ADMINISTRACIÓN GENERAL
JURISDICCIÓN INMOBILIARIA
25 SEP 2017
RECIBIDO
Por:
Hora:

Tecnología

JURISDICCION INMOBILIARIA
PODER JUDICIAL · REPUBLICA DOMINICANA

TI-N-2017-020

Para: **Licda. Elizabeth Diaz Castellano.**
Coordinadora del Comité de Compras y Licitaciones
Poder Judicial

Vía: **Licda. Mariloy Díaz Rodríguez.**
Administradora General.
Jurisdicción Inmobiliaria.

Del **Ing. Michael Geneux Polanco.**
Gerente de Tecnología
Jurisdicción Inmobiliaria

Fecha: 22 de septiembre 2017

Asunto: Remisión Evaluaciones Técnicas Pliego LPN-CPJ-12-2017

Distinguida Licda. Diaz:

En atención al oficio CCL-63-2017 que recibiéramos de parte del Comité de Compras y Licitaciones en fecha 22 de Agosto del año en curso , tenemos a bien remitir los resultados de las evaluaciones realizadas a las propuestas entregadas por las empresas oferentes en la licitación Pública Nacional LPN-CPJ-12-2017, para la adquisición de Equipos Tecnológicos para el control de riesgo y seguridad, correspondiente a la fase I del proyecto "Modelo de Administración de Riesgo en las Redes de la Jurisdicción Inmobiliaria".

Las empresas oferentes fueron: IQTEK, GBM, y Multicomputos.

Durante la evaluación de los requerimientos citados en el pliego y de las respectivas propuestas participaron el Ing. Michael Geneux (Gerente de Tecnología) y la Ing. Virginia Alejo (Encargada de Infraestructura y Comunicaciones).

Criterios de Evaluación.
Valoramos el total de cumplimiento de cada empresa, de acuerdo a los lotes donde realizaron sus propuestas. Adicionalmente fueron valorados los requerimientos por su tipo: RDC, RGS y RFT.

PODER JUDICIAL
JURISDICCIÓN INMOBILIARIA
GERENCIA TECNOLOGÍA

Resultados de la Evaluación

Para el Lote 1:

Las empresas oferentes en el Lote I son: IQTEK y GBM.

Requerimientos	Cantidad	IQTEK			GBM		
		Cumple	No Cumple	%/Req.	Cumple	No Cumple	%/Req.
Requerimientos de Contratación (RDC)	14	14	0	100.00%	10	4	71.43%
Requerimientos de Garantía y Soporte (RGS)	7	7	0	100.00%	5	1	85.71%
Requerimientos Técnicos(RFT) Firewalls de la Red Perimetral Externa	67	67	0	100.00%	67	0	100.00%
Requerimientos Técnicos(RFT) Firewalls de la Red Perimetral Interna	94	94	0	100.00%	69	25	73.40%
Total	**182**	**182**	**0**	**100.00%**	**152**	**30**	**83.52%**

- **La empresa IQTEK cumple con el 100.00% del total de los requerimientos técnicos de contratación, capacitación y garantía.**

- **La empresa GBM cumple con el 83.52% del total de los requerimientos técnicos de contratación, capacitación y garantía.**

En su propuesta 5 requerimientos de contratación, garantía y soporte **"no subsanables"** fueron considerados como "no cumple" con las especificaciones de los mismos en el pliego (**Ver formularios de evaluación anexos)**.

Asimismo, en 25 requerimientos técnicos, notamos que en el formulario de cumplimiento en el detalle de la columna **"Solución Propuesta"** los datos suministrados no se corresponden a la documentación remitida por el ofertante (GBM). **Ver formulario de evaluación anexos, lote 1. Nota:** Este punto fue socializado con el Comité de Compras y Licitaciones, el cual nos indicó que, de acuerdo a lo expresado anteriormente, estos **"No Cumple"** con los requerimientos del Pliego.

Para el Lote 2:

Las empresas oferentes en el Lote II son: IQTEK, Multicomputos y GBM.

Requerimientos	Cantidad	IQTEK			Multicomputos			GBM		
		Cumple	No Cumple	%/Req.	Cumple	No Cumple	%/Req.	Cumple	No Cumple	%/Req.
Requerimientos de Contratación (RDC)	13	12	1	92.31	12	1	92.31%	9	4	69.23%
Requerimientos de Garantía y Soporte (RGS)	7	7	0	100.00%	7	0	100.00%	5	1	71.43%
Requerimientos Técnicos(RFT) Balanceadores de Carga ADCs	128	127	1	99.22%	127	2	99.22%	124	4	96.88%
Total	**148**	**146**	**2**	**98.65%**	**145**	**3**	**97.97%**	**139**	**9**	**93.92%**

- **La empresa IQTEK cumple con el 98.65% del total de los requerimientos técnicos de contratación, capacitación y garantía.**

  En su propuesta 2 de sus requerimientos (RDC y RFT) fueron considerado como "no cumple" con las especificaciones de los mismos en el pliego (**Ver formularios de evaluación anexos)**. No obstante, desde el punto de vista **Técnico** consideramos que los mismos pueden ser Subsanable, pero la decisión final deberá ser tomada en conjunto con el **Comité de Compras y Licitaciones.**

- **La empresa Multicomputos cumple con el 97.97% del total de los requerimientos técnicos de contratación, capacitación y garantía.**

  En su propuesta 1 requerimiento de contratación, garantía y soporte **"no subsanables"** fue considerado como "no cumple" con las especificaciones de los mismos en el pliego **(Ver formularios de evaluación anexos)**.

  Asimismo 2 requerimientos técnico fueron considerados como "no cumple" con las especificaciones de los mismos en el pliego **(Ver formularios de evaluación anexos)**.

- **La empresa GBM cumple con el 93.92.% del total de los requerimientos técnicos de contratación, capacitación y garantía.**

  En su propuesta 5 requerimientos de contratación, garantía y soporte y 1 requerimiento técnico **"no subsanables"** fueron considerados como "no cumple" con las especificaciones de los mismos en el pliego **(Ver formularios de evaluación anexos)**.

  Asimismo 3 requerimientos técnico fueron considerados como "no cumple" con las especificaciones de los mismos en el pliego **(Ver formularios de evaluación anexos)**.

En Conclusión, durante la evaluación técnica de los **Requerimientos de Contratación (RDC), Requerimientos de Garantía y Soporte (RGS) y Requerimientos Funcionales y Técnicos (RFT)** de ambos Lotes; observamos que la empresa que resultó con mayor porcentaje fue **IQTEK.**

Cualquier duda o aclaración sobre estas evaluaciones, estamos a su disposición.

Sin otro particular.
Atentamente,

Ing. Michael Geneux Polanco

PODER JUDICIAL
JURISDICCIÓN INMOBILIARIA
GERENCIA TECNOLOGIA

Anexos:

- **Formularios de Evaluación IQTEK, Multicomputos y GBM.**

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
a) Requerimientos de Contratación, Garantía y Soporte							
Requerimientos de Contratación (RDC)							
Acreditaciones y Experiencia del Oferente							
RDC01	El Oferente debe contar con una experiencia mínima de tres (3) años y con tres (3) o más clientes, fuera o dentro del territorio dominicano, donde haya ejecutado proyectos de implementación de soluciones **Aplication Delivery Controllers (ADCs)** de manera satisfactoria y cualquier otro equipo que esté contemplado en la propuesta de implementación. Para esto el Oferente presentará una carta de recomendación por cada uno de los tres (3) o más clientes referenciados, tal como se lista en las especificaciones del Pliego.	Iqtek Solutions SRL cuenta con 5 años de experiencia en la implementación de soluciones firewalls, Swituches y otros equipos, se incluyen 4 cartas de Referencias, Supermercado Bravo, Grupo Ramos, Propagas e Infotep	N/A RNC 130876967 Común para lote 1 y 2	N	X		
RDC02	El Oferente debe contar con la Certificación del Fabricante para poder ofertar las soluciones de **Aplication Delivery Controllers (ADCs)** y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Para tal efecto, el Oferente presentará una Carta de Certificación del Fabricante, de que puede vender, dar soporte a los equipos y soluciones de este Fabricante en la República Dominicana.	Se incluyen las cartas de autorización de Fabricante de los dos involucrados en el proceso Cisco y Fortinet.	N/A Cartas Anexas Común para lote 1 y 2	N	X		
RDC03	El oferente de contar con un personal Certificado por el fabricante en cada una de las soluciones **Aplication Delivery Controllers (ADCs)** y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Nota: Se debe presentar documentación que demuestre dicha capacidad y conocimiento.	Se anexa certificaciones del personal por parte de los fabricantes en las soluciones propuestas.	N/A Certificaciones Anexas Común para lote 1 y 2	N	X		
RDC04	Las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** deben estar dentro del Informe de Gardner, **"Magic Quadrant for Application Delivery Controllers"**, dentro del cuadrante de **Líderes (Leaders).** Dicho informe de referencia deberá ser actualizado, es decir, debe ser la última publicación valida. Este documento debe ser anexado a la Propuesta.	Para referencia: https://www.fortinet.com/demand/gated/gartner-enterprise-firewall.html Las soluciones propuestas se encuentran en el cuadrante mágico de Garther	N/A Anexo cuadrante	S		X	**Ver repuesta a la Pregunta # 4**
RDC05	La instalación y migración de los servicios, equipos, configuraciones y demás debe ser contemplada como parte de la propuesta; incluyendo la puesta en funcionamiento de las políticas de seguridad y monitoreo descritos en los requerimientos técnicos y funcionales. El cableado, switches y demás componentes necesarios para la instalación y puesta en funcionamiento de las soluciones deben formar parte de la propuesta.	Se incluyen los servicios profesionales de instalación, Migración de los servicios configuraciones y demás para la puesta en funcionamiento de los requerimientos técnicos y funcionales	N/A Ver cronograma de instalación anexo Común para lote 1 y 2	N	X		
RDC06	Deben dejar en correcto funcionamiento todo lo relacionado a la infraestructura propuesta. La implementación de los equipos y aplicativos citados en este pliego no debe afectar las operaciones diarias de la JI, por lo que el oferente debe tomar las medidas necesarias para este requerimiento.	Se contempla el correcto funcionamiento de la solución	N/A Común para lote 1 y 2	N	X		
RDC07	Si el Oferente subcontrata o integrara todos o parte de los servicios a ofrecer deberá presentar un acuerdo entre las partes donde indique su intención de trabajar en colaboración (Joint-Venture) en el proyecto de implementación de las soluciones. El Subcontrato deberá contar con la anuencia de la Jurisdicción Inmobiliaria – Poder Judicial, siendo siempre el responsable ante la Institución el contratista (adjudicatario).	Estamos realizando una oferta de única Empresa Iqtek Solutions	N/A Común para lote 1 y 2	N	X		
Tiempos de Entrega y de Implementación							
RDC08	El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de **Aplication Delivery Controllers (ADCs)** en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.	Entrega en 45 días incluimos una carta de compromiso de entrega con las condiciones a la respuesta a la pregunta 4 de la circular numero 1	N/A Carta de compromiso Anexa Condiciones generales de la oferta Común para lote 1 y 2	N	X		
RDC09	La JI requiere que este proyecto sea ejecutado en un plazo no mayor a dos (2) meses, a partir de la entrega de los equipos.	2 Meses, a partir de la entrega de los equipos.	N/A Carta anexa Común para lote 1 y 2	N	X		
RDC10	El oferente elaborará un documento informando los productos entregados e instalados; y validando los requerimientos técnicos que han sido cumplidos; así como los riesgos que han sido mitigados. Nota: Este documento debe contener las descripción de todas las políticas implementadas.	Documento a ser entregado en el cierre del proyecto	N/A Común para lote 1 y 2	N	X		
Normas de Seguridad Industrial							
RDC11	El Oferente presentará como parte de su propuesta los procedimientos y políticas que utiliza para la Seguridad de su Personal y la propiedad privada de la JI. Así como los recursos, tales como equipo, señalización y protección.	Nos acogemos a las Normas contempladas en el código de trabajo y las políticas de seguridad a nuestro personal y propiedad privada de la JI y los recursos de señalización y protección, cascos, botas, guantes y otros	N/A Carta Anexa Común para lote 1 y 2	N	X		
Responsabilidades del Oferente							

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RDC12	La presentación de las Propuestas debe cumplir con los siguientes requisitos: • Deben describir claramente la Marca y el Modelo ofertado. • Deben describir los detalles técnicos de todos los equipos presentados. • Las propuestas deberán ser presentadas en idioma español. • La propuesta presentada deberá describir (el # de Parte, Licencia, Protocolos, entre otros) con que se cumplirá cada requerimiento. • Las propuestas deben describir de forma detallada, clara y precisa los Costos de los Equipos (Hardware/Software), Costos de las Licencias y los Costos de la Garantía y el soporte. • La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF) • El formato digital debe permitir realizar búsqueda dentro del documento (OCR). • Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.	Incluimos la marca y los modelos ofertados con sus números de partes, las licencias, detalle de todos los equipos y protocolos, con lo que se cumple cada requerimiento, se presentan en formato impreso y el formato digital (PDF) en USB	N/A Propuesta física y Digital Común para lote 1 y 2	N	X		
RDC13	El Oferente revisará y leerá detenidamente el contenido de este documento, y hará las preguntas necesarias conforme al protocolo descrito en estos términos de referencia.	Leído, Revisado y entendido	N/A Común para lote 1 y 2	N	X		
Requerimientos de Garantía y Soporte (RGS)							
Garantías y Soporte							
RGS01	Las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación contarán con una garantía en Piezas y Servicios (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). **Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.	La Solución propuestas de Firewalls Switches, Tokens, Licencias de Equipos, Software, entre otros contemplado en la propuesta de implementación cuentan con una garantía en Piezas y Servicios Actualización de Software, Upgrade de Software, Configuración de nuevas funcionabilidades y la asistencia en la Implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). Este soporte cuenta con la participación del fabricante y IQTEK Solutions	FPR4110-ASA-K9 FG-1500D-BDL-950-36 FC1-10-0ACVM-248-02-36 FC4-10-LV0VM-248-02-36 FC1-10-M3004-248-02-36 IQ-services incluidos por 3 años Común para lote 1 y 2	N	X		
RGS02	El Software de Administración de las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación contará con soporte (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). **Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.	Ver respuesta RGS01	FG-1500D-BDL-950-36 FC1-10-0ACVM-248-02-36 FC4-10-LV0VM-248-02-36 FC1-10-M3004-248-02-36 IQ-services incluidos por 3 años Común para lote 1 y 2	N	X		
RGS03	El periodo de vigencia de la garantía para las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, comenzará a aplicarse a partir de la instalación y puesta en funcionamiento de las mismas **Nota:**Para fines de Inicio del Periodo de Garantía y la Puesta en Funcionamiento de los Equipo estará aprobada a partir del Documento de Aceptación, el cual será firmado por la JI y el Oferente.	Aceptamos dicha Cláusula RGS03	N/A Común para lote 1 y 2	N	X		
RGS04	El Ciclo de vida (END OF LIFE) de las Soluciones propuestas de **Aplication Delivery Controller (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación deberá ser posterior al tercer (3er.) año de garantía, tomando como referencia la fecha de esta licitación (Entrega/Apertura de Ofertas). Por lo que se solicita para validar este requerimiento que se presente la constancia escrita del fabricante de la Solución de **Aplication Delivery Controller (ADCs)**. La propuesta debe incluir equipos de última generación del fabricante	ProductLifeCycle-2016 Los productos Ciscos y Fortinet presentados acaban de salir el año Pasado.	N/A Común para lote 1 y 2	N	X		
RGS05	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, el costo de renovación de Soporte y Licenciamiento no será mayor al 15% de adquisición del Equipo, durante los años 4to y 5to año Ejemplo: si el costo del soporte y de Licenciamiento cuando se adquirió el equipo fue de 100 Pesos, este no podrá costar más 115 Pesos, es decir, no podrá ser mayor a un 15%.	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas, el costo de renovación de Soporte y Licenciamiento no será mayor al 15% de adquisición del Equipo, durante los años 4to y 5to año.	N/A Carta Anexa Común para lote 1 y 2	N	X		
RGS06	El Fabricante y el Oferente de las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación deben presentar garantías (documentaciones) de que mantienen en la República Dominicana el inventario de todas partes y piezas necesarias para dar soporte a dicho equipo después de su puesta en producción.	Cartas de los fabricantes anexa con las informaciones requeridas para las garantías	N/A Común para lote 1 y 2	N	X		
Requerimientos de Capacitación							
	Como parte de la propuesta el Oferente ofrecerá a la JI los siguientes tres (3) cursos para cinco (5) participantes: Ø Instalación, Configuración y Administración de los **Aplication Delivery Controllers (ADCs).** Para estas capacitaciones el oferente deberá tomar en cuenta los siguientes aspectos:	Se incluyen 3 cursos para cinco 5 participantes de la JI con sus certificaciones					

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RGS07	• Las capacitaciones deberán cubrir la implementación de políticas y mejores prácticas de acuerdo a la función y uso de los equipos. • Las capacitaciones serán realizadas de forma Presencial. • El oferente deberá proveer el salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros. • Estas capacitaciones deberán ser impartidas en idioma español. • Estas capacitaciones deberán incluir las respectivas certificaciones para 5 participantes. • Adicional a los 5 participantes el oferente proveerá la facilidad de que la JI incluya participantes como oyente. • El calendario de las capacitaciones se realizará en coordinación con JI y estarán sujetos a la disponibilidad de la JI. • El oferente cubrirá con todos los costos de la capacitación. • Estas capacitaciones deben impartirse previo a la implementación de los equipos, para que la JI pueda definir las mejores prácticas a ponerse en ejecución durante el proceso de implementación de dichos equipos. Los instructores deberá ser docentes calificados y certificados por el/los fabricante/s de las soluciones a instalar. La empresa suplidora deberá correr con los gastos de alojamiento, viáticos y pasaje aéreo del personal docente, si se necesitaré participación de los instructores Extranjeros.	Cisco Firepower 4110 Firewalls perimetro de la Red Externa FortiGate I y Fortigate II para los Firewalls de Perimetro Externo FortiADC for Series Models Las capacitaciones serán realizadas de forma Presencial, salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros. Oyentes hasta 2 máximos En coordinación con nuestro departamento de Entrenamiento se realiza la logística de los cursos.	N/A Learning Credits TRN-CLC-001 TRN-CLC-000 TRN-CLC-004 BUNSE4 NSE6-ADC Común para lote 1 y 2	N	X		
D) Requerimientos Funcionales y Técnicos para 2 Balanceadores de Carga (Application Delivery Controllers (ADCs)) en la Red Perimetral							
Requerimientos Funcionales y Técnicos (RFT)							
RFT01	**2 Application Delivery Controller (ADCs),** o solución de balanceo de servidores y de enlaces que permita mejorar el desempeño de las mismas y al mismo tiempo generar un Esquema de alta disponibilidad; ambos instalados en modo HA.	Los controladores de entrega de aplicaciones FortiADC (ADC) optimizar la disponibilidad, la experiencia del usuario,Rendimiento y escalabilidad de Enterprise Entrega de la aplicación. La familia FortiADC Electrodomésticos proporciona una alimentación rápida,Aceleración inteligente y distribución de Exigentes en la empresa Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT02	El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado **"Appliance".**	Los controladores de entrega de aplicaciones FortiADC (ADC) optimizar la disponibilidad, la experiencia del usuario,Rendimiento y escalabilidad de Enterprise Entrega de la aplicación. La familia FortiADC Electrodomésticos proporciona una alimentación rápida,Aceleración inteligente y distribución de Exigentes en la empresa. Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir, un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.	FortiADC utiliza FortiOS con el sistema operativo desarrollado para cumplir las funciones de ADC. http://docs.fortinet.com/fortiadc-d-series/admin-guides	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT04	Los valores de desempeño solicitados deberán ser logrados por el equipo **"Appliance"** como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios **"Appliance"** que logren sumar el valor solicitado.	Los controladores de entrega de aplicaciones FortiADC (ADC) optimizar la disponibilidad, la experiencia del usuario,Rendimiento y escalabilidad de Enterprise Entrega de la aplicación. La familia FortiADC Electrodomésticos proporciona una alimentación rápida,Aceleración inteligente y distribución de Exigentes en la empresa. Para referencia visitar el siguiente link:	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
		https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf					
RFT05	Se debe ofrecer dos (2) equipos en Alta disponibilidad (HA) funcionando en configuración Activo- Activo / Activo-Pasivo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en clúster virtual de múltiples equipos.	El dispositivo FortiADC admite características de alta disponibilidad como activo-pasivo, Active-Active Cluster, active-activeVRRP Cluster, detección de fallos y sincronización de configuración. Los despliegues de alta disponibilidad pueden 99.999% de acuerdo de nivel de servicio uptimes. Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 406-407	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT06	Cada equipo debe cumplir con las siguientes características: • La solución debe soportar un Throughput en L4 de al menos 10 Gbps. • La solución debe soportar un Throughput en L7 de al menos 10 Gbps. • La solución debe soportar un Throughput en SSL de al menos 10 Gbps. • La solución debe soportar una Compresión de Throughput de al menos 3.5 Gbps. • La solución deberá tener al menos 32 GB de Memoria. • La solución debe soportar al menos 1,400,000.00 Millones de peticiones en L7 HTTP requests/sec. • La solución de soportar al menos 13,000.00 Transacciones en SSL (SSL transactions/sec (2K key certificates) • La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA. • La solución de soportar al menos 6,000.00 Transacciones en ECDHE (ECDHE transactions/sec)	Los valores soportados por el FortiACD 2000F son los siguientes: *Throughput en L4 40.0 Gbps *Throughput en L7 24.0 Gbps *Throughput en SSL 13.5 Gbps *Compresión de Throughput 18.0Gbps *Memoria 32 GB *Millones de peticiones en L7 HTTP 2.6 Millones requests/sec. Transacciones en SSL (SSL transactions/sec (2K key certificates) 37.000 Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	N	X		
RFT07	Cada equipo debe tener al menos las siguientes Interfaces de red: • 4x10GE SFP+ (4 puertos SFP+ de 10 Gbps (Transceivers Incluidos)) • 6x10/100/1000 CU (con opción de conectividad de 1 Gbps cobre o fibra (Transceivers Incluidos)). • 2x1G For Management. **Nota:** Además de lo anteriormente mencionado, estos equipos deben tener Soporte de Transceivers 10G SFP+: SR, LR;XFP	Los valores soportados por el FortiACD 2000F son los siguientes: 8x 10 GE SFP+, 8 x GE SFP 8 x GE RJ45 1 GE Management Interface Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT08	Las interfaces de 10G deben soportar velocidades de 1G o 10G dependiendo el transceiver usado.	FortiADC 2000F cuenta con 8 interfaces 1Gb SFP más 8 interfaces adicionales 1 Gb JR45 que pueden ser utilizados para estos fines. Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT09	Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 100 a 240 VAC.	Los valores soportados por el FortiACD 2000F son los siguientes: Doble fuente de poder redúndate AC. 100–240V AC, 63–47 Hz Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT10	Los equipos deberán ser instalados en rack estándar de 19", máximo	Los valores soportados por el FortiACD 2000F son los siguientes: 1U Appliance	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
	1RU.	Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf		[illegible]	^		
RFT11	Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.	Los appliances FortiADC pueden ser desplegados como unidades independientes o como clusters de alta disponibilidad (HA). Un clúster es dos o más nodos. Un nodo es una instancia del dispositivo / sistema. En un clúster, un nodo es el Nodo primario, también llamado nodo maestro. Los otros miembros del clúster son nodos secundarios, también llamados Nodos esclavos. El nodo primario tiene un papel especial. Tiene una relación uno-a-muchos con nodos miembros. Tanto la configuración Las actualizaciones y actualizaciones de software son iniciadas por el nodo primario y empujadas a los nodos miembros. El sistema selecciona el nodo primario basado en los siguientes criterios: Salud de enlace (si los enlaces de puertos de monitor están abajo, el nodo se considera hacia abajo) Resultados de control de salud del monitor IP remoto Ajuste de anulación (prefiere prioridad al tiempo de actividad) La mayoría de los puertos disponibles Mayor valor de tiempo de actividad El número de prioridad de dispositivo más bajo (1 tiene mayor prioridad que 2) Número de serie de clasificación más alta-Los números de serie se ordenan comparando cada carácter de izquierda a derecha, donde 9 Y z son los valores más grandes. El sistema da preferencia a valores más altos sobre valores más bajos. Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 406-417	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT12	Cada equipo debe incluir 32 GB de Memoria RAM mínimo	Los valores soportados por el FortiACD 2000F son los siguientes: Memoria 32 GB Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT13	Cada equipo debe incluir mínimo un Disco duro de 240 GB SSD.	Los valores soportados por el FortiACD 2000F son los siguientes: 240 GB SSD Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
	El oferente deberá especificar detalladamente las especificaciones técnicas de los equipos ofertados, a nivel de Hardware y Software. Ejemplo: • Tipo de Memoria.			[illegible]			

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT14	• Cantidad de Memoria en GB. • Cantidad Slot de Memoria. • Capacidad máxima de Memoria Soportada. • Procesador. • Capacidad y Velocidad del procesador. • Marca del Procesador. • Cantidad de Núcleos del Procesador • Generación del Procesador. • Tipo de disco Duro (Sata, Sata III o Hibrido, SSD Etc.)			N	X		
RFT15	Debe soportar Clúster Activo/Activo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).			S	X		
RFT16	La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda.			S	X		
RFT17	Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.	Normalmente en una configuración HA, el nodo maestro empuja la mayor parte de su configuración a los otros nodos miembros. Esto se conoce como sincronización de configuración HA. Si la sincronización automática está habilitada, la sincronización Se produce automáticamente cuando un dispositivo se une al clúster y se repite cada 30 segundos después. Si La sincronización no está habilitada, debe iniciar la sincronización manualmente. Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paqinas 411-418	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT18	Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de Tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en Cuanto se refiere a plataformas.	In an Active-Active cluster, the IP addresses for all interfaces are unique, including the management interface. When the appliance is in standalone mode, the physical port IP address is active; when it is in HA mode, the address assigned to it in the HA node IP list address is active. You can log into any node using the active IP address for its management port. FortiADC usa ECMP para distribuir la carga entre los diferentes appliances que se encuentren en el Cluster. Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páqinas 423-434	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT19	La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.	Normalmente en una configuración HA, el nodo maestro empuja la mayor parte de su configuración a los otros nodos miembros. Esto se conoce como sincronización de configuración HA. Si la sincronización automática está habilitada, la sincronización Se produce automáticamente cuando un dispositivo se une al clúster y se repite cada 30 segundos después. Si La sincronización no está habilitada, debe iniciar la sincronización manualmente. Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páqinas 411-412	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
Funciones de Administración de Tráfico							

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT20	La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.	Layer 4 Application Load Balancing TCP, UDP protocols supported Round robin, weighted round robin, least connections, shortest response L4 dynamic load balancing based on server parameters (CPU, Memory and disk) Persistent IP, has IP/port, hash header, persistent cookie, hash cookie, destination IP hash, URI hash, full URI hash, host hash, host domain hash Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT21	La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.	FortiADC soporta Definición de servic Método de equilibrio y miembros del https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Página 3	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT22	La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.	FORTIADC 2000F, Soporta tres modos de implementación Router Mode, One-Arm Mode, Direct Server Return, donde el One-Arm Mode hace la función de Proxy reverso. Referencia: http://docs.fortinet.com/uploaded/files/2832/fortiadc-dg-basic.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT23	La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.	En la configuración de server pools podemos modificar el Weight por defecto de los nuevos servidores, con este método podemos limitar la cantidad de peticiones a los servidores seleccionados. Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf páginas 141 - 145	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT24	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones.	FortiADC soporta: Definición de servicio virtual con persistencia heredada, carga Método de equilibrio y miembros del grupo Layer 4/7 server persistence Persistent IP, has IP/port, hash header, persistent cookie, hash cookie, destination IP hash, URI hash, full URI hash, host hash, host domain hash FortiADC soporta Definición de servicio virtual con persistencia heredada, carga Método de equilibrio y miembros del grupo https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Página 3	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
	La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting: • Round Robin. • Proporcional (Ratio). • Proporcional dinámico. • Respuesta más rápida. • Conexiones mínimas. • Menor número de sesiones.	FortiADC soporta: Equilibrio de carga de aplicación de capa 4 • Round Robin. • Proporcional (Ratio). • Proporcional dinámico.	FAD-2000F FC-10-AD2KF-973-02-36				

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT25	• Tendencia de menor cantidad de conexiones (observed). • Tendencia de desempeño (predictive).	• Respuesta más rápida. • Conexiones mínimas. • Menor número de sesiones. • Tendencia de menor cantidad de conexiones (observed). • Tendencia de desempeño (predictive). Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 32-33		S	X		
RFT26	Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM	FortiADC soporta: Equilibrio de carga de aplicación de capa 4 Balance de carga dinámico L4 basado en los parámetros del servidor (CPU, memoria y disco) https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT27	El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)	FortiADC soporta hasta 2048 Virtual Servers. Para referencia visitar el siguiente link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 548	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT28	El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.	FortiADC En las implementaciones de equilibrio de carga del servidor, el sistema utiliza controles de integridad para examinar a los miembros del conjunto de servidores reales. Para probar si una aplicación está disponible. También puede configurar controles de estado adicionales para encuestar servidores relacionados. Y puede incluir resultados para ambos en la regla de verificación de salud. Por ejemplo, puede configurar un Prueba de verificación y una prueba de verificación de salud RADIUS. En una aplicación web que requiere autenticación de usuario, el servidor web Se considera disponible sólo si el servidor web y el servidor RADIUS relacionado pasan la comprobación. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 276-278	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT29	La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica.	FortiADC soporta: Calidad de servicio (QoS) -FortiADC ahora puede garantizar el ancho de banda y la cola basada en la fuente / destino Dirección, dirección y servicio de red http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 31	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
	La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de: • Ping.	FortiADC soporta: Ping.	FAD-2000F FC-10-AD2KF-973-02-36 FAD-2000F				

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT30	• Chequeo a nivel de TCP y UDP a puertos específicos. • Monitoreo http y https. • Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft. • Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. • Ejecución de scripts para determinar la respuesta emulando un cliente. • Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. • Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la • . Monitoreo de aplicaciones de mercado: o LDAP o FTP o SMTP o IMAP/POP3 o Oracle o MSSQL o MySQL o RADIUS o SIP o Protocolo SASP o SOAP o WMI o SNMP	• Chequeo a nivel de TCP y UDP a puertos específicos. • Monitoreo http y https. • Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft. • Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos • Ejecución de scripts para determinar la respuesta emulando un cliente. • Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. •Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 45.80, 508 - 517	FC-10-AD2KF-973-02-36	S	X		
RFT31	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo. esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones. El control de persistencia de las conexiones se debe realizar por los siguientes: • Dirección IP origen. • Dirección IP destino. • Cookies. • Hash. • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia. • Sesiones SSL. • Microsoft Remote Desktop. • Entre otros.	FortiADC soporta las siguientes opciones de persistencia. • Dirección IP origen. • Dirección IP destino. • Cookies. • Hash. • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia. • Sesiones SSL. • Microsoft Remote Desktop. • Entre otros http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 33-34	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT32	Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.	FortiADC soporta las siguientes opciones de persistencia. • Dirección IP origen. • Dirección IP destino. • Cookies. • Hash. • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia. • Sesiones SSL. • Microsoft Remote Desktop. • Entre otros http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 33-34	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
		Persistencia de equilibrio de carga de servidor: agregó una opción de coincidencia entre servidores al método de afinidad de dirección de origen Esta opción es útil cuando la sesión de cliente para una aplicación tiene conexiones a través de varios puertos (v	FAD-2000F FC-10-AD2KF-973-02-36				

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT33	Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.	Múltiples servidores virtuales). Esta opción garantiza que el cliente siga accediendo al mismo servidor backend a través de Diferentes servidores virtuales durante la duración de una sesión. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 26		S	X		
RFT34	El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.	Las reglas de persistencia identifican el tráfico que no debe ser equilibrado de carga, sino que se reenvía al mismo backend Servidor que ha visto solicitudes de esa fuente antes. Normalmente, se configuran las reglas de persistencia para admitir el servidor Transacciones que dependen de una sesión cliente-servidor establecida, como transacciones de comercio electrónico o llamadas de voz SIP. El sistema mantiene las tablas de sesión de persistencia para asignar el tráfico del cliente a servidores back-end basados en la sesión Atributo especificado por la regla de persistencia http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 132 - 136	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT35	Soporte de Scripts de Programación que permita crear funcionalidades que por defecto no se encuentran en el menú de configuración u opciones a través de un lenguaje gráfico.	FortiADC SLB admite secuencias de comandos Lua para realizar acciones que actualmente no son compatibles con el conjunto de funciones incorporado Los scripts le permiten usar comandos y variables de script predefinidos para manipular la solicitud / respuesta HTTP o Seleccione una ruta de contenido. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 34, 171-178	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT36	Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: • Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.	FortiADC Soporta REST API—Remote configuration management with a REST API via HTTPS. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT37	Debe permitir la integración con plataformas de automatización a través del protocolo REST	FortiADC Soporta REST API—Remote configuration management with a REST API via HTTPS. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT38	Soporte de RESTful API	FortiADC Soporta REST API—Remote configuration management with a REST API via HTTPS. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT39	La solución debe tener la capacidad de ampliarse para soportar la creación de alta disponibilidad entre Datacenters a través de GSLB.	El Balance Global de Carga de Servidores (GSLB) de FortiADC Su red fiable y disponible mediante la ampliación de aplicaciones a través de Múltiples centros de datos para la recuperación de desastres o para mejorar la aplicación tiempos de respuesta. Los administradores pueden configurar reglas que direccionen el tráfico Basado en la disponibilidad del sitio, el rendimiento del centro de datos y la latencia de la red. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT40	La solución debe soportar la configuración de un portal de acceso unificado con capacidad de ofrecer n-factores de autenticación.	FortiADC contiene un portal de acceso unificado con capacidad de ofrecer n-factores de autenticación. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 38-39	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT41	Debe permitir la optimización de la interfaz y el tráfico presentado a los clientes que consumen las aplicaciones a través de la plataforma ADC (Front End Optimization).	FortiADC ofrece múltiples servicios que aceleran la entrega de Aplicaciones a los usuarios. El conjunto PageSpeed del rendimiento del sitio web Las herramientas de mejora pueden optimizar automáticamente HTTP, CSS, Javascript Y entrega de imágenes a los usuarios de la aplicación. Almacenamiento en caché en FortiADC Almacena de forma dinámica el contenido de aplicaciones populares, como imágenes. Videos, archivos HTML y otros tipos de archivos para aliviar los recursos del servidor Y acelerar el rendimiento general de la aplicación. Compresión HTTP Emplea GZIP y DEFLATE para comprimir inteligentemente muchos contenidos Utilizados por las últimas aplicaciones basadas en la web para reducir Ancho de banda y mejorar la experiencia de la aplicación de usuario. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT42	Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.	Cuando los servidores reales de back-end no están disponibles, FortiADC puede responder a los clientes que intentan HTTP / HTTPS Conexiones con una página de error HTML. Una vez que ha creado una página de error HTML, puede seleccionarla en el servidor virtual Configuraciones. No tiene que crear una página de error HTML si desea simplemente enviar un mensaje de error de texto básico cuando Los servidores back-end no están disponibles. En su lugar, puede introducir un mensaje de error en un cuadro de texto Configuración del servidor.	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
		http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 138					
RFT43	Debe soportar el protocolo TDS para balanceo de MSSQL y SQL SERVER.	FortiADC (Versión 4.7.0 y versiones posteriores) soporta el equilibrio de carga del servidor MySQL usando MySQL Proxy como MySQL Pila de protocolos de red. MySQL Proxy es una aplicación de Oracle que es capaz de analizar y construir el protocolo MySQL Paquetes. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 67	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT44	Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT. proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT.		FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT45	El sistema deberá soportar scripts de programación basados en un lenguaje estructurado que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script.	FortiADC SLB admite secuencias de c Los scripts le permiten usar comandos y variables de script predefinidos para manipular la solicitud / respuesta HTTP o Seleccione una ruta de contenido. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 34, 171-178	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT46	El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC.			S	X		
RFT47	Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP. La Base de datos de Geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline).	FortiADC Soporta: GEO IP security and logs IP Reputation (subscription required) https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Pagina 4 FortiADC Soporta: GEO IP security and logs IP Reputation (subscription required) https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf GeoIP paises https://threatmap.fortiguard.com/ Pagina 4	FAD-2000F FC-10-AD2KF-973-02-36 FAD-2000F FC-10-AD2KF-973-02-36	S	X		
Funciones Generales de Seguridad							
RFT48	Cada equipo debe soportar seguridad SSL con las siguientes características: • Incluir el soporte de Aceleración SSL usando Hardware Dedicado • Incluir mínimo 13,000.00 Transacciones por segundo SSL (2K Keys) • Incluir mínimo 6,000.00 Transacciones concurrente de Curva elíptica (ECDHE) • Soportar al menos 10 Gbps SSL (Throughput SSL) ◦ La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA. • Soporte de llaves SSL de 1024, 2048 y 4096 bits	Los valores soportados por el FortiACD 2000F son los siguientes: Throughput en L4 40.0 Gbps Throughput en L7 24.0 Gbps Throughput en SSL 13.5 Gbps Compresión de Throughput 18.0Gbps Memoria 32 GB Millones de peticiones en L7 HTTP 2.4 Millones requests/sec. Transacciones en SSL (SSL transactions/sec (2K key certificates) 37.000 Para referencia visitar el siguiente link:	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
		https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Para las llaves soportadas verificar las tablas en el link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 456-460					
RFT49	La solución debe soportar mirroring de sesiones SSL. Sin el equipo primario falla el equipo secundario debe mantener la sesión SSL.	FortiADC admite paquetes de reflejo (HTTPS / TCPS) a las interfaces de red especificadas. Cuando la función es Habilitado, el tráfico SSL se reflejará en los puertos especificados por el servidor virtual después de haber sido descifrado. La función admite IPv4 e IPv6. FortiADC puede enviar tráfico a hasta cuatro interfaces salientes, incluyendo Agregadas y VLAN. El tráfico reflejado se transmite como un solo paquete de flujo, utilizando el original La dirección IP de origen y de destino del cliente y los números de puerto. Las direcciones MAC de origen y destino son 0 (cero) en tráfico reflejado. La característica requiere un servidor virtual configurado en Capa 7 o Capa 2, con un perfil configurado Para HTTPS o TCPS. Es compatible con todas las plataformas FortiADC. Para las llaves soportadas verificar las tablas en el link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 460-461	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT50	El Stack TLS del equipo debe soportar las siguientes funcionalidades/características • Session ID. • Session Ticket. • OCSP Stapling (on line certificate status protocol). • Dynamic Record Sizing. • ALPN (Application Layer Protocol Negotiation). • Forward Secrecy.	El Stack TLS del equipo debe soportar las siguientes funcionalidades/características • Session ID. • Session Ticket. • OCSP Stapling (on line certificate status protocol). • Forward Secrecy. Para las llaves soportadas verificar las tablas en el link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 27,29,33,102,129	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT51	La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital SignatureAlgorithm (DSA) y Elliptic Curve Cryptography (ECDHE).	Los valores soportados por el FortiACD 2000F son los siguientes: Throughput en L4 40.0 Gbps Throughput en L7 24.0 Gbps Throughput en SSL 13.5 Gbps Compresión de Throughput 18.0Gbps Memoria 32 GB Millones de peticiones en L7 HTTP 2.4 Millones requests/sec. Transacciones en SSL (SSL transactions/sec (2K key certificates) 37,000 Para referencia visitar el siguiente link: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Para las llaves soportadas verificar las tablas en el link: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Páginas 456-460	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT52	El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall). Nota: Debe Agregar certificación.		FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT53	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.		FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT54	Cada equipo debe incluir protección contra ataques de DDoS de mínimo 2,500,000.00 SYN/sec	Puede habilitar la prevención básica de denegación de servicio (DoS) para combatir las inundaciones SYN. Cuando está habilitado, FortiADC utiliza El método de cookie SYN para rastrear conexiones entreabiertas. El sistema mantiene una tabla de mitigación de DoS para cada Configurado servidor virtual IPv4. Excede las conexiones entreabiertas para que no agoten los recursos del sistema. El límite de los paquetes syn/sec está basado el L7 RPS. Referencia: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT55	Firmado criptográfico de cookies para verificar su integridad.		FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT56	Capacidad de integración con dispositivos HSM "Hardware Security Module" (Módulo de Seguridad Hardware) externos. Deberá soportar al menos ThalesnShield YSafenet (Gemalto) Luna.	Un módulo de seguridad de hardware (HSM) es un dispositivo dedicado para gestionar claves digitales y realizar operaciones criptográficas Operaciones. Un HSM puede ser una tarjeta plug-in o un dispositivo externo directamente conectado a una computadora o red servidor. Diseñados para proteger el ciclo de vida de la criptografía, los HSM han sido utilizados por algunos de los La mayoría de las entidades conscientes de la seguridad para proteger su infraestructura criptográfica mediante la gestión segura, procesamiento, Y almacenar las claves criptográficas dentro de un dispositivo endurecido, inviolable. Debido a sus fortalezas en la seguridad de claves criptográficas y el cifrado de aprovisionamiento, descifrado, autenticación, Y servicios de firma digital para una amplia gama de aplicaciones, los HSM han sido utilizados por empresas de todo el mundo para Proteger sus transacciones, identidades y aplicaciones en línea. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 364	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT57	La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.	Puede utilizar el descifrado SSL mediante proxy directo en los casos en que no pueda copiar el certificado del servidor y el servidor privado. Clave para el FortiADC, ya sea porque es imprácticO o imposible (en el caso del tráfico saliente a desconocido Servidores de Internet). Cuando SSL está habilitado, FortiADC es un proxy para ambos lados de la conexión. El certificado del servidor Y la clave privada utilizada para negociar la conexión SSL con el cliente se derivan dinámicamente del certificado Presentado por el servidor real y encadenado con una CA intermedia de confianza por el cliente. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 449	FAD-2000F FC-10-AD2KF-973-02-36	S			
	Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el		FAD-2000F				

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
	puerto.	FortiADC cuenta con el soporte de STARTTLS. STARTTLS es una extensión de los protocolos de comunicación de texto sin formato. Permite una conexión de texto sin formato Para ser actualizado a una conexión encriptada (TLS o SSL) en lugar de usar una conexión Puerto para la comunicación cifrada. Especifique esta opción si ha implementado STARTTLS para Su servidor de correo; De lo contrario, seleccione http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 308	FC-10-AD2KF-973-02-36				
RFT58				S	X		
RFT59	Debe soportar HSTS (HTTP Strict Transport Security).	Esto es soportado mediante nuestra arquitectura de Seguridad Fortinet Security Fabric FortiADC/FortiWEB	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT60	Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías. • Scanners • Exploits Windows • Denial of Service • Proxies de Phishing • Botnets • Proxies anónimos	FortiADC Cuenta con el servicio de IP Reputación que está incluido en el licenciamiento de esta propuesta. Para referencia. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT61	La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: • Memoria cache. • Compresión tráfico HTTP • Optimización de conexiones a la aplicación a nivel TCP • Multiplexación de conexiones hacia los servidores	FortiADC soporta HTTP and TCP Optimization Aceleración 100x mediante el procesamiento TCP de descarga Agrupamiento de conexiones y multiplexación para HTTP y HTTPS Aceleración de la página HTTP para la optimización del servidor Web Y Aceleración TCP buffer Compresión y descompresión HTTP Caché HTTP (objetos estáticos y dinámicos) Asignación de ancho de banda con Quality of Service (QoS) Limitación de la velocidad de HTTP y de capa Para referencia. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT62	El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Edge, Google Chrome, Mozilla Firefox, Safari, etc.	FortiADC SLB admite la descarga de compresión. La descarga de compresión significa que el ADC maneja la compresión Procesamiento en lugar de los servidores back-end, lo que les permite dedicar recursos a su propia aplicación Procesos. Cuando se habilita la compresión para un perfil de servidor virtual, el sistema FortiADC comprime inteligentemente Tráfico HTTPS. La reducción del tamaño del contenido de respuesta del servidor acelera el rendimiento y mejora los tiempos de respuesta. FortiADC es compatible con los algoritmos estándar GZIP y DEFLATE de la industria. Para referencia.	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
		http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf					
RFT63	Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 3.5 Gbps o superior	FORTIADC 2000F tiene la capacidad de 18 Gbps Para referencia. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT64	Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.		FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT65	Debe soportar el protocolo HTTP y funcionar como Gateway para este protocolo.	FortiADC soporta el protocolo HTTP. Para referencia. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT66	Permitir la modificación de los Tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los Tags generados por el Web server o modificarlos.		FAD-2000F FC-10-AD2KF-973-02-36	S	X		
Firewall de Aplicaciones Web (WAF)							
RFT67	La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un Appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).	FORTIADC 2000F cuanta con la funcionalidad de WAF integrada con el debido licenciamiento que está incluido en la propuesta. Referencia: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT68	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.			S	X		
RFT69	La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs, Parámetros, métodos, de manera específica.	FORTIADC 2000F, Permite la personalización de políticas de URL. FortiADC 4_8_0 Handbook Configuring a URL Protection policy pgs 224 - 225 Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT70	Debe trabajar en un esquema proxy TCP Reverso y/o Transparente.	FORTIADC 2000F, Soporta tres modos de implementación Router Mode, One-Arm Mode, Direct Server Return, donde el One-Arm Mode hace la función de Proxy reverso. Referencia: http://docs.fortinet.com/uploaded/files/2832/fortiadc-dg-basic.pdf	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT71	Debe soportar la creación automática de políticas			S	X		
RFT72	Debe trabajar con políticas de seguridad por capas, donde se configura una política de seguridad base y las políticas de seguridad hijas heredan sus configuraciones y permita que solo cambios Específicos se apliquen a las políticas hijas.	FORTIADC 2000F, Permite la creación de perfiles con una estructura genérica que permite la modificación de las diferentes subpolíticas creadas FortiADC 4_8_0 Handbook Configuring a URL Protection policy pgs 238 - 261	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
		• Restringir el número de parámetros Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf páginas 248-250					
RFT84	El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)	XML se utiliza comúnmente para el intercambio de datos, y los hackers a veces tratan de explotar los agujeros de seguridad en el código XML para Ataque a los servidores web. Puede utilizar el firewall de aplicaciones web (WAF) de FortiADC para examinar Anomalías en código XML. El WAF también puede intentar validar la estructura del código XML en las solicitudes del cliente utilizando Un archivo de esquema XML de confianza. La configuración de la detección XML puede ayudar a garantizar que el contenido de las XML no contiene ningún ataque potencial Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf páginas 257	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT85	El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP.	Supported in Fortiweb		S	X		
RFT86	El WAF debe incluir protección contra Web Scraping.	Supported in Fortiweb		S	X		
RFT87	Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario.	Supported in Fortiweb		S	X		
RFT88	Permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento Cross-Domain, permitiendo evitar un CORS (Cross-Origin Resource Sharing).			S	X		
RFT89	Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario			S	X		
RFT90	Debe permitir el enmascaramiento de información sensible filtrada por el servidor	FortiADC permite definir Política de firma de ataque web: la base de datos de firmas incluye firmas que pueden detectar ataques conocidos y Exploits que se pueden encontrar en 22 scanpoints. En la configuración de la política, elige clases de scanpoints para Proceso: encabezados HTTP, cuerpo de solicitud HTTP y cuerpo de respuesta HTTP. Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf páginas 240	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT91	Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de Geolocalización.	FortiADC Soporta: GEO IP security and logs IP Reputation (subscription required) https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Pagina 4	FAD-2000F FC-10-AD2KF-973-02-36	S	X		
RFT92	Debe permitir la integración con servidores Antivirus.	Supported in Fortiweb		S	X		
RFT93	Debe brindar reportes respecto a la normativa PCI DSS 3.1 MINIMO.	Supported in Fortiweb		S	X		
RFT94	Debe proteger contra ataque DoS /DDoS de Capa 4 Y 7.	Puede habilitar la prevención básica de denegación de servicio (DoS) para combatir las inundaciones SYN. Cuando está habilitado, FortiADC utiliza El método de cookie SYN para rastrear conexiones entreabiertas. El sistema mantiene una tabla de mitigación de DoS para cada Configurado servidor virtual IPv4. Excede las conexiones entreabiertas para que no agoten los recursos del sistema. El límite de los paquetes syn/sec está basado el L7 RPS.	FAD-2000F FC-10-AD2KF-973-02-36	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripcion	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
		Referencia: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf					
RFT95	Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa.	Puede habilitar la prevención básica de denegación de servicio (DoS) para combatir las inundaciones SYN. Cuando está habilitado, FortiADC utiliza El método de cookie SYN para rastrear conexiones entreabiertas. El sistema mantiene una tabla de mitigación de DoS para cada Configurado servidor virtual IPv4. Excede las conexiones entreabiertas para que no agoten los recursos del sistema. El límite de los paquetes syn/sec está basado el L7 RPS. Referencia: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf		S	X		
RFT96	En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico para poseer información forense.	La utilidad tcpdump se admite a través de la interfaz de usuario de la	FAD-2000F FC-10-AD2KF-973-02-	S	X		
RFT97	Debe soportar tecnologías AJAX y JSON .	FortiADC WAF soporta protección de: XML & JSON Validation I Supports XML & JSON validation and format check I XML schema validation I Supports XML & JSON XSS, SQLI and limit check Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf páginas 18	FAD-2000F FC-10-AD2KF-973-02-	S	X		
RFT98	Debe proteger como mínimo: • Ataques de Fuerza Bruta. • Cross-site scripting (XSS). • Cross Site Request Forgery. • SQL injection. • Parameter and HPP tampering. • Sensitive information leakage. • Session high jacking. • Buffer overflows. • Cookie manipulation. • Various encoding attacks. • Broken access control. • Forceful browsing. • Hidden fields manipulation. • Requests muggling. • XML bombs/DoS. • Open Redirect.	FortiADC tiene protección para una gran base de datos de ataques. Debido a que a lista es muy extensa, favor verificar la tabla en el siguiente enlace Tabla 71 http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf	FAD-2000F FC-10-AD2KF-973-02-	S	X		
RFT99	Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.			S	X		
RFT100	Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP			S	X		
RFT101	Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas			S	X		
RFT102	Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.	FortiADC Soporta: GEO IP security and logs IP Reputation (subscription required) https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf Pagina 4	FAD-2000F FC-10-AD2KF-973-02-	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT103	Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.			S	X		
RFT104	Debe ofrecer protección sobre tráfico basado en Web Sockets.	Dentro de los protocolos soportados por FortiADC WAF Security se encuentran los protocolos basado en WEB o HTTP. Referencia: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT105	El WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.	FortiADC puede identificar los diferentes navegadores que están consumiendo los servicios publicados. Con estos datos FotiADC puede generar reportes personalizados Referencia: http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Página 509	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT106	Debe proteger las aplicaciones contra ataques de denegación de servicio a nivel de L4 y L7	FortiADC también admite nuestro servicio FortiGuard IP Reputation (suscripción requerida) que le protege de fuentes asociadas con ataques DoS / DDoS, esquemas de phishing, spammers, software malicioso y botnets Esto incluye protección L4 y L7. Referencia: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02	S	X		
Estándares de Red							
RFT107	Soporte VLAN 802.1q, Vlantagging.	Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 295 - 304	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT108	Soporte de 802.3ad para definición de múltiples troncales	Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 295 – 304	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT109	Soporte de NAT, SNAT	Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 462 – 469	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT110	Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.	Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 295 – 304	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT111	Soporte de Rate Shapping.			S	X		
RFT112	Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.	Soportado Referencia https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiADC_D_Series.pdf	FAD-2000F FC-10-AD2KF-973-02	S	X		

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT113	Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.			S		X	No describe como este equipo cumple con el requerimiento respectivo. El cumplimiento del mismo es subsanable siempre y cuando el oferente demuestre cumplimiento del mismo
RFT114	Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS,	Soporte para OSPF y BGP Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Paginas 462 – 469	FAD-2000F FC-10-AD2KF-973-02	S	X		
Administración del Sistema							
RFT115	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH2, interfaz de administración gráfica basada en Web seguro (HTTPS)	Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 337	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT116	La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.	FotiADC soporta authentication via el protocolo LDAP. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 266	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT117	La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.	FotiADC soporta authentication via el protocolo LDAP. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 266	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT118	La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.	FotiADC soporta la integración con RADIUS para la autenticación de usuarios para gestión de la herramienta. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 268	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT119	La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales	FotiADC cuanta con un certificado digital nativo con la opción de instalar un certificado externo para la comunicación cifrada. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 268	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT120	La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: • Protocolo SysLog • Notificación vía SMTP • SNMP versión.2.0 o superior.	FortiADC soporta envío de alertas y eventos a un Sistema Centralizado mediante: • Protocolo SysLog • Notificación vía SMTP • SNMP versión.2.0 o superior. http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 18	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT121	El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.			S	X		
RFT122	El equipo debe contar con un módulo de administración tipo lightsout que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.			S	X		
RFT123	La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real	Soportado http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.pdf Pagina 40	FAD-2000F FC-10-AD2KF-973-02	S	X		
	Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como	Soportado, FortiADC cuenta con un módulo de reportes para estos fines.	FAD-2000F FC-10-AD2KF-973-02				

Formulario de Cumplimiento Lote No.2: Balanceadores de Carga (Application Delivery Controllers (ADCs))
Licitante: IQTEK

Req. No.	Descripción	Solución Propuesta	Número de Parte	Subsanable S/N	Cumplimiento		Observaciones
					Cumple	No Cumple	
RFT124	latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.	http://docs.fortinet.com/uploaded/files/3841/fortiadc-v4.8.0-handbook.odf Para referencia Tabla 171 Pagina 403		S	X		
RFT125	Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (Ejemplo: Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.	La documentación de FortiADC cuenta con una serie de guías de implementación para productos populares como: IIS Exchange Microsoft Lync Apache. Para referencia: http://docs.fortinet.com/fortiadc-d-series/admin-guides	FAD-2000F FC-10-AD2KF-973-02	S	X		
RFT126	Se debe un incluir una Herramienta de Análisis con su respectivo Licenciamiento, la cual permitirá una mejor gestión la solución ADCs Propuesta.	Fortianalyzer incluido en el proyecto de los Firewalls internos, tiene la capacidad de recopilar los logs de FortiADC, analizar, generar alertar, reportes y correlacionar logs de seguridad		S	X		
Otros Requerimientos							
RFT127	Todos los equipos de este Lote serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos UPS independientes para alta disponibilidad.			S	X		
RFT128	Las Soluciones propuestas de **Aplication Delivery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad)			S	X		

Leyenda:

Requerimientos	Cantidad	Cumple	%/Req.	No Cumple
Requerimientos de Contratación (RDC)	13	12	92.31%	1
Acreditaciones y Experiencia del Oferente	7	6		
Tiempos de Entrega y de Implementación	3	3		
Normas de Seguridad Industrial	1	1		
Responsabilidades del Oferente	2	2		
Requerimientos de Garantía y Soporte (RGS)	7	7	100.00%	0
Garantías y Soporte	6	6		
Requerimientos de Capacitación	1	1		
Requerimientos Técnicos(RFT) Balanceadores de Carga ADCs	128	127	99.22%	1
Total	148	146	98.65%	2

Evaluadores:

Gerente de Tecnología, Ing. Michael Ganeux:

Encargada de Infraestructura, Ing. Virginia Alejo:

PODER JUDICIAL
JURISDICCIÓN INMOBILIARIA
GERENCIA TECNOLOGIA