo de autoridades ya sean administrativas o judiciales, Federales, Estatales o Municipales.

En consecuencia, **EL VENDEDOR** asume todas las responsabilidades como patrón con relación a los trabajadores que emplee, liberando de posibles indemnizaciones, demandas o cualquier reclamación que éstos iniciaran en contra de **LA UNIVERSIDAD**.

LA UNIVERSIDAD, no será responsable por ninguna reclamación que en contra de **EL VENDEDOR** presenten sus empleados o colaboradores, obligándose ésta última a sacar en paz y a salvo a **LA UNIVERSIDAD** de cualquier reclamación de esta naturaleza, ya sea laboral, administrativa, civil o penal, incluyéndose los accidentes de trabajo.

Asimismo, será obligación de **EL VENDEDOR** hacer la retención y entero de las contribuciones correspondientes de los trabajadores que emplee con motivo del presente contrato.

DÉCIMA SEXTA.- EL VENDEDOR otorgará a favor de **LA UNIVERSIDAD** las fianzas descritas en la carátula del presente contrato, expedidas por una compañía legalmente constituida y registrada, con oficinas en la ciudad de Guadalajara, Jalisco, y que se sujeten a la jurisdicción de los tribunales competentes de esta ciudad.

Adicionalmente **EL VENDEDOR** manifiesta expresamente lo siguiente:

(A) Su conformidad para que la fianza de cumplimiento se pague independientemente de que se interponga cualquier tipo de recurso ante instancias del orden administrativo o no judicial.
(B) Su conformidad para que la fianza que garantiza el cumplimiento del contrato, permanezca vigente durante la substanciación de todos los procedimientos judiciales o arbitrales y los respectivos recursos que se interpongan con relación al presente contrato, hasta que sea dictada resolución definitiva que cause ejecutoria por parte de la autoridad o tribunal competente.
(C) Su aceptación para que la fianza de cumplimiento permanezca vigente hasta que las obligaciones garantizadas hayan sido cumplidas en su totalidad a satisfacción de **LA UNIVERSIDAD**.

DÉCIMA SÉPTIMA.- Además de las causas previstas por la Ley, las partes convienen en que el presente contrato podrá ser rescindido por **LA UNIVERSIDAD** cuando **EL VENDEDOR** no haya cumplido con todas o alguna de las obligaciones que a su cargo se derivan de éste contrato, en especial si la entrega o instalación no cumple con las características pactadas.

Serán causas de rescisión del presente contrato las que a continuación se mencionan enunciativamente más no limitativamente:

a) Si **EL VENDEDOR,** por causas imputables a ella o a sus dependientes, no entrega los bienes, según lo acorado en el contrato y su anexo.
b) Si **EL VENDEDOR,** en su caso, no entrega los trabajos contratados totalmente terminados dentro del plazo señalado en el presente contrato y su anexo.
c) Si **EL VENDEDOR,** en su caso, suspende injustificadamente los trabajos objeto del presente o se niega a reparar o responder alguno que hubiere sido rechazado por **LA UNIVERSIDAD,** en un término de 30 (treinta) días.
d) Si **EL VENDEDOR** cayera en insolvencia o se declara en concurso mercantil.
e) Por muerte o disolución de **EL VENDEDOR**, según sea el caso.
f) En general por cualquier incumplimiento por parte de **EL VENDEDOR** a cualquiera de las obligaciones derivadas del presente contrato, su anexo o la ley.

En caso de incumplimiento por parte de **EL VENDEDOR** en cualquiera de las obligaciones previstas en este contrato **LA UNIVERSIDAD** podrá rescindir el contrato o exigir el cumplimiento del mismo.

Si **LA UNIVERSIDAD** opta por rescindir el contrato por causa imputable a **EL VENDEDOR,** está última, quedará obligada a cubrir los daños y perjuicios que por tal motivo ocasione a **LA UNIVERSIDAD,** los cuales no podrán ser inferiores al 20% (veinte por ciento) del monto total del presente instrumento.

DÉCIMA OCTAVA.- Acuerdan las partes que en caso de que el presente contrato incluya mantenimiento preventivo, mantenimiento correctivo y/o capacitación, las actividades relacionadas con los mismos se realizarán conforme lo determinen las partes.

DÉCIMA NOVENA.- Queda establecido que **EL VENDEDOR** no podrá ceder o transferir parcial o totalmente los derechos y las obligaciones derivadas del presente instrumento, sin el previo consentimiento por escrito de **LA UNIVERSIDAD,** siendo responsable de los daños y perjuicios que tal incumplimiento cause.

VIGÉSIMA.- Nada de lo previsto en este contrato ni de las acciones que se deriven de su suscripción, podrá considerarse o interpretarse para constituir o considerar a las partes y al personal de las mismas que colabore en la ejecución de este contrato como socios, agentes, representantes o empleados uno del otro, y ninguna de las disposiciones de este contrato será interpretada para forzar a la otra parte a asumir cualquier obligación o a actuar o pretender actuar como representante de la otra.

VIGÉSIMA PRIMERA.- El presente contrato, podrá ser modificado previo acuerdo por escrito entre las partes y durante la vigencia del mismo, apegándose a la normatividad aplicable, y a través de los instrumentos jurídicos correspondientes, obligándose las partes a las nuevas estipulaciones, a partir de la fecha de su firma.

VIGÉSIMA SEGUNDA.- Si alguna de las disposiciones contenidas en el presente contrato, llegara a declararse nula por alguna autoridad, tal situación no afectará la validez y exigibilidad del resto de las disposiciones establecidas en este contrato. Al respecto las partes negociarán de buena fe la sustitución o modificación mutuamente satisfactoria de la cláusula o cláusulas declaradas nulas o inválidas por otras en términos similares y eficaces.

En caso de que el presente contrato llegara a declararse nulo por la autoridad competente o el mismo se rescindiera por causa imputable a **EL VENDEDOR**, el mismo estará obligado a devolver a **LA UNIVERSIDAD** la o las cantidades que le hayan sido entregadas, más la actualización correspondiente conforme al Índice Nacional de Precios al Consumidor, tomando como base la fecha en que se realizó la primera entrega por parte de **LA UNIVERSIDAD** y la fecha en que sean devueltas las mismas, lo anterior independientemente de los daños y perjuicios que por tal motivo tenga derecho a reclamar a **LA UNIVERSIDAD**.

VIGÉSIMA TERCERA.- EL VENDEDOR se obliga a que los bienes serán nuevos y de la calidad señalada en las especificaciones del Anexo "A", y responderá por cualquier defecto en cualquiera de las partes de los bienes y accesorios objeto del presente, o por la instalación y puesta en marcha de los mismos.

La garantía está sujeta a que los bienes sean utilizados de acuerdo a las especificaciones y características de estos.

VIGÉSIMA CUARTA.- Ambas partes acuerdan que cualquier controversia relacionada con la interpretación, contenido o ejecución del presente contrato, se sujetará a lo establecido en el presente contrato y de manera supletoria a lo establecido en los documentos señalados a continuación y en el orden siguiente; en el anexo, las bases del procedimiento correspondiente, la propuesta presentada por **EL VENDEDOR**, la legislación federal, la universitaria y demás leyes aplicables.

En este sentido queda establecido que si existe alguna discrepancia en la información contenida en alguno de los documentos señalados en el párrafo anterior, siempre será aplicable la disposición que sea más favorable para **LA UNIVERSIDAD,** quedando sin efectos la disposición distinta.

VIGÉSIMA QUINTA.- Para todo lo relacionado con la interpretación y cumplimiento del presente contrato, las partes se someten voluntariamente a las leyes aplicables de la República Méxicana y a la jurisdicción y competencia de las autoridades de la ciudad de Guadalajara, Jalisco, renunciando a cualquier otro fuero o jurisdicción que pudiera corresponderles en virtud de su domicilio presente o futuro.

Las partes enteradas del contenido y alcance del presente contrato, manifiestan que en el mismo no existe mala fe, dolo o error y firman por triplicado en la carátula del mismo, en compañía de los testigos, en la ciudad de Guadalajara, Jalisco.

ANEXO "A"

Soluciones Telco

SECCIÓN VI - PROPUESTA ECONÓMICA

Guadalajara, Jalisco, a miércoles 13 de Octubre del 2021
Licitación Pública No. LI-SEMS-009-2021

Secretario Ejecutivo del Comité de Compras y Adquisiciones del Sistema de Educación Media Superior
Universidad de Guadalajara

PRESENTE:

PROPUESTA ECONÓMICA: Licitación número **LI-SEMS-009-2021**, para la **ADQUISICIÓN DE PUNTOS DE ACCESO INHALAMBRICOS Y NODOS DE RED, PARA EL SISTEMA DE EDUCACIÓN MEDIA SUPERIOR DE LA UNIVERSIDAD DE GUADALAJARA**.

PARTIDA	CANTIDAD	DESCRIPCIÓN TÉCNICA COTIZADA EN PROPUESTA ECONÓMICA	PRECIO UNITARIO	IMPORTE
1	203	Punto de acceso inalámbrico "tipo A" Marca Cisco Meraki Modelo MR36-HW Meraki MR36 Wi-Fi 6 Indoor AP El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, es una solución basada en el estándar IEEE 802.11ax para 5Ghz y 2.4Ghz que permite habilitar el acceso de red para los usuarios en general paradispositivos móviles (tablets, smartphones, laptops), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, se contemplan como mínimo las siguientes funcionalidades: • Operación de banda dual en 2.4 y 5Ghz, concurrente • Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet • Conexión a la red alámbrica en 1000BaseT • Firewall para bloqueo de tráfico capa 3 y capa 7 a nivel del punto de acceso, con la capacidad de identificar aplicaciones específicas • Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio. • Prevención de Intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación medianteun tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para el servicio de los clientes inalámbricos. Capacidad de integrarse al servicio de Umbrella para protección inalámbrica a nivel de DNS que prevenga el acceso asitios y dominios maliciosos, al igual que la capacidad de filtrar contenido basado en categorías (Requierelicencia de Umbrella). **Administración** • Gestión centralizada desde una consola de administración basada en Web, desde la cual se puede acceder,	$33,311.04	$6,762,141.12

SEMS
SECRETARÍA ADMINISTRATIVA

000056

BAJO PROTESTA DE DECIR VERDAD

[redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

configurar y monitorear todos los equipos de LAN o WLAN considerados en esta licitación

- De igual manera, desde la misma consola de administración basada en Web, se pueden generar los reportes de operación correspondientes a todos los equipos de LAN o WLAN objeto de esta licitación
- La consola es accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la Universidad de Guadalajara, soportando cualquier navegador moderno de Internet disponible
- Hay mecanismos que limiten el acceso a la consola, basado en la definición de direcciones IP públicas autorizadas
- El acceso a la consola de administración se realiza mediante un método de autenticación de dos factores (two-factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola de gestión soporta la integración con repositorios de identidad externos via SAML para un Single Sign On (SSO).
- El acceso a la consola de gestión es por HTTPS (puertos 8080 y 443) y sus certificados de seguridad son emitidos por entidades reconocidas en Internet
- La consola de administración soporta la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola
- La consola reportará sobre intentos de logins al sistema, mostrando qué cuenta intentó entrar, dirección IP, locación, estatus del intento y la hora y fecha del intento
- El sistema de gestión centralizado da la opción de empujar nuevo firmware a los AP's, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad
- El nivel jerárquico de los administradores de la consola es los siguientes:

o Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todos los contenedores (colección de dispositivos de red) dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura.

o El administrador con acceso completo (full access) podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenece:

- Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
- Resetear contraseñas
- Crear, editar y borrar redes
- Agregar nuevos dispositivos a las redes de la organización

o Administrador de Contenedor: Tendrá visibilidad en aquellas contenedores de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de contenedor podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:

- Crear, editar y borrar otras cuentas

SECRETARÍA ADMINISTRATIVA

000057

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

de administrador dentro del contenedor Crear, editar y borrar contenedores para las cuales cuente con privilegios

Características físicas y eléctricas de los equipos Puntos de acceso de red inalámbrica

Antenas integradas al interior del equipo del tipo omnidireccional

- Alimentación PoE de 37 – 57 V, compatible con IEEE 802.3af ó IEEE 802.3at, asegurando que la alimentación requerida por el equipo, asegure su operación a carga máxima
- Soporte de alimentación con eliminador de DC externo
- Consumo máximo de potencia de 15W
- Capacidad para energizarse vía eliminador de corriente directa
- Incluye tornillo de seguridad, así como bahía para candado Kensington
- Placa para montaje en pared

Servicios de Red

El equipo propuesto cuenta con los siguientes servicios de red:

- Interfaz de Radio Frecuencia:
  - Un radio a 2.4GHz 802.11b/g/n/ax y uno a 5GHz 802.11a/n/ac/ax
  - Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas
  - Que incluya embebido o agregado al AP un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades demonitoreo de entrada y salida de dispositivos que emitan beacons, mandando alertas de estos eventos.
  - Soporte de Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350Ghz (UNII- 2), 5.470- 5.600, 5.660-5.725 (UNII-2e) y 5.725-5.825GHz (UNII-3)
  - Arreglo de Antenas integradas al chasis del tipo omnidireccional con ganancia de 5.4dBi@2.4GHz y 6dBi@5GHz
  - Arreglo MU-MIMO 2x2 con dos tramas espaciales (spatial streams)
  - La solución cuenta con la funcionalidad de selección de la banda de operación por cada SSID:CCC

Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz
5GHz únicamente
Ambas bandas pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada

  - Ancho de banda de canales de 20, 40MHz y 80MHz
  - Tasa de datos combinada de 1.7Gbps
  - Certificado para especificación 802.11ax DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, 1024-QAM
  - Soporte de Maximal Ratio Combining (MRC)
  - Formación de haz (beamforming)
  - Agregación de paquetes
  - Soporte a Cyclic Shift Diversity (CSD)
- Interfaz alámbrica de red:

SECRETARÍA ADMINISTRATIVA

000058

BAJO PROTESTA DE DECIR VERDAD

[redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

- Una interfaz 10/100/1000Base-T Ethernet (RJ-45) con soporte de 802.3at para PoE
- VLAN tagging basado en IEEE802.1q
- Cada Access Point soporta los siguientes esquemas de direccionamiento IP:

Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrardirecciones IP privadas de la red local, o prescindir de un servidor DHCP

Modo Bridge, donde el Access Point relevan los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN

Roaming de capa 3 (L3), que permite al usuario mantener la misma dirección IP en caso de cambio de segmentode red, manteniendo la sesión activa todo el tiempo

Túnel VPN con IPSEC hacia un concentrador central, para el caso en que se requiera habilitar esquemas detrabajador remoto y oficina remota como si se encontraran en la oficina principal

- Calidad de Servicio:
  - Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
  - Soporte de DSCP 802.1p
  - Modelado de tráfico a nivel de capa 7 (L7)

Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se soporta la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.

La asignación de ancho de banda mediante el modelado de tráfico, puedese definir mediante dos mecanismos:

- Manual
  - Rangos CIDR/IP
  - hostname (URL)
  - Puertos UDP/TCP
  - Combinación de Red,Subnet y puerto
  - Red local (subredes y redes de clase completa en la LAN)
- Mediante categorías de tráfico
  - Blogging
  - Email
  - Compartición de archivos
  - Juegos
  - Noticias
  - Respaldo en línea
  - Peer-to-peer
  - Redes sociales y compartición de fotos
  - Actualizaciones de programas y antivirus
  - Deportes
  - VoIP y videoconferencia
  - Compartición de archivos vía web
- La política de modelado de tráfico permite la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios
- De igual manera, mediante la política de modelado de tráfico puede priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz) **Servicios de seguridad**

SECRETARÍA ADMINISTRATIVA

000059

BAJO PROTESTA DE DECIR VERDAD

[redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

La solución de Red Inalámbrica incluye las siguientes funcionalidades de seguridad:

a) Firewall

a. La solución inalámbrica de red soporta la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.

ii. Mediante las reglas de capa 3, se definirán políticas de acceso por:

1. Protocolo (UDP o TCP)
2. Host, subred o red origen
3. Puerto TCP o UDP origen
4. Host, subred o red destino
5. Puerto TCP o UDP destino

iii. Mediante las reglas de capa 7, se soporta la restricción de tráfico a partir de categorías definidas, entre ellas:

1. Blogging
2. Email
3. Compartición de archivos
4. Juegos
5. Noticias
6. Respaldo en línea
7. Peer-to-peer
8. Redes sociales y compartición de fotos
9. Actualizaciones de programas y antivirus
10. Deportes
11. VoIP y videoconferencia
12. Compartición de archivos vía web

b. Políticas basadas en identidad

i. La solución propuesta permite la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de Radius de la [INSTITUCIÓN]

c. Políticas basadas en grupos

iii. Políticas de firewall específicas para grupos está soportada por la solución propuesta.

iv. Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bienpodrán descargarse la información de grupos declarados en el controlador de dominio de la red interna

d. Control de acceso a la red inalámbrica: La solución soporta la creación de 15 SSIDs como máximo,permitiendo para cada uno los siguientes métodos de acceso:

v. Abierta y sin encripción para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo

vi. Llave compartida con anterioridad (Pre-Shared key) con WPA2, WPA3-Transition Mode y WPA3-Personal

vii. Control de acceso basado en dirección MAC mediante autenticación Radius

viii. WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:

1. Un servidor RADIUS incluido en la misma solución
2. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
3. Modalidad de sobrevivencia, en caso de que se pierda

SECRETARÍA ADMINISTRATIVA

090000

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales

vi. WPA3-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:

1. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
2. El servidor de RADIUS utiliza uno de los siguientes tipos de cifrado EAP
   a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales

viii. Capacidad para definir hasta 50 claves pre-compartidas de identidad (IPSK) para autenticar usuarios con servicios diferenciados dentro de una misma SSID sin tener que depender de un servidor de RADIUS o autenticación 802.1X

ix. Acceso vía portal cautivo (splash page), que permite habilitar los siguientes métodos de autenticación, conforme lo requiera la Universidad de Guadalajara

1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario
2. Portal "Click-through", donde el usuario se ve un portal de bienvenida y dar "click" a un botón para continuar su acceso
3. Portal captivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
   a. Un servidor RADIUS interno a la solución propuesta
   b. Un servidor RADIUS externo hosteado en alguna localidad de la Universidad de Guadalajara
   c. Autenticación hacia una base de datos de Directorio Activo de la Universidad de Guadalajara
   d. Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página oficial de la Universidad de Guadalajara en dicha red social

xi. Con excepción de la autenticación portal captivo es personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.

xii. De igual manera, se cuenta con la funcionalidad de Walled Garden, que permite el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente

xiii. De acuerdo a lo que requiera la Universidad de Guadalajara, la solución permite o bloquear el tráfico no-HTTP

b) Control de acceso a la red (Network Access Control)

a. La solución cuenta con la opción de verificación de la presencia de un software para la detección de antivirus actualizado

SECRETARÍA ADMINISTRATIVA

190000

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

en el dispositivo de usuario, previo a su autenticación a la red

c) Asignación de políticas de acceso por tipo de dispositivo

a. De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso

d) Filtrado de Contenido

a. La solución incluye en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos, sin requerir para tal efecto añadir una solución de seguridad externa

e) Detección y Prevención de Intrusos en el Canal Inalámbrico

a. La solución de red inalámbrica, cuenta con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:

vi. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz

vii. Descarga desde la consola central las últimas actualizaciones en firmas de ataques

viii. Habilita políticas de detección y remediación granulares sobre la misma consola de gestión de la solución

ix. El WIPS está basado en un motor heurístico que permite detectar los ataques más sofisticados, mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de desasociación e identificar las variantes a partir del comportamiento normal

x. Identifica y organizar las siguientes categorías de ataques como mínimo:

1. SSIDs no autorizados
2. Intentos de robo de identidad (spoofs) del AP
3. Inundación de paquetes que tengan como finalidad generar eventos de negación de servicio (DoS)

viii. Para efectos de remediar los ataques, la solución permite la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID

ix. Notifica de eventos de seguridad a los administradores de la red por medio de correo electrónico

Reportes y monitoreo

- Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución incluye dentro de la misma consola de gestión un inventario de equipo tanto operativo como desconectado, accesible para los administradores de la red
- Se puede cargar los planos de las ubicaciones en donde se desplieguen los AP, así como la alineación a Google Maps, con el propósito de tener la ubicación de cada AP bien definido.
- La solución cuenta con una aplicación móvil que facilite el monitoreo de los AP's desplegados, así como la capacidad de tomar fotos de cada AP montado para que se refleje en la plataforma de gestión fija.
- La solución puede mostrar diagnósticos de salud desde el punto de vista del cliente, permitiendo hacer "drill-down" en un cliente específico y obtener información sobre la salud del mismo

o Indicación gráfica de la salud de la conexión entre el cliente y su Access Point, con la tasa de transferencia negociada y la tasa de datos en transferencia en ese instante de tiempo

SECRETARÍA ADMINISTRATIVA

000062

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

- Indicación gráfica de la salud del Access Point, con desglose de utilización de canal, carga actual de clientes y utlización en el canal actual del cliente

- Capacidad de lanzar una captura de paquetes filtrada para el cliente desde ese Access Point
- Indicación de la calidad de la conexión de ese Access Point a su switch de acceso, mostrando el estatus del puerto, problemas de conectividad, exceso de broadcast/multicast/unknown unicast, y problemas de negociación
- Indicación de problemas de salud en el switch de acceso, desglosados por problemas de DNS, RADIUS, OSPF o host capa 3
- Pestaña de Conexiones de cliente con las estadísticas y el desglose de los problemas de conectividad inalámbrica experimentados por el cliente desglosados en las etapas de Asociación, Autenticación, DHCP y DNS
- Rendimiento del cliente representado de forma gráfica que permite obtener métricas de rendimiento del mismo desglosadas en
  - Gráfico de utilización histórica por aplicación, superpuesta con eventos de conexión del cliente como asociaciones, autenticaciones por RADIUS/802.1X, o roaming
  - Gráfico de calidad de señal histórica percibida por el cliente, superpuesta con los eventos de conectividad delmismo
  - Gráfico de latencia promedio histórica experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
  - Gráfico de utilización de canal experimentada por el cliente, superpuesta con los eventos de conectividad delmismo
  - Gráfico de utilización del Access Point al que el cliente está asociado, superpuesta con los eventos de conectividad del mismo
  - Gráfico de cantidad de clientes asociados al Access Point en el que se encuentra el cliente, superpuesto con los eventos de conectividad del mismo
  - Gráfico de tasas de datos del cliente negociadas con cada uno de los Access Points por los que se ha movido
- Historial de conectividad del cliente que desglose todos los movimientos del mismo y que sea filtrable por SSID, Access Point, Banda, Etapa de Fallo, Severidad de Fallo
  - La herramienta podrá aportar sugerencias de cómo solucionar ciertos problemas encontrados por el cliente y su posible causa raíz
- La solución muestra diagnósticos de salud desde el punto de vista del Access Point ofreciendo
- Información de salud de resumen desde el punto de vista del Access Point, indicando porcentualmente la cantidad de conexiones exitosas, fallidas y problemáticas, y desglosando las fallas en problemas de Asociación, Autenticación, DHCP y DNS
- Historial de rendimiento del Access Point, desglosado en
  Gráfico de utilización superpuesto con eventos de cambio de canal e intensidad de potencia
  Gráfico de cantidad de clientes asociados superpuesto con eventos de cambio de canal e intensidad de potencia Calidad de señal histórica promedio superpuesta con eventos de cambio de canal e intensidad de potencia Latencia inalámbrica promedio superpuesta con eventos de cambio de canal e intensidad de potencia

SECRETARÍA ADMINISTRATIVA

c90000

BAJO PROTESTA DE DECIR VERDAD [redacted] 2

Soluciones Telco

		• La solución puede mostrar información de diagnósticos globales sobre el rendimiento de la red inalámbrica ofreciendo los siguientes reportes de manera gráfica o Salud por Access Point, indicando con código de colores de semáforo (verde, amarillo, rojo) los Access Points enun mapa para ilustrar gráficamente problemas de salud o Listado de Access Points con mayor porcentaje de problemas de conectividad o Desglose de salud por tipo de dispositivo, indicando por sistema operativo los problemas de conectividad observados en la red o Conexiones fallidas desglosadas por porcentaje y tipo de fallo Fallos en Asociación Fallos en Autenticación Fallos en DHCP Fallos en DNS o Capacidad de hacer "drill-down" por tipo de fallo para ver todos los eventos relacionados al tipo de fallo porSSID, por Access Point y por Red o Desglose de latencia de paquetes por tipo de tráfico, ofreciendo las métricas de rendimiento histórico para Tráfico de Voz		

SECRETARÍA ADMINISTRATIVA

000064

BAJO PROTESTA DE DECIR VERDAD

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

Tráfico de Video Tráfico Best Effort Tráfico Background

- Capacidad para extraer toda esta información por medio de APIs para graficar en Dashboards personalizados
- La solución genera sobre demanda un reporte ejecutivo por la último día, la última semana, el último mes y sobre un período especifico de monitoreo, incluyendo los siguientes parámetros:
  - Utilización total de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos

SECRETARÍA ADMINISTRATIVA

000065

BAJO PROTESTA DE DECIR VERDAD [redacted] 2

durante el tiempo especificado

- Los Top 50 Access Points del sistema por utilización
- Los SSID's con mayor consumo
- Conteo individual de clientes durante el período seleccionado y por día
- Los Top 50 usuarios por utilización
- Las Top 50 aplicaciones con mayor presencia en la red
- Los Top 50 dispositivos por fabricante
- Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red

• Proporciona a los administradores con una lista de bitácoras de eventos y de cambios en la configuración.

• Cuentase de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación.

• Finalmente, la solución contabiliza y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo:

- Dispositivos que pasaron dentro del área de cobertura pero permanecieron un intervalo de tiempo pequeño
- Dispositivos que aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura
- Dispositivos que finalmente se conectaron a la red
- Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente
- Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales

Analíticos de ubicación de dispositivos

• La solución inalámbrica de red está equipada con la habilidad de detectar la presencia del dispositivo de usuario, basado en la información contenida en los mensajes de "probe request" generados por los radios WiFi encendidos en smartphones, laptops y tabletas.

• Con la información recabada, la controladora en la nube consolida analíticos históricos de los dispositivos WiFi, con graficas intuitivas y personalizables, facilitando la interpretación de tendencias tales como:

- Flujo de paseantes por día y hora
- Lealtad de usuarios basado en visitantes nuevos y repetidos
- Tiempo de permanencia de visitantes en la zona de cobertura

• La información de presencia, está disponible para su exportación a un sistema externo, que incluya:

- Dirección MAC del AP que reporta
- Dirección MAC del dispositivo de usuario
- Intensidad de señal recibida (RSSI) con la cual fue escuchado el dispositivo
- Estampa de tiempo
- Coordenadas X y Y de la ubicación del dispositivo, de acuerdo a la información entregada por todos los APs del sistema

Inyector de Energía a través de cable Ethernet (PoE)

Los puntos de acceso tipo A, incluyen un inyector de energía a través de cable Ethernet (PoE) que opera con un voltaje de entrada de entre 100 a 240 Volts de corriente alterna, proporcionar un voltaje de salida de 55V de corriente directa, potencia de salida de 30W acorde al estandar IEEE

SECRETARÍA ADMINISTRATIVA

BAJO PROTESTA DE DECIR VERDAD

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

		802.3at y es compatible con Ethernet 10/100/1000 Mbits/s full duplex. **Licenciamiento, Garantías y soporte** • Incluye todo el licenciamiento necesario para su correcto funcionamiento por lo menos durante 7 años. • Garantía de por vida en hardware de interiores. • Soporte técnico telefónico en español 24x7x365. • Tickets de soporte podrán ser abierto mediante la misma plataforma de gestión. • Reemplazo de partes de siguiente día hábil. • Esta garantía y soporte estará vigente por 7 años.		
2	223	Nodo de red CAT6 60 MTS Panduit TX6000™ Enhanced Category 6 U/UTP Copper Cable Panduit TX6-28™ Category 6 Performance 28 AWG UTP Patch Cords Panduit Mini-Com® Executive Series Faceplates Linkedpro Gabinete con Puerta Ventilada para Montaje en Pared Cuerpo Fijo con Rack 19" de 12 Unidades. Panduit NetManager™ High Capacity Horizontal Cable Managers Panduit NetRunner™ Vertical Cable Managers Panduit DP6™ PLUS Punchdown Patch Panels Linkedpro TomacorrienteMultiple Horizontal de 10 Contactospara Rack 19" de 1 Unidad Suministro e instalación de nodo de red de 60 metros con las siguientes características: Certificación del fabricante con una garantía de 25 años mínimo en el desempeño de la instalación de Cableado Estructurado, dicha garantía está detallada en un contrato en español y bajo leyes mexicanas, donde incluye mano de obra y producto. Los servicios de datos se instalarán con cable de par trenzado sin blindaje (UTP), Categoría 6, U/UTP, CM, Ignífugo, (PVC) Diámetro exterior nominal del cable (In.)0.225 Diámetro exterior nominal del cable (mm)5.7 Radio de plegado (mm)22, Número de pares 4, Conductor Material Cobre, Tipo de conductor Sólido, Medidor conductor (AWG)23 Estándares cumplidos Supera ISO 11801 Clase E y ANSI / TIA568.2-D Categoría 6 con garantía de espacio libre de canal, IEC 61156-5, UL 1685, cumple con IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt para aplicaciones PoE; Cumple con RoHS; Jack Categoría 6 en lado panel, estilo TP, ABS, en bronce fosforado chapado, esquema de cableado T568A/T568B, sin blindar, Jack plug en lado usuario enchufe modular terminable de campo Longitud total (mm) 46.2 Sin blindar (UTP), Ancho total (mm) 13.5, Altura total (mm) 15.8, Medidor de alambre compatible (AWG) 22-26, Supera los requisitos de rendimiento del canal ANSI/TIA 568-C.2 Categoría 6A e ISO 11801 Clase EA con hasta dos enchufes de canal de término de campo. Cumple o excede los requisitos propuestos de TIA Modular Plug Terminated Link con hasta dos enchufes de término de campo en el enlace, cumple con ANSI / TIA-1096-A (anteriormente FCC Parte 68), IEC 60603-7, IEC 60529 (IP 20), admite IEEE 802.3af / 802.3at (PoE / PoE +) y propone aplicaciones 802.3bt tipo 3 y tipo 4 (PoE ++). SoportaPower over HDBaseT hasta 100 vatios, compatible con RoHS Todos los componentes del cableado y accesorios son de la misma marca y categoría ya que se consideran paneles de parcheo modulares de 24 o 48 puertos, siendo utilizados solo los modulos necesarios, patch cords de 5	$9,673.23	$2,157,130.29

SECRETARÍA ADMINISTRATIVA

SEMS

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

		pies, fase *plate, etiquetas para identificación en ambos extremos, organizadores horizontales, soportes de pared de 6 unidades de rack, charolas de 19 pulgadas rackeables, cinchos, velcro y todo lo necesario para su correcta instalación.* *Si el edificio cuenta con infraestructura que se centralice en un IDF, se centraliza los ductos y cableado al rack existente.* *Se considera la canalización galvanizada para exteriores en pared gruesa que corresponda para cada nodo de datos incluyendo soportería, accesorios de unión, cruces en losa o muro con los respectivos resanes y reparaciones de acuerdo con las mejores prácticas de instalación y cumpliendo con los siguientes estándares:* *ANSI/TIA/EIA-568B Comercial Building Wiring Standard, que permite la planeación e instalación de un sistema de Cableado Estructurado que soporta independientemente del proveedor y sin conocimiento previo, los servicios y dispositivos de telecomunicaciones que serán instalados durante la vida útil del edificio.* *EIA/TIA-568-B.1 (Requerimientos Generales)* *EIA/TIA-568-B.2-1 (Componentes de Cableado – Categoría 6 Par Trenzado balanceado)* *ANSI/TIA/EIA-569-B Commercial Building Standard for Telecomunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro y entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios y/o closet de comunicaciones y cuarto de equipos.* *ANSI/EIA/TIA-606A Administration Standard for the Telecomunications Commercial Building dura of Comercial Buildings, que da las guías para marcar y administrar los componentes de un sistema de Cableado Estructurado.* *J-STD-607A Commercial Building Grounding (Earthing) and Bonding Requeriments for Telecomunications, que describe los métodos estándares para distribuir las señales de tierra a través de un edificio.* *UL 5A Estándar de UL para Canaletas Superficiales no Metálicas y sus Accesorios que analiza la resistencia física del material con que está hecha la canaleta. UL es el único Laboratorio reconocido por la ANSI/TIA/EIA 569A para prueba de materiales.* *UL 94 Estándar de UL que Prueba la Resistencia a la Propagación de la Flama en los productos.*		
3	20	Punto de acceso inalámbrico "tipo B" Marca Cisco Meraki Modelo MR86-HW Meraki MR86 Wi-Fi 6 Outdoor AP *El equipo de Punto de Acceso de red inalámbrica (Access Point) a considerar, es una solución basada en el estándar IEEE 802.11ax para 5Ghz y 2.4Ghz que permite habilitar el acceso de red para los usuarios en general para dispositivos móviles (tabletas, smartphones, laptops), así como a dispositivos fijos con adaptador inalámbrico. Como parte de la solución, se contemplan como mínimo las siguientes funcionalidades:* • *Operación de banda dual en 2.4 y 5Ghz, concurrente* • *Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet* • *Conexión a la red alámbrica en 1000BaseT*	$78,130.29	$1,562,605.80

CEMS
SECRETARÍA ADMINISTRATIVA

0000068

BAJO PROTESTA DE DECIR VERDAD

[redacted] 2

- *Firewall para bloqueo de tráfico capa 3 y capa 7 a nivel del punto de acceso, con la capacidad de identificar aplicaciones específicas*
- *Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio.*
- *Prevención de Intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación mediante un tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para el servicio de los clientes inalámbricos.*
- *Capacidad de integrarse al servicio de Umbrella para protección inalámbrica a nivel de DNS que prevenga el acceso a sitios y dominios maliciosos, al igual que la capacidad de filtrar contenido basado en categorías (Requiere licencia de Umbrella)*

Administración

- *Gestión centralizada desde una consola de administración basada en Web, desde la cual se puede acceder, configurar y monitorear todos los equipos de LAN o WLAN considerados en esta licitación*
- *De igual manera, desde la misma consola de administración basada en Web, se pueden generar los reportes de operación correspondientes a todos los equipos de LAN o WLAN objeto de esta licitación*
- *La consola es accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la Universidad de Guadalajara, soportando cualquier navegador moderno de Internet disponible*
- *Hay mecanismos que limiten el acceso a la consola, basado en la definición de direcciones IP públicas autorizadas*
- *El acceso a la consola de administración se realiza mediante un método de autenticación de dos factores (two- factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación*
- *El acceso a la consola de gestión soporta la integración con repositorios de identidad externos vía SAML para un Single Sign On (SSO).*
- *El acceso a la consola de gestión es por HTTPS (puertos 8080 y 443) y sus certificados de seguridad son emitidos por entidades reconocidas en Internet*
- *La consola de administración soporta la definición de cuentas de administrador basadas en roles, reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola*
- *La consola reportará sobre intentos de logins al sistema, mostrando qué cuenta intentó entrar, dirección IP, locación, estatus del intento y la hora y fecha del intento*
- *El sistema de gestión centralizado da la opción de empujar nuevo firmware a los AP's, para habilitar nuevas funcionalidades sin costos adicionales y entregar parches de seguridad*
- *El nivel jerárquico de los administradores de la consola es los siguientes:*

SEMS
SECRETARÍA ADMINISTRATIVA

000069

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

- *Administrador de Organización: Un Administrador de la Organización, cuenta con visibilidad en todos los contenedores (colección de dispositivos de red) dentro de la organización. Existirán dos tipos de administradores de la organización: (1) Acceso completo y (2) Sólo lectura.*
  - *El administrador con acceso completo (full access) podrá desempeñar las siguientes*

operaciones dentro de la organización a la que pertenece

- Crear, editar y borrar cuentas de acceso completo y sólo lectura a la organización
- Resetear contraseñas
- Crear, editar y borrar redes
- Agregar nuevos dispositivos a las redes de la organización

- Administrador de Contenedor: Tendrá visibilidad en aquellos contenedores de la organización para las cuales ha sido designado como administrador. Existirán dos tipos de administradores de red: (1) Acceso completo y (2) acceso de sólo lectura. Un administrador de contenedor podrá desempeñar las siguientes operaciones dentro de la organización a la que pertenezca:
  - Crear, editar y borrar otras cuentas de administrador dentro del contenedor
  - Crear, editar y borrar contenedores para las cuales cuente con privilegios

Características físicas y eléctricas de los equipos Puntos de acceso de red inalámbrica

- Conectores externos para antenas del tipo N
- Calificación ambiental IP67 (sellado contra el agua y el polvo)
- Temperatura de operación de -40 a 55 °C
- Alimentación compatible con IEEE 802.3at
- Incluye tornillos de seguridad, así como bahía para candado Kensington
- Placa para montaje en pared

Servicios de Red

El equipo propuesto cuenta con los siguientes servicios de red:

- Interfaz de Radio Frecuencia:
  - Un radio a 2.4GHz 802.11b/g/n/ax y uno a 5GHz 802.11a/n/ac/ax
  - Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas.
  - Que incluya embebido o agregado al AP un radio de Bluetooth Low Energy (BLE) (beacons bluetooth). Éste permitirá actividades de interacción con una aplicación móvil, mandando notificaciones. También permitirá actividades de monitoreo de entrada y

SEMS
SECRETARÍA ADMINISTRATIVA

000070

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

salida de dispositivos que emitan beacons, mandando alertas de estos eventos.

- Soporte de Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350Ghz (UNII-2), 5.470-5.600, 5.660-5.725 (UNII-2e) y 5.725-5.825GHz (UNII-3).
- Antena exterior con conector N, que permite conectar antenas omnidireccionales (4dBi@2.4GHz y 7dBi@5GHz) ó en caso de requerirse por la [INSTITUCIÓN]antenas sectoriales (11dBi@2.4Ghz ó 13dBi@5GHz) o de parche (8dBi@2.4Ghz y 6.5dBi@5GHz)
- Arreglo MU-MIMO 4x4 con cuatro tramas espaciales (spatial streams)
- La solución cuenta con la funcionalidad de selección de la banda de operación por cada SSID:
  - Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz
  - 5GHz únicamente
  - Ambas bandas, pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada
- Ancho de banda de canales de 20, 40MHz y 80MHz
- Tasa de datos combinada de 3.55Gbps
- Certificado para especificación 802.11ax DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, 1024-QAM
- Soporte de Maximal Ratio Combining (MRC)
- Formación de haz (beamforming)
- Agregación de paquetes
- Soporte a Cyclic Shift Diversity (CSD)

- Interfaz alámbrica de red:
  - Una interfaz 100/1000/2.5GBase-T Ethernet (RJ-45) con soporte de 802.3at para PoE
  - VLAN tagging basado en IEEE802.1q
  - Cada Access Point soporta los siguientes esquemas de direccionamiento IP:
    - Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP
    - Modo Bridge, donde el Access Point relevan los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN
    - Roaming de capa 3 (L3), que permite al usuario mantener la misma dirección IP en caso de cambio de segmento de red, manteniendo la sesión activa todo el tiempo
    - Túnel VPN con IPSEC hacia un concentrador central, para el caso en que se requiera habilitar esquemas de

SECRETARÍA ADMINISTRATIVA

000071

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

trabajador y oficina remotos como si se encontraran en la oficina principal

- Calidad de Servicio:
  - Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
  - Soporte de DSCP 802.1p
  - Modelado de tráfico a nivel de capa 7 (L7)
    - Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se soporta la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.
    - La asignación de ancho de banda mediante el modelado de tráfico puedese definir mediante dos mecanismos:
      - Manual
        - Rangos CIDR/IP
        - hostname (URL)
        - Puertos UDP/TCP
        - Combinación de Red,Subnet y puerto
        - Red local (subredes y redes de clase completa en la LAN)
      - Mediante categorías de tráfico
        - Blogging
        - Email
        - Compartición de archivos
        - Juegos
        - Noticias
        - Respaldo en línea
        - Peer-to-peer
        - Redes sociales y compartición de fotos
        - Actualizaciones de programas y antivirus
        - Deportes
        - VoIP y videoconferencia

SECRETARÍA ADMINISTRATIVA

000072

BAJO PROTESTA DE DECIR VERDAD [redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

- Compartición de archivos vía web

- La política de modelado de tráfico permite la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios
- De igual manera, mediante la política de modelado de tráfico puede priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz).

Servicios de seguridad

La solución de Red Inalámbrica incluye las siguientes funcionalidades de seguridad:

b) Firewall

a. La solución inalámbrica de red soporta la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.
   i. Mediante las reglas de capa 3, se definirán políticas de acceso por:
      1. Protocolo (UDP o TCP)
      2. Host, subred o red origen
      3. Puerto TCP o UDP origen
      4. Host, subred o red destino
      5. Puerto TCP o UDP destino
   ii. Mediante las reglas de capa 7, se soporta la restricción de tráfico a partir de categorías definidas, entre ellas:
      1. Blogging
      2. Email
      3. Compartición de archivos
      4. Juegos
      5. Noticias
      6. Respaldo en línea
      7. Peer-to-peer
      8. Redes sociales y compartición de fotos
      9. Actualizaciones de programas y antivirus
      10. Deportes
      11. VoIP y videoconferencia
      12. Compartición de archivos vía web

b. Políticas basadas en identidad
   i. La solución propuesta permite la asignación de políticas individuales de

SECRETARÍA ADMINISTRATIVA

BAJO PROTESTA DE DECIR VERDAD

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de Radius de la [INSTITUCIÓN]

c. Políticas basadas en grupos
   i. Políticas de firewall especificas para grupos está soportada por la solución propuesta.
   ii. Las políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna

d. Control de acceso a la red inalámbrica: La solución soporta la creación de 15 SSIDs como máximo, permitiendo para cada uno los siguientes métodos de acceso:
   i. Abierta y sin encriptación para eventos abiertos al público en general. Cualquier persona puede asociarse con su dispositivo
   ii. Llave compartida con anterioridad (Pre-Shared key) con WPA2, WPA3-Transition Mode y WPA3-Personal
   iii. Control de acceso basado en dirección MAC mediante autenticación Radius
   iv. WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
      1. Un servidor RADIUS incluido en la misma solución
      2. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
      3. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de

SECRETARÍA ADMINISTRATIVA

000074

BAJO PROTESTA DE DECIR VERDAD

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

RADIUS principales

WPA3-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, conlas siguientes opciones de autenticación:

4. Un servidor RADIUS externo de la Universidad de Guadalajara contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
5. El servidor de RADIUS utiliza uno de los siguientes tipos de cifrado EAP
   a. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   b. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   c. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
6. Modalidad de sobrevivencia, en caso de que se pierda comunicación con el servidor de RADIUS, almacenando localmente la información de autenticación de los clientes inalámbricos, y sirviendo como servidor de RADIUS local durante pérdidas de conectividad con los servidores de RADIUS principales

xi. Capacidad para definir hasta 50 claves pre-compartidas de identidad (IPSK) para autenticar usuarios con servicios diferenciados dentro de una misma SSID sin tener que depender de un servidor de RADIUS o autenticación 802.1X

xii. Acceso vía portal cautivo (splash page), que permite habilitar los siguientes métodos de autenticación, conforme lo requiera la Universidad de Guadalajara
   1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al

SECRETARÍA ADMINISTRATIVA

000075

BAJO PROTESTA DE DECIR VERDAD

[redacted] 2

Soluciones Telco

acceso a Internet del usuario

2. Portal "Click-through", donde el usuario se ve un portal de bienvenida y dar "click" a un botón para continuar su acceso
3. Portal captivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
   a. Un servidor RADIUS interno a la solución propuesta
   b. Un servidor RADIUS externo hosteado en alguna localidad de la Universidad de Guadalajara
   c. Autenticación hacia una base de datos de Directorio Activo de la Universidad de Guadalajara la Universidad de Guadalajara Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página oficial de la Universidad de Guadalajara en dicha red social

xiii. Con excepción de la autenticación portal captivo es personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.

xiv. De igual manera, se cuenta con la

SEMS
SECRETARÍA ADMINISTRATIVA

000076

BAJO PROTESTA DE DECIR VERDAD [redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

funcionalidad de Walled Garden, que permite el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente

xv. De acuerdo a lo que requiera la Universidad de Guadalajara la solución permite o bloquear el tráfico no-HTTP

f) Control de acceso a la red (Network Access Control)

a. La solución cuenta con la opción de verificación de la presencia de un software para la detección de antivirus actualizado en el dispositivo de usuario, previo a su autenticación a la red

g) Asignación de políticas de acceso por tipo de dispositivo

a. De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso

h) Filtrado de Contenido

a. La solución incluye en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos, sin requerir para tal efecto añadir una solución de seguridad externa

i) Detección y Prevención de Intrusos en el Canal Inalámbrico

a. La solución de red inalámbrica cuenta con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:

i. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz

ii. Descarga desde la consola central las últimas actualizaciones en firmas de ataques

iii. Habilita políticas de detección y remediación granulares sobre la misma consola de gestión de la solución

iv. El WIPS está basado en un motor heurístico que permite detectar los ataques más sofisticados, mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de de asociación e identificar las variantes a partir del comportamiento normal

v. Identifica y organizar las siguientes categorías de ataques como mínimo:

1. SSIDs no autorizados
2. Intentos de robo de identidad (spoofs) del AP
3. Inundación de paquetes que tengan como finalidad generar eventos de

SECRETARÍA ADMINISTRATIVA

000077

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

negación de servicio (DoS)

vi. Para efectos de remediar los ataques, la solución permite la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID

vii. Notifica de eventos de seguridad a los administradores de la red por medio de correo electrónico

Reportes y monitoreo

- Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución incluye dentro de la misma consola de gestión un inventario de equipo tanto operativo como desconectado, accesible para los administradores de la red
- Se puede cargar los planos de las ubicaciones en donde se desplieguen los AP, así como la alineación a

Google Maps, con el propósito de tener la ubicación de cada AP bien definido.

- La solución cuenta con una aplicación móvil que facilite el monitoreo de los AP's desplegados, así como la capacidad de tomar fotos de cada AP montado para que se refleje en la plataforma de gestión fija.
- La solución puede mostrar diagnósticos de salud desde el punto de vista del cliente, permitiendo hacer "drill-down" en un cliente específico y obtener información sobre la salud del mismo
    - Indicación gráfica de la salud de la conexión entre el cliente y su Access Point, con la tasa de transferencia negociada y la tasa de datos en transferencia en ese instante de tiempo
    - Indicación gráfica de la salud del Access Point, con desglose de utilización de canal, carga actual de clientes y utlización en el canal actual del cliente
    - Capacidad de lanzar una captura de paquetes filtrada para el cliente desde ese Access Point
    - Indicación de la calidad de la conexión de ese Access Point a su switch de acceso, mostrando el estatus del puerto, problemas de conectividad, exceso de broadcast/multicast/unknown unicast, y problemas de negociación
    - Indicación de problemas de salud en el switch de acceso, desglosados por problemas de DNS, RADIUS, OSPF o host capa 3
    - Pestaña de Conexiones de cliente con las estadísticas y el desglose de los problemas de conectividad inalámbrica experimentados por el cliente desglosados en las etapas de Asociación, Autenticación, DHCP y DNS
    - Rendimiento del cliente representado de forma gráfica que permite obtener métricas de rendimiento del mismo desglosadas en
        - Gráfico de utilización histórica por aplicación, superpuesta con eventos de conexión del cliente como asociaciones, autenticaciones por RADIUS/802.1X, o roaming

SAMS
SECRETARÍA ADMINISTRATIVA

000078

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

- Gráfico de calidad de señal histórica percibida por el cliente, superpuesta con los eventos de conectividad del mismo
- Gráfico de latencia promedio histórica experimentada por el cliente, superpuestacon los eventos de conectividad del mismo
- Gráfico de utilización de canal experimentada por el cliente, superpuesta con los eventos de conectividad del mismo
- Gráfico de utilización del Access Point al que el cliente está asociado, superpuesta con los eventos de conectividad del mismo
- Gráfico de cantidad de clientes asociados al Access Point en el que se encuentra el cliente, superpuesto con los eventos de conectividad del mismo
- Gráfico de tasas de datos del cliente negociadas con cada uno de los Access Points por los que se ha movido

- Historial de conectividad del cliente que desglose todos los movimientos del mismo y que sea filtrable por SSID, Access Point, Banda, Etapa de Fallo, Severidad de Fallo
  - La herramienta podrá aportar sugerencias de cómo solucionar ciertos problemasencontrados por el cliente y su posible causa raíz

- La solución muestra diagnósticos de salud desde el punto de vista del Access Point ofreciendo
  - Información de salud de resumen desde el punto de vista del Access Point, indicando porcentualmente la cantidad de conexiones exitosas, fallidas y problemáticas, y desglosando las fallas en problemas de Asociación, Autenticación, DHCP y DNS
  - Historial de rendimiento del Access Point, desglosado en
    - Gráfico de utilización superpuesto con eventos de cambio de canal e intensidad de potencia
    - Gráfico de cantidad de clientes asociados superpuesto con eventos de cambio de canal e intensidad de potencia
    - Calidad de señal histórica promedio superpuesto con eventos de cambio de canal eintensidad de potencia
    - Latencia inalámbrica promedio superpuesta con eventos de cambio de canal eintensidad de potencia

SECRETARÍA ADMINISTRATIVA

000079

BAJO PROTESTA DE DECIR VERDAD [redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

- La solución puede mostrar información de diagnósticos globales sobre el rendimiento de la red inalámbrica ofreciendo los siguientes reportes de manera gráfica
    - Salud por Access Point, indicando con código de colores de semáforo (verde, amarillo, rojo) los Access Points en un mapa para ilustrar gráficamente problemas de salud
    - Listado de Access Points con mayor porcentaje de problemas de conectividad
    - Desglose de salud por tipo de dispositivo, indicando por sistema operativo los problemas de conectividad observados en la red
    - Conexiones fallidas desglosadas por porcentaje y tipo de fallo
        - Fallos en Asociación
        - Fallos en Autenticación
        - Fallos en DHCP
        - Fallos en DNS
    - Capacidad de hacer "drill-down" por tipo de fallo para ver todos los eventos relacionados al tipo de fallo por SSID, por Access Point y por Red
    - Desglose de latencia de paquetes por tipo de tráfico, ofreciendo las métricas de rendimiento histórico para
        - Tráfico de Voz
        - Tráfico de Vídeo
        - Tráfico Best Effort
        - Tráfico Background
    - Capacidad para extraer toda esta información por medio de APIs para graficar en Dashboards personalizados
- La solución genera sobre demanda un reporte ejecutivo por el último día, la última semana, el último mes y sobre un período específico de monitoreo, incluyendo los siguientes parámetros:
    - Utilización total de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos durante el tiempo especificado
    - Los Top 50 Access Points del sistema por utilización
    - Los SSID's con mayor consumo
    - Conteo individual de clientes durante el período seleccionado y por día
    - Los Top 50 usuarios por utilización
    - Las Top 50 aplicaciones con mayor presencia en la red
    - Los Top 50 dispositivos por fabricante
    - Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red

Proporciona a los administradores con una lista de bitácoras de eventos y de cambios en la configuración.

- Cuentase de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De

SEMS
SECRETARÍA ADMINISTRATIVA

000080

BAJO PROTESTA DE DECIR VERDAD [redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación.

- Finalmente, la solución contabiliza y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo:
  - Dispositivos que pasaron dentro del área de cobertura, pero permanecieron un intervalo de tiempo pequeño
  - Dispositivos que, aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura
  - Dispositivos que finalmente se conectaron a la red
  - Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente
  - Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales

Analíticos de ubicación de dispositivos

- La solución inalámbrica de red está equipada con la habilidad de detectar la presencia del dispositivo de usuario, basado en la información contenida en los mensajes de "probe request" generados por los radios WiFi- encendidos en smartphones, laptops y tabletas.
- Con la información recabada, la controladora en la nube consolida analíticos históricos de los dispositivos WiFi, con gráficas intuitivas y personalizables, facilitando la interpretación de tendencias tales como:
  - Flujo de paseantes por día y hora
  - Lealtad de usuarios basado en visitantes nuevos y repetidos
  - Tiempo de permanencia de visitantes en la zona de cobertura
- La información de presencia está disponible para su exportación a un sistema externo, que incluya:
  - Dirección MAC del AP que reporta
  - Dirección MAC del dispositivo de usuario
  - Intensidad de señal recibida (RSSI) con la cual fue escuchado el dispositivo
  - Estampa de tiempo
  - Coordenadas X y Y de la ubicación del dispositivo, de acuerdo a la información entregada por todos los APs del sistema

Antenas

Los puntos de acceso tipo C, incluyen 2 antenas externas de banda dual MIMO tipo Sector ganancia de 9 dBi a 2.4 GHz, ganancia de 12 dBi a 5 GHz

Inyector de Energía a través de cable Ethernet (PoE)

Los puntos de acceso tipo C, incluyen un inyector de energía a través de cable Ethernet (PoE) que opera con un voltaje de entrada de entre 100 a 240 Volts de corriente alterna, proporcionar un voltaje de salida de 55V de corriente directa, potencia de salida de 30W acorde al estándar IEEE 802.3at y es compatible con Ethernet 10/100/1000 Mbits/s full duplex.

- Incluye todo el licenciamiento necesario para su correcto

SECRETARÍA ADMINISTRATIVA

000081

BAJO PROTESTA DE DECIR VERDAD [redacted]

Asesores 5749, Col. Arcos de Guadalupe, CP 45037, Zapopan, Jalisco.
Teléfono: (33) 1201 7494
www.solucionestelco.com

Soluciones Telco

		funcionamiento por lo menos durante 7 años. • Garantía de por vida en hardware de interiores. • Soporte técnico telefónico en español 24x7x365. • Tickets de soporte podrán ser abierto mediante la misma plataforma de gestión. Reemplazo de partes de siguiente día hábil.Esta garantía y soporte estará vigente por 7 años.		
			Subtotal	$10,481,877.21
			IVA	$1,677,100.35
			Total	$12,158,977.56

TOTAL CON LETRA: Doce millones, ciento cincuenta y ocho mil, novecientos setenta y siete pesos 56/100 M.N.
VIGENCIA: 45 días naturales posteriores a la presentación de esta propuesta económica.
GARANTÍA: Cobertura extendida por 7 años, proporcionada directamente por el fabricante y con atención directa de Soluciones y Servicios Integrales Telco S.A. de C.V.
FORMA DE PAGO: Anticipo del 30% y el 70% restante a contra entrega.
TIEMPO DE ENTREGA: Un máximo de 6 semanas naturales posteriores a la fecha de adjudicación del servicio.

ATENTAMENTE

Guadalajara, Jalisco, a miércoles 13 de Octubre del 2021

ATENTAMENTE:

[redacted]

Oscar Alejandro Zetina Salazar
Representante Legal
Soluciones y Servicios Integrales Telco SA de CV

SECRETARÍA ADMINISTRATIVA

000082

BAJO PROTESTA DE DECIR VERDAD

1.- Se testa una clave patronal del IMSS, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.
2.- Se testan veintisiete firmas, con fundamento en el artículo 21, párrafo 1, fracción I, de la Ley de Transparencia y Acceso a la Información Pública de Estado de Jalisco y sus Municipios; así como el artículo 3, punto 1, fracción IX de la Ley de Protección de Datos personales en posesión de Sujetos Obligados del Estado de Jalisco y sus municipios, y al Lineamiento Quincuagésimo Octavo, fracción I, de los Lineamientos Generales de Protección de Información Confidencial y Reservada por contener datos de carácter personal.