Bases de la licitación pública número LI-044-CGTI-2017, para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

Septiembre de 2017

ÍNDICE

SECCIÓN I

INSTRUCCIONES A LOS LICITANTES

A. Introducción

1. Fuente de los recursos

1.1 Los recursos corresponden al proyecto 236526, fondo 1.1.9.27 Federal ordinario 2017 de la Universidad de Guadalajara.

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 el contratante.

2. Licitantes Elegibles

2.1. Esta convocatoria se hace a todas las personas físicas o morales nacionales, debidamente constituidas que presten los servicios para el Bases de la licitación pública número LI-044-CGTI-2017, para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

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.
VI. Formato de propuesta económica.

5.2 El licitante deberá examinar todas las instrucciones, formularios, condiciones y especificaciones que figuren en los documentos de la licitación. Si el licitante **"no"** incluye toda la información

requerida en los documentos de la licitación o presenta una propuesta que no se ajuste 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 11 de octubre de 2017 a las 13:00 horas** en la sala de juntas de la Coordinación General Administrativa, ubicadas en el piso cuatro del Edificio de la Rectoría General de la Universidad de Guadalajara, localizada en Avenida Juárez 976, colonia Centro, en la ciudad de Guadalajara, Jalisco.

6.2 Para llevar a cabo esta reunión, los participantes deberán enviar sus preguntas por correo electrónico, en archivo formato Word, a más tardar el día 09 de octubre de 2017 a las 15:00 horas a las siguientes direcciones:

jorge.lozoya@redudg.udg.mx
almar@redudg.udg.mx
sencion.hector@redudg.udg.mx
elsad@redudg.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 Deberá asistir a la junta de aclaraciones el representante legal de la empresa o la persona acreditada por este mediante carta de la empresa, al licitante que no asista a la junta de aclaraciones, por sí o su representante, no obstante haber recibido las bases de la licitación le será desechada su propuesta.

7. Modificación de los Documentos de la Licitación

7.1 La Universidad de Guadalajara podrá, por cualquier causa y en cualquier momento, antes de que venza el plazo para la presentación de propuestas, podrá modificar las bases de la licitación, ya sea por iniciativa propia o en atención a una aclaración solicitada por un licitante interesado.

7.2 Las modificaciones serán notificadas, por correo electrónico, a todos los licitantes registrados y serán obligatorias para ellos.

7.3 La Universidad de Guadalajara 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 modificaciones hechas a las bases de la licitación. De la misma forma podrá prorrogar la fecha de la lectura de fallo, dentro del plazo de la vigencia de las propuestas, la cual les será notificada por correo electrónico, tanto la fecha de prorroga como la nueva fecha de la lectura de fallo.

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 la Universidad de Guadalajara 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 servicios a prestar, de acuerdo con el catálogo de conceptos de la **Sección III** de las presentes bases. Es importante precisar que su propuesta debe contener todos los conceptos a cotizar, aun cuando no tengan costo, como se especifica en el catálogo así como especificar la fecha de entrega de los bienes.

10. Requisitos para el proveedor

10.1 Los ofertantes deberán ser compañías legalmente establecidas en México que se dediquen al Bases de la licitación pública número LI-044-CGTI-2017, para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

10.2 Adicionalmente los ofertantes 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 Los licitantes deberán ofertar la totalidad del catálogo de conceptos, es importante señalar que la evaluación y la adjudicación de la propuesta se realizará a un solo proveedor.

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

10.5 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, podrá ser motivo de descalificación de la propuesta.

11. Precios y Vigencia

11.1 El licitante indicará, los precios unitarios y totales de su propuesta, de acuerdo a la presente licitación.

11.2 Precio fijo. Los precios cotizados por el ofertante serán fijos durante el contrato 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.

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 la 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 la Universidad de Guadalajara 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.

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 que deberá contener el nombre y el número de la licitación.

14.4 El licitante deberá especificar en su propuesta las condiciones de pago, garantías, tiempo de entrega y la vigencia de los precios, misma que deberá ser como mínimo 30 días a partir de la fecha de apertura de las propuestas.

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

15. Período de Validez de la Propuesta

15.1 La propuesta tendrá validez por **30 días** naturales después de la fecha de apertura de las propuestas, prescrita por la Universidad de Guadalajara, conforme a las bases de la licitación. Una propuesta cuyo período de validez sea más corto que el requerido, será rechazada por la Universidad de Guadalajara por no ajustarse a las bases de la licitación. Se adjunta modelo de carta en la **Sección V** de estas bases.

16. Formato y Firma de la Propuesta

16.1 El paquete original de la propuesta deberá estar firmado, 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 Folletos y demás información sobre las características y descripciones de los servicios requeridos, así como demás documentos que acrediten su experiencia, prestigio y reconocimiento para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

A.2 Bases y anexos de la licitación, 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 Formato de la propuesta económica, con base en el catálogo de conceptos de la Sección III de las bases.

B.2 Carta de seriedad de la propuesta.

B.3 Carta compromiso.

16.2 El licitante presentará (1) un ejemplar original de la propuesta, la cual no deberá contener textos entre líneas, borrones, tachaduras ni enmendaduras.

16.3 Formato de propuesta económica en la Sección VI de las presentes bases.

D. Presentación de Propuestas

17. Sellado y Marca de Propuesta

17.1 El original de la oferta será colocado dentro de un sobre que el licitante deberá cerrar y marcar respectivamente.

17.2 El sobre:

a) Estará rotulado con la siguiente dirección:

Universidad de Guadalajara
Av. Juárez 976, 4° piso
Atención: Dra. Carmen Enedina Rodríguez Armenta
Secretaria Ejecutiva del Comité General de Compras y Adjudicaciones de la Universidad de Guadalajara

Indicará: Propuesta para la licitación LI-044-CGTI-2017, para el el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información. La fecha de la convocatoria y la frase "NO ABRIR ANTES DE LAS 13:00 HORAS DEL DÍA 20 DE OCTUBRE DE 2017";

b) Si el sobre no fuese sellado y marcado siguiendo las instrucciones establecidas en estas bases, la Universidad de Guadalajara 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 a la Universidad de Guadalajara en la Coordinación General Administrativa, ubicada en el piso cuatro del Edificio de la Rectoría General de la Universidad de Guadalajara, localizada en Avenida Juárez 976, colonia Centro, en la ciudad de Guadalajara, Jalisco; antes de las **13:00 horas del 20 de octubre de 2017.**

18.2 La Universidad de Guadalajara podrá, a su discreción, prorrogar el plazo para la presentación de propuestas, mediante la modificación 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 a la Universidad de Guadalajara después del plazo y hora fijada para su recepción no se recibirá.

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 la Universidad de Guadalajara, como constancia de su participación en la licitación.

E. Apertura y Evaluación de Propuestas

21. Apertura de propuestas

21.1 La Universidad de Guadalajara abrirá las propuestas en sesión pública el **20 de octubre de 2017 a las 13:00 horas,** en la Sala de Juntas de la Coordinación General Administrativa, ubicada en el cuarto piso del Edificio de la Rectoría General de la Universidad de Guadalajara, localizado en Avenida Juárez 976, sector Juárez, en la ciudad de Guadalajara, Jalisco, con la participación de un representante por empresa licitante.

21.2 La Universidad de Guadalajara, 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, la Universidad de Guadalajara podrá, a su discreción, solicitar a cualquier licitante las aclaraciones de su oferta.

23. Revisión, Evaluación y Comparación de las Propuestas

23.1 La Universidad de Guadalajara examinará las propuestas para determinar si están completas, si contienen errores de cálculo, si se han suministrado las garantías requeridas, si los documentos han sido debidamente firmados y si, en general, las propuestas cumplen con los requisitos establecidos en las presentes bases, en el catálogo de conceptos y en la convocatoria de la licitación.

23.2 Toda oferta que no cumpla con los requisitos de las bases de la licitación será rechazada por la Universidad y no podrá ser modificada con posterioridad por el ofertante mediante correcciones.

23.3 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.

23.4 La comparación de las propuestas se hará tomando en cuenta el cumplimiento de la descripción de los bienes a contratar, los requisitos y las condiciones técnicas, el currículo de la empresa, los precios, los cuales incluirán todos los costos e impuestos aplicables.

23.5 La Universidad de Guadalajara podrá integrar una comisión técnica conformada por personal de la dependencia solicitante, de las áreas de la Universidad especialista en el tema de la adquisición y la Coordinación General Administrativa para hacer el análisis de las propuestas, para lo cual se elaborará una opinión técnica donde se asentará el resultado de la evaluación, en caso de que alguna empresa participante no cumpla técnicamente con la descripción solicitada se asentará en la opinión las causas y conceptos y se desecharán las propuestas que no cumplan con los requisitos establecidos en las presentes bases y en la convocatoria de la licitación.

23.6 Con base en la opinión técnica y la revisión documental y económica de las propuestas, la Coordinación de Servicios Generales de la Administración General formula el dictamen técnico de la licitación, en el cual se establece el resultado final de la revisión de las propuestas recibidas, mismo que se presenta al Comité General de Compras y Adjudicaciones de la Universidad de Guadalajara.

24. Comunicaciones con la Universidad de Guadalajara

24.1 Ningún licitante se comunicará con la Universidad de Guadalajara 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 del contrato, salvo las preguntas para la junta de aclaraciones, que serán remitidas por correo electrónico a más tardar a las **15:00 horas del 09 de octubre de 2017.**

24.2 Cualquier intento, por parte de un licitante, de ejercer influencia sobre las decisiones del Comité General de Compras y Adjudicaciones de la Universidad de Guadalajara en la evaluación y comparación de ofertas o adjudicaciones del contrato, podrá dar lugar al rechazo de su propuesta. Los casos en que se considere que ha existido influencia estarán determinados por el criterio de la Universidad de Guadalajara.

F. Adjudicación del Contrato

25. Criterios para la Adjudicación

25.1 La Universidad de Guadalajara adjudicará el contrato al licitante cuya oferta se ajuste sustancialmente a los documentos de la licitación y haya sido evaluada como la mejor y por tanto esté calificado para cumplir satisfactoriamente el contrato.

26. Derecho de la Universidad de Guadalajara de Aceptar Cualquier Propuesta y Rechazar Cualquiera o Todas las Propuestas

26.1 La Universidad de Guadalajara 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 suscripción del contrato, 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 de la Universidad de Guadalajara.

26.2 Los acuerdos, disposiciones y decisiones tomadas por los miembros del Comité General de Compras y Adjudicaciones, con respecto al resolutivo de la licitación, serán inapelables.

26.3 El Comité General de Compras y Adjudicaciones tendrá la facultad de decidir sobre cualquier controversia que pudiera presentarse durante el desarrollo de la licitación y de aplicar la normatividad universitaria.

27. Notificación de la Adjudicación

27.1 Antes de la expiración del período de validez de la oferta, la Universidad de Guadalajara notificará el fallo emitido por el Comité General de Compras y Adquisiciones mediante el acta de lectura de fallo en la fecha establecida en el acta de apertura de propuestas.

27.2 La Universidad de Guadalajara podrá diferir la fecha de la lectura de fallo, circunstancia que comunicará a los concursantes que hayan participado mediante correo electrónico.

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

27.4 A partir de la fecha de la lectura de fallo, la misma estará disponible en la Coordinación General Administrativa, para los licitantes que no hubieran asistido a dicho acto.

28. Firma del Contrato

28.1 Desde el momento en que reciba el Formulario de Contrato el licitante seleccionado tendrá **48 horas** para firmarlo y devolverlo a la Universidad.

Sección II.
CONDICIONES GENERALES

1. Entrega y Documentos

1.1. El licitante realizará el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

1.2. El licitante que requiera parte o la totalidad de la información de carácter comercial presentada, en virtud de que 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 Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

2. Pago

2.1 El pago al licitante se realizará en pesos mexicanos, contra entrega de los bienes requeridos, previa formalización de su recepción a entera satisfacción de la Universidad de Guadalajara, conforme se establezca en el contrato y presentada la fianza respectiva.

3. Precios

3.1 Los precios facturados por el licitante, por los bienes prestados de conformidad al contrato, no serán mayores a los que haya cotizado en su propuesta.

4. Modificaciones al Contrato

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

5. Resolución por Incumplimiento

5.1 La Universidad de Guadalajara 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 cumple con el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

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

c) En caso de incumplimiento en la entrega del equipo, por causa imputable a la empresa, 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 a la Universidad.

6. Resolución por Insolvencia

6.1. La Universidad de Guadalajara 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. La Universidad de Guadalajara podrá en cualquier momento terminar total o parcialmente el contrato por razones de conveniencia, mediante notificación escrita al licitante. La notificación indicará que la terminación se debe a conveniencia de la Universidad de 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:

Universidad de Guadalajara
Av. Juárez 976, 4º piso
Atención: Dra. Carmen Enedina Rodríguez Armenta
Secretario Ejecutivo del Comité General de Compras y Adjudicaciones.

10.2 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

Suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

1.- Presentación y estructura del documento

El presente documento describe los requerimientos necesarios para implementar un sistema de correlación de eventos para la red dorsal de datos de la Universidad de Guadalajara que permita recolectar los datos de los comportamientos de los equipos físicos que conforman la conectividad universitaria, así como un sistema basado en hardware de propietario de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, que brinde protección a las plataformas actualmente operando en la institución.

2.- Descripción del proyecto

2.1 Antecedentes

La universidad de Guadalajara a través de la CGTI cuenta con la infraestructura dorsal para la distribución de servicios de red por la cual transita el tráfico de datos de toda la institución, el monitoreo en tiempo real en todos los puntos, permite tomar acciones preventivas y correctivas que aumentan la disponibilidad de los servicios. Actualmente el monitoreo de servicios se realiza de manera independiente por dispositivo o enlace, para tener un panorama mas completo de los comportamientos de los dispositivos que conforman la red se requiere un sistema que pueda correlacionar los datos de todos los dispositivos de la red para su análisis en conjunto, lo anterior se logra con un correlacionador de datos de señalización configurado con los parámetros de operación acordes a los niveles de operación determinados por la institución.

Los sistemas de correo electrónico se encuentran actualmente expuestos a una serie de ataques de diferentes tipos ya sea por agentes externos o internos, la protección antispam, antivirus, anti-spyware y anti-phishing es una plataforma vital para asegurar la integridad de la información y de la continuidad de los servicios. Por lo que es necesario actualizar esta plataforma para poder mantener este servicio.

El presente documento describe los elementos de infraestructura necesarios para implementar un sistema de correlación de eventos para la red dorsal de datos de la Universidad de Guadalajara que permita recolectar los datos de los comportamientos de los equipos físicos que conforman la conectividad universitaria, así como un sistema basado en hardware propietario de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, que brinde protección a las plataformas actualmente operando en la institución.

2.2 Objetivo general

Implementar un sistema de correlación de eventos para la red dorsal de datos de la Universidad de Guadalajara que permita recolectar los datos de los comportamientos de los equipos físicos que conforman la conectividad universitaria, así como un sistema basado en hardware propietario de protección antispam, antivirus, anti-

spyware y anti-phishing para plataformas de correo universitarias que brinde protección a las plataformas actualmente operando en la institución.

2.2.1 Objetivo específico

Contar con estadísticas de operación de la red de datos y de los sistemas que en ellos transitan correlacionados para detección de patrones, para mejora del servicio.

Proteger con plataformas redundantes y actualizadas los servicios de correo electrónico contra spam, virus, spyware y phishing, así como de nuevas vulnerabilidades que surjan.

3.- Componentes del Proyecto

En la presente sección se describen los componentes, características y funcionalidades para la adquisición del sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias.

3.1 Suministro y configuración un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias.

Sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara		
Partida 1	**Cantidad**	**Descripción**
		• **Plataforma del tipo Next Generation - Security Information and Event Manager (Next Generation SIEM) que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad al menos de 50 equipos físicos. La plataforma deberá colectar los eventos de seguridad de múltiples marcas para lo cual se deberá incluir el licenciamiento necesario para esto y los servicios descritos:** 1) La plataforma deberá tener la capacidad de comportarse como una herramienta del tipo CMDB. 1.1) La plataforma deberá monitorear los cambios en los archivos de configuración de los servidores que la entidad defina. 1.2) La plataforma deberá ser del tipo Virtual Appliance con el fin de que la entidad pueda asignar recursos virtuales a la misma medida que se requieran. 1.3) La solución deberá ser con un sistema de bases de datos híbridos, lo que quiere decir que esté basado en NoSQL y SQL, no se aceptan soluciones basadas únicamente en motores de bases de datos del tipo SQL, esto con el fin de que soporten grandes volúmenes de datos sin afectar la estabilidad de la solución. 1.4) La solución deberá soportar características multi-tenancy. 1.5) La plataforma al ser un SIEM de nueva generación deberá contar con características NOC y SOC, por lo cuál deberá realizar:

		• Actualización constante de la base de datos de contextos, configuraciones, software instalado y servicios corriendo de los dispositivos monitoreados. • Análisis constante del desempeño de las aplicaciones, lo cual permita realizar una clasificación (triage) de la seguridad. • Visor personalizado de log de tráfico. • Herramienta de búsqueda sobre los logs de tráfico. 1.6) La plataforma es requerida por un periodo de 12 meses en un esquema 7 x 24 ante fabricante, con actualizaciones. 1.7) El SIEM debe ser capaz de aprovechar una variedad de fuentes públicas y privadas de datos para enriquecer los datos fuente, ya sea para proporcionar un contexto adicional o ayudar con la atribución (GeoIP- Whois, etc.). 1.8) El SIEM debe ser capaz de clasificar claramente los diferentes tipos de datos que recoge para ayudar en la analítica o consultas ad hoc por los analistas SOC. También debe ser capaz de clasificar tales datos basados en su sensibilidad o protección requerida de seguridad/privacidad donde sea apropiado. También debe ser capaz de agrupar datos similares. 1.9) El SIEM deberá permitir múltiples tipos de almacenamiento de datos dependiendo de cómo y cuándo se usen esos datos. 1.10) El SIEM debe tener la capacidad de mantener sus propias bases de conocimiento. Estos pueden incluir la documentación del flujo de trabajo del proceso, la documentación del producto, los procedimientos, los scripts y los fragmentos de código desarrollados por el SOC. 1.11) El SIEM debe proporcionar una capacidad nativa para consumir fuentes de inteligencia de amenazas de fuentes abiertas y comerciales. 1.12) El SIEM también debe ser capaz de realizar análisis tanto en tiempo real como similares basados en datos históricos dentro de la plataforma que debe proporcionar la capacidad de permitir el desarrollo de análisis personalizados y realizar análisis sin comprometer la velocidad o la estabilidad de la solución global. 1.13) El SIEM debe ser capaz de generar alertas basadas en condiciones programadas de una variedad de análisis de seguridad, disponibilidad y rendimiento. También debe soportar varias maneras de comunicar estas alertas y proporcionar un flujo de trabajo para su investigación y confirmación. 1.14) El SIEM debe proporcionar capacidades nativas para producir dashboards y análisis visuales predeterminados y personalizados para los consumidores típicos de SOC, así como proporcionar la capacidad de integrarse con soluciones de terceros que pueden proporcionar funciones similares a través de múltiples plataformas SOC. 1.15) El SIEM debe proporcionar la capacidad de proporcionar acciones correctivas manuales, secuenciadas y/o automatizadas sobre los controles de seguridad gestionados a través de la solución SIEM. Esto puede proporcionarse directamente a través del propio SIEM o a través de la integración con sistemas de gestión externa. 1.16) El SIEM debe tener su propia herramienta de gestión de tickets y permitir la integración con herramientas de terceros ConnectWise, ServiceNow, SalesForce y Remedy. 1.17) El SIEM también debe ser capaz de almacenar y administrar datos internos y de gestión de configuración del CLIENTE dentro de las Bases de Datos de Gestión de Configuración (CMDB). Esto necesitará incluir una

		capacidad nativa pero también debe soportar la integración con plataformas CMDB de terceros. 1.18) Se requiere que la solución incluyendo análisis de anomalías estadísticas y técnicas de aprendizaje automático. 1.19) La solución debe poderse implementar de forma distribuida, de tal forma que los colectores sean independientes del motor de correlación, permitiendo que ante una caída del enlace que comunica al motor de correlación, los eventos se puedan almacenar por un tiempo determinado. 1.20) La solución debe contar con capacidad de monitoreo activo de disponibilidad de performance mediante el monitoreo constante de SNMP, servicios TCP entre otros, de tal forma que permita generar estadísticas de uso de recursos como CPU, memoria, tráfico de red, entre otros. Desempeño 1.21) La solución de SIEM debe dar soporte a las siguientes características mínimas: • Número de Dispositivos: 50 • Número de Eventos por Segundo (EPS): 500 1.22) HyperVisor Soportado: VMWare ESXi 5.5 o Superior - HyperV - Amazon EC2 – KVM. 1.23) Que tenga la capacidad de crecimiento por lo menos a 2,000 dispositivos, 20,000 eventos por segundo y agentes Windows. **Nota:** La entidad suministrará el hardware y entorno de procesamiento requerido para la implementación de la solución. 1.24) Funciones de monitoreo y disponibilidad. 1.25) Deberá tener la capacidad de colectar archivos de configuración de red de los dispositivos monitoreados, almacenada en un repositorio de versiones. 1.26) Deberá soportar la capacidad de colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones. 1.27) Deberá soportar las características de detección automática de los cambios en la configuración de red de las plataformas monitoreadas. 1.28) Deberá soportar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas. 1.29) Deberá soportar con la característica de detección automática en cambios en archivos y carpetas de las plataformas Windows y Linux monitoreadas, donde se detalle el "Quien" y el "Que". 1.30) Deberá soportar con la característica de detección automática basada en agente de cambios en el registro de los sistemas Windows monitoreados. 1.31) Deberá contar con la característica de Monitoreo del sistema vía SNMP, WMI y PowerShell. 1.32) Deberá contar con la característica de Monitoreo de aplicaciones vía JMX, WMI y PowerShell. 1.33) Deberá contar con la característica de monitoreo de Hipervisor tales como VMWARE y Hype-V. 1.34) Deberá poder monitorear plataformas de almacenamiento tales como EMC, NetAPP, Nutanix, Nimble, etc. a nivel de desempeño y uso de almacenamiento.

		1.35) Deberá poder monitorear sistemas del tipo directorio activo y Exchange basado en WMI y PowerShell. 1.36) Deberá poder monitorear motores de bases de datos SQL Server, Oracle, MySQL entre otras vías JDBC. 1.37) Deberá poder Monitorear Infraestructura VoIP vía IPSLA, SNMP, CDR y CMR. 1.38) Debe realizar análisis del desempeño y flujo de las aplicaciones vía NetFlow, Sflow, Cisco AVC y NBAR. 1.39) Debe tener la capacidad de definir métricas customizadas. 1.40) Debe tener la Capacidad de detectar desviaciones de una línea base de la infraestructura monitoreada. 1.41) Debe tener la capacidad de monitorear dispositivos del entorno tales como Liebert UPS, HVAC, FPC y APC. 1.42) Deberá monitorear las caídas e inicios de los sistemas vía Ping, SNMP, WMI, así como análisis del inicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage. 1.43) Deberá hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos. 1.44) El SIEM debe proporcionar la capacidad de soportar solicitudes de información ad-hoc o programadas de la solución para satisfacer las necesidades de auditoría o cumplimiento. 1.45) El SIEM debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA 256. 1.47) El SIEM debe proporcionar reportes de auditoría y cumplimiento con templates de PCI, COBIT, ITIL, SOX, ISO, ISO 27001, HIPPA, GLBA, FISMA, NERC, GPG13, SANS Critical Controls. 1.48) El SIEM debe proporcionar una arquitectura altamente escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en la producción. 1.49) El SIEM debe soportar plataformas de desarrollo y lenguajes de programación para el desarrollo personalizado dentro de la solución y sus componentes tipo XML. Dispositivos y Aplicaciones Soportados 1.50) La solución deberá soportar al menos las siguientes plataformas a nivel de monitoreo de seguridad y de rendimiento: • Antivirus • Kaspersky • Symantec Endpoint Protection • McAfee EPO • Trend Micro OfficeScan • Trend Micro Intrusion Defense Firewall (IDF) • Sophos Endpoint Security and Control ESET NOD32 Cisco Security Agent (CSA) entre otros

		Application Servers Microsoft ASP.NET Oracle WebLogic IBM WebSphere Red Hat JBoss Sun GlassFish Apache Tomcat entre otros Authentication Servers Cisco Access Control Server (ACS) Juniper Steel-Belted Radius Microsoft Internet Authentication Service (IAS) Alcatel AAA RADIUS Blade Servers Cisco Unified Computer System (UCS) HP BladeSystem Dell Blade Server Cloud Services Amazon EC2 Databases IBM DB2 MySQL Microsoft SQL Server Oracle Database Server Directory Services Microsoft Active Directory 2000, 2003, 2008, 2012 DNS/DHCP Servers Infoblox DNS/DHCP BIND DNS Linux DHCP Microsoft DHCP/DNS 2003, 2008 Email Microsoft Exchange Postfix Mail Server Sendmail Environmental APC UPS Liebert UPS, HVAC, FPC

		APC NetBotz Generic UPS File Monitoring Linux Microsoft Windows Firewalls Cisco ASA, IOS Cisco Firewall Services Module (FWSM), Private Internet eXchange (PIX) Juniper Networks Secure Services Gateway (SSG), Integrated Security Gateways (ISG). Palo Alto Networks Check Point FireWall-1, Provider-1, IPSO Check Point VSX Fortinet FortiOS Linux ipchains McAfee Enterprise (Sidewinder) Dell SonicWALL SonicOS WatchGuard Microsoft Internet Security and Acceleration (ISA) Server Astaro Monitoring Dell servers HP servers IBM servers VMware ESX servers Network devices Storage devices Host OS Microsoft Windows 2000, 2003, 2008, 2012, XP, Vista, Windows 7 CentOS Linux Fedora Linux Red Hat Linux Debian Linux SUSE Linux HP-UX IBM AIX IBM OS/400 Oracle Solaris, SunOS

		Internet Security Gateways Blue Coat ProxySG Cisco IronPort Mail and Web Barracuda Spam Firewall FortiGate McAfee Web Gateway Websense Web Filter Websense Email Security Gateway Microsoft Internet Security and Acceleration (ISA) Server Squid Untangle Secure Gateway Astaro Security Gateway Network Intrusion Prevention Systems (IPS) Cisco IPS Snort IPS FortiGate FireEye Juniper IDP IBM Security/ISS SiteProtector McAfee IntruShield HP TippingPoint Next-Generation Intrusion Prevention System (IPS) Check Point SmartDefense ForeScout SourceFire IPS appliances and DefenseCenter Load Balancers/Application Firewall F5 BIG-IP Local Traffic Manager F5 BIG-IP WebAccelerator F5 BIG-IP Application Security Manager Citrix NetScaler Dispositivos y Aplicaciones Soportados Network Flow Cisco NetFlow v5, v9 sFlow Cisco Application Visibility and Control (AVC) Routers and Switches Cisco IOS, Nx-OS, CatOS Juniper Junos

		Alcatel-Lucent TiMOS, AOS Brocade/Foundry IronWare HP ProCurve Cisco MDS Avaya (Nortel) ERS, Nortel Passport HP/3Com Comware Huawei VPR Extreme ExtremeWare XOS Mikrotik Router Storage EMC Data Domain EMC Isilon EMC VNX NetApp Data ONTAP Filer EMC CLARiiON EMC VNX Dell EqualLogic VMware and Host attached storage Virtualization VMware ESX, ESXi, vSphere, vCenter Wireless LAN Cisco WLAN Aruba ArubaOS NetMotion Mobility XE Vulnerability Scanners McAfee Foundstone Qualys QualysGuard Rapid7 Nexpose Tenable Nessus nCircle Protocolos Soportados 1.51) La solución deberá soportar los siguientes protocolos de colección y/o monitoreo: • Web – HTTP/HTTPS • DNS • FTP/SCP • Generic TCP/UDP • ICMP

		• IMAP4 • JDBC • LDAP • POP3 • POP3S • SMTP • SOAP • SSH • Telnet/SSH • SNMP • WMI • JMX Características de Análisis de Seguridad en Tiempo Real. 1.52) El módulo de analítica de eventos de seguridad deberá cumplir con mínimo las siguientes características: • Deberá soportar la correlación de eventos de múltiples fuentes, tales como firewalls, UPS, servidores, estaciones de trabajo entre otros. • Deberá soportar correlación cruzada de eventos. 1.53) Integración por medio de API's con fuentes de información externa sobre amenazas, tales como dominios de Malware, IPs, URLs, Hash y Nodos de Tor. 1.54) Integración Nativa con fuentes de información de terceros tales como ThreatStream, CyberArk, SANS y Zeus. 1.55) Deberá tener la Capacidad de Colección de logs, parsing de logs, indexación de logs a una tasa de al menos 10.000 EPS. 1.56) Capacidad de hacer monitoreo de la integridad de archivos o FIM tanto para Windows como Linux. 1.57) Deberá tener la capacidad de modificar los parsers por medio de interface gráfica, sin que esta modificación afecte la colección de logs o genere caídas en los servicios de la solución. 1.58) Deberá permitir la creación de Parsers customizados a partir de platillas XML. 1.59) Deberá tener la capacidad de colectar logs de forma segura, desde dispositivos remotos. 1.60) Deberá contar con un framework de notificación de incidentes el cuál deberá estar basado en políticas. 1.61) Deberá tener la capacidad de ejecutar scripts de remediación cuándo un incidente ocurra. 1.62) Deberá contar con un sistema propio de tickets. 1.63) Deberá tener la capacidad de integrarse con sistemas de tickets externos en caso de que la entidad lo requiera, dicha integración deberá ser por API y mínimo deberá soportar ServiceNow, ConnectWise, and Remedy. 1.64) Debe ser capaz de detectar anomalías en la línea base definida. 1.65) La detección de incidentes deberá ser en tiempo real anterior al almacenamiento del evento, utilizando técnicas del tipo "Correlación Distribuida".

		1.66) Deberá contar con una consola de visualización de logs y eventos correlacionados la cuál cuente con un sistema para el filtrado de los mismos por medio de condiciones booleanas. 1.67) Deberán poder realizarse filtros por medio de expresiones regulares. 1.68) El reporte de incidentes deberá poder ser priorizado por los servicios críticos. 1.69) Deberá permitir la identificación dinámica de usuarios. Administración y Reportes 1.70) La solución deberá contar con las siguientes características de administración y reportes: • La plataforma deberá poder ser administrada vía HTTPS. • La plataforma deberá tener una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas y tablas, lo cuál permita tener una visión global de los incidentes de seguridad. • La comunicación de los módulos deberá ser asegurada por temas de confidencialidad por medio de HTTPS. 1.71) Deberá contar con un módulo para el cálculo de los SLA. 1.72) Deberá contar con un módulo gráfico que muestre la infraestructura existente, las conexiones de las mismas y los eventos generados en cada activo. 1.73) Deberá contar con un dashboard que permita identificar en un mapa los incidentes y su ubicación geográfica. 1.74) Deberá contar con un módulo para administrar las políticas de correlación. 1.75) Deberá contar con un módulo para la administración de los agentes. 1.76) Deberá contar con un módulo de administración para la característica de CMDB. 1.77) La plataforma deberá tener un gran número de reportes predefinidos y deberá permitir crear reportes customizados. 1.78) El sistema propuesto debe ser del mismo fabricante que el Grupo 2.
Partida 2	**Cantidad**	**Descripción**
		• Hardware con **Sistema AntiSpam:** 1) Características del equipo tipo 1 (1 unidades). 1.1) Mínimo de 4 interfaces de 1Gbps RJ-45. 1.2) Mínimo de 2 interfaces de 1Gbps SFP. 1.3) Fuente de poder redundante. 1.4) Tener al menos 4 TBytes de espacio en disco, crecerlo a 12 tbytes. 1.5) Soportar RAID tipo hardware: 1, 5, 10, 50, Hot Spare. 1.6) Permitir configurar por lo menos 800 dominios.

		1.7) Soportar crear al menos 800 políticas por recipiente por dominio. 1.8) Soportar crear al menos 3K políticas por recipiente por sistema. 1.9) Soportar configurar al menos 2K mailboxes cuándo este operando en modo servidor. 1.10) Soportar enrutear al menos 1.1 M mensajes por hora. 1.11) Soportar como mínimo 1.0 M mensajes por hora con el análisis de antispam habilitado. 1.12) Soportar como mínimo 900K mensajes por hora con el análisis de antispam y antivirus habilitados. 2) Requisitos Mínimos de Funcionalidad • Funcionalidades Generales: 2.1) Solución debe basarse en "appliance" de propósito especifico. No se tendrán en cuenta los equipos de uso general (PCs o servidores) en la que se puede instalar y/o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux. 2.2) La solución debe tener características antispam, antivirus, anti-spyware y anti-phishing. 2.3) La solución debe ser capaz de realizar la inspección del correo de internet entrante y saliente. 2.4) La solución debe contar con un wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger. 2.5) La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam. 2.6) La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb. 2.7) La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing. 2.8) La solución debe proporcionar soporte para múltiples dominios de correo electrónico. 2.9) La solución debe ser compatible con la implementación de políticas por destinatario de dominio, del tráfico entrante o saliente. 2.10) La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicas, tales como anti-spam, anti-virus, autenticación, entre otros. 2.11) La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes. 2.12) La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP. 2.13) La solución debe soportar cuarentena por usuario, permitiendo que cada usuario pueda gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web y POP3. 2.14) La solución debe ser capaz de programar el envío de informes de cuarentena. 2.15) La solución debe ser capaz de realizar el almacenamiento de correo electrónico (archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto.

		2.16) La solución debe ser capaz de mantener la cola de correo que en caso de fallo en la conexión de salida, retrasos o errores de entrega. 2.17) La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP. 2.18) La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados. 2.19) La solución debe contar con capacidades de evaluar, retener y/o bloquear correos que cuenten con amenazas avanzadas, día cero mediante el análisis de archivos con herramientas de sandboxing. 2.20) La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail. 2.21) La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico. 2.22) La solución debe ser capaz de realizar análisis bayesiano para determinar si un correo es spam. 2.23) La solución debe ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidos en el cuerpo del mensaje. 2.24) La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words). 2.25) La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (relay), rechazar (reject) o descartar (discard). 2.26) La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM. 2.27) La solución debe ser capaz de soportar las listas negras de terceros (Blacklist). 2.28) La solución debe ser compatible con el enrutamiento en IPv4 y IPv6. 2.29) La solución debe ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6. 2.30) La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP). 2.31) La solución debe soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema. 2.32) La solución debe ser capaz de ejecutar el análisis antivirus/ antispyware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ y RAR. 2.33) La solución debe permitir la sobre escritura, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware. 2.34) La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent). 2.35) La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidos. 2.36) La solución debe ser compatible con Sender Policy Framework (SPF). 2.37) La solución debe ser compatible con Domain Keys Identified Mail (DKIM). 2.38) La solución debe ser compatible con Domain Based Message Authentication (DMARC). 2.39) La solución debe poder retrasar el envío de correos sobredimensionados a horarios que sean de menor carga.

		2.40) La solución debe poder definir el reenvío de correo (relay) a una IP especifica con base a la IP origen del mensaje. 2.41) La solución debe permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto. 2.42) La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS). 2.43) La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen. 2.44) La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura/escritura (reading/writing) o de sólo lectura (read only). 2.45) La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog). 2.46) La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica. 2.47) La solución debe generar informes por demanda o programados a intervalos de tiempo específicos. 2.48) La solución debe generar y enviar informes en formato PDF o HTML. 2.49) Cuándo la solución se implementa para alta disponibilidad debe ser capaz de controlar el estado del enlace. 2.50) Cuándo la solución se implementa para alta disponibilidad para soportar la conmutación por falla de red. 2.51) Cuándo la solución se implementa para alta disponibilidad, debe soportar el modo activo/pasivo. 2.52) Cuándo la solución se implementa para alta disponibilidad, debe ser capaz de sincronizar los mensajes de e-mails en cuarentena. 2.53) Cuándo la solución se implementa para alta disponibilidad activo/pasivo debería ser posible sincronizar los mensajes de correo electrónico y configuraciones. 2.54) Cuándo la solución se implementa para alta disponibilidad debe ser capaz de detectar y reportar el fallo de un dispositivo. 2.55) La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter). Funcionalidades de Server Mode 2.56) La solución debe soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. Debe ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo web, POP3 y/o IMAP. 2.57) La solución, estando en server mode, debe poder sincronizar contactos y calendarios con clientes de correo (MUA). 2.58) En modo server, debe soportar los protocolos WebDAV y CalDAV para la publicación y sincronización de calendarios. 2.59) La solución debe contar con algún mecanismo para la fácil migración de buzones y cuentas desde un servidor a la nueva solución estando en server mode. Funcionalidades de DLP

		2.60) También debe proporcionar una solución DLP para detectar la información sensible que puede estar llegando por e-mail. 2.61) La funcionalidad DLP debe permitir definir la información a detectar como palabras, frases y expresiones regulares. 2.62) La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros. 2.63) La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (fingerprint) de documentos. 2.64) La funcionalidad DLP para permitir la creación de filtros por tipos de archivos. 2.65) La funcionalidad DLP debe permitir la generación y almacenamiento de impresiones digitales (fingerprint) de los archivos adjuntos de correo electrónico. 2.66) La funcionalidad DLP debe permitir el almacenamiento de impresiones digitales (fingerprint) de archivos antiguos y también para los nuevos archivos que se han actualizado. Funcionalidades de IBE 2.67) Debe soportar cifrado de mensajes basado en identidad (IBE- Identity Based Encryption), de tal forma que el destinatario no requiera de un PSK o certificado previamente instalado para su descifrado. 2.68) El cifrado de mensajes con IBE, debe soportar tanto el método push como pull, donde el mensaje cifrado estará almacenado en la plataforma de correo para su acceso remoto autenticado, o bien sea enviado como un adjunto al destinatario. 2.69) En ambos métodos de cifrado con IBE se debe contar con un registro del destinatario en la plataforma de correo, de tal forma que para ver los mensajes cifrados se requiera un proceso de autenticación. RFCs soportadas requeridas y compatibilidad. 2.70) Debe soportar cifrado SMTPS y SMTP over TLS. 2.71) Debe soportar el RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II). 2.72) Debe soportar el RFC 1918 (Address Allocation for Private Internets). 2.73) Debe soportar el RFC 1985 (SMTP Service Extension for Remote Message Queue Starting). 2.74) Debe soportar el RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes). 2.75) Debe soportar el RFC 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies). 2.76) Debe soportar el RFC 2505 (Anti-Spam Recommendations for SMTP MTAs). 2.77) Debe soportar el RFC 2634 (Enhanced Security Services for S/MIME). 2.78) Debe soportar el RFC 2920 (SMTP Service Extension for Command Pipelining). 2.79) Debe soportar el RFC 3207 (SMTP Service Extension for Secure SMTP over TLS). 2.80) Debe soportar el RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs). 2.81) Debe soportar el RFC 3463 (Enhanced Mail System Status Codes).

		2.82) Debe soportar el RFC 3464 (Extensible Message Format for Delivery Status Notifications). 2.83) Debe soportar el RFC 3635 (Definitions of Managed Objects for the Ethernet-like Interface Types) 2.84) Debe soportar el RFC 4954 (SMTP Service Extension for Authentication). 2.85) Debe soportar el RFC 5321 (SMTP). 2.86) Debe soportar el RFC 5322 (Internet Message Format). 2.87) Debe soportar el RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures). 2.88) Debe soportar el RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages) 2.89) Debe soportar el RFC 6409 (Message Submission). 2.90) Debe soportar el RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail). 2.91) Debe soportar el RFC 2088 (IMAP4 Non-synchronizing Literals). 2.92) Debe soportar el RFC 2177 (IMAP4 Idle Command). 2.93) Debe soportar el RFC 2221 (Login Referrals). 2.94) Debe soportar el RFC 2342 (IMAP4 Namespace). 2.95) Debe soportar el RFC 2683 (IMAP4 implementation recommendations) 2.96) Debe soportar el RFC 2971 (IMAP4 ID Extension). 2.97) Debe soportar el RFC 3348 (IMAP4 Child Mailbox Extension). 2.98) Debe soportar el RFC 3501 (IMAP4 rev1). 2.99) Debe soportar el RFC 3502 (IMAP Multiappend Extension). 2.100) Debe soportar el RFC 3516 (IMAP4 Binary Content Extension). 2.101) Debe soportar el RFC 3691 (Unselect Command). 2.102) Debe soportar el RFC 4315 (UIDPLUS Extension). 2.103) Debe soportar el RFC 4469 (Catenate Extension). 2.104) Debe soportar el RFC 4731 (Extension to SEARCH Command for Controlling What Kind of Information Is Returned). 2.105) Debe soportar el RFC 4959 (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response). 2.106) Debe soportar el RFC 5032 (WITHIN Search Extension). 2.107) Debe soportar el RFC 5161 (Enable Extension). 2.108) Debe soportar el RFC 5182 (Extension for Referencing the Last SEARCH Result). 2.109) Debe soportar el RFC 5255 (IMAP Internationalization). 2.110) Debe soportar el RFC 5256 (Sort and Thread Extensions). 2.111) Debe soportar el RFC 5258 (List Command Extensions). 2.112) Debe soportar el RFC 5267 (Contexts for IMAP4). 2.113) Debe soportar el RFC 5819 (Extension for Returning STATUS Information in Extended LIST). 2.114) Debe soportar el RFC 6154 (LIST Extension for Special-Use Mailboxes).

		2.115) Debe soportar el RFC 6851 (MOVE extension). 2.116) Debe soportar el RFC 7162 (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC). 2.117) Debe soportar el RFC 1939 (POP3). 2.118) Debe soportar el RFC 2449 (POP3 Extension Mechanism). 2.119) Debe soportar el RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface). 2.120) Debe soportar el RFC 1157 (SNMP v1). 2.121) Debe soportar el RFC 1213 (MIB 2). 2.122) Debe soportar el RFC 2578 (Structure of Management Information Version 2). 2.123) Debe soportar el RFC 2579 (Textual Conventions for SMIv2). 2.124) Debe soportar el RFC 2595 (Using TLS with IMAP, POP3 and ACAP). 2.125) Debe soportar el RFC 3410 (SNMP v3). 2.126) Debe soportar el RFC 3416 (SNMP v2). 2.127) El equipo deberá ser de las misma marca que la solución ofertada del sistema solicitado SIEM. 2.128) El equipo deberá enviar logs a sistema de FortiAnalyzer con el que cuenta la Universidad de Guadalajara. 3) Garantías y Requisitos 3.1) La solución deberá contar con 12 meses de soporte 8x5, actualizaciones de firmware, actualizaciones de antivirus, actualizaciones de antispam y reemplazo al siguiente día hábil. 3.2) El licitante deberá presentar carta del fabricante donde indique que es distr1ibuidor autorizado de la marca. 3.3) El licitante deberá presentar carta del fabricante o distribuidor donde indique que cuenta con el apoyo técnico y comercial de la solución propuesta 3.4) El sistema propuesto debe ser del mismo fabricante que el Grupo 1.
	1	• Insumos de Montaje y Raqueo UPS GXT4 2000 VA On-Line Doble Conversion, Rack/Torre2000 VA / 1800 W, 120V, with int. battery, with rackmount kit Voltaje de Entrada 120 Voltaje de Salida 120.
	1	External Battery Module UPS GXT4 500-2000 VA, Rack/TorreExternal Battery Cabinet for 500-2000 VA UPS (can order up to 6 for each UPS ordered).
	1	GXT4 1000 VA On-Line Doble Conversion, Rack/Torre 1000 VA / 900 W, 120V, with int. battery, with rackmount kit Voltaje de Entrada 120 Voltaje de Salida 120.
	1	GF Serier Global Frame Cabinetsystem Gen 2 600X1000X42ur.

	2	Jumper 2MM SC - LC MM 50/125 Duplex 05M.
	4	Jumper 2MM SC - LC MM 50/125 Simplex 14.50M Aquaoptimax.
	4	Convertidor de medios TP-LINK mono modo conector de fibra SC A RJ45 10/100MBPS dúplex total hasta 20 MC110CS.
	2	Charola para servidores montada en rack de aluminio capacidad de carga 50 KG.
	1	Servicio de embarque Gabinete IT (incluye empaque, embalaje, recolección, embarque, envio y entrega de Gabinete 2100 x800x1000mm.

4.- Documentación a entregar

El Ofertante deberá entregar como parte de su propuesta técnica la siguiente documentación:

a. La empresa deberá incluir carta original, dirigida a la convocante y relacionado a este proceso de adquisición, en hoja membretada del fabricante, firma autógrafa por el representante en México de la marca propuesta, donde se indique bajo protesta de decir verdad, lo siguiente:

- Que la empresa es distribuidor o integrador certificado en territorio mexicano de sus productos y servicios:

b. Copia de las constancias emitidas por el fabricante de los equipos propuestos donde se demuestre que el personal cuente con la certificación necesaria para la implementación y configuración requerida.

c. El ofertante deberá considerar en su propuesta una póliza de mantenimiento por 1 año que incluya soporte en sitio y remplazo de partes de hardware.

El ofertante que resulte el adjudicado deberá entregar una vez realizada la implementación la memoria técnica de la implementación en formato digital que contenga como mínimo:

1. Diseño de la solución.
2. Archivos de configuración de todo el sistema.
3. Sobre con cuentas y contraseñas para la administración.
4. Resultados de pruebas de operación y desempeño realizados a la infraestructura implementada.
5. Tablas de configuraciones presentes en cada dispositivo.
6. Estadísticas del desempeño de cada equipo.

La solución solicitada forma parte de un sistema conjunto por lo que las funcionalidades deberán validarse en conjunto y su configuración debe ser compatible con el hardware existente y con las configuraciones de la Universidad de Guadalajara y su adjudicación será a un solo licitante.

4.1 Capacitación

Deberá incluirse la capacitación certificada por el fabricante para 4 personas en la administración básica y avanzada de las 2 soluciones propuestas.

Deberá incluir capacitación para 6 personas por parte del fabricante en la administración de la librería de respaldo y de su integración con el ambiente de respaldos actuales (librería física y software de administración veeam).

4.2 Servicios Profesionales requeridos para la implementación del proyecto

Partida 1
La implementación y configuración de la solución ofertada deberá considerar:

- Planeación de cada una de las actividades con el fin de disminuir los tiempos de implementación de la solución.
- Planeación y diseño de implementación bajo mejores prácticas.
- Configuración de los equipos solicitados en rack estándar.
- Habilitar los equipos con la última versión estable del firmware.
- Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
- Planeación de la implementación a realizar asesorando a la entidad en el alcance de la correlación de seguridad a realizar en los dispositivos que se acuerden.
- Planeación de la implementación a realizar asesorando a la entidad en el alcance del monitoreo a realizar en los dispositivos que se acuerden.
- Creación de los conectores necesarios para un correcto monitoreo/correlación de las plataformas que se requieran.
- Desarrollar un plan de pruebas que permita garantizar la correcta operación del sistema integrado a la infraestructura actual.
- Se debe dar capacitación de la herramienta tanto en operación como en mantenimiento directamente por parte del fabricante.
- Se debe incluir soporte directo de fábrica en la configuración inicial del producto.
- Transferencia de conocimientos en sitio.

Partida 2
La implementación y configuración de la solución ofertada deberá considerar:

- Planeación de cada una de las actividades con el fin de disminuir los tiempos de implementación de la solución.
- Planeación y diseño de implementación bajo mejores prácticas.
- configuración de los equipos solicitados en rack estándar.
- Habilitar los equipos con la última versión estable del firmware.
- Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
- Planeación de la implementación a realizar asesorando a la entidad en el alcance de la seguridad en los sistemas que se acuerden.
- Planeación de la implementación a realizar asesorando a la entidad en el alcance del monitoreo a realizar en los dispositivos que se acuerden.
- Desarrollar un plan de pruebas que permita garantizar la correcta operación del sistema integrado a la infraestructura actual.
- Se debe dar capacitación de la herramienta tanto en operación como en mantenimiento directamente por parte del Fabricante.
- Se debe incluir soporte directo de fábrica en la configuración inicial del producto.
- Transferencia de conocimientos en sitio.

5.- Consideraciones adicionales

- La propuesta deberá considerar todo lo necesario para la completa y correcta operación de los componentes solicitados a configurar en el site donde la Universidad de Guadalajara lo indique.
- El licitante deberá comprobar experiencia en la configuración de los equipos propuestos en las partidas a través de cartas de fabricante o documentos de al menos 3 clientes.
- Se deberán considerar cables de fibra necesarios para la conectividad.
- Administración de tiempos para la entrega y configuración.
- Una vez que se designe al licitante adjudicado y partiendo de dicha fecha, éste deberá sujetarse a los siguientes tiempos para la entrega de la operación de los componentes solicitados:
    - Tiempo de entrega de la totalidad de los componentes solicitados: Un período máximo de 6 semanas.
    - Tiempo de configuración: Un período máximo de 4 semanas.
- En caso de que alguna actividad de la Universidad de Guadalajara se pudiera ver afectada dentro del proceso de configuración, se podría presentar un cambio en los tiempos de configuración solicitado por la Universidad de Guadalajara al proveedor.
- Las funcionalidades aquí plasmadas serán verificadas previamente a la "aceptación de la adquisición", por lo que el proveedor deberá considerar 2 días hábiles posteriores a la entrega de la operación de la solución para que la Coordinación General de Tecnologías de Información valide las funcionalidades en la operación con base en lo solicitado.
- Las condiciones de garantía, servicios de soporte y licenciamiento incluido correrán a partir de la fecha de aceptación mencionada en el punto anterior.
- El proveedor deberá incluir en su propuesta la transferencia de conocimiento a personal designado por la Universidad de Guadalajara sobre la administración y conocimiento general del equipo adquirido.
- La marca propuesta deberá ser de calidad reconocida en el mercado y que cuente con al menos ocho años de representación en México y/o Guadalajara.
- Que el proveedor tenga oficina en la ciudad de Guadalajara y con posibilidad de visitar sus instalaciones para garantizar el soporte solicitado.
- Que el proveedor tenga al menos 1 ingeniero certificado en la plataforma propuesta.

6.- Administración de tiempos para la entrega y configuración

Una vez que se designe al proveedor ganador y partiendo de dicha fecha, éste deberá sujetarse a los siguientes tiempos para la entrega de la operación de los componentes solicitados:

- Tiempo de entrega de la totalidad de los componentes solicitados: Un período máximo de 6 semanas.
- Tiempo de configuración: Un período máximo de 4 semanas.

En caso de que alguna actividad de la Universidad de Guadalajara, se pudiera ver afectada dentro del proceso de configuración, se podría presentar un cambio en los tiempos de configuración solicitado por la Universidad de Guadalajara al proveedor.

7.-Actividades a realizarse posteriores a la designación del proveedor

- Las funcionalidades aquí plasmadas serán verificadas previamente a la "aceptación de la adquisición", por lo que el proveedor deberá considerar 2 días hábiles posteriores a la entrega de la operación del o los equipos para que la Coordinación General de Tecnologías de Información valide las funcionalidades en la operación con base en lo solicitado.
- Las condiciones de garantía, servicios de soporte y licenciamiento incluido correrán a partir de la fecha de aceptación mencionada en el punto anterior.
- El proveedor deberá incluir en su propuesta la transferencia de conocimiento a personal designado por la CGTI sobre la administración y conocimiento general del equipo adquirido.
- El proveedor deberá entregar la memoria técnica que incluya todos los datos de configuración y características generales del equipo.

8.- Notas adicionales

Se deberá incorporar al contrato correspondiente, los requisitos y condiciones planteadas en este documento.

SECCIÓN IV
CARTA DE SERIEDAD DE LA PROPUESTA

Licitación No. LI-044-CGTI-2017

Dra. Carmen Enedina Rodríguez Armenta
Secretaria Ejecutiva del Comité General
de Compras y Adjudicaciones de la
Universidad de Guadalajara.
Presente.

En referencia a la convocatoria publicada el 29 de septiembre de 2017, mediante la cual se invita a participar en la Licitación Pública No. LI-044-CGTI-2017, relativa a la contratación para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información, 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 la Universidad de Guadalajara 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
Guadalajara, Jalisco a_____de_____de 2017

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

Sección V
CARTA COMPROMISO

Licitación No. LI-044-CGTI-2017

Dra. Carmen Enedina Rodríguez Armenta
Secretario Ejecutivo del Comité General
de Compras y Adjudicaciones de la
Universidad de Guadalajara.
Presente.

Luego de haber examinado los documentos de la licitación, de los cuales confirmamos recibo por la presente, los suscritos ofrecemos prestar los servicios para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información, de conformidad con dichos documentos, por la suma de $ ----------(monto total de la oferta en palabras y cifras) 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, correspondiente al 10% del monto total adjudicado en el contrato respectivo, para asegurar su debido cumplimiento.

Convenimos en mantener esta oferta por un período de 30 días naturales después 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 su aceptación por escrito incluida en el acta de lectura de fallo de la licitación constituirá un contrato obligatorio hasta que se prepare y firme un 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 2017

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

FORMATO DE PROPUESTA

HOJA MEMBRETADA DE LA EMPRESA

PROPUESTA ECONÓMICA: LICITACIÓN NÚMERO LI-044-CGTI-2017, para el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

PARTIDA	CANTIDAD	DESCRIPCIÓN	COSTO UNITARIO	SUBTOTAL
1				
			SUBTOTAL	
			IVA	
			TOTAL	

TOTAL CON LETRA.
VIGENCIA: DE LA PROPUESTA QUE NO DEBE SER MENOR A 30 DIAS NATURALES DESPUES DE LA FECHA DE LA APERTURA DE PROPUESTAS.
FORMA DE PAGO: CONTRA ENTREGA.
TIEMPO DE ENTREGA: ESPECIFICAR EL TIEMPO EN EL QUE ENTREGARA DE LOS BIENES.
GARANTÍA: ESPECIFICAR LA GARANTÍA DE LOS EQUIPOS.

LUGAR Y FECHA

FIRMA DEL RESPONSABLE DE LA ELABORACIÓN DE LA PROPUESTA

UNIVERSIDAD DE GUADALAJARA
VICERRECTORÍA EJECUTIVA
COORDINACIÓN GENERAL ADMINISTRATIVA

ACTA DE FALLO

LICITACIÓN: LI-044-CGTI-2017
DEPENDENCIA: Coordinación General de Tecnologías de Información
NOMBRE: Suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

En la Ciudad de Guadalajara, Jalisco siendo las 19:05 horas del día 30 de octubre del 2017, se reunieron en la sala de juntas de la Coordinación General Administrativa, ubicada en Av. Juárez número 976, piso cuatro del Edificio de la Rectoría General, los integrantes del Comité General de Compras y Adjudicaciones para emitir el siguiente fallo.

El Lic. José Andrés Orendáin de Obeso, Presidente del Comité General de Compras y Adjudicaciones, con base en las atribuciones contempladas en el Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara, se llevó al cabo el análisis de los documentos presentados por la Coordinación de Servicios Generales de la Administración General e hizo saber que el suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información, corresponde a la:

Empresa: SOONET S. DE R.L. DE C.V.

Partidas: 1 y 2

Por un monto total de: (número y letra) **$ 2,075,535.22** **IVA INCLUIDO**

Dos millones setenta y cinco mil quinientos treinta y cinco pesos 22/100 M.N.

En virtud de haber reunido las condiciones legales, técnicas y económicas requeridas por la Coordinación de Servicios Generales de la Administración General, garantizar satisfactoriamente el cumplimiento de las obligaciones respectivas y haber presentado la propuesta solvente más baja de conformidad con los artículos 19, 20, 25, 44, 45 y 47 del Reglamento de Adquisiciones, Arrendamiento y Contratación de Servicios de la Universidad de Guadalajara.

Dra. Carmen E. Rodríguez Armenta
Secretaria Ejecutiva del Comité General de Compras y Adjudicaciones

Lic. José Andrés Orendáin de Obeso
Presidente del Comité General de Compras y Adjudicaciones

DICTAMEN TÉCNICO

Guadalajara, Jalisco, 27 de octubre de 2017

LICITACIÓN: LI-044-CGTI-2017
DEPENDENCIA: Coordinación General de Tecnologías de Información
NOMBRE: Suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información.

1.- Propuestas declaradas solventes, porque cumplen con todos los requisitos solicitados:

No.	EMPRESA	IMPORTE INCLUYE I.V.A.
1	Sodenet S. de R.L. de C.V. Partidas: 1 y 2	$2,075,535.22
2	Initel, S.A. de C.V. Partidas: 1 y 2	$2,090,567.93
3	Estrategias en Tecnología Corporativa, S.A. de C.V. Partidas: 1 y 2	$2,418,504.30

2.- Criterios utilizados para la evaluación de la propuesta:

La Coordinación General de Tecnologías de Información, realizó 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, las bases y la junta de aclaraciones, así como los siguientes aspectos:

I) Se tomaron en cuenta sus antecedentes, su especialidad, su capacidad operativa y financiera manifestados en su expediente.

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

a) Que las propuestas contemplen todas y cada una de las condiciones generales de 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 tengan error, se efectuaran las correcciones correspondientes, el monto correcto será el que se considerará para el análisis de la propuesta.

Av. Juárez 976, Edificio de la Rectoría General, Piso 4, Colonia Centro C.P. 44100.
Guadalajara, Jalisco, México. Tels. [52] (33) 3134 2236, 3134 2237
www.cgadm.udg.mx

d) Se consideró la opinión técnica emitida por la Coordinación General de Tecnologías de Información, cuyos documentos se adjuntan como parte integrante del presente dictamen, así como la revisión de cumplimiento documental de las propuestas, que consistieron en lo siguiente:

- Verificación de cumplimiento de las especificaciones técnicas requeridas.
- Cumplimiento de los requisitos documentales para el proveedor.
- Condiciones de pago.
- Precio.
- Vigencia de la cotización.
- Garantías.

3.- Resultado de la revisión técnica de las propuestas, efectuada por la Coordinación General de Tecnologías de Información:

La licitación LI-044-CGTI-2017 consta de 2 partidas que incluye los requisitos indispensables que deben cubrir las propuestas, participan 3 proveedores que son: Estrategias en Tecnología Corporativa S.A. de C. V., Initel S.A. de C.V. y Sodenet S. de R.L. de C.V.,

Para las partidas 1 y 2 los tres proveedores cumplen con todos los requisitos solicitados en bases.

4.- De conformidad con la revisión y evaluación de las propuestas presentadas, con base en la opinión técnica de la Coordinación General de Tecnologías de Información y la Coordinación de Servicios Generales de la Administración General se sugiere que la adquisición de Suministro de un sistema de correlación de eventos para red dorsal de datos de la Universidad de Guadalajara y un sistema de protección antispam, antivirus, anti-spyware y anti-phishing para plataformas de correo universitarias, para la Coordinación General de Tecnologías de Información, se adjudique de la siguiente manera:

Empresa	**Monto incluye I.V.A.**
Sodenet S. de R.L. de C.V. Partidas: 1 y 2	$2,075,535.22

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 apego a lo establecido en los artículos 19, 20, 25, 44, 45 y 47 del Reglamento de Adquisiciones, Arrendamientos y Contratación de Servicios de la Universidad de Guadalajara.

ELABORÓ

LAE. Héctor Sención Solorzano
Jefe de la Unidad de Adquisiciones de la Coordinación de Servicios Generales de la Administración General

AUTORIZÓ

Ing. Esteban Segura Estrada
Coordinador de Servicios Generales
Administración General

Av. Juárez 976, Edificio de la Rectoría General, Piso 4, Colonia Centro C.P. 44100.
Guadalajara, Jalisco, México. Tels. [52] (33) 3134 2236, 3134 2237
www.cgadm.udg.mx