INSTITUTO FEDERAL DE TELECOMUNICACIONES
UNIDAD DE ADMINISTRACIÓN

INSTITUTO FEDERAL DE TELECOMUNICACIONES

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

En la Ciudad de México, Distrito Federal siendo las 12:00 horas, del 28 de octubre del 2014, en la sala de juntas de la Unidad de Administración del Instituto Federal de Telecomunicaciones (IFT), ubicada en Insurgentes Sur Núm. 838, Primer Piso, Colonia Del Valle, Código Postal 03100, Delegación Benito Juárez, México, Distrito Federal, se reunieron los servidores públicos cuyos nombres y firmas aparecen al final de la presente Acta, con el objeto de lleva a cabo la junta de aclaraciones a la convocatoria de la Licitación indicada al rubro, de acuerdo a lo previsto en los artículos 32 y 33 de las Normas en materia de adquisiciones, arrendamientos y servicios del Instituto Federal de Telecomunicaciones (Normas); 39 y 40 de los Lineamientos en materia de adquisiciones, arrendamientos y servicios del Instituto Federal de Telecomunicaciones (Lineamientos), así como del numeral III, incisos b) y b.2) de la convocatoria a la Licitación.

Este acto fue presidido por el Lic. Oscar E. Ibarra Martínez, Director General de Adquisiciones, Recursos Materiales y Servicios Generales, quien al inicio de esta junta, comunicó a los asistentes que de conformidad con los artículos 33 de las Normas, 39 y 40 de los Lineamientos, solamente se atenderán solicitudes de aclaración a la convocatoria de las personas que hayan presentado el escrito en el que expresen su interés en participar en esta Licitación a través de CompraNet, por sí o en representación de un tercero, y cuyas preguntas se hayan recibido con 24 (veinticuatro) horas de anticipación a este acto.

El Presidente del acto, fue asistido por el Lic. Ney Galicia Arrocena, Director de Área y el C. Mauro Alfredo Balderas Fajardo, Subdirector de Área, ambos dependientes de la Dirección General de Tecnologías de la Información y Comunicaciones, para resolver las preguntas de carácter técnico.

Y la C.P. Laura Berenice Vanegas Luna, Subdirectora de Recursos Materiales, para responder las preguntas de carácter administrativo.

A continuación el Presidente del acto, hizo constar lo siguiente:

---

1) Que se recibieron en tiempo y forma, las solicitudes de aclaración a la Convocatoria a la Licitación indicada al rubro y los escritos de interés en participar a través del sistema CompraNet, de conformidad con el artículo 33 de las Normas, conforme a lo siguiente:

Licitante	Escrito de Interés	Preguntas
INDRA SISTEMAS MÉXICO, S.A. DE C.V.	X	X
SM4RT SECURITY SERVICES, S.A. DE C.V.	X	X
CISCO SYSTEMS DE MÉXICO. S.A. DE C.V.	X	X
SCITUM, S.A. DE C.V	X	X
INTEGRADORES DE TECNOLOGÍA, S.A. DE C.V.	X	X
AXTEL S.A.B. DE C.V.	X	X
METRO NET S.A.P.I. DE C.V.	X	X

---

2) Que se recibieron solicitudes de aclaración a la convocatoria en el sistema CompraNet, de los Licitantes citados en la tabla siguiente, sin embargo no cumplen con lo señalado en el inciso b.2) de la Convocatoria así como en el artículo 42 fracción V de los Lineamientos, por lo que no se les dará respuesta.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

Licitante	Motivo	Preguntas
VANUME, S.DE R.L. DE C.V.	El escrito de Interés no cumple con los requisitos establecidos	No
ADVANCED DATA SERVICES, S.A. DE C.V.	Escrito de Interés y preguntas enviadas fuera del plazo establecido en la convocatoria a la licitación.	Si

---

3) Con fundamento en lo dispuesto por el artículo 40 de los Lineamientos y en atención al numero de solicitudes de aclaración recibidas, el IFT determina suspender la sesión y señala nueva fecha y hora para continuar con la misma para el 31 de octubre de 2014 a las 10:00, en este mismo lugar.

Derivado de lo anterior, a continuación se trascriben las solicitudes de aclaración recibidas para que los licitantes conozcan los planteamientos realizados a los que el IFT dará atención en la fecha y hora señalada anteriormente.

INDRA SISTEMAS MÉXICO, S.A. DE C.V.

No.	Preguntas
1	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente a la convocante indique la fecha de realización del estudio de mercado relacionado con el presente proceso de contratación.
2	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente al área solicitante, al área de adquisiciones y al Órgano Interno de Control de la convocante indicar si el estudio de mercado realizado utilizó de manera completa e integra los requisitos planteados en las presentes bases y sus anexos, por lo que solicitamos amablemente a la Convocante adicionalmente a la respuesta, incluir las bases utilizadas para el estudio de mercado.
3	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente al área solicitante, al área de adquisiciones y al Órgano Interno de Control de la convocante indicar si el estudio de mercado realizado utilizó de manera completa e integra los requisitos planteados en las presentes bases y sus anexos, adicionalmente solicitamos a la Convocante incluir en su respuesta, el resultado, que incluye las respuestas recibidas por parte de las empresas y contratos evaluados como parte del estudio de mercado.
4	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente a la convocante indique si la validación en el estudio de mercado se verificó la existencia de un número de empresas que pudieran ofrecer los servicios solicitados, así como el número de empresas que se determinó pueden cumplir con la totalidad de los requerimientos solicitados, incluyendo los requisitos relacionados con el SOC principal, SOC redundante, Centro de datos, entre otros establecidos en la presente.
5	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente a la convocante indique si el estudio de mercado realizado y las respuestas al mismo fue validado por el Órgano Interno de Control de la dependencia o la Secretaría de la Función Pública, con el objetivo de asegurar que un número mínimo de empresas cumplieran con los requisitos especificados en el mismo, obteniendo además el puntaje mínimo de 45 puntos o superior, que les permitiera presentar propuestas viables de ser evaluadas.
6	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente a la convocante indicar el número y nombre de las empresas evaluadas en el estudio de mercado que de acuerdo con la tabla de puntos y porcentajes establecida, tienen la capacidad de obtener de 59 a 60 puntos, de 50 a 59 puntos, de 45 a 50 puntos respectivamente, considerando los requisitos definidos para SOC/SOC redundante (establecido en el numeral "Equipamiento – Centro de Operaciones de Seguridad" del documento Criterios de Evaluación de Puntos y Porcentajes) y Centro de Datos (establecido en el numeral "3.2.2.3 Centro de Datos del SOC" del ANEXO TÉCNICO), Certificación de 27001 con plazo mínimo de 3 años, procesos específicos en el certificado 27001, número de procesos del certificado 27001 (establecido en el numeral "Metodología para la prestación del servicio" del documento Criterios de Evaluación de Puntos y Porcentajes) .
7	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente al Área Solicitante de la Convocante, indique si con base en la tabla de puntos y porcentajes, los requisitos establecidos tanto en el anexo técnico como en los requisitos para la obtención de puntos, y con base en el número de participantes que estarían en posibilidad de obtener de 59 a 60 puntos, de 50 a 59 puntos, y de 45 a 50 puntos de acuerdo con la respuesta a la pregunta 6 Administrativa de Indra, el proceso de contratación se desprende a partir de la investigación de mercado, según lo requerido en el Artículo 26 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Así como si el proceso de contratación está sustentado en una investigación de mercado que cumpliera con el propósito definido para dicha investigación, según lo establecido en el Artículo 29 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASP), emitido por la Cámara de Diputados y publicado en el Diario Oficial de la Federación. Cabe destacar que el artículo 29 del RLAASP (Reglamento) establece lo siguiente:

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	La investigación de mercado tendrá como propósito que las dependencias y entidades: I. Determinen la existencia de oferta de bienes y servicios en la cantidad, calidad y oportunidad requeridas por las mismas; II. Verifiquen la existencia de proveedores a nivel nacional o internacional con posibilidad de cumplir con sus necesidades de contratación, y III. Conozcan el precio prevaleciente de los bienes, arrendamientos o servicios requeridos, al momento de llevar a cabo la investigación. Lo anterior con el objetivo de prevenir que únicamente un número limitado de participantes puedan presentar propuestas solventes, limitando así la libre competencia e incrementando de esta manera los precios de contratación, contraviniendo que asegure al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes, de acuerdo a lo requerido el artículo 26 de la Ley.
8	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente al Área Responsable de Adquisiciones de la Convocante, indique si con base en la tabla de puntos y porcentajes, los requisitos establecidos tanto en el anexo técnico como en los requisitos para la obtención de puntos, y con base en el número de participantes que estarían en posibilidad de obtener de 59 a 60 puntos, de 50 a 59 puntos, y de 45 a 50 puntos de acuerdo con la respuesta a la pregunta 6 Administrativa, el proceso de contratación se desprende a partir de la investigación de mercado, según lo requerido en el Artículo 26 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Así como si el proceso de contratación está sustentado en una investigación de mercado que cumpliera con el propósito definido para dicha investigación, según lo establecido en el Artículo 29 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASP), emitido por la Cámara de Diputados y publicado en el Diario Oficial de la Federación. Cabe destacar que el artículo 29 del RLAASP (Reglamento) establece lo siguiente: La investigación de mercado tendrá como propósito que las dependencias y entidades: I. Determinen la existencia de oferta de bienes y servicios en la cantidad, calidad y oportunidad requeridas por las mismas; II. Verifiquen la existencia de proveedores a nivel nacional o internacional con posibilidad de cumplir con sus necesidades de contratación, y III. Conozcan el precio prevaleciente de los bienes, arrendamientos o servicios requeridos, al momento de llevar a cabo la investigación. Lo anterior con el objetivo de prevenir que únicamente un número limitado de participantes puedan presentar propuestas solventes, limitando así la libre competencia e incrementando de esta manera los precios de contratación, contraviniendo que asegure al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes, de acuerdo a lo requerido el artículo 26 de la Ley.
9	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente al Órgano Interno de Control de la Convocante, indique si con base en la tabla de puntos y porcentajes, los requisitos establecidos tanto en el anexo técnico como en los requisitos para la obtención de puntos, y con base en el número de

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	participantes que estarían en posibilidad de obtener de 59 a 60 puntos, de 50 a 59 puntos, y de 45 a 50 puntos de acuerdo con la respuesta a la pregunta 6 Administrativa, el proceso de contratación se desprende a partir de la investigación de mercado, según lo requerido en el Artículo 26 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Así como si el proceso de contratación está sustentado en una investigación de mercado que cumpliera con el propósito definido para dicha investigación, según lo establecido en el Artículo 29 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASP), emitido por la Cámara de Diputados y publicado en el Diario Oficial de la Federación. Cabe destacar que el artículo 29 del RLAASP (Reglamento) establece lo siguiente: La investigación de mercado tendrá como propósito que las dependencias y entidades: I. Determinen la existencia de oferta de bienes y servicios en la cantidad, calidad y oportunidad requeridas por las mismas; II. Verifiquen la existencia de proveedores a nivel nacional o internacional con posibilidad de cumplir con sus necesidades de contratación, y III. Conozcan el precio prevaleciente de los bienes, arrendamientos o servicios requeridos, al momento de llevar a cabo la investigación. Lo anterior con el objetivo de prevenir que únicamente un número limitado de participantes puedan presentar propuestas solventes, limitando así la libre competencia e incrementando de esta manera los precios de contratación, contraviniendo que asegure al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes, de acuerdo a lo requerido el artículo 26 de la Ley.
10	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente a la convocante indique de su estudio de mercado realizado cuales empresas de las que dieron respuesta o que fueron investigadas y que tienen la capacidad de entregar los servicios solicitados de acuerdo con las especificaciones de la presente licitación y sus anexos, cumplen explícitamente con todas y cada una de las siguientes características solicitadas para el SOC: - Certificación TIER 1 o ICREA 2. - Certificación 27001 con 3 años de antigüedad. - Certificación 27001 abarcando los procesos de Administración de cambios y Administración de incidentes de seguridad. - Contar con un SOC alterno propio de la compañía ubicado al menos a 50 km del SOC principal. En caso de que el número sea menor a 5, solicitamos amablemente a la convocante que con el objetivo de permitir la libre competencia, se eliminen los requisitos de certificación, número de años de antigüedad de los certificados, alcance en procesos certificados, así como cualquier otro requisito para el cual no se cumpla un número mínimo de 5 empresas que tienen la capacidad de dar cumplimiento y entregar los servicios.
11	Criterios específicos conforme a los cuales se evaluarán las proposiciones y se adjudicará el contrato respectivo. V.1 Criterios de Evaluación. Página 16. Solicitamos amablemente a la convocante indique del estudio de mercado realizado cuales empresas de las que dieron respuesta confirmaron explícitamente cumplir con la certificación 27001 tanto para al menos 3 procesos, como para al menos 8 procesos de los especificados en el Anexo Técnico, y en todos y cada uno de los procesos especificados en la

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	sección "Metodología para la prestación del servicio" del documento "CRITERIOS DE EVALUACIÓN DE PUNTOS Y PORCENTAJES".
12	3.2.1.2 Administración y monitoreo de la infraestructura de seguridad perimetral existente – Página 12 Solicitamos amablemente a LA CONVOCANTE indicar, ¿SI es correcto interpretar que el personal que forme parte del servicio "Gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT" deberá operar está infraestructura durante la duración del contrato?
13	3.2.1.4 Condiciones de los Servicios de Seguridad Administrada – Página 16. Se hace el requerimiento puntual de un enlace dedicado de al menos 4Mb entre el Centro de Datos Principal del IFT y el SOC del Proveedor Adjudicado, pero no se solicita ningún enlace al SOC redundante. Solicitamos amablemente indicar si nuestra apreciación es correcta.
14	3.2.1.4 Condiciones de los Servicios de Seguridad Administrada – Página 16. Se hace de conocimiento a los participantes que la falla en el enlace deberá estar resuelta en un plazo no mayor a 4 horas. Debido a que se está solicitando un SOC redundante, la falla no debería de existir a menos de que fallen los enlaces de ambos SOCs, ya que el SOC redundante deberá de entrar inmediatamente cuando se presente la falla en el SOC primario. ¿Es correcta nuestra interpretación?
15	3.2.1.4 Condiciones de los Servicios de Seguridad Administrada – Página 16. En caso de superar las 4 horas de plazo, solicitamos amablemente a LA CONVOCANTE indicar la medida de nivel de servicio y deductiva a la que se estará sujeto el LICITANTE GANADOR.
16	3.2.1.4 Condiciones de los Servicios de Seguridad Administrada – Página 17 Se solicita de forma trimestral la entrega de la información de correlación de eventos en un medio externo y en el punto 3.2.1.7 Servicio de correlación de eventos y administración de bitácoras se solicita de forma anual. Solicitamos amablemente a LA CONVOCANTE indicar, ¿cuál es el correcto o en todo caso indicar la diferencia entre ambos entregables?
17	3.2.1.7 Servicio de correlación de eventos y administración de bitácoras – Página 21 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá ser nueva y sin vicios ocultos y el LICITANTE GANADOR deberá presentar a LA CONVOCANTE las cartas de garantía por la duración del contrato de la solución propuesta?
18	3.2.1.7 Servicio de correlación de eventos y administración de bitácoras – Página 21 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá estar físicamente en las instalaciones del Centro de Datos Principal del IFT?
19	3.2.1.8 Análisis de vulnerabilidades y pruebas de penetración a) Análisis de Vulnerabilidades - Página 25 Solicitamos amablemente a LA CONVOCANTE indicar, ¿SI es correcto interpretar que la solución deberá ser nueva y sin vicios ocultos y el LICITANTE GANADOR deberá presentar a LA CONVOCANTE las cartas de garantía por la duración del contrato de la solución propuesta?
20	3.2.1.8 Análisis de vulnerabilidades y pruebas de penetración a) Análisis de Vulnerabilidades - Página 25 Solicitamos amablemente a LA CONVOCANTE indicar, ¿SI es correcto interpretar que la solución deberá estar físicamente en las instalaciones del Centro de Datos Principal del IFT?
21	3.2.1.9 Servicio de control de acceso Firewall – Página 30 Solicitamos amablemente a LA CONVOCANTE indicar, ¿SI es correcto interpretar que la solución deberá ser nueva y sin vicios ocultos y el LICITANTE GANADOR deberá presentar a LA CONVOCANTE las cartas de garantía por la duración del contrato de la solución propuesta?

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
22	3.2.1.9 Servicio de control de acceso Firewall – Página 30 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que las soluciones de Firewall de sitio principal y secundario pueden ser de distintos fabricantes?
23	3.2.1.9 Servicio de control de acceso Firewall – Página 30 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que las consolas de administración de los Firewalls pueden estar en el SOC del LICITANTE o también se deberán de tener físicamente en los centros de datos de LA CONVOCANTE?
24	3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos. – Página 41 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá ser nueva y sin vicios ocultos y el LICITANTE GANADOR deberá presentar a LA CONVOCANTE las cartas de garantía por la duración del contrato de la solución propuesta?
25	3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos. – Página 41 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá estar físicamente en las instalaciones del Centro de Datos Principal del IFT?
26	3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos. – Página 41 Solicitamos amablemente a LA CONVOCANTE indicar sí las soluciones de Protección de Aplicaciones WEB, Servidores de Archivos y de Base de datos, se deben de considerar en Alta Disponibilidad.
27	3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos. – Página 41 Solicitamos amablemente a LA CONVOCANTE sí la consola de administración deberá estar físicamente en el Centro de datos Principal de LA CONVOCANTE o puede estar físicamente en el SOC del LICITANTE
28	3.2.1.11 Servicios de protección para correo electrónico. – Página 51 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá ser nueva y sin vicios ocultos y el LICITANTE GANADOR deberá presentar a LA CONVOCANTE las cartas de garantía por la duración del contrato de la solución propuesta?
29	3.2.1.11 Servicios de protección para correo electrónico. – Página 51 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá estar físicamente en las instalaciones del Centro de Datos Principal del IFT?
30	3.2.1.11 Servicios de protección para correo electrónico. – Página 51 Solicitamos amablemente a LA CONVOCANTE indicar sí la solución se debe considerar en Alta Disponibilidad.
31	3.2.1.12 Servicio de filtrado de contenido Web. – Página 53 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá ser nueva y sin vicios ocultos y el LICITANTE GANADOR deberá presentar a LA CONVOCANTE las cartas de garantía por la duración del contrato de la solución propuesta?
32	3.2.1.12 Servicio de filtrado de contenido Web. – Página 53 Solicitamos amablemente a LA CONVOCANTE indicar, ¿Sí es correcto interpretar que la solución deberá estar físicamente en las instalaciones del Centro de Datos Principal del IFT?
33	3.2.1.12 Servicio de filtrado de contenido Web. – Página 53 Solicitamos amablemente a LA CONVOCANTE indicar sí la solución se debe considerar en Alta Disponibilidad.
34	3.2.1.14 Servicio de enrutamiento de enlace de Internet – Página 56 Solicitamos amablemente a LA CONVOCANTE indicar sí la solución se debe considerar en Alta Disponibilidad.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
35	3.2.1.14 Servicio de enrutamiento de enlace de Internet – Página 56 Solicitamos amablemente a LA CONVOCANTE, ¿Sí es correcto interpretar que EL LICITANTE únicamente debe proporcionar la infraestructura y el enlace será responsabilidad de LA CONVOCANTE?
36	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 Solicitamos amablemente indicar cuál debe ser la tasa de transferencia para la replicación de información entre el SOC Primario y el redundante solicitado por LA CONVOCANTE para realizar un correcto dimensionamiento.
37	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 Solicitamos amablemente indicar a LA CONVOCANTE cual es el nivel de servicio y las deductivas que se aplicarán para medir la replicación y funcionamiento del SOC redundante.
38	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 Solicitamos amablemente indicar a LA CONVOCANTE sí se realizarán pruebas de funcionamiento del SOC Redundante y con que periodicidad.
39	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 Solicitamos amablemente indicar a LA CONVOCANTE ¿Sí el requerimiento de un SOC redundante con las consideraciones solicitadas se desprenden de el resultado de un análisis de riesgo con base en las especificaciones y procedimientos definidos en el MAAGTICSI?, lo anterior debido a que si bien LA CONVOCANTE cuenta con redundancia en sus centros de datos ambos en la Zona Metropolitana, la distancia entre estás no equivalen a los 50 Kms solicitados.
40	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 Entendiendo que la necesidad de redundancia es también para incidentes de fuerza mayor, derivado a que la infraestructura administrada, se encuentran en ambos centros de datos de LA CONVOCANTE y estos mismos se localizan dentro del área metropolitana, el SOC redundante no tendría capacidad para operar la infraestructura en los tiempos de 4 hrs especificados por LA CONVOCANTE, por lo anterior, solicitamos amablemente a LA CONVOCANTE indicar ¿sí las consideraciones solicitadas se desprenden del resultado de un análisis de riesgo con base en las especificaciones y procedimientos definidos en el MAAGTICSI?
41	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 Solicitamos amablemente a LA CONVOCANTE indicar, ¿sí las características del SOC Redundante deben cumplir las mismas solicitadas para el SOC Principal?
42	3.2.2.1 Centro de Operaciones de Seguridad (SOC) – Página 58 ¿Solicitamos amablemente a LA CONVOCANTE indicar sí la certificación de 27001 es referente a los procesos de operación?
43	3.2.2.2 Centro de Monitoreo del SOC – Página 59 Solicitamos amablemente a LA CONVOCANTE indicar sí las Consolas de monitoreo para visualizar los eventos y monitoreo en tiempo real que ocuparán los operadores deben ser distintas a la solución e correlación de eventos solicitada por la CONVOCANTE en las presentes bases.
44	3.2.2.3 Centro de Datos del SOC Solicitamos amablemente a LA CONVOCANTE aclarar el requerimiento de Centro de Datos ya que en el anexo técnico índica que deberá de cumplir con al menos ICREA nivel 4 o TIER III y en la matriz de puntos y porcentajes solicita que sea ICREA 2 o TIER I.
45	6. Requisitos de especialidad 6.1.1 Recursos Humanos – Página 74 Solicitamos amablemente a LA CONVOCANTE indicar sí este personal es el mínimo para la ejecución de los servicios para poder dimensionar adecuadamente.
46	6. Requisitos de especialidad 6.1.1 Recursos Humanos – Página 74 Para el caso en que el SOC redundante se encuentre a más de 4 horas de distancia en auto, solicitamos amablemente a LA CONVOCANTE indicar de qué forma se deberá de presentar el cumplimiento de este punto en la propuesta para poder dimensionar adecuadamente.
47	6. Requisitos de especialidad 6.1.1 Recursos Humanos – Página 74 LA CONVOCANTE solicita contar como mínimo con los siguientes certificados por cada tecnología

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	propuesta (Firewalls, IDS/IPS, protección de aplicaciones, servidores de archivos y bases de datos, correlación de eventos, protección contra amenazas de nueva generación, filtrado de correo y herramienta de análisis de vulnerabilidades). Solicitamos amablemente indicar a LA CONVOCANTE a que servicio de IDS/IPS y protección contra amenazas de nueva generación se refiere ya que estos no se encuentran descritos como tal en las presentes bases.
48	6.1.2 Evidencia de Cumplimiento – Página 74 Solicitamos amablemente a LA CONVOCANTE indicar sí este personal es el mínimo para la ejecución de los servicios para poder dimensionar adecuadamente.
49	6.1.2 Evidencia de Cumplimiento – Página 74 Para el caso en que el SOC redundante se encuentre a más de 4 horas de distancia en auto, solicitamos amablemente a LA CONVOCANTE indicar de qué forma se deberá de presentar el cumplimiento de este punto en la propuesta para poder dimensionar adecuadamente.
50	6.1.2 Evidencia de Cumplimiento – Página 74 LA CONVOCANTE solicita 2 especialistas en administración de incidentes de seguridad comprobados mediante la certificación GIAC Incident Handler. Solicitamos amablemente a LA CONVOCANTE aceptar como alternativa la presentación del certificado CISM, siendo que esté también dentro de sus dominios de especialización se encuentran la administración de incidentes de seguridad como se demuestra en la siguiente url: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx. ¿Se acepta nuestra propuesta?

SM4RT SECURITY SERVICES, S.A. DE C.V.

No.	Preguntas
1	PÁGINA 4 Requisitos para la presentación de proposiciones ¿Es posible realizar subcontratación de servicios?
2	PÁGINA 6 Documento método de evaluación En relación a los contratos que deben presentarse a la convocante, ¿Pueden ser contratos en curso o deben ser concluidos?
3	PÁGINA 7 Metodología para la prestación de servicio-ISP/IEC 27001 En la metodología de la prestación de servicios, están enumerados una serie de procesos específicos. Se solicita atentamente a la convocante, acepte un nuevo listado de los procesos certificados ISO/IEC 27001, donde se muestra los los procesos y subprocesos considerados por cada categoría.
4	PÁGINA 32 Basado en tecnología ASIC "Application-Specific Integrated Circuit" y ser capaz de brindar una solución de "Complete Content Protection". Se solicita amablemente a la convocante poder aclarar este requerimiento debido a que limita la participación de otras tecnologías. ¿Aceptaría la convocante otras tecnologías que cuentan con la certificación de NSS Labs (2014) y se encuentran como líderes en el cuadrante Mágico de Gartner (2013)?
5	PÁGINA PÁGINA 32 Capacidad de re-ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware. Los motores de inspección y re-ensamblado de paquetes de la mayoría de los fabricantes son realizados por contextos de software en forma independiente de la plataforma de hardware. Aceptaría la convocante una plataforma similar en rendimiento y que no sea limitativa a una basada en hardware.
6	PÁGINA 32 Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance", no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX, AIX o Windows. Es correcto entender que la apreciación del "sistema operativo genérico" se refiere a las distribuciones comerciales y multipropósito que se distribuyen en el mercado y que las tecnologías del sistema operativo pre-endurecido del appliance cuenten con diferentes patentes registradas.
7	PÁGINA 33 Contar con un rendimiento (throughput) de Firewall de al menos 78 Gbps para paquetes de 1518 y 512 bytes, un rendimiento de VPN de al menos 48 Gbps, rendimiento de

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	detección de intrusos de al menos10 Gbps, rendimiento de antivirus en modo proxy de al menos 4.2 Gbps, rendimiento de antivirus en modo Flow de 12 Gbps. Es correcto entender que al ser un Sitio Secundario el throughput relevante es el total de Firewall y VPN?
8	PÁGINA 33 El equipo debe soportar 240,000 nuevas sesiones por segundo. Acepta la convocante incrementar de 240K a 280K sesiones por segundo? Debido al requerimiento solicitado de throughput y conexiones concurrentes en el Firewall.
9	PÁGINA 33 El equipo debe contar con al menos 10 Interfaces GigaEthernet RJ45, 10 Interfaces GigaEthernet SFP y 8 interfaces 10 GigEthernet SFP+. Podría la convocante especificar el tipo y número total de interfaces a utilizar durante la vida del proyecto? Esto debido a que lo solicitado en este punto son las interfaces totales que puede llegar a soportar un equipo y el incluir todas las interfaces de inicio encarece el proyecto.
10	PÁGINA 33 Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. Para simplificar la administración operativa, ¿Es correcto entender que están solicitando políticas de Firewall basadas en zonas para la definición del tráfico entrante/saliente?
11	PÁGINA 33 Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. Para simplificar la administración operativa, es correcto entender que están solicitando políticas de Firewall basadas en zonas para la definición del trafico entrante/saliente y que el control de tráfico multicast este inherente en la configuración global del firewall?
12	PÁGINA 33 Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). Esta funcionalidad no se solicita para el sitio principal, por tal motivo solicitamos amablemente a la convocante aclarar la necesidad de IPv6 en un Sitio Secundario?
13	PÁGINA 34 Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS. Podría la convocante aclarar su requerimiento puntual del protocolo de IS-IS, puesto que solo opera en Capa 2?
14	PÁGINA 34 La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow. Aceptaría la convocante el uso de netflow o jflow?
15	PÁGINA 34 Debe soportar la configuración de túneles L2TP y PPTP Acepta la convocante que este tráfico de encapsulación se encuentren dentro de un túnel IPSEC? Debido a que los anteriores son considerados inseguros.
16	PÁGINA 39 Sera posible configurar el equipo para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a contenido categorizado por el portal como contenido educativo. Es correcto entender que, este requerimientos se refiere a únicamente a autorizar y permitir el acceso a contenido educativo dentro de Youtube?
17	PÁGINA 39 Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS). A raíz de la vulnerabilidad de Heartbleed (CVE-2014-0160) no se considera seguro realizar la administración por medio de un WebGUI sobre HTTPS. Acepta la convocante un sistema de administración centralizada que no ha presento ningún tipo de afectación de esta vulnerabilidad y que este manejada por comunicaciones encriptadas mediante certificados digitales. Links de referencia Links de reportes de vulnerabilidades: http://www.fortiguard.com/advisory/FG-IR-14-011/

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk100173 http://watchguardsecuritycenter.com/2014/04/08/the-heartbleed-openssl-vulnerability-patch-openssl-asap/ http://goo.gl/9Ruf6
18	PÁGINA 39 La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario. Acepta la convocante que la interface gráfica se encuentre en inglés, debido a que regularmente las traducciones en español no necesariamente respetan los tecnicismos necesarios para configuración/administración y troubleshooting por los administradores.
19	PÁGINA 40 La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autentificarse con un TOKEN (Autentificación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante. Es correcto entender que la convocante, al referirse a la "autenticación por doble factor" sea válido el uso de certificados digitales? Los certificados digitales son seguros.
20	PÁGINA 16 El Proveedor Adjudicado deberá proporcionar el equipamiento necesario, la instalación y configuración para la puesta en marcha del servicio; así como la afinación, depuración y el mantenimiento del mismo durante la vigencia del contrato, en el entendido de que todos los equipos y licenciamientos requeridos formarán parte del servicio ofrecido por parte del Proveedor Adjudicado y que el IFT no adquirirá ninguno de los mismos. ¿El mantenimiento y soporte de los equipos en funcionamiento propiedad del IFT, deben de incluirse en la propuesta?
21	PÁGINA 16 El Proveedor Adjudicado deberá proporcionar el equipamiento necesario, la instalación y configuración para la puesta en marcha del servicio; así como la afinación, depuración y el mantenimiento del mismo durante la vigencia del contrato, en el entendido de que todos los equipos y licenciamientos requeridos formarán parte del servicio ofrecido por parte del Proveedor Adjudicado y que el IFT no adquirirá ninguno de los mismos ¿El licitante debe incluir el mantenimiento y soporte de los equipos en funcionameinto propiedad del IFT, a patir de que venza el mantenimiento actual, en la propuesta?
22	PÁGINA 24 En el punto del "Servicio de correlación de eventos y administración de bitácoras" Con el fin de dimensionar adecuadamente la propuesta, pudiera especificar el número y tipo de dispositivos (es decir S.O, dispositivos de red, bases de datos, etc.) que deberán ser integrados
23	PÁGINA 24 En el punto del "Servicio de correlación de eventos y administración de bitácoras ¿Deberan ser incuidas en el servicio de "Correlación de eventos y adminsitración de bitacoras", las bitacoras de las aplicaciones del IFT? ¿En qué formato se enviarán las bitacoras de las aplicaciones al sistema de correlación?
24	PÁGINA 58 3.2.2.1 Centro de Operaciones de Seguridad (SOC) Se solicita amablemente a la convocante que las certificaciones del SOC secundario sean las mismas que las certificaciones del SOC primario.
25	PÁGINA 73 6.1.2 Evidencia de cumplimiento Se solicita atentamente a la convocante que una persona (especialista) pueda contar con dos o mas certificaciones.
26	PÁGINA 73 2 Especialistas en administración de incidentes de seguridad Comprobable mediante certificado de:

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	• GIAC Incident Handler Se solicita atentamente a la convocante acepte la certificación GHFI (Certified Forensic Investigator) para la certificación GIAC ya que cubre los alcances de CHFI además de cubrir temas de forensia de información y análisis de incidentes.
27	PÁGINA 73 3 Especialistas certificado en seguridad de sistemas. Comprobable mediante certificado de: • CISSP (Certified Information Systems Security Professional). Se solicita a la convocante que para el caso del especialista CISSP acepte la certificación CISM de ISACA, ya que la certificación cubre los alcances equivalentes del CISSP. Los profesionales con la certificación CISM son capaces de realizar tareas de administración, diseño y supervisión de sistemas de Seguridad de la información.

CISCO SYSTEMS DE MÉXICO. S.A. DE C.V.

No.	Preguntas
1	Servicio de control de acceso Firewall. a) Firewall sitio principal "Boston" NUMERAL 3.2.1.9 PAGINA 31 ¿Por concepto de "Blade Software" se debe asumir que se está dirigiendo el requerimiento al fabricante Checkpoint en este concurso, o se debe asumir que se requiere la capacidad dentro de la solución propuesta de adicionar bloques de protección en modalidad appliance o virtualizada para realizar funciones de Firewall, IPS, filtrado de URL, protección de Antimalware?
2	Servicio de control de acceso Firewall. a) Firewall sitio principal "Boston" NUMERAL 3.2.1.9 PAGINA 32 Se dice: Debe permitir crear controles de acceso a por lo menos 150 aplicaciones/servicios/protocolos predefinidos. Se sugiere a la convocante que siendo un proyecto de protección informática se evalúen soluciones que soporten al menos aquellas que cumplan con controles en el orden del millar de aplicaciones, ya que la categoría en la que cae un equipo con controles en el orden de centenas es considerado o bien un UTM genérico con dificultades para realizar inspeciones de mayor capacidad por la naturaleza de dicha solución de hacer todo en uno, es decir, muchas funciones, pero con poco desempeño, o bien cae en una categoría de ser un equipo con capacidades obsoletas, es decir, equipo no vigente y no a la vanguardia de los requerimientos actuales de protección dictados por la industria. ¿Se acepta nuestra sugerencia?
3	Servicio de control de acceso Firewall. a) Firewall sitio principal "Boston" NUMERAL 3.2.1.9 PAGINA 32 Se dice: Deberá contar con un throughput de 11 Gbps para firewall. ¿Por qué se solicita la capacidad de 11 Gbps en la capa de Internet? ¿La convocante acaso cuenta con un enlace de ese orden de ancho de banda? Se soliicta a la convocante ajustar este desemepeño en beneficio del costo-capacidad real a utilizar del equipo solicitado.
4	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 32 ¿Por qué se pide Antispam en este equipo? No es congruente dicha solicitud si bien se está pidiendo lo mismo en la sección de "solucion de protección de Correo Electrónico". Las funcionalidades descritas no pertenecen a un Firewall como dice el título del inciso b) y tampoco pertenecen a un Next-Gen Firewall. Se solicita a la convocante permitir proponer una solución

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	integral que cumpla con los bloques de protección requeridos en modalidad appliance para realizar de manera correcta cada función del marco de seguridad solicitado.
5	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 32 ¿Por qué se pide capacidades de AV en la capacidad del Firewall si las soluciones de filtrado web y seguridad web ya contienen esto? No es congruente dicha solicitud si bien se está pidiendo lo mismo en la sección de "solucion de protección Web". Las funcionalidades descritas no pertenecen a un Firewall como dice el título del inciso b) y tampoco pertenecen a un Next-Gen Firewall. Se solicita a la convocante permitir proponer una solución integral que cumpla con los bloques de protección requeridos en modalidad appliance para realizar de manera correcta cada función del marco de seguridad solicitado.
6	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 32 ASIC y el termino "Complete Content Protection" son exclusivos a Fortinet. Solicitar estos dos conceptos es cerrar a que no puedan participar otros fabricantes en la proposición de propuestas para Firewall. Se solicita a la convocante aperturar la participación removiendo este requerimiento.
7	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 33 ¿Por qué se requiere un firewall de 78 Gbps para internet? Si el ancho de banda del servicio de Internet no sobrepasa los 500Mbps, esta capacidad es excesiva y perjudicaría a la convocante en términos costo-capacidad real utilizada. Se solicita a la convocante indicar cuál es el ancho de banda del enlace de Internet y especificar como promedio máximo la misma capacidad para el equipo destinado a la protección del medio.
8	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 33 ¿Por qué se requiere una funcionalidad de VPN de 48 Gbps e IPS de 10 Gbps para internet? Si el ancho de banda del servicio de Internet no sobrepasa los 500Mbps, estas capacidades son excesivas y perjudicarían a la convocante en términos costo-capacidad real utilizada. Se solicita a la convocante indicar cuál es el ancho de banda del enlace de Internet y especificar como promedio máximo la misma capacidad para el equipo destinado a la protección del medio.
9	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 33 Se dice: El equipo debe soportar al menos 11 millones de sesiones concurrentes. Se solicita a la convocante ajustar este número a un requerimiento asociado a la capacidad en términos de Mbps del enlace de Internet que el Firewall de ese bloque deberá proteger.
10	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 33 Se dice: El equipo debe soportar 240,000 nuevas sesiones por segundo. Se solicita a la convocante ajustar este número a un requerimiento asociado a la capacidad en términos de Mbps del enlace de Internet que el Firewall de ese bloque deberá proteger.
11	1Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 33

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Se dice: El equipo debe contar con al menos 10 Interfaces GigaEthernet RJ45, 10 Interfaces GigaEthernet SFP y 8 interfaces 10 GigaEthernet SFP+. Dado que el equipo no estará conectado a enlaces de 10 Gbps en Internet, se sugiere reducir la cantidad puertos de 10 Gbps a 2 o bien eliminar este requerimiento y considerar interfaces Gigabit Ethernet.
12	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 34 Se dice: La solución deberá tener la capacidad de balancear carga entre servidores. Si es una solución de propósito específico como lo indica el titulo del servicio y del inciso, ¿por qué se requiere que tenga un balanceador de servidores? Este requerimiento lo orienta al fabricante Fortinet. Se solicita a la convocante aperturar este requerimiento para permitir la participación de otros fabricantes.
13	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 34 Se dice: En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID. Si es una solución de propósito específico como lo indica el titulo del servicio y del inciso, ¿por qué se requiere que tenga un balanceador de servidores? Este requerimiento lo orienta al fabricante Fortinet. Se solicita a la convocante aperturar este requerimiento para permitir la participación de otros fabricantes.
14	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 34 Se dice: En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible. Si es una solución de propósito específico como lo indica el titulo del servicio y del inciso, ¿por qué se requiere que tenga un balanceador de servidores? Este requerimiento lo orienta al fabricante Fortinet. Se solicita a la convocante aperturar este requerimiento para permitir la participación de otros fabricantes.
15	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 34} Se dice: Soporte a políticas de ruteo (policy routing). El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál tráfico sale por un enlace y qué tráfico sale por otro enlace. Es comprensible el requerimiento, sin embargo, como su nombre lo indica "policy routing" es una capacidad característica de un equipo ruteador que en conjunto con la solución de Firewall se configuran para lograr el deseo de elección de ruta. Se le sugiere a la convocante permitir implementar medidas como Policy NAT para tener el mismo efecto solicitado como Policy routing, ya que éste bloque de seguridad se encontrará atrás del equipo de ruteo que recibe el enlace de Internet y es factible lograr lo solicitado bajo una composición integrable en la arquitectura.
16	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 34 Se dice: Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS. IS-IS no es un protocolo utilzado comunmente, es más utilizado EIGRP y no sólo un fabricante lo cumple. Se solicita a la convocante aceptar un protocolo de Ruteo Interior que sea más común en la convivencia en el mercado entre los diferentes equipos de seguridad y de ruteo.
17	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" 3.2.1.9 34 Se dice: La solución permitirá la integración con analizadores de tráfico mediante el

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	protocolo sFlow. Dado que sFLow es un protocolo de exportación de tráfico Capa 2 en modalidad de muestreo (no todo el tráfico). Se puede asumir que siendo un requerimiento mínimo, ofrecer un protocolo del mismo propósito con capacidad de exportación mayor a un muestreo no es objeto de descalificación. ¿Se aceptan propuestas con capacidades ya sea Netflow o sFLow?
18	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 34 Se dice: Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. ¿Se puede asumir que el el propósito de este requerimiento es tener capacidad de tener políticas de control de acceso tanto para túneles de IPSec sitio a sitio, sitio a cliente y SSL de cliente?
19	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 36 Se dice: Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP. Se sugiere a la convocante eliminar este requerimiento, ya que de no ser así hará inflexible la operación de la solución.
20	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 36 Se dice: La detección de intrusos debe poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un Switch con un puerto configurado en SPAN o MIRROR. ¿Se acepta que para fuera de linea el redireccionamiento del tráfico sea lógico dentro del firewall, sin necesidad de incluir elementosy configuraciones externas como switches?
21	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dice: La solución de Firewall debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S. Para lograr lo que se solicita es necesario descifrar el túnel de TLS en la solución de Web y de correo electrónico. ¿Es correcto entender que la convocante desea inspeccionar dicho tráfico con los sacrificios implícitos?
22	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dice: La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle). Para lograr lo que se solicita es necesario descifrar el túnel de TLS en la solución de Web y de correo electrónico. ¿Es correcto entender que la convocante desea inspeccionar dicho tráfico con los sacrificios implícitos?
23	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dcie: La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario. Para lograr lo que se solicita es necesario descifrar el túnel de TLS en la solución de Web y de correo electrónico. ¿Es correcto entender que la convocante desea inspeccionar dicho tráfico con los sacrificios implícitos?
24	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa"

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	NUMERAL 3.2.1.9 PAGINA 37 Se dice: Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. Para lograr lo que se solicita es necesario descifrar el túnel de TLS en la solución de Web y de correo electrónico. ¿Es correcto entender que la convocante desea inspeccionar dicho tráfico con los sacrificios implícitos?
25	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dice: Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
26	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dice: La función de antivirus deberá poder configurarse en modo Proxy, así como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
27	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dice: Función de antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
28	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	"appliance", que permita la aplicación de esta protección por política de control de acceso. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
29	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
30	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La función de antivirus integrada deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos HTTP, FTP, IMAP, POP3, SMTP. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
31	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La función de antivirus integrada tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
32	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La función de antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging). Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
33	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La función de antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo. Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
34	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: Capacidad de actualización automática de firmas de antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas). Se le sugiere a la convocante re considerar dicha solicitud, en virtud que las soluciones basadas en Antivirus son tecnología obsoleta porque son poco eficaces dado que están basadas en firmas. Las soluciones existentes consideradas como tecnología de vanguardia que están pensadas para ataques actuales proveen protección más allá de las firmas, como lo son las soluciones de Anti Malware Avanzado. ¿Se puede asumir que siendo un requerimiento mínimo, ofrecer una solución con capacidad de Anti Malware mayor no es objeto de descalificación?
35	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje. ¿Cuál es la razón por la que se requiere también hacer funciones de antispam en la solución de Firewall siendo que se solicita una solución de seguridad email en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
36	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: La capacidad antispam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address). ¿Cuál es la razón por la que se requiere también hacer funciones de antispam en la solución de Firewall siendo que se solicita una solución de seguridad email en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Email.
37	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	PAGINA 38 Se dice: La capacidad antispam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de SPAM. ¿Cuál es la razón por la que se requiere también hacer funciones de antispam en la solución de Firewall siendo que se solicita una solución de seguridad email en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Email.
38	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje. ¿Cuál es la razón por la que se requiere también hacer funciones de antispam en la solución de Firewall siendo que se solicita una solución de seguridad email en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Email.
39	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 38 Se dice: El firewall deberá contar con la facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. ¿Cuál es la razón por la que se requiere también hacer funciones de antispam en la solución de Firewall siendo que se solicita una solución de seguridad email en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Email.
40	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 Se dice: Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
41	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 Se dice: Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida. ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
42	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 "Se dice: Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
43	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 Se dice: La solución de filtrado de contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Navegadores tales como Google, Yahoo! y Bing. ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
44	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 Se dice: • Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos. ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
45	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 Se dice: Será posible exceptuar la inspección de HTTPS por categoría. ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
46	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 39 Se dice: Sera posible configurar el equipo para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	contenido categorizado por el portal como contenido educativo. ¿Cuál es la razón por la que se requiere también hacer funciones de filtrado web en la solución de Firewall siendo que se solicita una solución de seguridad web en este mismo anexo? Solicitar dicha capacidad duplicada en el Firewall duplicará de igual manera el costo para la convocante? Se sugiere eliminar este requirimiento en esta sección, ya que se ha solicitado más adelante en el mismo anexo una solución específica de seguridad Web.
47	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 40 Se dice: La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autentificarse con un TOKEN (Autentificación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante. Las soluciones de Tokens generalmente son centralizadas para autentificarse ante multiples sistemas que van mas allá del firewall. Esto aumenta el nivel de la seguridad. ¿Se acepta la integración con soluciones centralizadas de AAA basado en tokens u otro tipo de One-time-password?
48	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 40 Se dice: o Generación de reportes calendarizados y en formatos portables tales como PDF y DOC. ¿Se acepta el formato html, el cual es más portable que cualquier formato para ser visualizado no sólo en PC, sino en dispositivos móviles también?
49	49 Servicios de protección para correo electrónico. 3.2.1.11 PAGINA 53 Se dice: o Hash MD5 o SHA-1 de los binarios maliciosos. Se recomienda a la convocante utilizar SHA-256, ya que es superior a los mecanismos de hash propuestos. Este requerimiento puede hacer vulnerable la solución, puesto que es un requerimiento no actualizado de acuerdo a las ofertas pensadas contra ataques presentes.
50	50 Servicio de filtrado de contenido Web. 3.2.1.12 PAGINA 54 Se dice: Permitir el control de al menos 85 categorías de sitios Web y al menos 15 categorías de sitios Web 2.0. ¿Por qué se menciona explícitamente 85 categorías y no 81 categorías? ¿Se conoce que el número 85 es el número mágico para poder garantizar el control de las aplicaciones y micro-aplicaciones con que cuentan las actuales páginas Web? Aventurarse a pedir un número específico de categorías no garantiza que todos los fabricantes ordenen sus categorías bajo las mismas reglas. Se sugiere a la convocante solicitar un rango de categorías acorde al Estudio de Mercado realizado, es decir, de 70 - 90 categorías, y con la obligación funcional de identificar y controlar entre 200 - 300 aplicaciones y micro-aplicaciones (Facebook chat, post, Facebook juegos, Dropbox upload, etc) para de esta manera garantizar que sin importar la categoría nombrada, se inspeccione lo más importante, los objetos que pudieran contener las páginas web.
51	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" NUMERAL 3.2.1.9 PAGINA 37 Se dice: Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping; En el entendido de que las apliaciones de tipo P2P no son consideradas como de uso apropiado para la institucion y las necesidades laborales, las mejores practicas indican que es recomendable bloquear el acceso a estos servicios, en el caso de requerirse para un usuario o grupo de usuarios se puede lograr via las politicas de control de acceso; es correcto entender que no teniendo un uso justificado en las politicas de trafico de la institucion este trafico debera ser bloqueado mas que simplemente ajustado a un ancho de banda?
52	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" 3.2.1.9

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	PAGINA 36 Se dice: La interfaz de administración de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad "appliance", sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso; Es correcto entender que la administracion debera estar completamente integrada a la plataforma, debiendo estar instalada en equipamiento diferente al appliance dedicado a la inspeccion del trafico por obvias razones de rendimiento y capacidad de almacenamiento?
53	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" 3.2.1.9 PAGINA 39 Se dice: La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario, El idioma español no se encuentra definido como un estandar en la administracion de las plataformas de tecnologia y por ende solo un par de fabricantes lo soportan de manera nativa; se solicita a la convocante considerar el idioma español como opcional en el requerimiento a razon de permitir la libre competencia en el requerimiento, se acepta la solicitud?
54	Servicio de control de acceso Firewall. b) Firewall sitio secundario "Iztapalapa" 3.2.1.9 PAGINA 40 Se dice: La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autentificarse con un TOKEN (Autentificación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante, existen mecanismos de autenticacion que permiten a las herramientas aprovechar la infraestructura existenten en red (AD, LDAP, RADIUS) sin necesidad de integrar un componente adicional (Token), es correcto considerar estos metodos de autenticacion mas robustos como validos y adicionales al uso del token?

SCITUM, S.A. DE C.V.

No.	Preguntas
1	PAGINA 3 CRITERIOS DE EVACUACIÓN DE PUNTOS Y PORCENTAJES. CAPACIDAD DE RECURSOS HUMANOS. Numeral 1, inciso b). Dice: "Documento de alta del Instituto Mexicano del Seguro Social (IMSS) que acredite al menos 90 días de antigüedad para cada uno de los recursos destinados a este proyecto". En el supuesto de que un licitante tenga su nómina en la modalidad de outsourcing (práctica empresarial muy común apegada a la legislación laboral vigente) se solicita A LA CONVOCANTE acepte que las altas del IMSS del personal a presentar estén a nombre del outsourcer, acompañado del respectivo contrato de prestación de servicios que acredite la relación entre la razón social del licitante y el mencionado outsourcer
2	PAGINA 3 CRITERIOS DE EVACUACIÓN DE PUNTOS Y PORCENTAJES. CAPACIDAD DE RECURSOS HUMANOS. Numeral 2 "Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales", dice: Se deberán acreditar los conocimientos y competencias para cada una de las personas que cubrirán los roles solicitados como parte de esta contratación, el licitante deberá presentar: Las cédulas o títulos profesionales que los acrediten como egresados de las carreras de licenciatura en informática, ingeniería en computación, ingeniería en sistemas o alguna carrera afín a estas. Toda vez que el personal del licitante cuente certificaciones vigentes emitidas por los organismos facultados que avalan sus conocimientos para proporcionar los servicios motivo de esta licitación y con el objetivo de incluir la mayor cantidad de Cerficaciones para garantizar el nivel de especialización. Solicitamos a la convocante acepte que se acredite la capacidad del personal mediante carta bajo protesta de decir verdad firmada por el representante legal que indique que el personal asignado cuenta con la formación y grado de especialización para desempeñar el rol

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	asignado, además del respaldo de la experiencia en al menos 5 proyectos similares y la Certificaciones vigentes. ¿Se acepta nuestra solicitud?
3	PAGINA 3 CRITERIOS DE EVALUACIÓN DE PUNTOS Y PORCENTAJES. I. CAPACIDAD DE RECURSOS HUMANOS. Numeral 2 "Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales", dice: Se deberán acreditar los conocimientos y competencias para cada una de las personas que cubrirán los roles solicitados como parte de esta contratación, el licitante deberá presentar: a) Las cédulas o títulos profesionales que los acrediten como egresados de las carreras de licenciatura en informática, ingeniería en computación, ingeniería en sistemas o alguna carrera afín a estas. Referente al requerimiento: Debido a que el título o cédula profesional no garantiza necesariamente la competencia, habilidad y grado de especialidad del recurso humano solicitado para cada rol, es decir, puede existir personas que cumplan con las certificaciones pero que no necesariamente cumplan con alguno de los dos documentos mencionados, se solicita a la convocante acepte carta de pasante o carta de comprobación de estudios de maestría para obtener el grado de licenciatura o posgrado, emitida por la institución educativa correspondiente.
4	PAGINA 4 CRITERIOS DE EVACUACIÓN DE PUNTOS Y PORCENTAJES. CAPACIDAD DE RECURSOS HUMANOS, Numeral 2 "Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales", penúltimo párrafo. Dice: "Si el licitante cumple con el 100% de las certificaciones solicitadas, se asignarán 6 puntos". Se solicita a la convocante precise y aclare las certificaciones con las que deben contar los roles enunciados en la tabla correspondiente, donde menciona que el cumplimiento puede realizarse mediante la comprobación de "alguno" de los certificados solicitados, sin embargo al final de la tabla refiere que para obtener el puntaje correspondiente, el licitante deberá cumplir con el 100% de las certificaciones solicitadas.
5	PAGINA 5 CRITERIOS DE EVACUACIÓN DE PUNTOS Y PORCENTAJES. CAPACIDAD DE RECURSOS ECONÓMICOS Y EQUIPAMIENTO. Numeral 2, "Equipamiento – Centro de Operaciones de Seguridad (SOC, por sus siglas en ingles).". Dice: El proveedor deberá señalar la ubicación e infraestructura del SOC, la cual deberá cumplir al menos con todas las especificaciones descritas en el documento Especificaciones Técnicas, apartado 3.2.2 Componente 2: Servicio de administración y entrega. El proveedor deberá incluir el certificado vigente de TIER o ICREA para su SOC. ¿Es correcto inferir que los certificados que deberán incluirse para el centro de datos del SOC deberán ser ICREA nivel 4 o en su defecto TIER III, de conformidad a lo especificado en la página 60 del Anexo Técnico? Debido a que por razones de seguridad y de facilidad en las operaciones a nivel nacional, los centro de datos de nuestros SOCs se ubican en las instalaciones de Triara.Com, S.A. de C.V. y el certificado ICREA o TIER solicitado se encuentra a nombre de esta razón social; se solicita a la convocante acepte si para acreditar este requerimiento se podrá presentar el certificado referido, acompañado de una carta emitida por Triara.Com, S.A. de C.V. donde acredite nuestra legal estancia, uso, operación y ocupación de dichas instalaciones, firmada por el representante legal del mismo.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
6	PAGINA 5 Equipamiento – Centro de Operaciones de Seguridad (SOC, por sus siglas en ingles). El proveedor deberá señalar la ubicación e infraestructura del SOC, la cual deberá cumplir al menos con todas las especificaciones descritas en el documento Especificaciones Técnicas, apartado 3.2.2 Componente 2: Servicio de administración y entrega. El proveedor deberá incluir el certificado vigente de TIER o ICREA para su SOC. En el supuesto de que el centro de datos del SOC del licitante participante se encuentre en proceso de re-certificación en alguno de los estándares ICREA o TIER, se solicita a la convocante, permita validar la certificación correspondiente, mediante una carta de la institución evaluadora correspondiente donde especifique que el certificado sigue vigente en lo que se re-expide. Adicionalmente, solicitamos a la convocante el pronunciamiento de nuestra petición. En caso de que la respuesta sea negativa, agradecemos se funde y motive.
7	PAGINA 4 Convocatoria. El contrato será abierto en los términos del artículo 49 de las Normas, las cantidades mínimas y máximas del presupuesto (antes del impuesto al Valor Agregado) que podrá el Instituto ejercer en cada ejercicio, son las siguientes: De la lectura de la convocatoria y anexo técnico no se puede inferir la volumetría asociada a cada servicio para estar en posición de cotizar con precisión los mínimos y máximos. Se solicita a la convocante precise y aclare la volumetría asociada para poder permitir a los participantes una equitativa competencia en el presente proceso, mismo que permitirá a la convocante una evaluación objetiva y con apego a derecho.
8	PAGINA 6 CRITERIOS DE EVACUACIÓN DE PUNTOS Y PORCENTAJES. EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE (EE) Experiencia En cada contrato presentado por el licitante, deberá indicar el número de página en el que se muestre la siguiente información: objeto, vigencia y monto del contrato. Los años mínimos de experiencia acumulada demostrable que deberán acreditar los licitantes es de siete (7) años. ¿Es correcto interpretar que por experiencia acumulada, se entenderá la cantidad de años naturales continuos e ininterrumpidos en que el licitante ha venido prestando servicios similares a los solicitados en la presente convocatoria? En caso de respuesta diferente, se solicita a la convocante precise y aclare.
9	PAGINA 6 CRITERIOS DE EVACUACIÓN DE PUNTOS Y PORCENTAJES. EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE (EE) Especialidad ¿Es correcto interpretar que la totalidad de los contratos solicitados en este subrubro deberán ser concluidos, es decir, no estar vigentes?
10	PAGINA 7 Criterios de evacuación de puntos y porcentajes. Metodología para la prestación del servicio ... "El licitante deberá presentar evidencia de contar con una certificación ISO/IEC 27001 vigente, obtenida con una antigüedad mayor a tres (3) años. Esta certificación deberá considerar los siguientes procesos aplicables a su Centro de Operaciones de Seguridad. a) Proceso de atención na clientes. b) Proceso de aprovisionamiento inicial. c) Proceso de afinación inicial de los servicios prestados por el SOC. d) Proceso de afinación continúa de los servicios prestados por el SOC. e) Proceso de control de cambios.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	f) Proceso de respuesta a incidentes. g) Proceso para notificación de incidentes de seguridad. h) Proceso de atención en crisis" Se solicita a la convocante que, para no limitar la participación de los licitantes, los 8 procesos requeridos puedan ser sustituidos por cualesquiera otros 8 procesos siempre y cuando estén relacionados con la operación de un SOC y que se encuentren certificados bajo la norma ISO/IEC 27001 ¿Se acepta nuestra solicitud?
11	PAGINA 22 VI.3 Propuesta económica Propuesta económica, desglosando el costo unitario mensual por entregable, subtotal, I.V.A., Totales y los descuentos que en su caso otorguen a la Convocante, tomando en cuenta los entregables descritos en el numeral 3.6.1 Temporalidad del Anexo No 1. En tanto en el numeral 3.6.1 de la Anexo No 1, no se mencionan entregables, sino servicios, es correcto interpretar que la propuesta económica se deberá presentar en función a los servicios solicitados y no en función de los entregables de cada servicio solicitado, favor de precisar.
12	PAGINA 22 VI.3 Propuesta económica Propuesta económica, desglosando el costo unitario mensual por entregable, subtotal, I.V.A., Totales y los descuentos que en su caso otorguen a la Convocante, tomando en cuenta los entregables descritos en el numeral 3.6.1 Temporalidad del Anexo No 1. Para asegurar los principios de equidad en el presente proceso licitatorio para todos los participantes, solicitamos a la convocante establezca desde este momento el formato común para todos los licitantes en el que deberá ser presentada la propuesta económica.
13	PAGINA 11 ANEXO TECNICO NUMERAL 3.2.1.1 NUEVOS SERVICIOS, PÁRRAFO 1 DICE: El Componente de Servicios de Seguridad Administrada estará integrado por al menos los siguientes nuevos servicios de seguridad para la red del IFT: • Gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT. • Servicios de correlación de eventos y administración de bitácoras. • Servicios de análisis de vulnerabilidades y pruebas de penetración. • Servicios de control de Acceso Firewall • Servicios de protección de aplicaciones Web, servidores de archivos y bases de datos. • Servicios de protección de amenazas de nueva generación para tráfico de correo electrónico. • Servicios de Monitoreo Proactivo de Seguridad en Internet • Servicio de Enrutamiento de Enlace de internet ¿Se solicita a la convocante precise y aclare si tiene esperado integrar algún otro servicio durante la vigencia del contrato que no esté contemplado en este documento motivo de esta licitación?
14	PAGINA 12 ANEXO TECNICO NUMERAL 3.2.1.2 ADMINISTRACIÓN Y MONITOREO DE LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL EXISTENTE, PÁRRAFO 1 DICE: El Proveedor Adjudicado deberá considerar, como parte del proyecto, la administración y monitoreo de los dispositivos de seguridad perimetral que actualmente se encuentran instalados en el IFT, sean arrendados o propiedad del Instituto. Con la finalidad de acatar el punto señalado, referente a la toma de operación (administración y soporte) de los dispositivos de seguridad existentes:

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	¿ Es correcto interpretar que La CONVOCANTE proporcionará los equipos en cuestión (infraestructura existente) completamente funcionando, con licenciamiento de soporte vigente, y con memorias técnicas de configuración actualizadas (mismas que se validarán en la mesas de trabajo como parte del inicio del proyecto)? De lo contrario se solicita a la convocante precise y aclare este punto.
15	PAGINA 12 ANEXO TECNICO NUMERAL 3.2.1.1 NUEVOS SERVICIOS, PÁRRAFO 2 DICE: Todo el equipo provisto y colocado en sitio por el Proveedor Adjudicado para este proyecto, deberá: • Ser nuevo, de última generación y dedicado sólo a la solución diseñada para el Instituto. • Cuando la solución lo permita, ser equipo de propósito específico (appliance) para cada servicio que así lo requiera. • Cumplir con un ciclo de vida básico de al menos 12 meses posteriores a la fecha de término del proyecto, es decir, no estar en condiciones de fin de vida (EoL) o fin de soporte (EoS) por parte del fabricante, durante al menos la vigencia del contrato. ¿Es correcto entender que para poder comprobar que el equipo es nuevo, de última generación y cumple con un ciclo de vida de al menos 12 meses posteriores a la fecha de término del proyecto, es decir, que no está en condiciones de fin de vida (EoL) o fin de soporte (EoS) por parte del fabricante, durante al menos la vigencia del contrato, se deberá entregar carta por parte del fabricante que haga constar que cada una de las tecnologías que conforman los nuevos servicios cumple con los requerimientos anteriores?
16	PAGINA 12 ANEXO TECNICO NUMERAL 3.2.1.2 ADMINISTRACIÓN Y MONITOREO DE LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL EXISTENTE, PÁRRAFO 1 DICE: El Proveedor Adjudicado deberá considerar, como parte del proyecto, la administración y monitoreo de los dispositivos de seguridad perimetral que actualmente se encuentran instalados en el IFT, sean arrendados o propiedad del Instituto. Se Solicita a la convocante precise y aclare ¿si estos equipos arrendados o propios del Instituto cuentan con las licencias equipo spare, y soporte necesarios por parte del fabricante durante la vigencia del contrato, y quién será el responsable de llevar a cabo el levantamiento de tickets con el fabricante, los RMA's, etc. de los equipos de los servicios existentes?
17	PAGINA 12 ANEXO TECNICO NUMERAL 3.2.1.2 ADMINISTRACIÓN Y MONITOREO DE LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL EXISTENTE, PÁRRAFO 2 DICE: Es importante que el Proveedor Adjudicado tome en cuenta que algunos de estos equipos deberán migrarse, o bien instalarse y configurarse desde cero. En la tabla que se muestra a continuación, se listan las cantidades y modelos de los equipos, y se da la descripción de uso de cada uno y si deberá o no ser considerado para migración de localidad. Fila 6 de la tabla de equipos existentes ¿Es correcto interpretar que el único equipo que se migrará o se instalará desde cero será el Cisco ISE?
18	PAGINA 12 ANEXO TECNICO NUMERAL 3.2.1.2 ADMINISTRACIÓN Y MONITOREO DE LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL EXISTENTE, PÁRRAFO 2 Es importante que el Proveedor Adjudicado tome en cuenta que algunos de estos equipos deberán migrarse, o bien instalarse y configurarse desde cero. En la tabla que se muestra a continuación, se listan las cantidades y modelos de los equipos, y se da la descripción de uso

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	de cada uno y si deberá o no ser considerado para migración de localidad. Fila 6 de la tabla de equipos existentes ¿Podría la convocante indicarnos si los dos equipos Cisco ISE se encuentran en alta disponibilidad? De no ser así, ¿Podría la convocante indicarnos si cada equipo por separado tendrá que ser configurado por separado?
19	PAGINA 12 ANEXO TECNICO NUMERAL 3.2.1.1 NUEVOS SERVICIOS, PÁRRAFO 4. DICE: En caso de que las instalaciones del centro de datos del IFT sufran modificaciones durante la vigencia del contrato (como parte de mejoras a las instalaciones, requerimientos internos o incluso atendiendo observaciones de auditorías), será responsabilidad del proveedor adjudicado proporcionar los recursos necesarios para reubicar, configurar, reinstalar y ajustar los Componentes Habilitadores que lo necesiten. El Proveedor Adjudicado deberá considerar al menos dos modificaciones durante la vigencia del contrato derivadas por reubicaciones o cambio de equipo en los centros de datos del Instituto. ¿Es correcto entender que en las dos modificaciones consideradas en este proyecto deberá contemplarse la obra cívica, montado y configuración de componentes tecnológicos de seguridad, cableado estructurado?
20	PAGINA 13 ANEXO TECNICO NUMERAL 3.2.1.2 ADMINISTRACIÓN Y MONITOREO DE LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL EXISTENTE, Tabla de dispositivos de los servicios existentes, Deep Security ¿Se solicita LA CONVOCANTE precise y aclare la descripción del servicio de gestión de la solución deDeep Security?
21	PAGINA 14 ANEXO TECNICO NUMERAL 3.2.1.3 SERVICIOS DE TRANSFERENCIA DE CONOCIMIENTOS, PÁRRAFO 2 DICE: La transferencia de conocimientos de los componentes de administración de bitácoras y correlación de eventos, análisis de vulnerabilidades, protección de aplicaciones, servidores de archivos y bases de datos, control de ataques de denegación de servicios y balanceador de carga de enlaces de Internet deberán ser impartidos directamente por el fabricante. Se solicita a LA CONVOCANTE considere que la transferencia de conocimientos en los que no se solicita que el fabricante los imparta, el licitante pueda ofrecerlos, siempre y cuando, compruebe que el personal de la transferencia de conocimientos de cada solución tecnológica está certificado en dicha solución tecnológica
22	PAGINA 14 ANEXO TECNICO NUMERAL 3.2.1.3 SERVICIOS DE TRANSFERENCIA DE CONOCIMIENTOS. PÁRRAFO 1 DICE: El Proveedor Adjudicado deberá considerar dentro de su propuesta la transferencia de conocimientos de todas las soluciones tecnológicas de seguridad (incluidas las que son propiedad o ya están arrendadas por el IFT) considerando el número de asistentes por solución tecnológica que se presenta en la siguiente tabla: ¿Es correcto interpretar que la transferencia de conocimientos de todas las soluciones tecnológicas de seguridad (incluidas las que son propiedad o ya están arrendados por el IFT) se ofrecerán por única vez en las fechas que acuerden el IFT y el licitante ganador, y que no se considerarán sesiones de actualización de versiones de las soluciones tecnológicas, ni sesiones extras en caso de ingreso o rotación de personal?
23	PAGINA 16 ANEXO TECNICO NUEMERAL 3.2.1.4 CONDICIONES DE LOS SERVICIOS DE SEGURIDAD ADMINISTRADA.

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	PÁRRAFO 5 DICE: Es responsabilidad del Proveedor Adjudicado solucionar todos los incidentes de seguridad que involucren los servicios contratados, deberá documentar las actividades realizadas en la solución y en los casos en que el IFT lo requiera, realizar el análisis forense del mismo. ¿Es correcto el entendido de que los incidentes de seguridad que involucran los servicios contratados se limitan a los equipos que conforman la propuesta del licitante y a los equipos que conforman el servicio de Administración de la Seguridad existentes?
24	PAGINA 16 ANEXO TECNICO NUEMERAL 3.2.1.4 CONDICIONES DE LOS SERVICIOS DE SEGURIDAD ADMINISTRADA. PÁRRAFO 5 DICE: Es responsabilidad del Proveedor Adjudicado solucionar todos los incidentes de seguridad que involucren los servicios contratados, deberá documentar las actividades realizadas en la solución y en los casos en que el IFT lo requiera, realizar el análisis forense del mismo. ¿La convocante requerirá el alcance legal para los casos de análisis forense derivados de un incidente de seguridad?
25	PAGINA 16 ANEXO TECNICO NUEMERAL 3.2.1.4 CONDICIONES DE LOS SERVICIOS DE SEGURIDAD ADMINISTRADA, PÁRRAFO 1 DICE: Las soluciones se deberán considerar para dar soporte a los dispositivos conectados a la red institucional del IFT. El Proveedor Adjudicado deberá considerar como parte del servicio propuesto el crecimiento que pueda darse a lo largo de la vigencia del proyecto en usuarios o equipos conectados a la infraestructura del IFT en al menos un 10% anual. ¿Es correcto entender que cuando la convocante dice "Las soluciones se deberán considerar para dar soporte a los dispositivos conectados a la red institucional del IFT" se refiere a que "las soluciones deberán proteger a los dispositivos conectados a la red institucional del IFT"?
26	PAGINA 17 ANEXO TECNICO NUEMERAL 3.2.1.4 CONDICIONES DE LOS SERVICIOS DE SEGURIDAD ADMINISTRADA, PÁRRAFO 1 DICE: El Proveedor Adjudicado a través del SOC deberá realizar respaldos a las configuraciones y políticas de todos los dispositivos administrados al menos 1 vez cada 24 horas e inmediatamente después de cada cambio programado. Estos respaldos deberán ser almacenados en dispositivos que cuenten con mecanismos de control de acceso seguro y sólo serán accesibles a personal autorizado por el IFT, en caso necesario se deberán entregar dichos respaldos a el IFT a través de los mecanismos que de común acuerdo se establezcan para el efecto. Las políticas de retención deberán considerar la conservación de los respaldos por 90 días para cada respaldo. Se pide amablemente a la convocante nos permita realizar los respaldos de las configuraciones de cada una de las tecnologías que conforman los nuevos servicios y de los servicios existentes, cada que se realiza un cambio programado, ya que de esa manera se tendrían contempladas todas las configuraciones de los equipos.
27	PAGINA 17 ANEXO TECNICO NUEMERAL 3.2.1.4 CONDICIONES DE LOS SERVICIOS DE SEGURIDAD ADMINISTRADA, PÁRRAFO 2 DICE: "--- En caso necesario el IFT podrá solicitar la entrega de las bitácoras con una frecuencia diferente o en atención a algún incidente de seguridad específico." ¿Es correcto entender que la

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	convocante proporcionará los medios de almacenamiento para estas solicitudes de entrega de las bitácoras con frecuencia diferente o en atención a algún incidente de seguridad específico?
28	PAGINA 18 ANEXO TECNICO NUEMERAL 3.2.1.5 PRODUCTOS, TABLA DE REPORTES, PUNTO E.3.2.1.5.4 "Respaldo de las bitácoras generadas por los servicios de administración de filtrado de contenido, detección/prevención de intrusos, control de acceso firewall, protección contra amenazas de nueva generación y protección de aplicaciones Web, servidores de archivos y bases de datos." ¿Es correcto entender que el respaldo de las bitácoras se hará únicamente sobre los dispositivos que se mencionan en este punto y no en ningún otro dispositivo contemplado en las fuentes de logs?
29	PAGINA 19 ANEXO TECNICO NUEMERAL 3.2.1.5 PRODUCTOS, E.3.2.1.5.8 REPORTE DE INCIDENTES POR CÓDIGO MALICIOSO DICE:. Este documento deberá contener, al menos: R.3.2.1.5.8.1 Incidentes ocasionados por malware en general identificado en el Instituto. R.3.2.1.5.8.2 Identificación de equipos más atacados, fuentes de malware y acciones de remediación ejecutadas. Con base al contenido del reporte en cuestión. Será la CONVOCANTE tan amable de clarificar referente a la remediación de equipos sujetos a incidentes por código malicioso: ¿Las acciones de remediación ejecutadas serán llevadas a cabo por personal de la CONVOCANTE?,¿ El alcance del PROVEEDOR será emitir recomendaciones para remediar y/o bien limitar el alcance y magnitud del incidente de seguridad por código malicioso detectado?
30	PAGINA 20 ANEXO TECNICO NUEMERAL 3.2.1.6 SERVICIO DE GESTIÓN DE INFRAESTRUCTURA Y MONITOREO DE EVENTOS DE LOS COMPONENTES DE SEGURIDAD PERIMETRAL DEL IFT. TABLA S.1.1 . [Servicio de gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT.], Característica/Propósito. El Proveedor Adjudicado tomará la administración de los equipos de seguridad perimetral provistos por el IFT como parte del proyecto. El Proveedor Adjudicado deberá realizar un monitoreo 7 x 24 (las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato) a la infraestructura de seguridad involucrada en los servicios de seguridad administrada. El Proveedor Adjudicado deberá instalar el software y hardware necesario, así como administrar los recursos humanos que integre al proyecto con el fin de dar cumplimiento a los niveles de servicio definidos. Se pide amablemente a la convocante nos indique si el monitoreo será realizado de manera local o remota.
31	PAGINA 20 ANEXO TECNICO NUEMERAL 3.2.1.6 SERVICIO DE GESTIÓN DE INFRAESTRUCTURA Y MONITOREO DE EVENTOS DE LOS COMPONENTES DE SEGURIDAD PERIMETRAL DEL IFT

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Tabla S.1.1. [Servicio de gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT.], Característica/Propósito. El Proveedor Adjudicado tomará la administración de los equipos de seguridad perimetral provistos por el IFT como parte del proyecto. El Proveedor Adjudicado deberá realizar un monitoreo 7 x 24 (las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato) a la infraestructura de seguridad involucrada en los servicios de seguridad administrada. El Proveedor Adjudicado deberá instalar el software y hardware necesario, así como administrar los recursos humanos que integre al proyecto con el fin de dar cumplimiento a los niveles de servicio definidos. ¿Es correcto entender que los niveles de servicio de los componentes tecnológicos de seguridad propuestos por el licitante dependerán únicamente de la disponibilidad de los equipos que conforman tal propuesta y no de los componentes que interactuarán con los equipos de seguridad de los servicios existentes o de la infraestructura propia del IFT?
32	PAGINA 21 3.2.1.7 Servicio de correlación de eventos y administración de bitácoras. Tabla S.1.2 - [Servicio de correlación de eventos y administración de bitácoras.] ...En caso de entregar el reporte dentro del plazo señalado, se considerará como un servicio no prestado y será sujeto a las penalizaciones correspondientes conforme a lo establecido en el capítulo correspondiente de este Anexo técnico. Se hace la observación a la convocante que el párrafo referenciado debería decir: "En caso de NO entregar el reporte dentro del plazo señalado, se considerará como un servicio no prestado y será sujeto a las penalizaciones correspondientes conforme a lo establecido en el capítulo correspondiente de este Anexo técnico.", ¿Es correcta nuestra apreciación?
33	PAGINA 22 ANEXO TECNICO NUEMERAL 3.2.1.7 SERVICIO DE CORRELACIÓN DE EVENTOS Y ADMINISTRACIÓN DE BITÁCORAS, PÁRRAFO 2. DICE: "Dicha solución deberá realizar la administración de toda la información de seguridad generada por todos los dispositivos de la infraestructura de red de distintos fabricantes y proveedores ..." Se pide amablemente a la convocante nos enliste los dispositivos de red de distintos fabricantes y proveedores que se tienen contemplados integrar a la solución de correlación para esta licitación
34	PAGINA 23 ANEXO TECNICO NUEMERAL 3.2.1.7 SERVICIO DE CORRELACIÓN DE EVENTOS Y ADMINISTRACIÓN DE BITÁCORAS, PÁRRAFO 2. DICE: El servicio deberá soportar todas las plataformas que tiene el IFT, incluyendo sistemas operativos, dispositivos de red, bases de datos, entre otros. Es correcto interpretar que las tecnologías que no envían bitácoras como por ejemplo soluciones en la nube, no estarán sujetas a la solicitud de la recolección de las mismas
35	PAGINA 24 ANEXO TECNICO NUEMERAL 3.2.1.8 ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN; Tabla S.1.3- [Servicio de análisis de vulnerabilidades y pruebas de penetración.]; Primera fila: Descripción. Determinar el nivel de riesgo que presenta la infraestructura del Instituto frente a las distintas amenazas a las que puede enfrentarse de acuerdo a su ubicación, uso, sensibilidad, entre otros factores relevantes. Para determinar el nivel de riesgo al que estaría

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	expuesta la infraestructura del Instituto de acuerdo a la ubicación, uso y sensibilidad, es necesario realizar un análisis de riesgos. Las pruebas de penetración y análisis de vulnerabilidades identifican el nivel de criticidad de una vulnerabilidad en un activo tecnológico, por lo cual ¿Es correcto interpretar que del resultado del análisis de vulnerabilidades y pruebas de penetración se determine no el riesgo sino el nivel de criticidad de las vulnerabilidades basándose en un estándar para medirse de acuerdo a las características de seguridad de la información y en la priorización de la remediación para ponderarlo al valor identificado?.
36	PAGINA 24 ANEXO TECNICO NUEMERAL 3.2.1.8 ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN; TABLA S.1.3- [SERVICIO DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN.] Tercera fila: Descripción. Oficinas del IFT consideradas en el alcance del proyecto. Dispositivos de red y aplicaciones definidas para este servicio. Se solicita amablemente a la CONVOCANTE listar las ubicaciones fuera de la Cuidad de México o Área Metropolitana donde se realizarán las pruebas
37	PAGINA 24 ANEXO TECNICO NUEMERAL 3.2.1.7 SERVICIO DE CORRELACIÓN DE EVENTOS Y ADMINISTRACIÓN DE BITÁCORAS. PÁRRAFO 4. DICE: "... Al cabo de los 365 días se entregará un respaldo a el IFT en formato legible para sus equipos (formato abierto) considerando mecanismos de seguridad que aseguren su integridad y confiabilidad." ¿Es correcto interpretar que la entrega de información se puede hacer en el mismo formato con el que la herramienta administra la información? Con este formato se tiene un proceso más eficiente y se protegen las bitácoras de ser leídas en dispositivos ajenos a la solución propuesta por el licitante.
38	PAGINA 24 ANEXO TECNICO NUEMERAL 3.2.1.7 SERVICIO DE CORRELACIÓN DE EVENTOS Y ADMINISTRACIÓN DE BITÁCORAS. PÁRRAFO 3 DICE: ...El almacenamiento en donde se concentre la información de las bitácoras deberá contar con mecanismos de cifrado que resguarden su integridad. Se pide amablemente a la convocante nos aclare a que se refiere con "mecanismos de seguridad que resguarden su información" ?
39	PAGINA 25 ANEXO TECNICO NUEMERAL 3.2.1.8 ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN, A) ANÁLISIS DE VULNERABILIDADES; PÁRRAFO 4 DICE: Se deberá ejecutar un proceso trimestral incremental de análisis de vulnerabilidades sobre las aplicaciones, infraestructura existente y nuevos desarrollos, se deberán de considerar hasta 25 IP's y 5 URL's nuevas mensualmente, la información del análisis se deberá incluir en la correlación . Las IP's y URL's serán proporcionadas por el IFT. Derivado al requerimiento de ejecutar el proceso de forma trimestral para análisis de vulnerabilidades ¿Es correcto interpretar que el incremento de hasta 25 direcciones IP y 5 URL's se realizará de forma trimestral y no mensual como se hace mención?
40	PAGINA 25 ANEXO TECNICO NUEMERAL 3.2.1.8 ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN, A) ANÁLISIS DE VULNERABILIDADES PÁRRAFO 1, VIÑETA 3. DICE:

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Obtener reportes estadísticos de activos más atacados, patrones más frecuentes de ataque (fuentes, horarios, tipos, etc.), tipos de ataque más realizados, activos más vulnerables, activos con más impacto probable, entre otros. Derivado de que este tipo de análisis no refleja la visibilidad requerida en los reportes estadísticos, se propone a la CONVOCANTE que los datos de los reportes estadísticos para activos más atacados, patrones más frecuentes de ataque (fuentes, horarios, tipos, etc.), sean obtenidos a través del servicio de correlación de eventos y se limite a los activos más vulnerables y activos con más impacto probable, entre otros. ¿Se acepta nuestra propuesta?
41	PAGINA 52 ANEXO TECNICO NUEMERAL 3.2.1.11 SERVICIOS DE PROTECCIÓN PARA CORREO ELECTRÓNICO. Periodicidad de revisión del ANS El Proveedor Adjudicado deberá entregar el reporte de disponibilidad del servicio a mes vencido y deberá presentarse dentro de los 10 días naturales posteriores al cierre del mes al que corresponda. El Administrador del contrato por parte de la Dirección General de Tecnologías de la Información y Comunicaciones del IFT tendrá cinco días hábiles para la aprobación del contenido de dicho reporte o para solicitar las correcciones que considere pertinentes. En caso de entregar el reporte dentro del plazo señalado, se considerará como un servicio no prestado y será sujeto a las penalizaciones correspondientes conforme a lo establecido en el capítulo correspondiente de este Anexo técnico. Se hace la observación a la convocante que el párrafo referenciado debería decir: "En caso de NO entregar el reporte dentro del plazo señalado, se considerará como un servicio no prestado y será sujeto a las penalizaciones correspondientes conforme a lo establecido en el capítulo correspondiente de este Anexo técnico."
42	PAGINA 52 ANEXO TECNICO NUEMERAL 3.2.1.11 SERVICIOS DE PROTECCIÓN PARA CORREO ELECTRÓNICO. PÁRRAFO 1, BULLET 6 DICE: La herramienta solicitada deberá poder interactuar con la solución de detección antimalware basado en Web para detener ataques combinados a través de múltiples vectores de amenazas. Será la CONVOCANTE tan amable de aclarar: ¿Cuál es la solución de detección de antimalware basada en Web que utiliza?
43	PAGINA 55 ANEXO TECNICO NUEMERAL 3.2.1.13 SERVICIO DE MONITOREO PROACTIVO DE SEGURIDAD EN INTERNET. Tabla S.1.8 - [Servicio de monitoreo proactivo de seguridad en Internet] Fila 2 Operación. La periodicidad del Documento de alerta temprana dice: "Por cada amenaza detectada, no mayor a 24 horas de la detección o publicación." ¿Es correcto entender que el documento de alerta temprana deberá ser generado por cada vez que sea detectada una amenaza que afecte directamente al Instituto, en un tiempo no mayor a 24 horas de la detección o publicación?
44	PAGINA 56 ANEXO TECNICO NUEMERAL 3.2.1.13 SERVICIO DE MONITOREO PROACTIVO DE SEGURIDAD EN INTERNET. PÁRRAFO 3. La naturaleza del servicio es detectar de manera proactiva algún ataque, sin embargo si durante el monitoreo se detecta que un ataque ya sucedió y tuvo un impacto en la organización también deberá emitirse el mismo informe. Se pide amablemente a la convocante nos indíque ¿Cuál es

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	el tiempo que se tiene considerado para la entrega del "Documento de Alerta Temprana" para las amenazas que ya impactaron en el Instituto?
45	PAGINA 57 ANEXO TECNICO NUEMERAL 3.2.1.14 SERVICIO DE ENRUTAMIENTO DE ENLACE DE INTERNET Tablas S.1.9 - [Servicio de enrutamiento de enlace de Internet], Nivel de servicio mínimo esperado. 99.9% mensual ¿Es correcto entender que para poder cumplir con el nivel de servicio del 99.9% para el "Servicio de Enrutamiento de Enlace de Internet", se debe considerar un escenario de alta disponibilidad?
46	PAGINA 58 ANEXO TECNICO -Especificaciones Técnicas, apartado 3.2.2.1 Centro de Operaciones de Seguridad (SOC) Es correcto interpretar que para acreditar los 10 años de experiencia del SOC del licitante participante se deberá presentar al menos un contrato de servicios que incluyan servicios administrados de seguridad cuya ejecución date de 10 años atrás de la fecha de publicación de la presente convocatoria? En caso contrario, se solicita a la convocante establezca que evidencia deberá presentarse para comprobar que el SOC del licitante participante cuenta con por lo menos 10 años de experiencia. Favor de precisar y aclarar.
47	PAGINA 58 ANEXO TECNICO NUMRAL 3.2.2.1 VIÑETA 7 DICE: El SOC deberá de tener las alianzas y/o fuentes de información de inteligencia de seguridad para tener acceso a la información relativa a nuevas y viejas amenazas, el comportamiento de las amenazas y su remediación; estás funcionalidades deberán estar inmersas en el mecanismo de identificación y detección de amenazas y deberá mostrar las principales amenazas en el Portal de Servicio a el IFT. ¿Es correcto interpretar que las alianzas o fuentes de información pueden ser demostradas a través de la contratación de un servicio?
48	PAGINA 69 ANEXO TECNICO NUEMERAL 4.1.1 INICIO DE ACTIVIDADES, PÁRRAFO 3 DICE: El Proveedor Adjudicado, deberá definir y aplicar las configuraciones necesarias para interconectar sus herramientas tecnológicas para la prestación de los servicios contratados. Este análisis, así como los ajustes de configuración a los equipos deberán aplicarse dentro de los primeros 90 días del proyecto una vez notificado el fallo al Proveedor Adjudicado. ¿La convocante proporcionará todos los permisos, accesos necesarios y del personal necesario involucrado en las diferentes áreas del IFT, con el propósito de llevar a cabo la configuración de cada uno de los componentes tecnológicos de seguridad que conforman la propuesta del licitante así como aquellos componentes de seguridad que ya están en operación?
49	PAGINA 69 ANEXO TECNICO NUEMERAL 4.1.1 INICIO DE ACTIVIDADES, PÁRRAFO 1 DICE: El Proveedor Adjudicado debe iniciar las actividades del servicio a partir del primer día hábil después de la fecha de notificación del fallo para la adjudicación del contrato. ¿Es correcto entender que cuando la convocante menciona "iniciar actividades del servicio" se refiere a la toma de la gestión de los equipos de los servicios existentes y a las mesas de trabajo para la configuración y puesta a punto de los componentes tecnológicos de seguridad que conforman los servicios nuevos?
50	PAGINA 30

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	ANEXO TECNICO NUEMERAL Tabla S.1.4, Propósito - [Servicio de control de acceso Firewall] Propósito. Contar con una solución en alta disponibilidad que ofrezca protección perimetral a la red del IFT con la finalidad de proteger la infraestructura, las aplicaciones, la información y los servicios de Internet de accesos no autorizados. Con el objetivo de llevar a cabo la instalación de los equipos que ofrecerán el servicio de Firewall en Boston e Iztapalapa, ¿Podría la convocante indicarnos si será responsable de proporcionar los switches para el escenario de alta disponibilidad?
51	PAGINA 32 ANEXO TÉCNICO NUMERAL. 3.2.1.9 Servicio de control de acceso Firewall, Inciso b. Firewall sitio secundario "Iztapalapa". La solución de firewall que se instalará en el sitio principal del IFT denominado "Iztapalapa" deberá implementarse bajo Derivado del nombre que recibe este sitio, en caso de la caída del sitio principal, ¿La convocante será la encargada de llevar a cabo el ruteo necesario para redirigir el tráfico al sitio secundario? ¿Será la convocante la responsable de proveer de los enlaces necesarios para llevar a cabo tal ruteo?
52	PAGINA 19 ANEXO TÉCNICO. NUMERAL. Tabla de Entregables, E.3.2.1.5.10 Reporte de actividades relacionados con el servicio de filtrado de contenido Web. R.3.2.1.5.10.5 Actividades relacionadas con accesos por riesgo Se pide amablemente a la convocante nos aclare en qué consiste este reporte

---

INTEGRADORES DE TECNOLOGÍA, S.A. DE C.V.

No.	Preguntas
1	CRITERIOS DE EVALUACION DE PUNTOS Y PORCETAJES CAPACIDAD DEL LICITANTE 1. Capacidad de Recursos Humanos. Al apartado 1 del método de evaluación, referente al párrafo "1. Experiencia en asuntos relacionados con la materia del servicio "se solicita de la manera más atenta solo pidan el certificado de una sola persona para cada rol, quedando de la siguiente forma.

No. de personas	Rol
1	Especialista certificado en auditoría de sistemas
1	Especialista certificado en seguridad de sistemas.
1	Especialista en hackeo ético de sistemas.
1	Especialista en administración de seguridad de la información.
1	Especialista en administración de incidentes de seguridad
1	Administrador del Servicio

2	CRITERIOS DE EVALUACION DE PUNTOS Y PORCETAJES CAPACIDAD DEL LICITANTE 1. Capacidad de Recursos Humanos. Inciso b) Se solicita a la convocante considerar que el personal propuesto cuente con seguro social o se presente un escrito a través del cual el representante legal manifieste bajo protesta de decir verdad que el personal propuesto es y será de la exclusiva y única competencia del Licitante por lo que cualquier obligación o responsabilidad legal de cualquier naturaleza, que se derive de la relación laboral, con el personal propuesto, liberando al IFT de cualquier reclamación o acción legal que pudiera ejercitarse en su contra por tal motivo

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
3	CRITERIOS DE EVALUACION DE PUNTOS Y PORCETAJES CAPACIDAD DEL LICITANTE En el punto 2 de Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales. Se solicita a la Convocante considere disminuir la cantidad de especialistas a uno mínimo con al menos un certificado de especialización y dejar como opcional al especialista GIAC, debido que esa certificación solo la cumple una empresa y se estará limitando la libre participación.
4	CRITERIOS DE EVALUACION DE PUNTOS Y PORCETAJES CAPACIDAD DEL LICITANTE propuesta de trabajo punto 1 Se solicita a la convocante pedir mínimo el cumplimiento de un proceso ISO 27001 para otorgar mínimo dos puntos.
5	ANEXO TECNICO En el punto 3.2.1.2 Administración y monitoreo de la infraestructura de seguridad perimetral existente. Solicitan la administración y monitoreo de los dispositivos de seguridad perimetral que actualmente se encuentran instalados. Agradeceremos nos indiquen si la parte de reemplazo de partes del listado anexo en la tabla ya viene contemplada o si solicitan también se considere.
6	ANEXO TECNICO punto 3.2.1.3 Servicios de trasferencia de conocimientos Se solicita a la convocante en el punto 3.2.1.3 Servicios de trasferencia de conocimientos, nos confirme cuantos serán los participantes que tomaran dichos cursos.
7	ANEXO TECNICO punto 3.2.1.4 Condiciones del servicio administrada punto 1 Se solicita a la convocante referente al punto 3.2.1.4 Condiciones del servicio administrada punto 1, donde comenta que el crecimiento anual de equipos conectados es del 10%, el IFT requiriere que integremos equipo de conectividad denominados Switches y nodos de red para que dichos usuarios puedan conectarse a las red si es así especificar características que deben tener estos equipos de conectividad.
8	ANEXO TECNICO 3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos. 3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos. En el párrafo donde dice "El proveedor adjudicado deberá de considerar que la solución deberá soportar el análisis de los aplicativos web, bases de datos y servidores de archivos como sigue: • 6 servidores de aplicación web. • 12 servidores de base de datos. • 1 servidor de SharePoint. • 1 servidor de archivos." Se solicita de la manera más atenta a la Convocante nos proporcionen las capacidades de los servidores, para dimensionar de manera más eficiente.
9	ANEXO TECNICO Punto 3.2.1.14 Servicio de enrutamiento de enlace de Internet

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Referente al punto 3.2.1.14 Servicio de enrutamiento de enlace de Internet, se solicita saber que ancho de banda de internet e Interfaz va a recibir el equipo de routeo además si van a manejar AH para también conocer el ancho de banda e interfaz del enlace redundante.
10	ANEXO TECNICO 3.2.2.1 Centro de Operaciones de Seguridad (SOC) Respecto al punto Centro de Operaciones de Seguridad (SOC), favor de considerar la opción de presentar como mínimo un proceso.
11	ANEXO TECNICO 3.2.1.5 Productos Tanto para las pruebas de penetración como para el análisis de vulnerabilidades mencionan en primera instancia que serán trimestrales y en otra sección que serán mensuales, es necesario especificar claramente cada cuando serán, ya que están solicitando reportes detallados con las vulnerabilidades que se encuentren Agradeceremos a la convocante nos aclare la periodicidad de éste servicio
12	ANEXO TECNICO Se solicita a la Convocante nos indique a cuantas IPs y a que elementos se realizará tanto el AV como el PT
13	ANEXO TECNICO Solicitamos a la Convocante nos proporcione las características de las herramientas a utilizar para el AV y PT y si también requieren que el appliance tenga algún tipo de característica específica.

Axtel S.A.B. de C.V.

No.	Preguntas
1	**Fecha y Lugar para la prestación de "Los Servicios"** Fecha: A partir del 11 de noviembre de 2014 y hasta el 31 de octubre de 2017. PÁG. 1 Se solicita a la convocante confirmar que los licitantes podremos realizar la instalación de la infraestructura, configuración y puesta a punto de la misma como máximo 12 semanas, después del fallo del presente concurso de licitación. Se acepta nuestra propuesta?
2	**3.2.1.1. Nuevos Servicios Pág- 11 de 74** El Proveedor Adjudicado debe considerar en su propuesta de solución, los elementos necesarios para habilitar dichas soluciones, tales como: gabinetes para montaje de equipo, cables certificados, accesorios, etiquetas, entre otros), en el entendido que todos ellos forman parte de los servicios administrados. PÁG. 11 Se solicita a la convocante definir el nivel de certificación de cableado que requiere para que los licitantes estemos en igualdad de condiciones al momento de realizar la oferta económica.
3	**3.2.1.1. Nuevos Servicios Pág- 11 de 74** Todo el equipo provisto y colocado en sitio por el Proveedor Adjudicado para este proyecto, deberá: • Ser nuevo, de última generación y dedicado sólo a la solución diseñada para el Instituto.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	• Cuando la solución lo permita, ser equipo de propósito específico (appliance) para cada servicio que así lo requiera. PÁG. 11 y12 Se solicita a la convocante determinar cuáles serán las soluciones que deberemos considerar los licitantes para incluir equipo nuevo de propósito específico, de tal forma que sea claro para todos los licitantes y estar en igualdad de condiciones tanto técnica como económicamente. En caso de que la respuesta la pregunta anterior sea negativa por parte de la convocante, se solicita nos indique cómo será la forma de evaluación que llevará a cabo para determinar qué solución de seguridad será la adjudicada si cada licitante entregará una solución con cantidades de equipos diferente.
4	**3.2.1.1. Nuevos Servicios Pág- 11 de 74** Todo el equipo provisto y colocado en sitio por el Proveedor Adjudicado para este proyecto, deberá: • Ser nuevo, de última generación y dedicado sólo a la solución diseñada para el Instituto. • Cuando la solución lo permita, ser equipo de propósito específico (appliance) para cada servicio que así lo requiera. • Cumplir con un ciclo de vida básico de al menos 12 meses posteriores a la fecha de término del proyecto, es decir, no estar en condiciones de fin de vida (EoL) o fin de soporte (EoS) por parte del fabricante PÁG. 12 Se solicita a la convocante aclare si cuando se refiere a "equipo provisto y colocado en sitio por el proveedor adjudicado" se refiere a que el equipamiento ofertado para la habilitación de la solución por parte del proveedor será instalado en el centro de datos propio de la convocante.
5	3.2.1.1. Nuevos Servicios Todo el equipo provisto y colocado en sitio por el Proveedor Adjudicado para este proyecto, deberá: • Ser nuevo, de última generación y dedicado sólo a la solución diseñada para el Instituto. • Cuando la solución lo permita, ser equipo de propósito específico (appliance) para cada servicio que así lo requiera. • Cumplir con un ciclo de vida básico de al menos 12 meses posteriores a la fecha de término del proyecto, es decir, no estar en condiciones de fin de vida (EoL) o fin de soporte (EoS) por parte del fabricante. PÁG. 12 Se solicita a la convocante aclare si en caso que el equipamiento para proporcionar los servicios solicitados sean instalados en los centros de datos de la convocante, estos cuentan con los facilities (espacio, clima, energía, cableado, organizadores, piso falso, etc) necesarios para garantizar la operación de este equipamiento?
6	3.2.1.1. Nuevos Servicios En caso de que las instalaciones del centro de datos del IFT sufran modificaciones durante la vigencia del contrato (como parte de mejoras a las instalaciones, requerimientos internos o incluso atendiendo observaciones de auditorías), será responsabilidad del proveedor adjudicado proporcionar los recursos necesarios para reubicar, configurar, reinstalar y ajustar los Componentes Habilitadores que lo necesiten. El Proveedor Adjudicado deberá considerar al menos dos modificaciones durante la vigencia del contrato derivadas por reubicaciones o cambio de equipo en los centros de datos del Instituto. PÁG. 12

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

<table>
<tr><th>No.</th><th>Preguntas</th></tr>
<tr><td></td><td>Se solicita a la convocante aclare en el caso de reubicación o cambio de equipos en los centros de datos del instituto, que direcciones deberán ser consideradas para estas reubicaciones, en el interior de la Republica o DF y Área Metropolitana.</td></tr>
<tr><td>7</td><td>3.2.1.1. Nuevos Servicios

Es importante que el Proveedor Adjudicado tome en cuenta que algunos de estos equipos deberán migrarse, o bien instalarse y configurarse desde cero. En la tabla que se muestra a continuación, se listan las cantidades y modelos de los equipos, y se da la descripción de uso de cada uno y si deberá o no ser considerado para migración de localidad.
PÁG. 12
Se solicita a la convocante aclare si este equipamiento tiene soporte y mantenimiento por los 36 meses del contrato, en caso de ser negativa la respuesta indicando cual es la fecha de término de mantenimiento que se tiene contratado.

<table>
<tr><th>Dispositivo</th><th>Marca</th><th>Modelo / Versión</th><th>Cantidad</th><th>Descripción de función</th><th>Vigencia del contrato de soporte con el fabricante</th></tr>
<tr><td>APS</td><td>Arbor</td><td>PRA-APS-2104</td><td>1</td><td>Protección de ataques de DDoS</td><td></td></tr>
<tr><td>Balanceador de carga</td><td>F5</td><td>LTM2000</td><td>2</td><td>Balanceo de enlaces de Internet</td><td></td></tr>
<tr><td>IPS</td><td>SourceFire</td><td>3D7120</td><td>1</td><td>Sistema de protección de intrusos</td><td></td></tr>
<tr><td>Defense Center</td><td>SourceFire</td><td>Defense Center 750</td><td>1</td><td>Consola de administración de IPS</td><td></td></tr>
<tr><td>Firewall / VPN</td><td>Cisco</td><td>ASA 5525-X</td><td>1</td><td>Establece conexiones VPN y hace el filtrado de contenido Web de los clientes que se conectan remotamente</td><td></td></tr>
</table>
</td></tr>
</table>

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas

	ISE	Cisco	Cisco ISE Software versión 1.2	2	Autentica y autoriza el acceso de usuarios y dispositivos a la red, ya sea por medios cableados o inalámbricos .	
	Deep Security	Trend Micro	Versión 8.0	152	Plataforma integral de seguridad para servidores físicos / virtuales (152 licencias)	
	Deep Discovery	Trend Micro	NA	1	Seguridad avanzada de red	

8

3.2.1.2 Administración y monitoreo de la infraestructura de seguridad perimetral existente
El Proveedor Adjudicado deberá considerar, como parte del proyecto, la administración y monitoreo de los dispositivos de seguridad perimetral que actualmente se encuentran instalados en el IFT, sean arrendados o propiedad del Instituto.
PÁG. 12
Se solicita a la convocante entregar una lista de los dispositivos de seguridad que son propiedad de la convocante y cuales son propiedad de un tercero.

Dispositivo	Marca	Modelo / Versión	Cantidad	Descripción de función	Propiedad de: convocante / tercero
APS	Arbor	PRA-APS-2104	1	Protección de ataques de DDoS	
Balanceador de carga	F5	LTM2000	2	Balanceo de enlaces de Internet	
IPS	SourceFire	3D7120	1	Sistema de protección de intrusos	
Defense Center	SourceFire	Defense Center 750	1	Consola de administración de IPS	

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas						
	Firewall / VPN	Cisco	ASA 5525-X	1	Establece conexiones VPN y hace el filtrado de contenido Web de los clientes que se conectan remotamente		
	ISE	Cisco	Cisco ISE Software versión 1.2	2	Autentica y autoriza el acceso de usuarios y dispositivos a la red, ya sea por medios cableados o inalámbricos.		
	Deep Security	Trend Micro	Versión 8.0	152	Plataforma integral de seguridad para servidores físicos / virtuales (152 licencias)		
	Deep Discovery	Trend Micro	NA	1	Seguridad avanzada de red		
9	3.2.1.2 Administración y monitoreo de la infraestructura de seguridad perimetral existente El Proveedor Adjudicado deberá considerar, como parte del proyecto, la administración y monitoreo de los dispositivos de seguridad perimetral que actualmente se encuentran instalados en el IFT, sean arrendados o propiedad del Instituto. PAG. 12 Se solicita a la convocante entregar los archivos de techsupport de los siguientes dispositivos:						

Dispositivo	Marca	Modelo / Versión	Cantidad	Descripción de función	Techsupport solicitado
APS	Arbor	PRA-APS-2104	1	Protección de ataques de DDoS	SI

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas

	Balanceador de carga	F5	LTM2000	2	Balanceo de enlaces de Internet	SI
	IPS	Source Fire	3D7120	1	Sistema de protección de intrusos	SI
	Firewall / VPN	Cisco	ASA 5525-X	1	Establece conexiones VPN y hace el filtrado de contenido Web de los clientes que se conectan remotamente	SI
	ISE	Cisco	Cisco ISE Software versión 1.2	2	Autentica y autoriza el acceso de usuarios y dispositivos a la red, ya sea por medios cableados o inalámbricos.	SI

Lo anterior para determinar las condiciones de operación de los dispositivos y saber si deberemos realizar la sustitución de los mismos desde el inicio del proyecto ya que el proveedor será el único responsable del servicio.

10

3.2.1.3 Servicios de transferencia de conocimientos

El Proveedor Adjudicado deberá considerar dentro de su propuesta la transferencia de conocimientos de todas las soluciones tecnológicas de seguridad (incluidas las que son propiedad o ya están arrendadas por el IFT) considerando el número de asistentes por solución tecnológica que se presenta en la siguiente tabla:
La transferencia de conocimientos debe considerar el material de apoyo para los participantes en formato impreso y/o electrónico. Los cursos deberán programarse en horario de Lunes a Viernes a partir de las 8:00 y hasta las 18:00 hrs. La transferencia de conocimientos de los componentes de administración de bitácoras y correlación de eventos, análisis de vulnerabilidades, protección de aplicaciones, servidores de archivos y bases de datos, control de ataques de denegación de servicios y balanceador de carga de enlaces de Internet deberán ser impartidos directamente por el fabricante.
PAG. 13

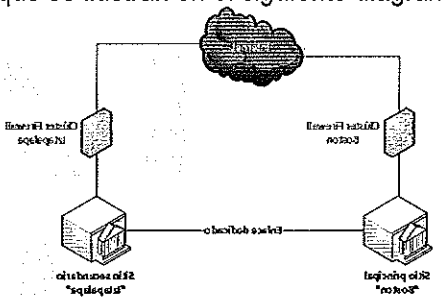
Se solicita a la convocante confirmar si por transferencia de conocimientos se refiere a que esta deberá ser impartida por un centro autorizado por el fabricante de las soluciones de seguridad solicitadas y a ofertar por los licitantes (de acuerdo a la tabla de la página 14) y que de ser así

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	en este caso el material que se entregará a los participantes será solo de forma impresa ya que en formato electrónico no será factible la entrega por los derechos de autor del material. Favor de pronunciarse al respecto.
11	Los servicios de transferencia de conocimientos podrán ser proporcionados en las instalaciones de centros de capacitación o laboratorios de los fabricantes o del Proveedor Adjudicado considerando, para cada caso, el temario y el número de asistentes indicados en el siguiente cuadro: PAG. 14 Se solicita a la convocante aclare si la transferencia de conocimiento deberá ser impartida en el área metropolitana, en caso de no ser así, especificar en donde deberá ser impartida.
12	3.2.1.4 Condiciones de los Servicios de Seguridad Administrada El IFT podrá realizar un monitoreo de disponibilidad con sus propias herramientas con el fin de validar la información proporcionada por el Proveedor Adjudicado en los reportes mensuales, por lo que el Proveedor Adjudicado deberá aceptar la instalación de los agentes necesarios en la infraestructura inmersa en el servicio, si fuese necesario. PAG. 16 Se solicita a la convocante definir que la herramienta válida de monitoreo de disponibilidad en caso de haber diferencias y para evotar controversias se tomarán las estadísticas de la herramienta que oferte cada uno de los licitantes.
13	3.2.1.5 Productos Entregable: Reporte mensual de Capacidades: R.3.2.1.5.1.2 Datos de ocupación de disco, memoria, procesador, desempeño y rangos de operación establecidos. PAG. 18 Se solicita a la convocante especifique a que métrica se refiere con la descripción "Rangos de operación establecidos" o en su defecto explicar a qué se refiere con esta solicitud
14	3.2.1.6 Servicio de gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT. En caso de entregar el reporte dentro del plazo señalado, se considerará como un servicio no prestado y será sujeto a las penalizaciones correspondientes conforme a lo establecido en el capítulo correspondiente de este Anexo técnico. PAG: 21 Se solicita a la convocante confirmar si hubo un error al describir el párrafo y el párrafo deberá indicar lo siguiente : En caso de NO entregar el reporte dentro del plazo señalado, se considerará como un servicio no prestado y será sujeto a las penalizaciones correspondientes conforme a lo establecido en el capítulo correspondiente de este Anexo técnico
15	3.2.1.7 Servicio de correlación de eventos y administración de bitácoras El Proveedor Adjudicado deberá considerar el procedimiento de administración de las bitácoras, el cual deberá definir la identificación de las bitácoras que se activarán para cada dispositivo, el tamaño máximo de cada bitácora, los eventos que se deberán incluir para cada dispositivo y la forma en que se realizará la transferencia a un almacenamiento debidamente catalogado, que permita en el futuro su consulta sin mayores esfuerzos por parte del IFT (formato abierto). PAG. 24

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Se solicita a la convocante definir la capacidad de almacenamiento de las bitácoras que deberemos considerar los licitantes.
16	3.2.1.8 Análisis de vulnerabilidades y pruebas de penetración b) Pruebas de Penetración En el caso de requerir viajar para la prestación de este servicio el Proveedor Adjudicado deberá considerar los viáticos correspondientes para el traslado de su personal a la ubicación donde el IFT requiera la ejecución del servicio. PAG. 29 Se solicita a la convocante definir las localidades y número de eventos que deberemos considerar los licitantes para la ejecución de las pruebas de penetración ya que es muy general indicar que el IFT podrá o no requerir el servicio y si lo requiere el IFT determinará la ubicación en donde se deberá llevar a cabo el servicio. Es importante mencionar a la convocante que para estar en igualdad de condiciones todos los licitantes, se solicita incluir este tipo de servicios en el formato económico de forma independiente al precio mensual del servicio como lo solicita, siempre considerando los licitantes que este tipo de servicios formará parte integral del servicio solicitado por la convocante y en caso de ser requerido por la convocante, está tendrá el monto que deberá pagar al licitante el cual formará parte de su presupuesto general del servicio y con esto evitar un perjuicio al erario al pagar por servicios que posiblemente no utilizará la convocante, se acepta nuestra propuesta?
17	3.2.1.8 Análisis de vulnerabilidades y pruebas de penetración b) Pruebas de Penetración En el caso en que las pruebas de penetración se realicen en las localidades físicas del IFT, éste asignará un lugar físico de trabajo para que el Proveedor Adjudicado desarrolle las actividades correspondientes. Para ello se proporcionará: • Dos (2) nodos de red con conectividad a la red interna. • Dos (2) direcciones IP que tengan visibilidad de los dispositivos a ser auditados. Se solicita a la convocante definir las direcciones físicas de las localidades del IFT que los licitantes deberemos considerar para llevar a cabo las actividades correspondientes a las pruebas de penetración
18	3.2.1.9 Servicio de control de acceso Firewall El proyecto considera las instalaciones del IFT en las cuales se contará con salida a Internet para tráfico de usuarios conforme a lo establecido en los proyectos vigentes del Instituto, por lo tanto, el IFT requiere como parte de este servicio que el Proveedor Adjudicado considere la implementación de dispositivos de control de acceso Firewall en alta disponibilidad en los sitios que se ilustran en el siguiente diagrama: 

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Se solicita a la convocante proporcione las direcciones físicas de los siguientes sitios: • Boston • Iztapalapa • Centro de datos IFT Se solicita a la convocante confirmar que el enlace dedicado que aparece en el diagrama no deberemos considerarlo, en caso contrario favor de especificar las características que deberemos considerar para su dimensionamiento. • Ancho de banda: Tipo de interface de entrega:
19	3.2.2.1 Centro de Operaciones de Seguridad (SOC) Contar con un SOC redundante, que en caso de que se presente algún evento donde le impidiera continuar con la operación, este le permita dar continuidad al servicio. De igual forma, este deberá encontrarse en territorio mexicano y a una distancia mínima de 50 km del SOC principal. PAG. 58 Se solicita a la convocante, para garantizar la redundancia se considere "redundancia física y lógica en el SOC" y esta se realice mediante enlaces redundantes con diferente tecnología de acceso desde el SOC del proveedor al centro de datos de la convocante para garantizar la continuidad del servicio.} ¿Se acepta nuestra propuesta?
20	3.2.2.1 Centro de Operaciones de Seguridad (SOC) Contar con un SOC redundante, que en caso de que se presente algún evento donde le impidiera continuar con la operación, este le permita dar continuidad al servicio. De igual forma, este deberá encontrarse en territorio mexicano y a una distancia mínima de 50 km del SOC principal. PAG. 58 Se solicita a la convocante para permitir la libre participación de los licitantes omita la distancia mínima de 50 Kms del SOC redundante al SOC principal y solo quede la característica de que el SOC secundario se localice en territorio mexicano.
21	CAPACIDAD DEL LICITANTE (CL) I. Capacidad de los Recursos Humanos 1. Experiencia en asuntos relacionados con la materia del servicio Inciso b) PAG.3 de 8 Con la intención de abrir a la participación el procedimiento, se le solicita a convocante permita que sólo el 50% del personal pertenezca a la empresa licitante y sea comprobado por medio del pago del IMSS y el resto del personal sea subcontratado. ¿Se acepta nuestra propuesta?
22	3.2.2.3 Centro de Datos del SOC El Proveedor Adjudicado deberá alojar las soluciones de su Centro de Operaciones de Seguridad en un centro de datos independiente a las instalaciones del SOC, que cuente con al menos las siguientes características: Video vigilancia continua 7 x 24 (7 días a la semana durante las 24 del día). Sistema de control de acceso físico de al menos doble factor. Sistema de energía ininterrumpida (UPS). Redundancia en el aprovisionamiento de energía. Cableado estructurado con certificación nivel 6 o superior.

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Aire acondicionado de alta precisión. Sistema de detección y supresión de fuego. Infraestructura de comunicaciones y seguridad interna para los enlaces de comunicaciones. Infraestructura de servidores que soportan la operación del SOC. Personal de seguridad corporativa privada o pública en esquema de 7 x24 (7 días a la semana durante las 24 del día). Certificación en alguno de los estándares de diseño y funcionamiento de Centros de Cómputo, al menos ICREA nivel 4 o TIER III. PAG. 60 Se solicita a la convocante para no encarecer la propuesta económica del servicio solicitado, omita tener un segundo centro de operaciones de seguridad (SOC) en un centro de datos independiente a las instalaciones del SOC principal ya que esto encarecerá la propuesta económica que liberaremos los licitantes hacia la convocante y que desde nuestro punto de vista los componentes del servicio al estar instalados en el centro de datos del IFT y no en los centros de datos de los licitantes no afectará la disponibilidad de los servicios solicitados, exceptuando el monitoreo y administración para los cuales los licitantes tendremos hasta un máximo de 4 horas para restablecer los servicios de monitoreo y administración de las soluciones de seguridad instaladas en el centro de datos del IFT. ¿Se acepta nuestra propuesta?
23	3.2.2.4 Productos De la tabla de la página 60 en la columna entregable: E.3.2.2.4.1 Metodología del SOC E.3.2.2.4.2 Matriz de Escalamiento de Problemas e Incidentes E.3.2.2.4.3 Memorias Técnicas PAG. 60 Se solicita a la convocante confirmar que los documentos solicitados solo los deberá entregar el licitante ganador?
24	3.2.3. Componente 3: Administración del servicio El propósito de este componente es asegurar que el proyecto termine en tiempo, bajo el presupuesto acordado y cumpliendo con todos sus requerimientos. 3.2.3.1 Productos De la tabla de la página 61 en la columna entregable: E.3.2.3.1.1 Presentación de la Junta de inicio del proyecto E.3.2.3.1.2 Plan de Administración del Proyecto E.3.2.3.1.3 Reportes de Avance E.3.2.3.1.4 Plan de Transición E.3.2.3.1.5 Presentación de Cierre E.3.2.3.1.6 Acta de Cierre PAG. 61 Se solicita a la convocante confirmar que los documentos solicitados solo los deberá entregar el licitante ganador? PAG. 61 Se solicita a la convocante confirmar que los documentos solicitados solo los deberá entregar el licitante ganador?
25	CONVOCATORIA PAGINA 9 PUNTO G PROPUESTA ECONOMICA PAG. 9

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Con el fin de homologar la evaluación de las ofertas económicas se solicita a la convocante nos proporcione el formato de propuesta económica
26	CAPACIDAD DEL LICITANTE (CL) I. Capacidad de los Recursos Humanos 1. Experiencia en asuntos relacionados con la materia del servicio Inciso b) PAG. 3 de 8 Se solicita amablemente a la convocante que para acreditar al menos 90 días de antigüedad de cada recurso humano, se pueda cubrir con los últimos pagos del las cuotas del los dos últimos bimestre del IMSS. Se acepta nuestra propuesta?
27	CAPACIDAD DEL LICITANTE (CL) I. Capacidad de los Recursos Humanos 1. Experiencia en asuntos relacionados con la materia del servicio Inciso b) PAG. 3 de 8 Se solicita a la convocante se sirva considerar que para el caso del IMSS, el licitante que no cuente con una constancia a su nombre, debido a que una empresa de su mismo grupo corporativo es quien aporta el capital humano, se acepte una carta bajo protesta de decir verdad en la que se manifieste dicha situación, y en la que se considere a mi representada como el único patrón de todas y cada una de las personas que intervengan en el desarrollo y ejecución del objeto de este contrato, sin necesidad de que la empresa filial que aporta el capital humano deba participar conjuntamente para cubrir con el requisito señalado en la declaración de referencia para presentar el documento del IMSS. Cabe resaltar que este tipo de estructuras corporativas es como opera la mayoría de las empresas en la actualidad. Favor de pronunciarse al respecto.
28	CAPACIDAD DEL LICITANTE (CL) I. Capacidad de los Recursos Humanos 3. Dominio de herramientas relacionadas con el servicio. PAG. 4 de 8 Es claro nuestro entender que para el personal que solicitan en este punto, no es necesario entregar la comprobación del IMSS y que este requerimiento sólo aplica para el rol de especialistas y administrador del servicio del inciso a). Favor de pronunciarse al respecto.
29	EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE (EE) Experiencia PAG: 6 de 8 Es correcto entender que para la comprobación de los siete años de experiencia con 5 contratos, el número máximo de años es de siete y que a partir de estos siete años se va a aplicar la regla de tres? De no ser correcta nuestra apreciación, solicitamos nos definan el número mínimo y máximo de años a cumplir. Favor de pronunciarse al respecto.
30	PROPUESTA DE TRABAJO (PT) 1. Metodología para la prestación del servicio El licitante deberá presentar evidencia de contar con una certificación ISO/IEC 27001 vigente, obtenida con una antigüedad mayor a tres (3) años. Esta certificación deberá considerar los siguientes procesos aplicables a su Centro de Operaciones de Seguridad. a) Proceso de atención a clientes. b) Proceso de aprovisionamiento inicial. c) Proceso de afinación inicial de los servicios prestados por el SOC. d) Proceso de afinación continua de los servicios prestados por el SOC. e) Proceso de control de cambios. f) Proceso de respuesta a incidentes.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	g) Proceso para notificación de incidentes de seguridad. h) Proceso de atención en crisis. PAG: 7 de 8 En la medida que; los procesos aplicables y sus nombres textuales de los procesos varían de acuerdo a cada entidad certificadora, se solicita amablemente a la convocante que permita acreditar el cumplimiento de éste requisito con la puntuación máxima presentando certificado que acredite un ALCANCE SUPERIOR, que incluya los aspectos del sistema de gestión del proveedor, sus actividades de gobernabilidad, las operaciones con clientes que aseguran la disponibilidad, integridad y confidencialidad de la información así como la mejora continua, además del cumplimiento legal y regulatorio aplicable. Todo ello comprobable mediante certificado oficial. Se acepta nuestra solicitud
31	CAPACIDAD DEL LICITANTE (CL) 2. Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales Especialista en administración de incidentes de seguridad PAG. 4 de 8 Se solicita amablemente a la convocante que para cumplir con la Especialidad en Administración de incidentes de seguridad sea suficiente con sólo un recurso, considerando que las funcionalidades requeridas en los diferentes roles son similares a este rol. Se acepta nuestra propuesta?
32	CAPACIDAD DEL LICITANTE (CL) 3. Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales Especialista certificado en seguridad de sistemas PAG. 4 de 8 Se solicita amablemente a la convocante que para cumplir con los Especialistas certificados en seguridad de sistemas, sea suficiente con sólo un recurso, considerando que las funcionalidades requeridas en los diferentes roles son similares a este rol. Se acepta nuestra propuesta?
33	CAPACIDAD DEL LICITANTE (CL) 1. Competencia o habilidad en el trabajo de acuerdo a sus conocimientos académicos o profesionales Especialista en administración de incidentes de seguridad. PAG 4 de 8 Se solicita amablemente a la convocante que para la comprobación del Especialista en administración de incidentes de seguridad pueda ser comprobada mediante alguno de los siguientes certificados GIAC Incident Handler y/o el ITIL OSA. Se acepta nuestra propuesta?
34	III. Forma y términos que regirán los diversos actos del procedimiento de Licitación, Inciso L) PAG 10 Se solicita a la convocante se sirva precisar que, para la formalización de los contratos o pedidos, se deberá recabar, en primer término, la firma del servidor público de la convocante, con las facultades necesarias para celebrar dichos actos y posteriormente, se recabará la firma del proveedor. La fecha del contrato o pedido, será aquella en la que el proveedor lo hubiere firmado. Asimismo, que el plazo de entrega de los bienes, o de iniciación para la prestación del servicio, comenzará el día natural siguiente de la firma del contrato o pedido por el proveedor, o bien, en el plazo que se establezca contando a partir de la citada firma. Lo anterior de conformidad con el artículo 84 primer párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
35	VI. Documentos y datos que deben presentar los Licitantes, VI.1. Documentación distinta a las proposiciones, Inciso A), primer viñeta PAG 19 Se solicita a la convocante tenga a bien considerar que, para el caso de las personas morales el requisito relativo a que con el fin de acreditar la existencia legal, tratándose del acta constitutiva y de todas las modificaciones que ha tenido, se tenga por cumplido con la exhibición del acta constitutiva y el instrumento notarial en el que consta la última modificación que ha tenido el licitante y que en el contenido de este aparecen la totalidad de las modificaciones corporativas. Lo anterior con la finalidad de facilitar la revisión de documentación pues tratándose de empresas, como es el caso de mi representada, que han tenido una cantidad considerable de modificaciones, la documentación requerida resulta voluminoso e innecesario.
36	ANEXO NUM. 4 PAG 28 Se solicita atentamente a la convocante tenga a bien confirmar que para el caso de las empresas que no se encuentren en dicho supuesto bastará con manifestar que se trata de una empresa grande como es el caso de mi representada.
37	ANEXO NUM. 7 MODELO DE CONTRATO, CLÁUSULA QUINTA.- FORMA DE PAGO PAG 37 Es correcto entender que el pago de los servicios se realizará 20 días posteriores a la presentación de las facturas de conformidad con lo que establece el artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
38	ANEXO NÚM. 7 MODELO DE CONTRATO, CLÁUSULA DÉCIMA CUARTA.- MODIFICACIONES DEL CONTRATO PAG 41 Se solicita atentamente a la convocante tenga a bien confirmar que las modificaciones no podrán rebasar en su conjunto el 20% de conformidad a lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector público.
39	ANEXO NUM 7 MODELO DE CONTRATO, CLÁUSULA DÉCIMA QUINTA.- PENAS CONVENCIONALES PAG 41 Se solicita atentamente a la convocante tenga a bien esclarecer que las deducciones serán calculadas en base al valor diario de los servicios suministrados parcial o deficientemente de conformidad con el criterio No. AD-05 de fecha Octubre de 2008 (actualizado diciembre de 2010) emitido por la Unidad de Normatividad de la Secretaría de la Función Pública.
40	ANEXO NÚM. 7, MODELO DE CONTRATO, CLÁUSULA DÉCIMA SEXTA.- SUBCONTRATACIÓN PAG 42 Se solicita atentamente a la convocante tenga a bien confirmar que no se considerará como subcontratación la utilización de recurso humano de empresas que pertenezcan al mismo grupo de mi representada y en virtud a que la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público no lo prohíbe.
41	ANEXO TÉCNICO, TÍTULO PENA CONVENCIONAL Y/O DEDUCCIONES, SUBTÍTULO PENAS CONVENCIONALES PAG 3 DEL ANEXO TÉCNICO Se solicita atentamente a la convocante tenga a bien esclarecer que las penas convencionales serán calculadas en base al valor diario de los servicios no entregados o prestados con atraso de conformidad con el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el artículo 96 del reglamento y en base al el criterio No. AD-05 de fecha Octubre de 2008 (actualizado diciembre de 2010) emitido por la Unidad de Normatividad de la Secretaría de la Función Pública.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
42	ANEXO TÉCNICO, TÍTULO PENA CONVENCIONAL Y/O DEDUCCIONES, SUBTÍTULO DEDUCCIONES PAG 3 DEL ANEXO TÉCNICO Se solicita atentamente a la convocante tenga a bien esclarecer que las deducciones serán calculadas en base al valor diario de los servicios suministrados parcial o deficientemente de conformidad con el criterio No. AD-05 de fecha Octubre de 2008 (actualizado diciembre de 2010) emitido por la Unidad de Normatividad de la Secretaría de la Función Pública.
43	ANEXO TÉCNICO, TÍTULO GARANTÍA DE CUMPLIMIENTO PAG 3 DEL ANEXO TÉCNICO Por tratarse de un contrato plurianual, es decir que abarca más de un ejercicio fiscal, se solicita atentamente a la convocante considerar que el licitante ganador pueda entregar la fianza de cumplimiento de contrato solicitada por el 10% del monto máximo total a erogar en el periodo que corresponda, misma que deberá ser renovada dentro de los primero 10 primeros días naturales de cada ejercicio fiscal, con fundamento en lo que establece el artículo 87 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
44	3.6.1. Temporalidad del Anexo Técnico PAG 67 Es correcto suponer que el mes 27 de la relación de servicios esta duplicado?, Podrían enviar el archivo correcto?

METRO NET S.A.P.I. DE C.V.

No.	Preguntas
1	De la Convocatoria, pagina 5. En la convocatoria refiere que el fallo será el 11 de noviembre del 2014 y en la página 3 inciso d refiere: "que la contratación abarcará más de un ejercicio fiscal, el plazo de ejecución será a partir del 11 de noviembre de 2014 y hasta el 31 de octubre de 2017, la vigencia del contrato será a partir de su formalización y hasta el 31 de octubre de 2017." Preguntas: a) ¿Cuánto será el tiempo que la convocante otorgará al licitante ganador para la implementación de los "componentes habilitadores" es decir, de las soluciones tecnológicas que solicita?, para mi representada no es claro este punto, ya que no entendemos como la convocante espera contar con el servicio a partir del día del fallo. ¿Podría precisar?, b) ¿Cuándo es la fecha de inicio de las operaciones del servicio?, ¿y a partir de cuándo mi representada podrá facturar en caso de ser adjudicada?, esta información es necesaria para establecer y dimensionar los recursos requeridos para ejecutar los servicios. Solicitamos muy amablemente a la convocante proporcionar un calendario que nos indique las fechas establecidas para la ejecución del proyecto.
2	Del Anexo Técnico, Pagina 12, Punto 3.2.1.2 Administración y Monitoreo de la infraestructura de seguridad perimetral. Pregunta: Refiere "Es importante que el Proveedor Adjudicado tome en cuenta que algunos de estos equipos deberán migrarse, o bien instalarse y configurarse desde cero.", en la tabla que entregan indican que dispositivos "no deben migrarse", pero no indican si deben configurarse desde cero, podría precisar uno por uno el estado de ellos?, esta información es relevante para el dimensionamiento de los recursos humanos y el plan de trabajo a entregar.
3	Del Anexo Técnico, Página 16, viñeta 6 Pregunta: Refiere: "Los Componentes Habilitadores serán administrables de forma remota por el Proveedor Adjudicado y radicarán físicamente en las instalaciones del IFT. En caso necesario, el Proveedor Adjudicado asignará en sitio a personal de su plantilla para la atención de incidentes o mantenimiento necesario del equipo involucrado en el proyecto, previo acuerdo con el IFT

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	respecto de los horarios y alcance de los servicios.". Cuantas personas requiere la convocante?, ¿debemos considerar personal 7x24 ó 5x8?
4	Del Anexo Técnico, pagina 22, ultima viñeta. Pregunta: Refiere: " … (que se encuentre dentro del cuadrante de líderes en el reporte más reciente para soluciones tipo SIEM publicado por la empresa Gartner, Inc.)..", solicitamos a la convocante muy amablemente elimine esta condición de las bases, ya que Gartner realiza análisis de tecnología bajo condiciones que ellos determinan y el que el SIEM se encuentre publicado en el cuadrante mágico de Gartner no garantiza la funcionalidad del servicio que requiere la convocante, solicitamos que la convocante acepte que si el SIEM ofertado por mi representada cumple con los requerimientos técnicos y funcionalidad solicitada esto sea suficiente para brindar el servicio.
5	Del Anexo Técnico, Página 27, ultima viñeta. Pregunta: Refiere: "Deberá de tener una precisión de menos de 3.4 errores por millón de escaneo (un error siendo un falso positivo, falso negativo, o negación de servicio)." Solicitamos muy amablemente a la convocante eliminar esta condición ya que representa una característica que solo cumple una herramienta y en nuestra opinión representa un "candado" o condición que no permite la libre participación y al ser un servicio lo que solicitan, esto resulta irrelevante.
6	Del anexo técnico, página 57, inciso 3.2.2.1 Centro de Operaciones de seguridad. Pregunta: Refiere: "Contar con por lo menos, 10 años de experiencia en la operación de un SOC a la fecha de inicio de los servicios objeto de este proyecto." Solicitamos muy amablemente a la convocante eliminar esta condición, ya que consideramos que el que el SOC tenga 3, 5 o 10 años no agrega valor en la eficiencia y cumplimiento de los requerimientos del servicio solicitado. Lo anterior con el fin de permitir la libre participación y que no represente una barrera de entrada o "candado" y no restringir el concurso a empresas que ofrecen estos servicios y que no necesariamente tienen 10 años de experiencia.
7	Del anexo técnico, página 57, inciso 3.2.2.1 Centro de Operaciones de seguridad. Pregunta: Refiere: "Contar con un SOC redundante, que en caso de que se presente algún evento donde le impidiera continuar con la operación, este le permita dar continuidad al servicio. De igual forma, este deberá encontrarse en territorio mexicano y a una distancia mínima de 50 km del SOC principal.." Solicitamos muy amablemente a la convocante eliminar la condición de la distancia mínima de 50Km del SOC Principal, ya que la eficiencia y cumplimiento de los requerimientos de la licitación no dependen de la distancia del centro principal y el redundante. Lo anterior con el fin de permitir la libre participación y que no represente una barrera de entrada o "candado" y no restringir el concurso a empresas que ofrecen estos servicios y cuyos centros de operaciones de seguridad SOC principal y alterno pueden no estar a dicha distancia.
8	Del anexo técnico, página 57, inciso 3.2.2.1 Centro de Operaciones de seguridad. Pregunta: Refiere: "El SOC deberá contar con la certificación ISO/IEC 27001:2005 con una antigüedad de al menos 3 años para sus procesos de Administración de cambios y Administración de incidentes de seguridad" Solicitamos muy amablemente a la convocante que elimine la condición de la antigüedad de al menos 3 años y acepte que el SOC cuente con la certificación ISO/IEC 27001:2005, ya que también la antigüedad no garantiza la eficiencia y cumplimiento de los servicios solicitados en la presente licitación. Lo anterior con el fin de permitir la libre participación y que no represente una

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	barrera de entrada o "candado" y no restringir el concurso a empresas que ofrecen estos servicios.
9	Del anexo técnico, página 57, inciso 3.2.2.1 Centro de Operaciones de seguridad. Pregunta: Refiere: "Todas las acciones que realicen los operadores deberán de quedar registradas en un subsistema de auditoría, al cual tendrá acceso el IFT con privilegios de "sólo lectura" y el Proveedor Adjudicado deberá asegurar la protección de los registros. " Podría la convocante precisar si aceptaría.
10	Del Anexo Técnico, página 72 Pregunta: Refiere: Los recursos humanos deberán formar parte de la plantilla del personal del Proveedor Adjudicado y será el personal asignado a la administración y operación del servicio contratado. El Proveedor Adjudicado deberá comprobar mediante el alta del IMSS al menos 90 días de antigüedad para cada uno de los recursos destinados a este proyecto. Los recursos de nuestra empresa trabajan subcontratados por una de las empresas del grupo empresarial por servicios profesionales. Solicitamos muy amablemente a la convocante que acepte la documentación de nuestra empresa afiliada.
11	Del Anexo técnico, página 73 Evidencia del cumplimiento Pregunta: Refiere: "CRISK Certified in Risk and Information Systems Control", como una de las certificaciones requeridas, ¿podría precisar la convocante si se trata de CRISC?, que es realmente la certificación de la ISACA?, es decir, no es CRISK, si no CRISC. Así mismo solicitamos hacer la misma precisión en todo el cuerpo del anexo donde refieren CRISK y debería ser CRISC.
12	Sección: 6.1.2 Evidencia de cumplimiento-Rol- Especialista en administración de incidentes de seguridad, página: 73 Pregunta: Solicitamos muy amablemente am la Convocante presentar de forma alternativa la certificación CHFI (Certified Hacking Forensic Investigator) , la cual es equivalente a la GIAC debido a que cubre los alcances de CHFI y como valor adicional abarca el tema de Forensia, seguridad de la información y análisis de incidentes.
13	Sección: 6.1.2 Evidencia de cumplimiento, página 73 Pregunta: Para el caso de las certificaciones de los especialistas se solicita a la convocante que acepte que un recurso pueda tener más de una certificación y participar en varios roles.
14	Sección: 3.2.2.1 Centro de Operaciones de Seguridad (SOC), página 58 Pregunta: Podría la convocante confirmar si las certificaciones y cumplimientos que se solicitan para SOC principal se deben cumplir de igual manera para el SOC alterno.
15	Sección: Documento método de evaluación, página 6 Pregunta: En cuanto a los contratos se piden 10 ¿deben ser contratos concluidos o en curso?, en caso de ser contratos en curso, se tomara como experiencia únicamente la cantidad de finalizados de dichos contratos?
16	Sección: Metodología para la prestación de servicio-ISP/IEC 27001, página 7 Pregunta: Para el caso de la Metodología de la prestación del servicio se enlistan una serie de procesos, que entendemos se deben cumplir, sin embargo, durante el proceso de Certificación las empresas eligen el alcance que buscan cumplir, es decir, denominan de diferente manera el

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	nombre de los procesos a certificar por lo que apegarse a la lista de procesos solicitado es prácticamente imposible que coincida aunque el alcance de la certificación sea superior. Por lo anterior se solicita muy amablemente a la convocante que acepte procesos y subprocesos certificados equivalentes, que incluso pudieran ser un número mayor de procesos certificados y que también son relevantes para la prestación del servicio.
17	IV Requisitos que los licitantes deben cumplir página 12 y 13 inciso a)..... En este sentido, con fundamento a lo establecido en el Artículo 27 de las Normas y conforme a lo señalado por el ACUERDO POR EL QUE SE ESTABLECEN LAS DISPOSICIONES QUE SE DEBERÁN OBSERVAR PARA LA UTILIZACIÓN DEL SISTEMA ELECTRÓNICO DE INFORMACIÓN PÚBLICA GUBERNAMENTAL DENOMINADO COMPRANET, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 28 DE JUNIO DE 2011, las proposiciones presentadas deberán ser firmadas electrónicamente, a través de COMPRANET, en sustitución de la firma autógrafa, Pregunta: Se solicita amablemente a la convocante confirmar que no es necesario firmar autógrafamente todos los documentos presentados (propuestas técnica, económica y demás documentación) para la presente licitación, será suficiente con que se firmen electrónicamente los resúmenes de las propuestas técnica y económica que genera el sistema Compranet.
18	3.2.1.9 Servicio de control de acceso Firewall inciso a): Operar bajo el concepto de Blades de Software, página 31 Pregunta: Se solicita a la convocante que operar bajo el concepto blade de software sea opcional ya que hay un solo fabricante, siempre y cuando el equipo ofertado cumpla con las funcionalidades requeridas. Se acepta nuestra propuesta?
19	3.2.1.9 Servicio de control de acceso Firewall inciso a): Contar con capacidad para integrarse a un directorio activo, página 31 Pregunta: Acepta la convocante que esta funcionalidad se pueda ofertar con un equipo adicional de la misma marca, ofertado como una solución integral?
20	3.2.1.9 Servicio de control de acceso Firewall inciso b): Basado en tecnología ASIC "Application-Specific Integrated Circuit" y ser capaz de brindar una solución de "Complete Content Protection, página 32 Pregunta: Se solicita a la convocante que la solución ofertada pueda ser entregada con procesadores de red, siempre y cuando se oferte la solución con las capacidades solicitadas. Se acepta nuestra propuesta?
21	3.2.1.9 Servicio de control de acceso Firewall inciso b): El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de accesos por VPN SSL y IPSec Client to Gateway, página 33 Pregunta: Se solicita la convocante que la funcionalidad de VPN SSL pueda ser ofertado con un equipo adicional de la misma marca que sea ofertado como una solución integral. Se acepta nuestra propuesta?
22	3.2.1.9 Servicio de control de acceso Firewall inciso b): Contar con un rendimiento (throughput) de Firewall de al menos 78 Gbps para paquetes de 1518 y 512 bytes, un rendimiento de VPN de al menos 48 Gbps, rendimiento de detección de intrusos de al menos 10 Gbps, rendimiento de antivirus en modo proxy de al menos 4.2 Gbps, rendimiento de antivirus en modo Flow de 12 Gbps. Página 33. Pregunta:

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Se solicita a la convocante que la solución ofertada tenga un performance de al menos 65 Gbps de Firewall. Se acepta nuestra propuesta?
23	3.2.1.9 Servicio de control de acceso Firewall inciso b): En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible, página 34 Pregunta: Es correcto interpretar que la funcionalidad de balanceo se refiere a la descrita por el protocolo ECMP.
24	3.2.1.9 Servicio de control de acceso Firewall inciso b): Debe soportar la configuración de túneles L2TP y PPTP, página 34 Pregunta: Se solicita a la convocante de manera respetuosa que la funcionalidad de túneles L2TP sea opcional. Se acepta nuestra propuesta?
25	3.2.1.9 Servicio de control de acceso Firewall inciso b): Capacidad de realizar SSL VPNs. Página 34 Pregunta: Se solicita la convocante que la funcionalidad de VPN SSL pueda ser ofertado con un equipo adicional de la misma marca que sea ofertado como una solución integral. Se acepta nuestra propuesta?
26	3.2.1.9 Servicio de control de acceso Firewall inciso b): Soporte de renovación de contraseñas para LDAP y RADIUS, página 34 Pregunta: Es correcto interpretar que se refiere a las contraseñas de usuarios de administración?
27	3.2.1.11) Servicio de protección para correo electrónico, página 52 Pregunta: Deberá 'poder analizar correos electrónicos en busca de amenazas como son exploits día cero, ataques escondidos en archivos comprimidos ZIP/RAR/TENF y ligas (URL) maliciosas. La Convocante acepta carta del fabricante para este punto que no está propiamente documentado por el fabricante, sin embargo la solución ofertada cumple con los requerimientos.
28	3.2.1.11 Servicio de protección para correo electrónico, página 52 Pregunta: En el entorno virtual de análisis, el malware deberá ser inspeccionado y examinado en diversas máquinas virtuales correspondientes a varios sistemas operativos, aplicaciones, navegadores y complemento de navegadores. Se solicita a la convocante que la funcionalidad para analizar máquinas virtuales pueda ser ofertado con un equipo adicional de la misma marca que sea ofertado como una solución integral. Se acepat nuestra propuesta?
29	Basado en tecnología ASIC "Application-Specific Integrated Circuit" y ser capaz de brindar una solución de "Complete Content Protection". página : 32 Pregunta Se solicita a la convocante poder aclarar este requerimiento debido a que limita la participación de otras tecnologías. Aceptaría la convocante otras tecnologías que cuentan con la certificación de NSS Labs (2014) y se encuentran como líderes en el cuadrante Mágico de Gartner (2013)
30	Firewall Capacidad de re-ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware. Página 32 Pregunta : Los motores de inspección y re-ensamblado de paquetes de la mayoría de los fabricantes son realizados por contextos de software en forma independiente de la plataforma de hardware. Aceptaría la convocante una plataforma similar en rendimiento y que no sea limitativa a una basada en hardware.

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
31	3.2.1. 9Servicio de control de acceso al Firewall. Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance", no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX, AIX o Windows. página 32 Pregunta : Es correcto entender que la apreciación del "sistema operativo genérico" se refiere a las distribuciones comerciales y multipropósito que se distribuyen en el mercado y que las tecnologías del sistema operativo pre-endurecido del appliance cuenten con diferentes patentes registradas.
32	3.2.1. 9Servicio de control de acceso al Firewall. El equipo debe soportar 240,000 nuevas sesiones por segundo. página : 33 Pregunta: Acepta la convocante incrementar de 240K a 280K sesiones por segundo? Debido al requerimiento solicitado de throughput y conexiones concurrentes en el Firewall.
33	3.2.1. 9Servicio de control de acceso al Firewall. El equipo debe contar con al menos 10 Interfaces GigaEthernet RJ45, 10 Interfaces GigaEthernet SFP y 8 interfaces 10 GigEthernet SFP+. página 33 Pregunta: Podría la convocante especificar el tipo y número total de interfaces a utilizar durante la vida del proyecto? Esto debido a que lo solicitado en este punto son las interfaces totales que puede llegar a soportar un equipo y el incluir todas las interfaces de inicio encarece el proyecto.
34	34. 3.2.1. 9Servicio de control de acceso al Firewall. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. Página 33 Pregunta: Para simplificar la administración operativa, es correcto entender que están solicitando políticas de Firewall basadas en zonas para la definición del trafico entrante/saliente?
35	35. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. Página 33 Pregunta: Para simplificar la administración operativa, es correcto entender que están solicitando políticas de Firewall basadas en zonas para la definición del trafico entrante/saliente y que el control de tráfico multicast este inherente en la configuración global del firewall?
36	36. Firewall Sitio principal Boston. Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario. Página 33 Pregunta: Esta funcionalidad no se solicita para el sitio principal, por tal motivo solicitamos amablemente a la convocante aclarar la necesidad de IPv6 en un Sitio Secundario
37	37. Firewall. La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autentificarse con un TOKEN (Autentificación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante. Página 40 Pregunta: Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).
38	38. Sera posible configurar el equipo para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a contenido categorizado por el portal como contenido educativo. Página 39

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

No.	Preguntas
	Pregunta: Es correcto entender que, este requerimientos se refiere a únicamente a autorizar y permitir el acceso a contenido educativo dentro de Youtube
39	39. Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS). Página 39 Pregunta: A raíz de la vulnerabilidad de Heartbleed (CVE-2014-0160) no se considera seguro realizar la administración por medio de un WebGUI sobre HTTPS. Acepta la convocante un sistema de administración centralizada que no presentó ningún tipo de afectación de esta vulnerabilidad y que este manejada por comunicaciones encriptadas mediante certificados digitales. Links de referencia Links de reportes de vulnerabilidades: http://www.fortiguard.com/advisory/FG-IR-14-011/ http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk100173 http://watchguardsecuritycenter.com/2014/04/08/the-heartbleed-openssl-vulnerability-patch-openssl-asap/ http://goo.gl/9Ruf6
40	40. Debe soportar la configuración de túneles L2TP y PPTP. Página 34 Pregunta: Acepta la convocante que este tráfico de encapsulación se encuentren dentro de un túnel IPSEC? Debido a que los anteriores son considerados inseguros?
41	41. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS. Página 34 Pregunta: Podría la convocante aclarar su requerimiento puntual del protocolo de IS-IS, puesto que solo opera en Capa 2?
42	42. Firewall. Página 34 Pregunta: Se solicita a la convocante indicar el ancho de banda que maneja, el número de VPN´s
43	43. Firewall. Página 34 Pregunta: Podría indicar la convocante el nivel de crecimiento de equipos firewall que tendrá en los próximos 3 años?

Se informa que esta Licitación es electrónica con base en el artículo 25 fracción II de las Normas, por lo que este acto se realiza a través de CompraNet; asimismo se hace constar que a este acto no asistió persona alguna que manifestara su interés de estar presente en el mismo.

De conformidad con el artículo 32 de las Normas, esta Acta forma parte integrante de la convocatoria a la Licitación.

ACTA DE JUNTA DE ACLARACIONES
LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA
NÚM. LA-043D00001-N178-2014
PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

Para efectos de notificación y de conformidad con el segundo párrafo del artículo 39 de las Normas, se difundirá un ejemplar de la presente acta en CompraNet, en la dirección https://compranet.funcionpublica.gob.mx, dicho procedimiento sustituirá a la notificación personal. Asimismo, se difundirá en el portal del Instituto en el vínculo http://www.ift.org.mx/iftweb/licitacion-publica/ y se mantendrá un ejemplar para su consulta en la Dirección General de Adquisiciones, Recursos Materiales y Servicios Generales, ubicada en Insurgentes Sur Núm. 838, Quinto Piso, Colonia Del Valle, Delegación Benito Juárez, C.P. 03100, México D.F., al cual tendrá acceso el público o cualquier interesado para consulta, por un término de 5 (cinco) días hábiles a partir de la fecha del presente acto, siendo de la exclusiva responsabilidad de los licitantes, acudir a enterarse de su contenido y obtener copia de la misma.

No habiendo otro asunto que agregar, se dio por terminado este Acto, siendo las 14:00 horas del mismo día de su inicio.

Esta acta consta de 57 páginas, firmada para efectos legales y de conformidad los asistentes a este Acto, para proceder a su envío a través de CompraNet.

POR EL INSTITUTO FEDERAL DE TELECOMUNICACIONES

NOMBRE	ÁREA / PUESTO	FIRMA
LIC. OSCAR E. IBARRA MARTÍNEZ	DIRECTOR GENERAL DE ADQUISICIONES, RECURSOS MATERIALES Y SERVICIOS GENERALES	
LIC. JUAN CARLOS JIMÉNEZ ÁNGELES	DIRECTOR DE PROCEDIMIENTOS DE ADQUISICIONES	
LIC. NEY GALICIA ARROCENA	DIRECTOR DE ÁREA EN LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	
C.P. LAURA BERENICE VANEGAS LUNA	SUBDIRECTORA DE RECURSOS MATERIALES	
C. MAURO ALFREDO BALDERAS FAJARDO	SUBDIRECTOR DE ÁREA EN LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT"

POR LA CONTRALORÍA INTERNA

NOMBRE	ÁREA	FIRMA
NO HUBO ASISTENCIA		

POR LOS OBSERVADORES

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL	REPRESENTANTE	FIRMA
NO HUBO ASISTENCIA		

ESTA HOJA DE FIRMAS PERTENECE AL ACTA DE JUNTA DE ACLARACIONES DE LA LICITACIÓN PÚBLICA NACIONAL Y ELECTRÓNICA NÚM. LA-043D00001-N178-2014 PARA LA ADJUDICACIÓN DEL CONTRATO, RELATIVO A LOS "SERVICIOS DE SEGURIDAD ADMINISTRADA PARA EL IFT" ----------

---