INFORME LEGAL

A: COMISION EVALUADORA
DE: ABOG. MARTA BEATRIZ GRANCE
FECHA:
REF.: LICITACIÓN PÚBLICA NACIONAL NRO. 10/2016 – "ACTUALIZACION DE RED CORPORATIVA"

Me dirijo a esa Comisión, a fin de elevar la Evaluación del Cumplimiento de los requisitos legales de las ofertas presentadas para la **Licitación Pública Nacional Nº 10/2016** de referencia, cuya **Apertura de Sobres Ofertas**, para la verificación cuantitativa del cumplimiento de los requisitos, se realizó el día 11 de Octubre **del corriente año**, en la **Gerencia Operativa de Contrataciones** de **COPACO S.A.**, de acuerdo al **Acta de Apertura Nº 29/2016** , en el cual consta la presentación de 2 (dos) firmas participantes **LOGICALS PARAGUAY S.A e INFOCENTER S.A** según el siguiente detalle:

OFERENTE	PRECIO TOTAL EN GUARANIES (IVA INCUIDO)
1) LOGICALS PARAGUAY S.A	GS. 3.548.000.000
2) INFOCENTER S.A	Gs. 2.950.000.000

TOTAL OFERENTE 1: Guaraníes Tres Mil Quinientos y Ocho Millones. I.V.A Incluido.-

TOTAL OFERENTE 2: Guaraníes Dos Mil Novecientos cincuenta Millones. I.V.A Incluido.-

MARTA B. GRANCE
Abogada
Mat. C.S.J. 9989

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

COPACO S.A.

COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Edificio San Esteban
Independencia Nacional e/ Fulgencio R. Moreno y Haedo

La Evaluación de las Ofertas se basó en la verificación del cumplimiento de los ***requisitos sustanciales*** de la documentación legal, considerando los siguientes documentos:

DOCUMENTOS SUSTANCIALES

OFERENTES	Formulario De Oferta debidamente firmado	Garantía de Mantenimiento de Oferta	Documento que acredita la Representación del firmante de la Oferta	Declaración Jurada de no hallarse comprendido en las prohibiciones del Art. 40	Declaración Jurada que garantice que el Oferente no se encuentra involucrado en prácticas que violen los derechos de los menores
1) LOGICALS PARAGUAY S.A	Presenta	Presenta COPIA	Presenta	**Presenta**	**Presenta**
2) INFOCENTER S.A	Presenta	Presenta	Presenta	**Presenta**	**Presenta**

A continuación han sido verificados a través de la Constancia del ***SIPE*** los siguientes:

OFERENTE	Doc. De Identidad y/o Pasaporte	Registro Único del Contrib (RUC)	Constancia del RUC (SET)	Constitución o Estatutos	Impuesto al Valor Agregado (IVA)	Balanc. Gral. Y Estado de Resultados	Impuesto a la Renta-Resumen de facturación-Impuesto a la Renta Personal	DD.JJ Art. 40	Certif. de cumplimiento con el Seguro Social o Constancia de no estar inscripto	CERTIF. DE Cumplimiento Tribut. Controversia	Declar. Jurada de Menores Res. DNCP 941/2010	Poder del Repres	DD JJ de no haber incurrido en incumplimiento de contratos
1)LOGICALS PARAGUAYS.A	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo
2)INFOCENTER	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

MARTA B. GRANCE
Abogada
Mat. C.S.J. 9989

Cabe mencionar que a fin de Evaluar la Capacidad Legal de las firmas oferentes, se procedió a verificar las documentaciones a través del **Sistema de Información de Proveedores del Estado (SIPE)** ya que en la **Sección VII - Anexo I in fine** habilita válidamente a las empresas la presentación simplificada de las ofertas a través del **SIPE**... *Documentos Sustanciales conforme a la **cláusula 31.2 de las IAO**

Los oferentes que estén inscriptos en el **Sistema de Información de Proveedores del Estado (SIPE)**, al momento de la presentación de las ofertas no necesitarán acompañar los documentos que consten en la Constancia emitida por el sistema, bastando la presentación de la misma, **siempre que dichos documentos se hallen "ACTIVOS".**

La inscripción en el **SIPE** no constituirá requisito previo para la presentación ni adjudicación de los oferentes; no obstante los adjudicatarios deberán inscribirse al **SIPE** como requisito previo a la obtención del **Código de Contratación.**

Así también y resguardando la Legalidad de la presente Licitación se señala que se ha observado lo establecido de manera taxativa en el ***Decreto Nº 21909/03 Reglamentaria de la Ley 2051/2003 - Art. 60: Análisis***. *La **Convocante** deberá determinar si las Ofertas se ajustan sustancialmente a los requisitos del **Pliego de Bases y Condiciones** verificando que:... **inc. 2.** El Formulario de la Oferta esté debidamente completado y preparado,* concordante con el ***Art. 61 (Decreto 21909/03) Método de Evaluación*** ***inc. 1.*** *Se verificará el cumplimiento de cada Oferta respecto al suministro de la documentación básica de carácter sustancial **(Garantía de Mantenimiento de la Oferta debidamente extendida, formulario de la Oferta debidamente firmado y completado, Poderes suficientes del firmante de la Oferta)** solicitada en el **Pliego de Bases y Condiciones**, eliminándose a aquellas que no cumplan con el suministro de dicha documentación, o que dicha documentación sea insatisfactoria.; en concordancia con **Art. 58 del Decreto Reglamentario Nº 21909/03**, Reglamentaria de la **Ley Nº 2051/03** que establece: Conformidad de la Oferta con el **Pliego de Bases y Condiciones**. La determinación por parte de la **Convocante** si una Oferta se ajusta al **Pliego de Bases y Condiciones**, se basará solamente en contenido de la propia Oferta. Una Oferta se ajusta sustancialmente al **Pliego de Bases y Condiciones** cuando concuerda con todos los términos, condiciones y especificaciones de los mismos, sin desviación, reserva u omisiones significativas. Constituye una desviación, reserva u omisión significativa aquella que:*

1. *Afecta de manera sustancial el alcance y la calidad de los bienes y servicios conexos o de las obras, especificados en el **Pliego de Bases y Condiciones**.*
2. *Limita de manera sustancial, en discrepancia con lo establecido en el **Pliego de Bases y Condiciones** , los derechos de la **Convocante** o las obligaciones del oferente emanadas del contrato; o*
3. *De rectificarse afectaría la competencia en igualdad de condiciones perjudicando a los demás oferentes cuyas ofertas se ajustan sustancialmente al **Pliego de Bases y Condiciones**, tales como la falta de **Garantía de Mantenimiento de la Oferta** o extensión de ésta en desacuerdo con los requerimientos del Pliego , la falta de presentación de formularios de Oferta y lista de precios debidamente firmados y completados, ausencia o insuficiencia de los poderes del firmante de la Oferta para obligar al oferente, entre otras.*

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

MARTA B. GRANCE
Abogada
Mat. C.S.J. 9989

Toda Oferta que no se ajuste sustancialmente al ***Pliego de Bases y Condiciones*** *será rechazada por la* ***Convocante.*** *No podrá posteriormente convertirse en una Oferta que se ajuste sustancialmente al* ***Pliego de Bases y Condiciones****, aquella que carecía de este requisito originalmente, y que tras la corrección de desviaciones, reservas u omisiones significativas el oferente pretenda su aceptación.*

Con relación al **Art. 1 de la Resolución DNCP Nro. 849/2015** donde se establece sobre la Calificación legal. **Prohibiciones de los Incs. "a" y "b" del Artículo 40**. El Comité de Evaluación confirmará que el Oferente no se encuentra comprendido en las prohibiciones establecidas en el **Art. 40, Incs. "a" y "b" de la Ley 2051/03,** se informa que a través del Sistema de Intercambio de Información de la **Secretaria de la Función Pública** se informa que en el marco de la presente Licitación Pública Nacional la empresa ***LOGICALS S.A*** no posee entre sus Accionistas a ningún funcionario público del Estado cuya nómina es la siguiente.

1) ***ANTONIO ALFONSO DOMINGUEZ NOTARIO C.I Nro. 885.593***
2) ***CINTIA ADRIANA PAVON KAMM C.I Nro. 1.118.014***

Del mismo modo se ha verificado que los integrantes de la empresa ***INFOCENTER S.A*** no posee entre sus accionistas a ningún funcionario público del Estado cuya nómina es la siguiente:

1) ***SIXTO RAMON FIGUEREDO NOTARIO C.I Nro. 1.157.723***
2) ***LIDA CONCEPCION VERA GONZALEZ C.I Nro. 692.060***
3) ***CARLOS ANTONIO GALLARDO BARRANTES C.I Nro. 5.323.231***

Todo esto a fin de cumplir con el requisito legal que recomienda a los organismos, entidades y municipalidades la utilización del mismo en los procesos regidos por la Ley 2051/03 disponiendo su difusión en el portal de Contrataciones Públicas y en donde la **SECRETARIA DE LA FUNCION PUBLICA (SFP)** deja expresa constancia de que no tiene confirmación formal de la carga total de datos de funcionarios y contratados en el **SINARH** por cada Organismos y Entidades del Estado en este Ejercicio Fiscal, por lo que se aclara que la presente constancia es emitida según datos actuales obrantes en el sistema a la fecha; No obstante se informa que los nombres mencionados más arriba **no registran datos ni antecedentes de pertenencia a ninguna Institución Pública del Estado** .-

Con relación al Informe solicitado por la **Gerencia Operativa de Contrataciones** a la **Gerencia de Talento Humano** de la Compañía respecto a que si las mencionadas personas, representantes de las empresas oferentes se registran como empleados de **COPACO, el Departamento Administrativo de Talento Humano** por Nota de fecha 20 de Octubre de 2016 remitió lo solicitado informando que **no se registra como empleado de la Compañía**.-

MARTA B. GRANCE
Abogada
Mat. C.S.J. 9989

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Atendiendo a los criterios anteriormente expuestos, y teniendo en consideración lo dispuesto en la **Ley N° 2051/2003** de las Contrataciones Públicas, la **Ley Nº 3.439/2007** "Que modifica la **Ley Nº. 2051/2003 "De Contrataciones Públicas**", como así también los **Decretos Reglamentarios Nros. 21.909/03 y 5174/05,** Así también se indica que la presente evaluación es netamente de naturaleza Legal y con carácter sugerente pero no así determinante y concluyente en el presente procedimiento se realizan a la **COMISIÓN EVALUADORA** las siguientes sugerencias:

1) Proceder a la Evaluación de las Ofertas presentadas por las firmas **LOGICALS PARAGUAY S.A e INFOCENTER S.A.** considerando que han cumplido con los requisitos legales indicados en el Pliego de Bases y Condiciones, con los cuales acreditan su Capacidad Legal, quedando habilitada para la presente **Licitación Pública Nacional**-

2) Redactar el Informe Final.

ES MI INFORME.-

MARTA B. GRANCE
Abogada
Mat. C.S.J. 9989

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

COPACO
Comunicación en todo Sentido!

MEMORÁNDUM

A : Lic. Jesús Ramírez**(Coordinador)**

Ref. : Informe de Capacidad Financiera**LPN Nº 10/2016 - SBE**

Fecha : 13-10-2016

Me dirijo a usted, en su carácter de Coordinador de la Comisión de Trabajo conformada para la Apertura de Sobres y Evaluación de Ofertas de la Licitación Pública NacionalNº 10/2016 – SBE, **"ACTUALIZACIÓN DE REDCORPORATIVA" - ID 308266.**

De conformidad a lo establecido en la **Sección II** del PBC - Criterios de Evaluación y Requisitos de Calificación; **Numeral 2.** Requisitos para Calificación Posterior; **Inciso (a), Capacidad Financiera**, se ha procedido al análisis de la información proveída por las Firmas ***Logicalis Paraguay S.A.*** *e* ***InfocenterS.A..***

Al respecto, el PBC establece que: "La Convocante efectuará la calificación del Oferente, empleando únicamente los requisitos aquí estipulados. Los requisitos que no estén incluidos en el siguiente texto no podrán ser utilizados para evaluar las calificaciones del Oferente".

A continuación se expone el resultado de la referida evaluación:

2. Requisitos para Calificación Posterior

a) Capacidad Financiera	LOGICALIS PARAGUAY S.A.	INFOCENTER S.A.
a. Ratio de Liquidez: activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los años 2013, 2014 y 2015.	***Cumple***	***Cumple***
b. Endeudamiento: activo total / pasivo total No deberá ser mayor a 0,80, en promedio, en los años 2013, 2014 y 2015.	***Cumple***	***Cumple***
c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital El promedio en los años 2013, 2014 y 2015 no deberá ser negativo.	***Cumple***	***Cumple***

El análisis fue realizado teniendo en cuenta los datos contenidos enlos Balances Generales y Estados de Resultados correspondientes a los años 2013, 2014 y 2015. Se adjunta la Planilla de Cálculoscorrespondiente.

Atentamente,

Econ. Carlos F. Ortega Barrios
Div. Económico Financiero

COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.
Edif. Gral. Bernardino Caballero
Alberdi e/ Oliva y Gral. Díaz
Asunción - Paraguay

LICITACIÓN PÚBLICA NACIONAL Nº 10/2016 - SBE

"ACTUALIZACIÓN DE RED CORPORATIVA"- ID Nº 308.266

Indices Financieros

LOGICALIS PARAGUAY S.A.

	2013	2014	2015	PROMEDIO
Activo Corriente	9.248.638.740	45.619.663.093	35.483.385.100	1,77
Pasivo Corriente	11.740.223.341	20.525.913.880	15.378.396.999	
Ratio de Liquidez	**0,79**	**2,22**	**2,31**	
Pasivo Total	11.740.223.341	20.525.913.880	15.378.396.999	0,42
Activo Total	29.767.048.389	46.083.680.096	36.054.008.311	
Ratio de Endeudamiento	**0,39**	**0,45**	**0,43**	
Utilidad Neta	5.806.230.183	7.506.275.860	10.345.213.823	7169%
Capital	110.000.000	110.000.000	110.000.000	
Ratio de Rentabilidad %	**5278%**	**6824%**	**9405%**	

INFOCENTER S.A.

	2013	2014	2015	PROMEDIO
Activo Corriente	22.825.237.208	40.504.640.562	35.280.914.818	1,36
Pasivo Corriente	20.365.072.866	30.961.534.959	21.429.677.705	
Ratio de Liquidez	**1,12**	**1,31**	**1,65**	
Pasivo Total	23.073.973.981	38.819.788.124	32.870.246.802	0,68
Activo Total	37.821.618.400	53.216.181.955	47.859.016.435	
Ratio de Endeudamiento	**0,61**	**0,73**	**0,69**	
Utilidad Neta	1.326.031.034	674.669.755	836.637.051	11,31%
Capital	8.365.000.000	8.365.000.000	8.365.000.000	
Ratio de Rentabilidad %	**15,85%**	**8,07%**	**10,00%**	

Econ. Carlos F. Ortega Barrios
Div. Económico Financiero

INFORME TÉCNICO

Fecha: 31.10.16

En relación al llamado por **Licitación Pública Nacional N° 10/2016"ACTUALIZACIÓN DE RED CORPORATIVA" SUBASTA A LA BAJA ELECTRONICA con ID Nº 308266**, en el día y la hora señalada para el efecto, se procedió a la apertura de los Sobres Ofertas de las siguientes empresas, conforme al Acta de Apertura de Ofertas Nro. 29/2016 de fecha 11 de octubre de 2016:

- **LOGICALIS PARAGUAY S.A.**
- **INFOCENTER S.A.**

Se han analizado específicamente lo establecido en la Sección II Criterios de Evaluación y Requisito de Calificación parte 1 y 2 (b), Sección VII, Anexo 1 del Pliego de Bases y Condiciones.

Sección II
Criterios de Evaluación y Requisitos de Calificación

1. Criterios de Evaluación

- *Se seleccionará provisoriamente al oferente o postor ganador del proceso de competencia de subasta determinado en el Acta de Sesión Pública Virtual, cuyas documentaciones serán analizadas en detalle para verificar el cumplimento de los requisitos de calificación.*

  La Empresa seleccionada conforme al Acta de Sesión Pública Virtual con Código Verificador: 7ffe05f17b23d0643bbfb4ac3769d33c, y de oferta más baja es la Empresa **INFOCENTER S.A.**

- *Posteriormente se verificará que se haya proveído la documentación que avale el cumplimento de los criterios **técnicos**, legales y financiero conforme a los requisitos de calificación.*

  Los criterios técnicos que avalan el cumplimiento de las Especificaciones Técnicas fueron comprobados de las Carpetas: **Oferta Original, "A" DataSheets y WhitpePapers, "B" CD Infocenter Catálogo** provista por la Empresa **INFOCENTER S.A.** En consecuencia, todos los folios **sin letras** pertenecen a la Carpeta **Oferta Original**, los folios con **letra "A"** a la Carpeta **"A" DataSheets y WhitePapers**, los folios con letra **"B"** al **"B" CD Infocenter Catálogo**

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1 - ESPECIFICACIONES TÉCNICAS

1.5 –DETALLE DE LAS ESPECIFICACIONES TECNICAS

El equipamiento ofertado debe cumplir todos y cada uno de los siguientes Ítems:

1.5.1 - SWITCHES PRINCIPALES

Descripción	Requerimiento mínimo	Ofertado
Marca	Especificar	Cumple, Fs. 147
Modelo	Especificar	Cumple, Fs. 147
Cantidad	4	Cumple, Fs. 147
1.5.1.1.	Debe ser de arquitectura modular y rackeable en infraestructuras de 42 unidades de rack y debe incluir todos los accesorios necesarios para su montaje	Cumple, Fs. "A" 77
1.5.1.2.	Debe poseer al menos cuatro (4) slots para módulos de interfaces.	Cumple, Fs. "A" 77
1.5.1.3.	Cada equipo debe estar equipado de acuerdo a la arquitectura pretendida con al menos 36 interfaces de 40G con los siguientes alcances: • Mínimo 28 interfaces de 40G con alcance de 100 mtrs sobre 1 pelo de FO. • Mínimo 2 interfaces de 40G con alcance de 10 Km • Mínimo 1 interfaces de 40G con alcance de 40 Km • El resto de las interfaces sin módulos ópticos	Cumple, Fs. "A" 136 y Fs. 147
1.5.1.4.	Debe poseer módulos de supervisoras redundantes ubicados físicamente separados del resto de las Line Cards. El equipo debe contar con todos los componentes necesarios para cumplir con el rendimiento solicitado y garantizar que en caso de que haya pérdida de una supervisora, no exista disminución en el rendimiento así como ningún paquete de trafico descartado (Zero Packet Drop)	Cumple, Fs. "A" 78
1.5.1.5.	Debe poseer al menos 6 módulos de Hardware de Switch Fabrics ubicados físicamente separados del resto de las Line Cards y de las Supervisoras. Estos módulos deben proveer hacia y desde cada slot de interfaces de un ancho de banda de switching mínimo de 3,5 Tbps(aunque el equipo no disponga al día de hoy de módulos de interfaces que hagan uso de este ancho de banda)	Cumple, Fs. "A" 78
1.5.1.6.	Debe poseer un ancho de banda de switching por slot mínimo de 3,5Tbps	Cumple, "B" Cisco Nexus 9500 Series Switches Architecture White Paper 8
1.5.1.7.	Debe poseer un ancho de banda de switching agregado del equipo mínimo de 15 Tbps	Cumple, Fs. "A" 79, "A" 194

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefa Div. Redes y Comunicaciones

1.5.1.8.	Debe poseer al menos 6 módulos de Hardware de Switch Fabrics ubicados físicamente separados del resto de las Line Cards y de las Supervisoras. Estos módulos deben proveer hacia y desde cada slot de interfaces de un ancho de banda de forwarding mínimo de 2,5 Tbps (aunque el equipo no disponga al día de hoy de módulos de interfaces que hagan uso de este ancho de banda)	Cumple Fs. "A" 136
1.5.1.9.	Debe poseer un ancho de banda de forwarding por slot mínimo de 2,5Tbps	Cumple Fs. "A" 136
1.5.1.10.	Debe poseer un ancho de banda de forwarding agregado del equipo mínimo de 11 Tbps	Cumple Fs. "A" 82
1.5.1.11.	Circulación de aire Front to Back	Cumple Fs. "A" 78
1.5.1.12.	Debe poseer al menos 3 fuentes de alimentación redundantes para una tensión de alimentación de 220 VAC a 50 Hz, cualquier falla en como mínimo el 50% de ellas en simultaneo debe permitir que el equipo continúe en operación sin impacto en su rendimiento.	Cumple Fs. "A" 79
1.5.1.13.	Consumo máximo por puerto 10G = 3,85W/puerto	Cumple Fs. "A" 78
1.5.1.14.	Consumo máximo por puerto 40G = 15,4W/puerto	Cumple Fs. "A" 78
1.5.1.15.	Debe soportar el reemplazo en caliente de todos los componentes redundantes, como las supervisoras, switch fabrics, fuentes de energía y ventiladores, que deben ser redundantes 2+1.	Cumple Fs. "A" 78, "A" 80
1.5.1.16.	Debe poseer la configuración de CPU y memoria (RAM y Flash) suficiente para la aplicación de todas las características que se describen en este llamado	Cumple Fs. "A" 80
1.5.1.17.	El chasis equipado al máximo debe soportar por lo menos 190 puertos de 1 Gbps	Cumple Fs. "A" 77
1.5.1.18.	El chasis equipado al máximo debe soportar por lo menos 570 puertos de 10 Gbps, cada puerto debe soportar ópticas con alcance mínimo desde 100m a 40 Km (detallar)	Cumple Fs. "A" 77
1.5.1.19.	El chasis equipado al máximo debe soportar por lo menos 144 puertos de 40 Gbps, cada puerto debe soportar ópticas con alcance mínimo desde 100m a 40 Km (detallar) sobre 2 pelos de FO y 150 mtrs. sobre un solo pelo de FO (detallar).	Cumple Fs. "A" 77 y Fs. 148
1.5.1.20.	El chasis equipado al máximo debe soportar por lo menos24 puertos de 100 Gbps, cada puerto debe soportar ópticas con alcance mínimo desde 100m a 10 Km (detallar)	Cumple Fs. "A" 77
1.5.1.21.	El equipo en su máxima población de interfaces debe soportar full line rate en tráfico unicast y multicast en el 100% de los puertos para cualquier tamaño de paquetes (de 64 a 9216 bytes) probados de acuerdo a la RFC 2544, RFC 2889 y RFC 3918.	Cumple, "B" Cisco Nexus 9516 – Miercom. 7
1.5.1.22.	El equipo en su máxima población de interfaces debe soportar una latencia máxima de 1,6 µsegundos en paquetes de 64 bytes y 3,5 µsegundos en paquetes de 9216 bytes en tráfico unicast y multicast en el 100% de los puertos probados de acuerdo a la RFC 2544, RFC 2889 y RFC 3918.	Cumple, "B" Cisco Nexus 9516 – Miercom. 9
1.5.1.23.	Debe soportar el protocolo TRILL o similar	Cumple, "B" Data Center Overlay Technologies 3

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Báez Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.24.	Debe soportar la funcionalidad que permita realizar la interconexión en L2 entre Datacenters sobre cualquier tipo de plataforma IP, sin necesidad de utilizar protocolos como MPLS, BGP, etc. y que no esté basada en flooding de MACs	Cumple Fs. "A" 84
1.5.1.25.	A los efectos de esta licitación cada equipo debe configurarse con al menos 36 puertos 40G de baja latencia con soporte de funcionalidades de capa 2 y capa 3.	Cumple Fs. "A" 136
1.5.1.26.	Debe soportar IEEE 802.1q (VLAN FrameTagging).	Cumple Fs. "A" 199
1.5.1.27.	Debe soportar IEEE 802.1s (Multi-InstanceSpanning-Tree), permitiendo al menos 64 instancias simultáneas de SpanningTree por switch virtual.	Cumple, "B" Cisco NX-OS Software 10
1.5.1.28.	Debesoportar IEEE 802.1w (Rapid Spanning Tree Protocol).	Cumple, "B" Cisco NX-OS Software 10
1.5.1.29.	Debe soportar IEEE 802.1d (SpanningTreeProtocol) por VLAN.	Cumple, "B" Cisco NX-OS Software 10
1.5.1.30.	Debe poseer capacidad de al menos 160.000 direcciones MAC.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules. 5
1.5.1.31.	Debe soportar al menos 4000 (cuatro mil) VLANs simultáneamente por switch virtual	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules. 5
1.5.1.32.	Debe soportar IGMP Snooping v1, v2 y v3.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules. 5
1.5.1.33.	Debe soportar IEEE 802.1Qbb	Cumple, "B" Cisco NX-OS Software 6
1.5.1.34.	Debe soportar IEEE 802.1Qaz	Cumple, "B" Cisco NX-OS Software 6
1.5.1.35.	Debe soportar IEEE 802.1BR	Cumple, "B" Cisco NX-OS Software 6.
1.5.1.36.	Debe soportar IEEE 802.1p (Class of Service) para cada puerto.	Cumple, "B" Cisco NX-OS Software 10

Gerencia de Tecnología de Información

Amancio Daira Ferreira
Jefe Departamento Soporte Técnico

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.37.	Debe soportar IEEE 802.3ad LACP.	Cumple, "B" Cisco NX-OS Software 10
1.5.1.38.	Debe soportar IPv4 e IPv6.	Cumple, "B" Cisco NX-OS Software 4
1.5.1.39.	Debe soportar enrutamiento estático.	Cumple, "B" Cisco NX-OS Software 10
1.5.1.40.	Debe soportar RIPv2 (RFC 2453, 2082 o 1723).	Cumple, "B" Cisco NX-OS Software 11
1.5.1.41.	Debe soportar OSPF (RFC 2328, 3101, 3137, 3623 y 2370).	Cumple, "B" Cisco NX-OS Software 11
1.5.1.42.	Debe soportar BGPv4 (RFC 4271, 3065 o 1965, 4456 o 2796, 1997 y 2385).	Cumple, "B" Cisco NX-OS Software 10
1.5.1.43.	Debe permitir el enrutamiento entre VLANs.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.44.	Debe permitir el enrutamiento entre VxLANs.	Cumple, "B" Data Center Overlay Technologies. 12
1.5.1.45.	Debe soportar al menos 128.000 Rutas prefijas - longestprefix match (LPM)-.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules. 5
1.5.1.46.	Debe poseer un mecanismo de autenticación para acceso al equipo local o remoto basada en un servidor de autenticación/autorización del tipo TACACS+ o RADIUS.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.47.	Debe poseer listas de control de acceso (ACL) basadas en criterios de capa 3 y capa 4 en todas las interfaces y las VLAN para el ingreso o egreso de tráfico.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.48.	Debe ser capaz de proteger la interfaz de comandos del dispositivo a través de una contraseña.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.49.	Debe soportar SSH v2 para el acceso a la interface de línea de comandos.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.50.	Debe permitir la creación de listas de acceso basadas en direcciones IP para limitar el acceso al equipo a través de Telnet y SSH. Debe ser posible definir las direcciones IP de origen de las sesiones de Telnet y SSH.	Cumple, "B" Cisco NX-OS Software 6

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Duarte Correira
Jefe Departamento Soporte Técnico GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.51.	Debe permitir el control del volumen de tráfico unicast, multicast y broadcast de una interface mediante la asignación de porcentajes permitidos para cada uno de los tráficos o mediante la asignación de volumen de los paquetes.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.52.	Debe poseer mecanismos de AAA (Authentication, Authorization y Accounting).	Cumple, "B" Cisco NX-OS Software 6
1.5.1.53.	Debe poder controlarse los comandos que los usuarios o grupos de usuarios pueden ejecutar en determinados elementos de la red.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.54.	Debe soportar un mecanismo de protección "Root Bridge" del algoritmo "Spanning-Tree" para la defensa contra ataques del tipo " Denial of Service " en capa 2.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.55.	Debe poder permitir la suspensión de la recepción de BPDU (Bridge Protocol Data Units) como se especifica en la norma IEEE 802.1w.	Cumple, "B" Cisco NX-OS Software 2
1.5.1.56.	Debe poseer un mecanismo de control de multicast a través de IGMPv1 (RFC 1112) , IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376), en todas las interfaces de los switches.	Cumple, "B" Cisco NX-OS Software 5
1.5.1.57.	Debe permitir el enrutamiento multicast PIM (Protocol Independent Multicast) en "sparse-mode" (RFC 2362 o 4601).Dense-Mode	Cumple, "B" Cisco NX-OS Software 5
1.5.1.58.	Numero de instancias de MultipleSpanningTree (MTS) de al menos 64.	Cumple, "B" Cisco NX-OS Software 10
1.5.1.59.	Debe soportar al menos 9.999 tuneles tipo (VTEP)	Cumple, "B" Cisco NX-OS Software 3.
1.5.1.60.	Debe soportar al menos 9.999 VXLANs (por VLAN)	Cumple, "B" Cisco NX-OS Software 3.
1.5.1.61.	Debe soportar Full routing de VXLANs a line rate	Cumple, "B" VXLAN Overview Cisco Nexus 9000 Series Switches 8
1.5.1.62.	Debe soportar la clasificación, marcación y reclasificación de tráficobasada en CoS ("Class of Service " - Capa 2) y DSCP ("DifferentiatedServicesCode Point" - Capa 3) conforme con las definiciones de la IETF (Internet Engineering Task Force).	Cumple, "B" Cisco Nexus 9500 Series Switches Architecture White Paper 13

Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.63.	Debe ser posible la especificación de ancho de banda por clase de servicio.	Cumple, "B" Cisco Nexus 9500 Series Switches Architecture White Paper 13
1.5.1.64.	Para los paquetes que superan la especificación anterior, debe ser posible configurar acciones tales como: transmisión con remarcación del valor de DSCP, descartar el paquete, etc.	Cumple, "B" Cisco Nexus 9500 Series Switches Architecture White Paper 13
1.5.1.65.	Debe permitir el mapeo de prioridades de capa 2, definidas por la norma IEEE 802.1p, en prioridades de capa 3 (IETF DSCP - DifferentiatedServicesCode Point definido por el Internet Engineering Task Force) y viceversa.	Cumple, "B" Cisco Nexus 9500 Series Switches Architecture White Paper 13
1.5.1.66.	Debe soportar los mecanismos de QoS WRR (Weighted Ronda Robin) y WRED (Weighted Random Early Detection).	Cumple, "B" Cisco Application Centric Infrastructure 3
1.5.1.67.	Debe tener por lo menos 4 colas de salida por puerto (egressport) las cuales podrán ser configurables y ajustar el número de colas de prioridad.	Cumple, "B" Cisco Application Centric Infrastructure 3.
1.5.1.68.	Debe permitir la gestión y la administración por el puerto de consola.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 4
1.5.1.69.	Debe permitir la actualización de software sin interrupción del servicio.	Cumple, "B" Cisco NX-OS Software. 1
1.5.1.70.	Debe soportar la sincronización de su reloj vía protocolo NTP	Cumple, "B" Cisco NX-OS Software. 11
1.5.1.71.	Debe soportar SNMP v1, v2 y v3.	Cumple, "B" Cisco NX-OS Software. 11
1.5.1.72.	Debe soportar Full MPLS	Cumple, "B" Cisco NX-OS Software 9

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.1.73.	Debe soportar BGP EVPN	Cumple, "B" Cisco Nexus 9500 Platform Common Equipment 8
1.5.1.74.	Debe soportar Full Layer 3 routing en IPv4 e IPv6 para unicast y multicastroutingen al menos los siguientes protocolos: EnIPv4: • Static Routes • BGP (iBGP y eBGP) • OSPFv2 • ISIS • VRF • VRRP • BFD • DHCP Relay • MPLS • PIM-SM y PIM-SSM En IPv6: • Static Routes • BGP (iBGP y eBGP) • OSPFv3 • VRF • VRF Route Leaking • VRRPv3 • DHCP Relay • MPLS • PIM-SM y PIM-SSM Para ambos casos de IPv4 e IPv6 se deben soportar los siguientes atributos de BGP enhacements: • disable-peer-as-check • allow-as in • best-as-path-relax • transport connection-mode passive • remove private-as enhancements • MD5 authentication for prefix based neighbors • E-BGP next-hop unchanged • IPv6 Route updates over a IPv4 Peering En Multicast: • IGMP v1/2/3 • IGMP Snooping • PIM – Sparse • ASM • Anycast RP • MSDP	Cumple, "B" Cisco NX-OS Software 10, 11

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.75.	Debe soportar como mínimo 1000 peers de E-BGP con BFD	Cumple, "B" Cisco Nexus 9500 Platform Switches 10
1.5.1.76.	Debe soportar Networking overlay con cualquier protocolo de encapsulación de extensión L2 utilizando VXLANs con soporte de integración con Microsoft Hyper-V., con cualquier virtualizador vasado en Hipervisores	Cumple, "B" Cisco NX-OS Software 12
1.5.1.77.	Debe soportar como mínimo 64.000 tenants independientes, cada uno de ellos con su propia topología virtual, bridge domain, instancias de routing virtual y políticas de seguridad.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals 45
1.5.1.78.	Debe poder tomar decisiones inteligentes de QoS basadas en el estado actual de carga de la red que debe obtener a través de información de Capa 3 en ECMP de manera de manejar adecuadamente el tráfico de baja latencia/alta disponibilidad que pudiere ocurrir. El oferente debe detallar como se logra esta prestación.	Cumple, "B" Cisco NX-OS Software 4
1.5.1.79.	Debe soportar protocolos de Capa 2 para el agregado de interfaces a través de varios chassis(multi-sytem-link aggregation) .Detallar.	Cumple, "B" Cisco NX-OS Software 10
1.5.1.80.	Debe soportar un tiempo de convergencia menor a 1 segundo en caso de interrupción del link de cualquier dispositivo conectado a través de (MC-LAG) independientemente del tamaño de la red.	Cumple, "B" Cisco NX-OS Software 12
1.5.1.81.	Debe soportar un Fabric (conjunto de todos los dispositivos que forman el Datacenter que soporte como mínimo 1 Millón de máquinas virtuales (endpoints).	Cumple, "B" Cisco Nexus 9500 Platform Common Equipment 8
1.5.1.82.	Debe soportar tecnología para extender redes de L2 entre D.C. Distribuido	Cumple, "B" Cisco NX-OS Software 12
1.5.1.83.	Debe soportar la migración transparente de maquina virtuales vía una optimización del routing en sentido horizontal (West-East) mediante VxLANs.	Cumple, "B" Cisco Application Centric Infrastructure 3
1.5.1.84.	Debe soportar mecanismos de mitigación de tormentas de ARP Distribution /Flood. Detallar.	Cumple, "B" Cisco Nexus 9500 Platform Switch 11
1.5.1.85.	Debe soportar en hardware (ASICs) todos los mecanismos de aprendizaje esenciales de la red (MACs, IPs, VTEP IDs, etc.).	Cumple, "B" Data Center Overlay Technologies 15

Ing. [illegible] Ramirez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.86.	Debe soportar Jumbo Frames (al menos 9216 bytes)	Cumple, "B" Cisco NX-OS Software 3
1.5.1.87.	Deben ser monitoreables y gerenciables a través de distintos protocolos como mínimo SNMP, sFlow, etc.	Cumple, "B" Cisco NX-OS Software 6
1.5.1.88.	Debe soportar multipath en Capa 2 a traves de ECMP	Cumple, "B" Cisco NX-OS Software 6.
1.5.1.89.	Debe soportar herramientas de diagnóstico y debug. Detallar.	Cumple, "B" Cisco NX-OS Software 5
1.5.1.90.	Debe soportar SDN para ser controlado en sentido vertical y horizontal (North/South/East/West) a través de APIs. Detallar.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 2
1.5.1.91.	Debe ser 100% gerenciable, monitoreable y configurable a través de la plataforma SDN de los controladores requeridos en esta propuesta	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 2
1.5.1.92.	Debe ser 100% gerenciable, monitoreable y configurable a través de APIs mediante RPC (remote procedure calls), JSON (JavaScript Object Notation) y XML, todo ellos sobre HTTP/HTTPS	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3
1.5.1.93.	Los equipos no deben interconectar sus módulos de interfaces (Line Cards) con los Switch Fabrics a través de un midplane.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3
1.5.1.94.	Debe soportar la gestión vía GUI a través de una interface web o de una herramienta de gestión (ver detalle de los controladores SDN requeridos).	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.95.	Debe soportar programación XML.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric **Infrastructure 3**
1.5.1.96.	Debe soportar FTP o TFTP para la actualización del sistema operativo.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3
1.5.1.97.	Debe soportar RMON.	Cumple, "B" Cisco Nexus 9000 Series NX-OS System Management 1
1.5.1.98.	Debe poseer un hardware programable a través de un modelo OS Object mediante iAPIs (IntelligentApplicationProgramming Interface) hacienda uso de llamadas RPC usando JSON o XML sobre HTTP/ HTTPS.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3
1.5.1.99.	Debe cumplir al menos con las siguientes normas de Compatibilidad Electromagnética (EMC) e Interferencia Electromagnética (EMI): CFR 47 Part 15 Class A, VCCI Class A, EN 55022, EN 55024, AS/NZS CISPR22 Class A, ICES003 Class A, KN22 Class A y EN61000-6-1.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules 8
1.5.1.100.	Debe cumplir al menos con las normas de seguridad UL y EN 60950-1.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules 8
1.5.1.101.	Debe cumplir con la norma RoHS6.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules 8
1.5.1.102.	Garantía de (1) año como mínimo para todo el equipo, incluyendo sin costo adicional asistencia por garantía, con mano de obra, repuesto y partes con traslado de equipos desde el lugar de uso al proveedor y viceversa. No se aceptará sustitución temporal, el reemplazo debe ser definitivo	Cumple, Fs. 248

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnologia de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.1.103.	El Equipo debe estar acompañado de todos los accesorios necesarios para su correcta instalación y funcionamiento	Cumple, Fs. 194
1.5.1.104.	El reemplazo de partes o del equipo en caso de daños, debe ser en un plazo máximo al día siguiente útil, una vez adjudicado se exigirá una nota del fabricante donde demuestre dicho compromiso	Cumple, Fs. 194
1.5.1.105.	El servicio de instalación comprende: Instalación física en el rack a ser proveído por el oferente, debe proveer servicio de configuración del equipo a ser provista en este llamado	Cumple, Fs. 194
1.5.1.106.	Los técnicos de la empresa oferente Deben estar certificados por el fabricante, y los mismos deben residir en el país. Se exigirá la presentación de los certificados de al menos 4 técnicos pertenecientes a la empresa autorizada por el fabricante. La documentación emitida por el fabricante; no debe exceder dos años de antigüedad.	Cumple Fs. 210- 125.
1.5.1.107.	Se deben presentar reportes expedidos por terceras partes (no por el fabricante) en donde se certifique que los equipos cumplen con la performance declarada	Cumple 197-209

1.5.2 - SWITCHES SECUNDARIOS

Descripción	Requerimiento mínimo	Ofertado
Marca	Especificar	Cumple, Fs. 155
Modelo	Especificar	Cumple, Fs. 155
Cantidad	4	Cumple, Fs. 155
1.5.2.1.	Debe ser rackeable en infraestructuras de 42 unidades de rack y debe incluir todos los accesorios necesarios para su montaje	Cumple, "B" Cisco Nexus 9300 Platform Switches. 4
1.5.2.2.	Debe tener una altura máxima de 2RU	Cumple, "B" Cisco Nexus 9300 Platform Switches. 2
1.5.2.3.	Cada equipo debe estar equipado de acuerdo a la arquitectura pretendida con al Menos 48 interfaces de 1/10G y 6 interfaces 40G con los siguientes alcances mínimos: • 5interfacesomás,de40Gconalcancede100mo.sobre1pelodeFO • 1interfaceomás,de40Gconalcancede10Km • 4interfacesomás,de10Gconalcancede10Km • 16interfacesomás,de 10Gs obre FO con alcance de 10 Km con SFP + incluidos en ambos extremos. • 18interfacesomás,de1G1000Base-TX • 6interfacesomás,de1G1000BaseSX • 4interfacesomás,de1G1000BaseLXconalcancede10Km	Cumple, "B" Cisco Nexus 9300 Platform Switches. 2 y Fs. 155

Gcia. de Tecnología de Información.

Amancio Dutra Ferreira

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.2.4.	Debe poseer al menos 3 fuentes de alimentación para una tensión de alimentación de 220 VAC a 50 Hz, la falla de hasta 25% de ellas debe permitir que el equipo continúe en operación sin impacto en su rendimiento.	Cumple, "B" Cisco Nexus 9300 Platform Switches. 4
1.5.2.5.	Debe soportar Hot Swap de las fuentes de poder así como de las turbinas de ventilación que deben ser redundantes 2+1	Cumple, "B" Cisco Nexus 9300 Platform Switches. 4
1.5.2.6.	Debe poseer un ancho de banda de switching mínimo de 1,4 Tbps	Cumple, "B" Cisco Nexus 9300 Platform Leaf Switches for Cisco Application Centric Infrastructure. 3
1.5.2.7.	Debe poseer un ancho de banda de forwarding mínimo de 1,1 MPPS de 64 bytes	Cumple, "B" Cisco Nexus 9300 Platform Leaf Switches for Cisco Application Centric Infrastructure Pg.3
1.5.2.8.	Debe soportar una latencia máxima de 1,1 µsegundos entre cualquiera de sus puertos	Cumple, "B" Cisco Nexus 9300 Platform Switches. 5
1.5.2.9.	Debe poseer al menos 50MB de buffer de almacenamiento temporal de tráfico para todos sus puertos	Cumple, "B" Cisco Nexus 9300 Platform Switches. 5
1.5.2.10.	Debe soportar al menos 127K de rutas con el máximo prefijo (longestprefix match, LPM)	Cumple, "B" Cisco Nexus 9300 Platform Switches. 12
1.5.2.11.	Debe soportar al menos 96K de direcciones MAC	Cumple, "B" Cisco Nexus 9300 Platform Switches. 12
1.5.2.12.	Debe soportar al menos 32K de rutas multicast en un Multiple System Link Aggregation control protocol.	Cumple, "B" Cisco Nexus 9300 Platform Switches. 12.
1.5.2.13.	Debe soportar al menos 32K de grupos de snooping de IGMP	Cumple, "B" Cisco Nexus 9300 Platform Switches. 12

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.2.14.	Debe soportar al menos 3800 listas de acceso ingresantes y al menos 1000 salientes	Cumple, "B" Cisco Nexus 9300 Platform Switches. 12.
1.5.2.15.	Debe tener una capacidad mínima de backplane de 1.4Tbps	Cumple, "B" Cisco Nexus 9300 Platform Switches. 2
1.5.2.16.	Debe soportar al menos 4096 VLAN	Cumple, "B" Cisco Nexus 9300 Platform Switches. 12.
1.5.2.17.	Debesoportar al menos 1000 Virtual Routing and Forwarding (VRF) Full MPLS	Cumple, "B" Cisco NX-OS Software 12
1.5.2.18.	Debe soportar al menos 64 instancias simultaneas de Multiple SpanningTree (MST)	Cumple, "B" Cisco NX-OS Software 2.
1.5.2.19.	Debe soportar al menos 250 VXLAN tunnelendpoints (VTEP)	Cumple, "B" Cisco NX-OS Software 2
1.5.2.20.	Debe soportar al menos 32 miembros en un mismo Port Channel	Cumple, "B" Cisco Nexus 9300-EX Platform Switches. 3
1.5.2.21.	Debe soportar SDN para ser controlado en sentido vertical y horizontal (North/South/East/West) a través de APIs. Detallar.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 2
1.5.2.22.	Debe soportar Networking overlay con cualquier protocolo de encapsulación de extensión L2 utilizando VXLANs con soporte de integración con Microsoft Hyper-V., con cualquier virtualizador vasado en Hipervisores	Cumple, "B" Cisco NX-OS Software 3
1.5.2.23.	Debe soportar al menos 520 Port Channels	Cumple, "B" Cisco Nexus 9300-EX Platform Switches. 6
1.5.2.24.	Debe soportar al menos 500 de STP en VLANs	Cumple, "B" Cisco Nexus 9300-EX Platform Switches. 6

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Aldercie
Jefe Div. Redes y Comunicaciones

1.5.2.25.	El equipo en su máxima población de interfaces debe soportar full line rate en tráficounicast y multicast en el 100% de los puertos para cualquier tamaño de paquetes (de 64 a 9216 bytes) probados de acuerdo a la RFC 2544, RFC 2889 y RFC 3918.	Cumple, "B" Cisco Nexus 9516 – Miercom.
1.5.2.26.	Debe soportar la migración transparente de maquina virtuales vía una optimización del routing en sentido horizontal (West-East) mediante VxLANs.	Cumple, "B" Cisco Application Centric Infrastructure 3
1.5.2.27.	Debe soportar mecanismos de mitigación de tormentas de ARP Distribution /Flood. Detallar.	Cumple, "B" Cisco NX-OS Software 3
1.5.2.28.	Debe soportar Jumbo Frames (al menos 9216 bytes)	Cumple, "B" Cisco NX-OS Software 3
1.5.2.29.	Deben ser monitoreables y gerenciables a través de distintos protocolos como mínimo SNMP, etc.	Cumple, "B" Cisco NX-OS Software 6.
1.5.2.30.	Debe soportar multipath en Capa 2 a traves de ECMP	Cumple, "B" Cisco NX-OS Software 4
1.5.2.31.	Debe soportar herramientas de diagnostico y debug. Detallar.	Cumple, "B" Cisco NX-OS Software 5
1.5.2.32.	Debe contar con Buffer interno integrado de modo a dar mayor performance entre el acceso y el uplink en la arquitectura ToR de al menos 50MB.	Cumple, "B" Cisco Nexus 9300 Platform Leaf Switches for Cisco Application Centric Infrastructure 7
1.5.2.33.	Debe soportar en hardware (ASICs) todos los mecanismos de aprendizaje esenciales de la red (MACs, IPs, VTEP IDs, etc.).	Cumple, "B" Data Center Overlay Technologies 15
1.5.2.34.	Debe poseer un mecanismo de autenticación para acceso al equipo local o remoto basada en un servidor de autenticación/autorización del tipo TACACS+ o RADIUS.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.35.	Debe poseer listas de control de acceso (ACL) basadas en criterios de capa 3 y capa 4 en todas las interfaces y las VLAN para el ingreso o egreso de tráfico.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.36.	Debe ser capaz de proteger la interfaz de comandos del dispositivo a través de una contraseña.	Cumple, "B" Cisco NX-OS Software 6

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.2.37.	Debe soportar Full Layer 3 routing en IPv4 e IPv6 para unicast y multicastrouting en al menos los siguientes protocolos: EnIPv4: • Static Routes • BGP (iBGP y eBGP) • OSPFv2 • ISIS • VRF • VRRP • BFD • DHCP Relay • MPLS • PIM-SM y PIM-SSM En IPv6: • Static Routes • BGP (iBGP y eBGP) • OSPFv3 • VRF-Lite • VRF Route Leaking • VRRPv3 • DHCP Relay • MPLS • PIM-SM y PIM-SSM Para ambos casos de IPv4 e IPv6 se deben soportar los siguientes atributos de BGP enhacements: • disable-peer-as-check • allow-as in • best-as-path-relax • transport connection-mode passive • remove private-as enhancements • MD5 authentication for prefix based neighbors • E-BGP next-hop unchanged • IPv6 Route updates over a IPv4 Peering En Multicast: • IGMP v1/2/3 • IGMP Snooping • PIM – Sparse • ASM • Anycast RP • MSDP	Cumple, "B" Cisco NX-OS Software 10, 11
1.5.2.38.	Debe soportar SSH v2 para el acceso a la interface de línea de comandos.	Cumple, "B" Cisco NX-OS Software 6

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Dto. Redes y Comunicaciones

1.5.2.39.	Debe poseer un hardware programable a través de un modelo OS Object mediante iAPIs (IntelligentApplicationProgramming Interface) hacienda uso de llamadas RPC usando JSON o XML sobre HTTP/ HTTPS.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3
1.5.2.40.	Debe permitir la creación de listas de acceso basadas en direcciones IP para limitar el acceso al equipo a través de Telnet y SSH. Debe ser posible definir las direcciones IP de origen de las sesiones de Telnet y SSH.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.41.	Debe permitir el control del volumen de tráfico unicast, multicast y broadcast de una interface mediante la asignación de porcentajes permitidos para cada uno de los tráficos o mediante la asignación de volumen de los paquetes.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.42.	Debe poseer mecanismos de AAA (Authentication, Authorization y Accounting).	Cumple, "B" Cisco NX-OS Software 6
1.5.2.43.	Debe poder controlarse los comandos que los usuarios o grupos de usuarios pueden ejecutar en determinados elementos de la red.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.44.	Debe poder permitir la suspensión de la recepción de BPDU (Bridge Protocol Data Units) como se especifica en la norma IEEE 802.1w.	Cumple, "B" Cisco NX-OS Software 2
1.5.2.45.	Debe poseer un mecanismo de control de multicast a través de IGMPv1 (RFC 1112) , IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376), en todas las interfaces de los switches.	Cumple, "B" Cisco NX-OS Software 5
1.5.2.46.	Debe permitir el enrutamiento multicast PIM (ProtocolIndependentMulticast) en "sparse-mode" (RFC 2362 o 4601).	Cumple, "B" Cisco NX-OS Software 5
1.5.2.47.	Debe soportar al menos 9.999 VXLAN (por VLAN)	Cumple, "B" Cisco Nexus 9000 Series NX-OS Verified Scalability 3
1.5.2.48.	Debe soportar la clasificación, marcación y reclasificación de traficobasada en CoS ("Class of Service " - Capa 2) y DSCP ("DifferentiatedServicesCode Point" - Capa 3) conforme con las definiciones de la IETF (Internet Engineering Task Force).	Cumple, "B" Cisco Application Centric Infrastructure 3
1.5.2.49.	Debe ser posible la especificación de ancho de banda por clase de servicio.	Cumple, "B" Cisco Application Centric Infrastructure 3

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.2.50.	Para los paquetes que superan la especificación anterior, debe ser posible configurar acciones tales como: transmisión con remarcación del valor de DSCP, descartar el paquete, etc.	Cumple, "B" Cisco Application Centric Infrastructure 3
1.5.2.51.	Debe permitir el mapeo de prioridades de capa 2, definidas por la norma IEEE 802.1p, en prioridades de capa 3 (IETF DSCP - DifferentiatedServicesCode Point definido por el Internet Engineering Task Force) y viceversa.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.52.	Debe soportar los mecanismos de QoS WRR (Weighted Ronda Robin) y WRED (WeightedRandomEarlyDetection).	Cumple, "B" Cisco Application Centric Infrastructure 3
1.5.2.53.	Debe tener por lo menos cuatro (04) colas de salida por puerto (egressport) las cuales podrán ser configurables y ajustar el número de colas de prioridad.	Cumple, "B" Cisco NX-OS Software
1.5.2.54.	Debe permitir la gestión y la administración por el puerto de consola.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 4
1.5.2.55.	Debe permitir la actualización de software sin interrupción del servicio.	Cumple, "B" Cisco NX-OS Software. 1
1.5.2.56.	Debe soportar routing, bridging y gateway a Line Rate de Line-rate utilizando cualquier protocolo de encapsulación de extensión L2.	Cumple, "B" Cisco Nexus 9300 Platform Switches 11
1.5.2.57.	Debe soportar SNMP v1, v2 y v3.	Cumple, "B" Cisco NX-OS Software 6
1.5.2.58.	Debe soportar programación XML.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3
1.5.2.59.	Debe soportar FTP o TFTP para la actualización del sistema operativo.	Cumple, "B" Cisco Nexus 9500 Platform Switches for Cisco Application Centric Infrastructure 3

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.2.60.	Debe soportar RMON.	Cumple, "B" Cisco Nexus 9000 Series NX-OS System Management 1
1.5.2.61.	Debe cumplir al menos con las siguientes normas de Compatibilidad Electromagnética (EMC) e Interferencia Electromagnética (EMI): CFR 47 Part 15 Class A, VCCI Class A, EN 55022, EN 55024, AS/NZS CISPR22 Class A, ICES003 Class A, KN22 Class A y EN61000-6-1.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules 8
1.5.2.62.	Debe cumplir al menos con las normas de seguridad UL y EN 60950-1.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules 8
1.5.2.63.	Debe cumplir con la norma RoHS 6.	Cumple, "B" Cisco Nexus 9500 Platform Line Cards and Fabric Modules 8
1.5.2.64.	Debe soportar a futuro interfaces de acceso a 25Gbps (el oferente detallara cuando estarán disponibles)	Cumple, "B" Cisco Nexus 9300-EX Platform Switches 4
1.5.2.65.	Garantía de (1) año como mínimo para todo el equipo, incluyendo sin costo adicional asistencia por garantía, con mano de obra, repuesto y partes con traslado de equipos desde el lugar de uso al proveedor y viceversa. No se aceptará sustitución temporal, el reemplazo debe ser definitivo	Cumple Fs. 248
1.5.2.66.	El Equipo debe estar acompañado de todos los accesorios necesarios para su correcta instalación y funcionamiento	Cumple Fs. 160
1.5.2.67.	El reemplazo de partes o del equipo en caso de daños, debe ser en un plazo máximo de al día siguiente útil, una vez adjudicado se exigirá una nota del fabricante donde demuestre dicho compromiso	Cumple Fs. 160
1.5.2.68.	El servicio de instalación comprende: Instalación física en el rack de la institución, Configuración del equipo de manera a que pueda ser usada dentro de la infraestructura existente y a ser proveída en este llamado	Cumple Fs. 160
1.5.2.69.	Los técnicos de la empresa oferente deben estar certificados por el fabricante, y los mismos deben residir en el país. Se exigirá la presentación de los certificados de al menos 4 técnicos pertenecientes a la empresa autorizada por el fabricante. La documentación emitida por el fabricante; no debe exceder dos años de antigüedad.	Cumple Fs. 210- 125
1.5.2.70.	Se deben presentar reportes expedidos por terceras partes (no por el fabricante) en donde se certifique que los equipos cumplen con la performance declarada	Cumple 197-209

Lic. Jesus Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.3 - SERVIDORES PARA CONTROLADOR SDN

Item	Requerimiento mínimo	Ofertado
Marca	Especificar	Cumple, Fs. 160
Modelo	Especificar	Cumple, Fs. 160
Cantidad	3	Cumple, Fs. 160
1.5.3.1	Debe tener un Factor de forma del producto de 1RU y ser montable en rack universales de 19"	Cumple, "B"Cisco UCS C220 M4 Rack Server - 1
1.5.3.2	Debe tener al menos 8 compartimentos frontales con capacidad de Hot Swap	Cumple, "B"Cisco UCS C220 M4 Rack Server - 2
1.5.3.3	Debe poseer al menos 2 CPUs con al menos 6 Cores por procesador, 64 bits y velocidad mínima de 1,9GHz	Cumple, "B"Cisco UCS C220 M4 Rack Server – 2
1.5.3.4	Debe poseer memoria caché Tipo L3	Cumple, "B"Cisco UCS C220 M4 Rack Server – 1
1.5.3.5	Debe poseer al menos 15MB de memoria cache de último nivel (Last-level Cache, LLC)	Cumple, "B"Cisco UCS C220 M4 Rack Server – 1
1.5.3.6	Debe poseer al menos 64GB de Memoria RAM (inicial, instalado) con capacidad final de 1,5TB (mínima)	Cumple, "B"Cisco UCS C220 M4 Rack Server – 1
1.5.3.7	Debe poseer tecnología DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v o superior	Cumple, "B"Cisco UCS C220 M4 Rack Server – 1
1.5.3.8	Debe poseer un controlador de almacenamiento ARRAY Tecnologías soportadas SAS y SATA	Cumple, "B"Cisco UCS C220 M4 Rack Server – 1
1.5.3.9	Debe soportar la capacidad de mezclar unidades de discos de tecnologías SAS y SATA	Cumple, "B"Cisco UCS C220 M4 Rack Server – 2

Lic. [illegible] Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.3.10	Debe soportar una capacidad de conexión de como mínimo unidades de 128 SATA y SAS con ocho puertos internos de 12 Gb de capacidad de BUS	Cumple, "B"Cisco UCS C220 M4 Rack Server – 3
1.5.3.11	Debe poseer un controlador RAID SATA y SAS en un mínimo de 8 puertos internos para conectar 128 unidades	Cumple, "B"Cisco UCS C220 M4 Rack Server – 3
1.5.3.12	Debe soportar la protección de balance y rendimiento para aplicaciones críticas con los niveles RAID 0, 1, 5, 6, 10, 50 y 60	Cumple, "B"Cisco UCS C220 M4 Rack Server – 3
1.5.3.13	Debe poseer tipo de controlador interfaz PCI-e	Cumple, "B"Cisco UCS C220 M4 Rack Server – 3
1.5.3.14	Debe poseer al menos 2 discos de 600GB 12G SAS 15K RPM SFF HDD o superior	Cumple, Fs. 161
1.5.3.15	Debe poseer al menos 1 disco SSD de 120GB SATA o superior	Cumple, Fs. 161
1.5.3.16	Debe poseer un controlador gráfico Tipo Integrado	Cumple, Fs. 161
1.5.3.17	Debe poseer 2 (dos) Puertos 10Gb SFP+	Cumple, Fs. 161
1.5.3.18	Debe estar equipado con al menos 2 interfaces 10GBase-CX4 de 5 mts.	Cumple, Fs. 161
1.5.3.19	Debe poseer 2 (dos) Puertos Gigabit Ethernet	Cumple, "B" Cisco UCS C220 M4 Rack Server - 1
1.5.3.20	Debe poseer 1(uno) 16GB Flash USB Drive	Cumple, Fs. 161
1.5.3.21	Debe poseer 1 Interface serial RS-232D-Sub de 9 pines (DB-9)	Cumple, "B" Cisco UCS C220 M4 Rack Server - 4
1.5.3.22	Debe poseer 2 USB Hi-Speed USB	Cumple, "B" Cisco UCS C220 M4 Rack Server - 4
1.5.3.23	Debe poseer 1 puertos VGA VGA - HD D-Sub de 15 pines (HD-15)	Cumple, "B" Cisco UCS C220 M4 Rack Server - 4
1.5.3.24	Debe poseer almenos 2 fuentes de alimentacióneléctrica redundante que opere en 1+1 en 230VAC (50/60Hz) y de 700W de potencia	Cumple, "B" Cisco UCS C220 M4 Rack Server - 4

Lic. Jesús Ma. Ramírez O.
Ceia. de Tecnología de Información

Amancio Daiea Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.3.25	Debe soportar una temperatura de funcionamiento de 35 °C y una humedad de 5-93% sin condensación	Cumple, "B" Cisco UCS C240 M4 High-Density - 110
1.5.3.26	Debe cumplir con las normas de EnergyStar (reducción del consumo y el costo de la energía, además de proteger al medio ambiente utilizando productos y practicas especificas)	Cumple, "B" Seven Reasons Why Cisco UCS Is Better - 2
1.5.3.27	La Garantía debe ser de (1) año como mínimo para todo el equipo, incluyendo sin costo adicional asistencia por garantía, con mano de obra, repuesto y partes con traslado de equipos desde el lugar de uso al proveedor y viceversa. No se aceptará sustitución temporal, el reemplazo debe ser definitivo	Cumple, "B" Cisco UCS C240 M4 High-Density - 71
1.5.3.28	Todos los equipos deben ser nuevos de fabricación reciente, encontrarse en comercialización activa en el mercado para el que fueron diseñados	Cumple, Fs. 162
1.5.3.29	El Equipo debe estar acompañado de todos los accesorios necesarios para su correcta instalación y funcionamiento	Cumple, Fs. 162
1.5.3.30	El reemplazo de partes o del equipo en caso de daños, debe ser en un plazo máximo de al día siguiente útil, una vez adjudicado se exigirá una nota del fabricante donde demuestre dicho compromiso	Cumple, Fs. 162
1.5.3.31	El servicio de instalación comprende: Instalación física en el rack a ser proveído por el oferente, debe proveer servicio de configuración del equipo a ser provista en este llamado	Cumple, Fs. 162

1.5.4 - CONTROLADOR SDN

Descripción	Requerimiento mínimo	Ofertado
Marca	Especificar	Cumple, Fs. 162
Versión	Especificar	Cumple, Fs. 162
1.5.4.1	El software del controlador ofertado debe funcionar en HA en al menos 3 servidores robustos, rackeables de doble fuente.	Cumple, "B" Cisco Application Centric Infrastructure: 3,5,6,12
1.5.4.2	La solución propuesta debe ser en su totalidad SDN en un 100%	Cumple, "B" Software-Defined Networking: 1
1.5.4.3	Debe ser el principal componente de la arquitectura de la solución SDN en donde se unifiquen, automaticen, administren y orquesten todas las funciones de la red.	Cumple, "B" Software-Defined Networking: 1

Amancio Daira Ferreira
Jefe Departamento Soporte Técnico
GTI

Lic. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Dpto. Redes y Comunicaciones

1.5.4.4	Debe trabajar en Cluster para optimizar el rendimiento y unifica el funcionamiento del entorno físico y virtual. Facilitando la contingencia y la escalabilidad.	Cumple, "B" Cisco Application Centric Infrastructure: 5,6
1.5.4.5	Debe proveer una solución 100% SDN centralizada a través de APIs en sentido vertical y horizontal (North-South-West-East)	Cumple, "B" Software-Defined Networking: 1
1.5.4.6	El software ofertado no podrá ser del tipo Open Source. Debe de ser ofertado por una empresa legalmente constituida localmente, con experiencia, con centro de soporte 7X24 de al menos 2 niveles de escalabilidad.	Cumple, Fs. 162
1.5.4.7	Debe soportar HA (High Availability).	Cumple, "B" Cisco Application Centric Infrastructure:12
1.5.4.8	Se debe de instalar en los 3 servidores controladores mencionados anteriormente con las características mínimas descriptas en el ITEMServidores para Controlador SDN	Cumple, "B" Software-Defined Networking: 3
1.5.4.9	Debe de funcionar en HA e inclusive debe de funcionar a un 100% con 1 solo Servidores para Controlador SDN enlínea para los casos de contingencia.	Cumple, Fs. 163
1.5.4.10	Debe proveer una plataforma de Gestión para ambiente físico, virtual y Cloud	Cumple, "B" Software-Defined Networking: 3,4
1.5.4.11	Debe centralizar todas las políticas de la red	Cumple, "B" Software-Defined Networking: 1
1.5.4.12	Debe proveer toda la administración de fallas, evento y de rendimiento	Cumple, "B" Software-Defined Networking: 2
1.5.4.13	Debe proveer el monitoreo de aplicaciones y cambios en la topología de la red instantánea y automáticamente.	Cumple, "B" Software-Defined Networking: 2
1.5.4.14	Debe proveer la configuración y el inventario de TODOS los dispositivos de la red.	Cumple, "B" Software-Defined Networking: 2
1.5.4.15	Debe proveer un monitoreo de todos los elementos críticos, con niveles de puntuación según sea su estado de correcto funcionamiento (Switches, perfiles de aplicación,etc.)	Cumple, "B" Software-Defined Networking: 2
1.5.4.16	Debe contar con funcionalidades de autodiscovery, para un despliegue rápido, con autoconfiguración y descubrimiento de infraestructura usando protocolos estándares como Dynamic Host Configuration Protocol (DHCP), Link Layer Discovery Protocol (LLDP), Intermediate System-to-Intermediate System (IS-IS) Protocol	Cumple, "B" Cisco Application Centric Infrastructure Zero-Touch Fabric:1

Lic. Jesús Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.4.17	Debe de considerar toda la estructura de red y operar como un gran firewall distribuido basado en el contexto, que hace cumplir políticas en forma integral en todo el Datacenter.	Cumple, "B" Cisco Application Centric Infrastructure Zero-Touch Fabric:2
1.5.4.18	Debe mantener los planos de control y datos de manera independiente y separada del fabric físico de manera tal que en caso de falla total del cluster la red continúe operando sin interrupción ni degradación del tráfico.	Cumple, "B" Cisco Application Centric Infrastructure Zero-Touch Fabric:3
1.5.4.19	Debe controlar cualquier switch virtual (vSwitch) que resida en diferentes hipervisores con lo que cuenta actualmente la compañía.	Cumple, "B" Software-Defined Networking: 2
1.5.4.20	Debe proporcionar 100% de integración directa e interoperabilidad con soluciones de cloud computing del tipo IaaS	Cumple, "B" Software-Defined Networking: 2
1.5.4.21	Debe soportar como mínimo 64.000 tenants independientes, cada uno de ellos con su propia topología virtual, bridge domain, instancias de routing virtual y políticas de seguridad.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals: 45
1.5.4.22	Debe soportar algún mecanismo de autenticación (como mínimo RADIUS, LDAP y Local).	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals: 152
1.5.4.23	Debe soportar mecanismos de filtrado en base a roles (Role-Based Access Control) para su integración con el resto de los sistemas de Informática.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals: 144
1.5.4.24	Debe ser capaz de filtrar el conteo de paquetes de modo tal que el desglose de los contadores permita al personal de operaciones usar en estas situaciones para ayudar en la resolución integral de problemas en sistemas, lo que permite que los administradores filtren clientes, grupos, terminales, etc. específicos en los que estén interesados y cuenten solamente los paquetes que coincidan con los criterios especificados.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals: 37
1.5.4.25	Debe ser capaz de contar cada paquete que ingresa y sale de la estructura y proporcionan contextualización en el conteo de paquetes, sin que esto afecte el rendimiento de la red. El hardware crítico de la red propuesta debe estar integrado de modo tal que puedan levantar esta funcionalidad sin degradar o consumir recursos que puedan dar penalidades en el rendimiento de la red	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:221

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.4.26	Debe ser capaz de conectar servicios L4-7 a perfiles ANP podemos mencionar que los servicios L4-7 pueden ser independientes de la ubicación; es decir, estos servicios se pueden conectar en cualquier lugar de la estructura de modo que, cuando el administrador conecte la función de servicio de una red de aplicaciones, la estructura debe determina automáticamente dónde están ubicados y aprovisiona todas las encapsulaciones que correspondan a esos nodos de servicio para automatizar el reenvío de las rutas de datos. Estas funciones de servicio L4-7 deben ser aprovisionadas en forma gráfica de servicio, además de que puede contener una o más funciones de servicio (firewall, equilibrador de cargas, etc.). Estos gráficos de servicio deben reflejar la conducta deseada de esa red de aplicaciones.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:169
1.5.4.27	Debe ser capaz de manejar al menos 10.000 puertos 1GE, 10GE, 40GE o 100GE.	Cumple, "B" Cisco Application Centric Infrastructure: 7
1.5.4.28	Debe proveer información de telemétrica de la red para que pueda ser analizada por otros productos de seguridad. Detallar.	Cumple, "B" Cisco Application Centric Infrastructure: 7
1.5.4.29	Debe soportar el espejado de tráfico (port mirroring) de cualquiera de sus interfaces para ser analizada por otras plataformas. Como mínimo se deberá soportar el espejado de 2 interfaces en simultáneo.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:70
1.5.4.30	Debe soportar 802.1Q VLANs	Cumple, "B" Cisco Application Centric Infrastructure: 3
1.5.4.31	Debe soportar mecanismos de filtrado de tráfico en Capas 2 a 7 con su correspondiente reporte o logging.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:91
1.5.4.32	Debe soportar la administración remota a través de SSHv2 o TLS1.2	Cumple, "B" Cisco Application Centric Infrastructure Security:3
1.5.4.33	Debe soportar la inspección dinámica de ARPs	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:223
1.5.4.34	Debe soportar la exportación de flujos de tráfico hacia herramientas externas de análisis del mismo	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:38
1.5.4.35	Garantía de (1) año como mínimo que incluye el software con upgrade y soporte, sin costo adicional asistencia por garantía, con mano de obra, con traslado desde el lugar de uso al proveedor y viceversa. No se aceptará sustitución temporal, el reemplazo debe ser definitivo	Cumple, Fs. 248.

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.4.36	Debe soportar aplicaciones y cargas de trabajo. Estar preparada para ser una infraestructura de uso general que se pueda personalizar en torno a la conectividad por medio de una política, de la automatización y de la programabilidad.	Cumple, "B" Cisco Application Centric Infrastructure:4
1.5.4.37	Debe soportar scripting de programación sobre los equipos.	Cumple, "B" Cisco Application Centric Infrastructure Fundamentals:188
1.5.4.38	Los técnicos de la empresa oferente deben estar certificados por el fabricante, y los mismos deben residir en el país. Se exigirá la presentación de los certificados de al menos 4 técnicos pertenecientes a la empresa autorizada por el fabricante. La documentación emitida por el fabricante; no debe exceder dos años de antigüedad.	Cumple Fs. 210-125

1.5.5 – SWITCHES DE CONEXIÓN A EDIFICOS DE COPACO

Descripción	Requerimiento mínimo	Ofertado
Marca	Especificar	Cumple Fs. 185
Modelo	Especificar	Cumple Fs. 185
Cantidad	7	Cumple Fs. 185
1.5.5.1	Cada equipo debe estar equipado de acuerdo a la arquitectura pretendida con al menos 24 interfaces 10/100/1000BaseTX y 2 interfaces de 10G con los siguientes alcances: • 2 interfaces de 10GE con alcance de 10 Km	Cumple, "B" Cisco Catalyst 3650 Series Switches – 3 y Fs. 185
1.5.5.2	Debe poseer fuentes eléctricas redundantes de 220/240VAC-50/60Hz	Cumple, "B" Cisco Catalyst 3650 Series Switches -3, 22
1.5.5.3	Debe soportar un mínimo de 32K de direcciones MAC	Cumple, "B" Cisco Catalyst 3650 Series Switches - 19
1.5.5.4	Debe poseer una capacidad de switching de al menos 85 Gbps	Cumple, "B" Cisco Catalyst 3650 Series Switches – 19
1.5.5.5	Debe soportar una capacidad de routing de al menos 68 MPPS de 64 bytes	Cumple, "B" Cisco Catalyst 3650 Series Switches - 19
1.5.5.6	Debe soportar una tecnología que mediante una interfaceespecífica le permita agruparse con otros equipos similares (Stacking) formando una única entidad desde el punto de vista de plano de control y de datos de al menos 200 puertos físicos. La interface para su agrupación no deberá poseer un ancho de banda menor a 160 Gbps	Cumple, "B" Cisco Catalyst 3650 Series Switches - 19
1.5.5.7	Debe soportar un mínimo de 24K de rutas IPv4 (aprendidas tanto por ARP como por protocolos de routing)	Cumple, "B" Cisco Catalyst 3650 Series Switches - 19

Lic. Jesús Ma. Ramirez O.
Geja. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.5.8	Debe soportar como mínimo 4096 VLAN IDs	Cumple, "B" Cisco Catalyst 3650 Series Switches - 19
1.5.5.9	Debe soportar Jumbo Frames de al menos 9198 bytes	Cumple, "B" Cisco Catalyst 3650 Series Switches - 19
1.5.5.10	Debe poseer un Sistema Operativo que permita mediante un upgrade de software (sin modificación del hardware) ser controlador de una futura red WiFi en cada edificio.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 28
1.5.5.11	Debe poseer al menos las siguientes certificaciones: • CISPR22 Class A • EN55022 Class A • ICES 003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS 13438 Class A • EN55024 • CISPR24 • KN24 • UL 60950-1 SecondEdition • EN 60950-1 SecondEdition • IEC 60950-1 SecondEdition	Cumple, "B" Cisco Catalyst 3650 Series Switches - 27
1.5.5.12	Debe soportar la retención de las direcciones MAC conectadas a un puerto y permitir solamente a esas direcciones la comunicación a través de ese puerto del Switch	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.13	Debe poder limitarse la cantidad de MACs retenida	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.14	Debe poseer un mecanismo de mitigación de MAC Address flooding.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.15	Debe proveer mecanismos de DHCP snooping.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.16	Debe soportar DAI (Dynamic ARP inspection)	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.17	Debe soportar un mecanismo de seguridad que evite el "Spoofing" de paquetes a nivel IP, MAC Address, puerto y VLAN	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.18	Debesoportar (RPF) Unicast Reverse Path Forwarding	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.5.19	Debe soportar el espejado de tráfico (port mirroring) de cualquiera de sus interfaces para ser analizada por otras plataformas. Como mínimo se deberá soportar el espejado de 2 interfaces en simultáneo.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 12
1.5.5.20	Debe soportar autenticación al menos en RADIUS, LDAP, 802.1X, MAC y Web	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.21	Debe soportar Virtual Private LANs Service	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15
1.5.5.22	Debe soportar configuración de notificación de mensaje de registro de eventos de tabla dirección MAC	Cumple, "B" Cisco Catalyst 3650 Series Switches - 13
1.5.5.23	Debe soportar filtrado de IGMP en puertos de entradas y de enlace.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.24	Debe soportar filtrado de tráfico en base a información de Capas 2 a 4 en IPv4 e IPv6	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.25	Debe soportar SSHv1, SSHv2, y SNMPv3	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.26	Debe soportar técnica que ayuden a proteger contra equipos conectados sin permisos y pudieran causar un rediseño del STP	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.27	Debe soportar una funcionadad que evite que, un equipo conectado se convierta en el switch raíz.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.28	Debe soportar IPv4 e IPv6 simultáneamente	Cumple, "B" Cisco Catalyst 3650 Series Switches - 2
1.5.5.29	Debe poder agruparse links físicos utilizando LACP entre los distintos miembros del stack	Cumple, "B" Cisco Catalyst 3650 Series Switches - 11
1.5.5.30	Debe poseer un mecanismo de protección de links con un tiempo de convergencia menor a 100ms. Detallar.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.31	Debe soportar Rapid Spanning Tree Protocol (RSTP) y Multiple Spanning Tree Protocol (MSTP) de acuerdo a la IEEE 802.1s/w tanto en el equipo stand alone como en todo el conjunto del stack.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 14
1.5.5.32	Debe soportar protocolos de ruting IPv4 e IPv6 tanto en unicast como en multicast utilizando al menos rutas estáticas, RIPv1, RIPv2, OSPF, BGPv4 e IS-ISv4 para IPv4 y OSPFv3 para IPv6 con prestaciones de equal-costrouting para balanceo de tráfico entre links tanto para el equipo stand alone como cualquier miembro de stack.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.5.33	Debe soportar VRF	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15
1.5.5.34	Debesoportar Policy-based routing (PBR)	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15
1.5.5.35	Debesoportar multicast routing al con Protocol-independent multicast (PIM), PIM sparse mode (PIM−SM), PIM dense mode (PIM-DM), PIM sparse-dense mode (PIM-SM/DM) y source-specific multicast (SSM)	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15
1.5.5.36	Debe soportar el clasificado de trafico mediante 802.1p CoS y DSCP por origen y destino de numero IPv4, por origen y destino de MAC address y por origen y destino de cualquier Puerto de Capa 4 (TCP/UDP)	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15
1.5.5.37	Debe soportar priorización de trafico mediante Shaped round robin (SRR) y también mediante una técnica que proporcione habilidad para eludir la congestión en las colas de entrada y salida antes de una interrupción	Cumple, "B" Cisco Catalyst 3650 Series Switches - 16
1.5.5.38	Debe soportar la determinación del ancho de banda de cualquier interfase (Committedinformationrate o CIR) en incrementos como minimo de 8 Kbps.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 16
1.5.5.39	Debe soportar el límite del ancho de banda de cualquier interfase (RateLimiting) en base a origen y destino de IPv4, origen y destino de MAC address, origen y destino de cualquier puerto de Capa 4 (TCP/UDP) o cualquier combinación de ellos	Cumple, "B" Cisco Catalyst 3650 Series Switches - 16
1.5.5.40	Debe soportar al menos 8 colas de prioridad por puerto y como mínimo y 2000 policers de QoS por switch.	Cumple, "B" Cisco Catalyst 3650 Series Switches - 15
1.5.5.41	Debe soportar el menos el siguiente conjunto de especificaciones de la IEEE: IEEE 802.1s IEEE 802.1w IEEE 802.11 IEEE 802.1x IEEE 802.1x-Rev IEEE 802.3ad IEEE 802.3af IEEE 802.3at IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS prioritization IEEE 802.1Q VLAN IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X RMON I y RMON II SNMPv1, SNMPv2c y SNMPv3	Cumple, "B" Cisco Catalyst 3650 Series Switches - 24
1.5.5.42	Debe cumplir con las normas de EnergyStar (reducción del consumo y el costo de la energía, además de proteger al medio ambiente utilizando productos y practicas especificas)	Cumple, "B" Cisco Catalyst 3650 Series Switches - 24

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.5.43	La Garantía debe ser de (1) año como mínimo para todo el equipo, incluyendo sin costo adicional asistencia por garantía, con mano de obra, repuesto y partes con traslado de equipos desde el lugar de uso al proveedor y viceversa. No se aceptará sustitución temporal, el reemplazo debe ser definitivo	Cumple Fs. 248
1.5.5.44	Todos los equipos deben ser nuevos de fabricación reciente, encontrarse en comercialización activa en el mercado para el que fueron diseñados	Cumple. Fs. 168
1.5.5.45	El Equipo debe estar acompañado de todos los accesorios necesarios para su correcta instalación y funcionamiento	Cumple. Fs. 168
1.5.5.46	El reemplazo de partes o del equipo en caso de daños, debe ser en un plazo máximo de al día siguiente útil, una vez adjudicado se exigirá una nota del fabricante donde demuestre dicho compromiso	Cumple. Fs. 168
1.5.5.47	El servicio de instalación comprende: Instalación física en el rack de la compañía, Configuración del equipo de manera a que pueda ser usada dentro de la infraestructura existente y a ser provista en este llamado de acuerdo a la necesidad de COPACO.	Cumple. Fs. 168

1.5.6 – FIREWALLS

Descripción	Requerimiento mínimo	Ofertado
Marca	Especificar	Cumple. Fs. 169
Modelo	Especificar	Cumple. Fs. 169
Cantidad	2	Cumple. Fs. 169
1.5.6.1	Cadaequipodebeestarequipadodeacuerdoalaarquitecturapretendidaconalmenos8interfaces10/100/1000BaseTX,3interfaces1000BaseSXy3interfacesde1G1000Base LXconalcancede10Km.	Cumple, "B" Cisco ASA with FirePOWER -7 y Fs. 169
1.5.6.2	Debe soportar un Throughput mínimo para control de aplicaciones genéricas de 1 Gbps y de 650 Mbps aplicando reglas de IPS.	Cumple, "B" Cisco ASA with FirePOWER - 5
1.5.6.3	Debe soportar un Throughput mínimo para control de aplicaciones HTTP de 375 Mbps considerando paquetes de 440 bytes	Cumple, "B" Cisco ASA with FirePOWER - 5
1.5.6.4	Debe soportar un mínimo de 500.000 sesiones concurrentes	Cumple, "B" Cisco ASA with FirePOWER - 5
1.5.6.5	Debe soportar una cantidad mínima de 20.000 nuevas conexiones por segundo	Cumple, "B" Cisco ASA with FirePOWER - 5
1.5.6.6	Debe soportar como mínimo 3.000 aplicaciones bien conocidas	Cumple, "B" Cisco ASA with FirePOWER - 5
1.5.6.7	Debe soportar un sistema de filtrado de URLs basado en la reputación y categorización de las mismas de al menos 280 Millones de URLs categorizadas en al menos 80 categorías	Cumple, "B" Cisco ASA with FirePOWER - 5

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.6.8	Debe poseer un Sistema de: administración, configuración, reportes, monitoreo y logging centralizado en el propio dispositivo y que permita la visualización grafica de: • Actividad y estado general de la red • Usuarios y detalles de las aplicaciones que ejecutan • Comunicación entre máquinas virtuales • Vulnerabilidades y amenazas • Malwares • Correlación de todos estos eventos	Cumple, "B" Cisco ASA with FirePOWER –2
1.5.6.9	Debe soportar un Throughput mínimo de inspección de trafico UDP de 2 Gbps	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.10	Debe soportar un Throughput mínimo de inspección de trafico TCP multiprotocolo (HTTP, SMTP, FTP, IMAPv4, BitTorrent y DNS) de 1 Gbps	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.11	Debe soportar un Throughput mínimo de VPNs 3DES/AES de 300 Mbps	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.12	No debe poseer un límite en la cantidad de usuarios y/o nodos a inspeccionar y/o proteger.	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.13	Debe soportar al menos 750 peers de VPNsIPSec (site to site)	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.14	Debe soportar al menos 200 VLANs	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.15	Debe soportar como mínimo 2 contextos virtuales customizables por COPACO y poder expandirse en el futuro al menos hasta 20 sin necesidad de cambiar el hardware	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.16	Debe soportar como mínimo los modos Activo/Activo y Activo/Standby de operación HA	Cumple, "B" Cisco ASA with FirePOWER – 6, 10
1.5.6.17	Debe poseer al menos 1 slot para expansión de interfaces	Cumple, "B" Cisco ASA with FirePOWER–7
1.5.6.18	Debe poseer al menos 1 interface Gigabit Ethernet, 2 puertos USB y una interface serial dedicadas amanagement	Cumple, "B" Cisco ASA with FirePOWER – 7
1.5.6.19	Debe poseer un disco de estado sólido para almacenamiento de configuraciones y trafico temporal de 120 GB	Cumple, "B" Cisco ASA with FirePOWER – 7
1.5.6.20	Debe poseer una memoria RAM y una memoria Flash de al menos 8 GB cada una.	Cumple, "B" Cisco ASA with FirePOWER – 7
1.5.6.21	Debe ser una solución de software y hardware basado en appliances, el cual tenga la capacidad de realizar su monitoreo y prevención de manera en línea además de ser de un sólo fabricante.	Cumple, "B" Cisco ASA with FirePOWER – 13
1.5.6.22	Debe permitir la autenticación de usuarios y administradores a través de integración con RADIUS.	Cumple, "B" 200204-

Lic. Jesús Ma. Ramírez O.
Jefe de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
STI

		Integration-of-FireSIGHT-System-with-ACS – 1
1.5.6.23	El monitoreo debe ser transparente para los usuarios y operar en la capa 2 del modelo de OSI, independiente de las interfaces, no requieren de una dirección IP ni una dirección MAC.	Cumple, "B" ASA FirePOWER Module User Guide – 1-2
1.5.6.24	Debe permitir una inspección inteligente, basándose en el análisis estadístico de flujo de datos en la red, optimizando el proceso para identificar y proteger la red contra ataques.	Cumple, "B" ASA FirePOWER Module User Guide – 1-2
1.5.6.25	El dispositivo debe permitir configuración en modo transparente; es decir, de detección en línea, pero sin bloquear tráfico. El sistema sólo alerta que eventos serían bloqueados.	Cumple, "B" ASA FirePOWER Module User Guide – 1-2
1.5.6.26	Debe soportar un motor de detección que inspeccione no solo los detalles de la capa de red, además información residente en cabeceras de los paquetes, a través de una gama amplia de protocolos.	Cumple, "B" ASA FirePOWER Module User Guide – 23-88
1.5.6.27	Debe permitir la configuración de modo transparente para todo el tráfico o apenas para paquetes especificados por dirección IP, protocolo, VLAN ID incluyendo frames 802.1q.	Cumple, "B" ASA FirePOWER Module User Guide – Chapter Running H/F 1
1.5.6.28	Debe permitir la creación de reglas y filtros de acceso.	Cumple, "B" ASA FirePOWER Module User Guide – 7-1
1.5.6.29	Debe tener la capacidad de detectar tráfico anómalo o vulnerabilidades en aplicaciones.	Cumple, "B" ASA FirePOWER Module User Guide – 11-10
1.5.6.30	Debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola política por interfaz).	Cumple, "B" ASA FirePOWER Module User Guide – 2-32
1.5.6.31	Debe contar como mínimo con las siguientes técnicas de análisis de trafico: identificación del protocolo a través del puerto utilizado; identificación de protocolos que utilizan puertos aleatorios; identificación de protocolos en forma independiente del puerto utilizado.	Cumple, "B" ASA FirePOWER Module User Guide – 6-9
1.5.6.32	Debe ser resistente a diversas técnicas de URL obfuscation en ataques basados en HTML.	Cumple, "B" ASA FirePOWER Module User Guide – 15-13
1.5.6.33	Debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.	Cumple, "B" ASA FirePOWER Module User Guide – 4-14
1.5.6.34	Debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, enviar correo electrónico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.	Cumple, "B" ASA FirePOWER Module User Guide – 19-7

Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.6.35	Debe soportar el modo de implementación Inline, en donde se monitorea y protege los segmentos de datos, con tráfico activo de red pasando por el, lo que permite prevenir los ataques de estos segmentos y bloqueado en tiempo real.	Cumple, "B" ASA FirePOWER Module User Guide – 14-5
1.5.6.36	Debe soportar el modo de implementación Pasivo, permitiendo el monitoreo a través de los HUBs y / o puertos port mirroring de switches, siendo el tráfico de red reflejando en el, lo que le permite monitorear el tráfico de ataques.	Cumple, "B" ASA FirePOWER Module User Guide – 18-1
1.5.6.37	Deberá soportar la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.	Cumple, "B" ASA FirePOWER Module User Guide – 11-1
1.5.6.38	Debe de soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP) sobre SIP.	Cumple, "B" ASA FirePOWER Module User Guide – 7-5
1.5.6.39	Debe tener la capacidad de construir un perfil para la identificación de dispositivos móviles, para lo cual debe incluir la siguiente información: track usuarios, vulnerabilidades, aplicaciones. (sin necesidad de hardware o software separado).	Cumple, "B" FireSIGHT Management Center 4
1.5.6.40	Deberá ser capaz de hacer recomendación de afinación (tuning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.	Cumple, "B" ASA FirePOWER Module User Guide – 6-1
1.5.6.41	Debe proveer la detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero, como una funcionalidad dentro del mismo IPS y sin necesidad del uso de aplicaciones adicionales como sistema de detección de anomalías o scanners.	Cumple, "B" ASA FirePOWER Module User Guide – 23-5
1.5.6.42	Debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.	Cumple, "B" ASA FirePOWER Module User Guide – 4-6
1.5.6.43	Deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un análisis a través de NMAP, este deberá ser incluido como parte del mismo módulo de correlación.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1183
1.5.6.44	Debe de proveer monitoreo de segmentos de red en modo promiscuo analizando encabezamiento (header) y el área de datos (payload) de los paquetes que transitan en la red (deep packet inspection), detectando ataques y tráfico no autorizado o sospechoso.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 791
1.5.6.45	Deberá identificar vulnerabilidades de los host de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1415
1.5.6.46	Debe tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.	Cumple, "B" Firepower Management Center Configuration

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferrei
Jefe Departamento Soporte Técnico

		Guide, Version 6.0: 1107, 1594
1.5.6.47	Debe poder realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y .ENC (estándar para el software de análisis de protocolos). El archivo puede ser usado par hacer playback del ataque. Se aceptaran propuestas que consideren la captura de tráfico para el análisis de evidencia en formato compatible con libpcap (compatible a su vez con TCPDUMP), y opcionalmente en formato ENC.	Cumple, "B" Introduction to Cisco ASA: 54
1.5.6.48	Debe permitir un análisis dinámico y en tiempo real en para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros: Redes existentes; Host activos; Nuevos Host o servers en la red; Nuevas MAC address en la red; Maquinas virtuales nuevas o existentes; Sistema operativo de cada uno de los host identificados; Servicios activos de cada uno de los host identificados; Aplicaciones activas de cada uno de los host identificados; Vulnerabilidades de cada uno de los host identificados.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1622
1.5.6.49	El dispositivo deberá poder crear perfiles de trafico con reglas especificas para monitorear el tráfico entre dos host de la red y crear una alarma cuando cierto umbral sea rebasado.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1331
1.5.6.50	Debe ser capaz de recopilar información pasiva de los hosts de la red y sus actividades, tales como: sistema operativo; servicios, puertos abiertos; aplicaciones y vulnerabilidades, permitiendo la correlación de datos, eliminación de falsos positivos y políticas de cumplimiento. (sin necesidad de hardware o software separado).	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1347
1.5.6.51	Debe tener la capacidad de ser administrado a través de conexiones SSH, CLI y HTTPS.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1741, 1745
1.5.6.52	Debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1351
1.5.6.53	Debe ser capaz de proporcionar mayor visibilidad sobre como se consume el ancho de banda, ya sea por dirección o puerto, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red. (sin necesidad de hardware o software separado).	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 205
1.5.6.54	Debe soportar sincronización de horario a través de NTP (Network Time Protocol).	Cumple, "B" Firepower Management Center Configuration Guide, Version

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Dtv. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
STI

		6.0: 206
1.5.6.55	Debe proveer la capacidad de realizar un respaldo de la configuración de la plataforma en tiempo real, o por un horario definido.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 141
1.5.6.56	Debe soportar IP Reputation, además debe permitir la creación de listas negras y listas blancas y debe contar con una base de datos propia, pero además debe permitir el poder configurar cualquier base de datos de terceros.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1192
1.5.6.57	Debe contar con al menos las siguientes de objetos de IP Reputation: Bots, CnC, Malware, Attacker, Suspicious.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 661
1.5.6.58	Debe proporcionar la capacidad inteligente para correlacionar los eventos de intrusión priorizándolo por tipo de bandera de impacto con diferentes categorías de alertas.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 944
1.5.6.59	Debe soportar integración a través del directorio activo y/o LDAP para determinar el comportamiento de la red a través de direcciones IP asociadas a los eventos sospechosos.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1223
1.5.6.60	Debe proporcionar un completa visión del comportamiento de la red para detectar nuevas amenazas, incluyendo la capacidad de establecer líneas de base de trafico a través de técnicas de flujos.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1155
1.5.6.61	Debe contar con al menos las siguientes categorías de reglas: File-Executables; DoS; DoS Exploit; P2P; Pua-Adware; Scada; Web-IIS; SQL; Indicator-Obfuscation; Sensitive-Data; RPC; Botnet.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 661, 1433,1578,
1.5.6.62	Debe poder soportar reglas por plataforma tal como: Apple; Cisco; Compaq; HP; IBM; Juniper; Microsoft; Nokia; RedHat; Suse; Sun; Juniper.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1172

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico

1.5.6.63	Debe soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source IP, Destination IP, Source port; Destination port; Rule overhead, Metadata.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1406
1.5.6.64	Debe contar con la capacidad de crear reglas que permitan enviar trafico directamente a través del dispositivo sin que sea inspeccionado.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1551
1.5.6.65	Debe contar con la capacidad de crear un perfil de trafico, con base al fuljo de datos recolectados durante un periodo especifico.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1683
1.5.6.66	Debe soportar interfaces en modo MDI/MDIX (Medium Dependent Interface).	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 393
1.5.6.67	Debe tener de forma nativa recursos de detección y prevención de ataques de DoS y DDoS. Esta capacidad debe permitir el control de comunicaciones por mecanismos "Rate-based" para condiciones de Syn-Flood y control de conecciones simultaneas máximas para direcciones IP, CIDR.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 956
1.5.6.68	Debe soportar la creación de objetos por nombre ya sea por: network, puertos, Vlan, URL, filtros de aplicación y zonas de seguridad.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1033
1.5.6.69	Debe poder controlar las aplicaciones en cualquier puerto.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 938
1.5.6.70	Debe detectar mínimo 1700 aplicaciones y categorizarlas por riesgo y relevancia empresarial.	Cumple, "B" Cisco ASA with FirePOWER : 1
1.5.6.71	Debe estar basado sobre firmas en vulnerabilidades permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1626

Lic. Jesus Ma. Ramirez O.
Gerente de Tecnologia de Información

Amancio Daira Ferreira
Jefe Departamento Soporte Técnico
STI

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

1.5.6.72	Debe controlar la detección de archivos a través de las acciones permitiendo el acceso total, medio bloqueo o el reinicio .	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 773
1.5.6.73	Debe permitir la funcionalidad de gestión SNMP e integrarse a productos de red de terceros para proporcionar indicadores clave de estado operacional a grupos de operaciones de red y de operaciones de seguridad.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 502
1.5.6.74	Debe de proveer la opción de consulta, de un histórico de los eventos sucedidos en los equipos ofertados desde la consola principal, con el fin de realizar análisis forense.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1147, 1654
1.5.6.75	Debe permitir soportar monitoreo en redes MPLS.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1569
1.5.6.76	Debe proteger contra ataques sobre aplicaciones Web como: shell command injections, Server-site injection, cross-site scripting, directory traversal.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1203
1.5.6.77	Debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 226
1.5.6.78	Debe contar con la capacidad de crear un perfil de tráfico, con base al fuljo de datos recolectados durante un periodo especifico.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 831
1.5.6.79	Debe ser capaz de reducir significativamente el esfuerzo del operador y la aceleración de respuesta a las amenazas por dar prioridad a las alertas de forma automática.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 831
1.5.6.80	Debe ser capaz de proporcionar de forma automática los adecuados controles permitiendo la protección el tráfico enviado a través de puertos de comunicación no estándares.	Cumple, "B" Firepower Management Center Configuration

Lic. Jesús Ma. Ramírez O.
Jefa de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

		Guide, Version 6.0: 892
1.5.6.81	Deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad para emitir una alarma cuando algunos de los servicios no permitidos por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 906
1.5.6.82	Debe ser capaz de esperar pasivamente la recopilación de información sobre los flujos de sesión para todos los hosts, incluyendo el tiempo inicio/fin, puertos, servicios y cantidad de datos.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1186
1.5.6.83	Deberá ser capaz de crear un mapa de flujo de tráfico entre host de la red, para guardar registro de la cantidad de tráfico entre los dispositivos de la red.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 478
1.5.6.84	Deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 791
1.5.6.85	Deberá permitir una integración automática para realizar un cambio de configuración o enviar información a módulos de terceros como: Scanners de vulnerabilidades; SEM/SIEM systems; Firewall; Routers; Switches.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1254
1.5.6.86	Deberá incluir un sistema de integración con directorio activo, del mismo fabricante, que provea las siguientes características: - Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente. - Deberá permitir tener la información de contacto de los usuarios que están siendo atacados. - Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión. - Deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario. - Deberá de poder generar un mapa de tráfico generado/recibido por usuario. - Deberá ser capaz de mantener un mapa de los usuarios, ip actual, tipo de aplicación usada, y un historial de las IPS que ese usuario ha usado en el tiempo.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1654
1.5.6.87	Deberá de soportar syslog para eventos de filtrado y errores del sistema.	Cumple, "B" Firepower Management

		Center Configuration Guide, Version 6.0: 1397
1.5.6.88	Deberá de soportar la capacidad de generar alertas a través de: syslog, correo electrónico y SNMP.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1400
1.5.6.89	Debe soporta creación de ACL (Access Control List – Lista de Control de Acceso), especificando las direcciones IP que se les permite comunicarse con la dirección.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1740
1.5.6.90	Deberá tener una funcionalidad de "packet level" para realizar actividades de análisis forense.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 9
1.5.6.91	Debe tener la capacidad de creación de reglas basadas en: segmento monitoreado (puerto del appliance); dirección IP origen y destino; puertos origen y destino.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1305
1.5.6.92	Deberá soportar el remontaje de paquetes TCP fragmentados.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1604
1.5.6.93	Deberá soportar la búsqueda de firmas por nombre a través de la interfaz gráfica.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 747
1.5.6.94	Deberá soportar la desfragmentación de paquetes IP fragmentados y/o coincidentes.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1102
1.5.6.95	Debe de soportar inspección de tráfico en GRE.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1554

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.6.96	Deber contar con cobertura de filtros que protejan las vulnerabilidades de internet Explorer.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1624
1.5.6.97	Debe soportar la creación de reglas rápidas (Fast-path) que permita el envío de trafico directamente a través del dispositivo sin inspección.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 386
1.5.6.98	Debe soportar geolocalización; permitiendo obtener al menos la siguiente información: país, código postal, longitud, latitud, zona horaria.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 714
1.5.6.99	Debe permitir bloquear tráfico por geolocalización; ya sea por país o continente.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 718
1.5.6.100	El dispositivo debe hacer la inspección de emails y sus adjuntos para detectar malware conocido y desconocido.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 164
1.5.6.101	El dispositivo debe detectar y proteger contra malware conocido y desconocido mientras se utiliza el browser para navegar sitios web.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1203
1.5.6.102	El dispositivo debe utilizar información de reputación de URL para mejorar sus niveles de detección y protección de amenazas malwares conocidas y desconocidas.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1318
1.5.6.103	El dispositivo debe permitir la detección y prevención de comunicaciones malwares en aplicaciones conocidas y desconocidas, esto incluye la utilización de protocolos http y smtp.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 782
1.5.6.104	El dispositivo debe permitir la detección, prevención y el registro log de comunicaciones malware en paquetes UDP y TCP.	Cumple, "B" Firepower Management Center Configuration

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico

		Guide, Version 6.0: 1119
1.5.6.105	El dispositivo debe utilizar protocolo HTTPS para las comunicaciones con sus recursos de análisis externos (cloud).	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 288
1.5.6.106	El dispositivo debe correlacionar e alertar sobre malwares que utilicen vectores de ataque diferentes (email, web browsing, filetransfer).	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 10
1.5.6.107	El dispositivo debe permitir la detección y prevención de malwares en archivos: 7z, ACCDB, ARJ, Binary_data, java_bytecode, BINHEX, BZ (bzip2), CPIO_CRC, CPIO_NEWC, CPIO_ODC, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE (powerpoint, word, excel), OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC.	Cumple, "B" Cisco ASA with FirePOWER : 1
1.5.6.108	El dispositivo debe permitir la detección y control de uso de los siguientes tipos de archivos: 7z, ACCDB, ARJ, Binary_data, java_bytecode, BINHEX, BZ (bzip2), CPIO_CRC, CPIO_NEWC, CPIO_ODC, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE (powerpoint, word, excel), OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC, 9XHIVE, DMG, ISO, NTHIVE, PCAP, PGD, REG, SYLKc, SYMANTEC, VMDK, BMP, DWG, IMG_PICT, MAYA, PSD, WMF, SCRENC, UUENCODED, EPS, AUTORUN, MACHO, RPM, TORRENT, AMF, AMR, ASF, DICM, FFMPEG, FLAC, FLIC, FLV, IVR, M3U, MIDI, MKV, MOV, MP3, MP4, MPEG, OGG, PLS, R1M, RA, REC, RIFF, RIFX, RMF, S3M, SAMI, SMIL, SWF, WAV, WEBM, HLP, MWL, ONE, WP, XLW, MSSZDD.	Cumple, "B" Cisco ASA with FirePOWER : 1
1.5.6.109	El dispositivo debe permitir la creación de blacklists y whitelist.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 27
1.5.6.110	El dispositivo deberá de inspección la presencia de malware a nivel de archivos que utilicen los siguientes protocolos de aplicación: HTTP, SMTP, IMAP, POP3, FTP,SMB.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 10
1.5.6.111	El dispositivo debe permitir la creación de reglas de detecciones customizadas para archivos.	Cumple, "B" Firepower Management Center Configuration Guide, Version

Lic. Jesús Ma. Ramirez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico

		6.0: 770
1.5.6.112	El dispositivo debe detectar y bloquear malware desconocido de forma dinámica (on-demand) en file shares (protocolo CIFS).	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 455
1.5.6.113	El dispositivo debe permitir el administrador ver todos los ataques contra un sistema específico.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1739
1.5.6.114	El dispositivo debe permitir obtener automáticamente el HASH para el malware y/o archivo.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 10
1.5.6.115	El dispositivo debe permitir capturar amuestra del archivo siendo transferido.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 27
1.5.6.116	El dispositivo debe permitir hacer log de los URL's cuando el malware es detectado durante comunicación con websites.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 783
1.5.6.117	El dispositivo debe permitir automáticamente capturar PCAP's para toda la actividad de ataques malware vía red.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1216
1.5.6.118	El dispositivo debe permitir automáticamente ver y registrar datos detallados de comunicaciones para toda la actividad de red que pueda estar relacionada con malwares.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 759
1.5.6.119	El dispositivo deberá ser capaz de mostrar la trayectoria de archivos de forma gráfica, histórica y cada uno de los eventos asociados a las detecciones de uno o más archivos malwares y sus comunicaciones dentro de la red, siendo capaz de identificar las remediaciones a los host que estén infectados.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 763
1.5.6.120	El dispositivo deberá de ser capaz de entregar un reporte visual, histórico y detallado de la trayectoria de todos los sistemas protegidos y permitir identificar archivos de malware descargados, y/o cualquier tipo	Cumple, "B" Firepower Management Center

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Duira Ferreira
Jefe Departamento Soporte Técnico

	de aplicación dañina y sus comunicaciones.	Configuration Guide, Version 6.0: 763
1.5.6.121	El dispositivo deberá tener un servicio de actualización y sincronización de nuevos hallazgos de malware en archivos previamente vistos o detectados en el ambiente, este servicio deberá de operar globalmente y deberá permitir una capacidad de análisis continúa en el ambiente protegido.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 769
1.5.6.122	El dispositivo deberá ser capaz de analizar archivos anexos (attachments) incluidos en correos electrónicos así como URL que estén incluidos en el cuerpo del correo electrónico.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 992
1.5.6.123	El dispositivo debe correlacionar informaciones de reputación, comunicaciones malware generadas por aplicaciones y otros eventos de infección detectados en el ambiente para crear incidentes que indican la quiebra de seguridad o comprometimiento de hosts en el ambiente protegido.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1687
1.5.6.124	El dispositivo debe tener de forma nativa recursos de detección y prevención de intrusos de red de próxima generación (NGIPS) donde debe ser posible la customización de detecciones de ataques Malware y comunicaciones CNC hechas por el propio administrador.	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 1230
1.5.6.125	El dispositivo debe documentar la trayectoria del archivo, que permite identificar el movimiento lateral de un malware dentro de la red afectada. Estas informaciones deben incluir: a. fecha y hora de la primera vez que el malware fue identificado, tanto en la red como en la cloud de seguridad colectiva; b. fecha y hora de la última vez que el malware fue identificado, tanto en la red como en la cloud de seguridad colectiva; c. identificar en cada host contaminado, la hora de contaminación y cual fue la forma de identificación (archivo creado, copiado, movido, ejecutado y escaneado); d. Nombre del archivo utilizado para contaminación	Cumple, "B" Firepower Management Center Configuration Guide, Version 6.0: 760
1.5.6.126	Debe poseer al menos una fuente de alimentación de 200 a 240 VAC en 50/60Hz.	Cumple, "B" Cisco ASA with FirePOWER : 8

1.5.7 – RACKs

Descripción	Requerido mínimo	Ofertado
Marca	Especificar	Cumple, Fs. 178
Modelo	Especificar	Cumple, Fs. 178
Cantidad	2 (dos)	Cumple, Fs. 178

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Duira Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.7.1	Rack o Gabinete para alojamiento de equipos informáticos en general, color Negro o Gris. Deberá ser cerrado con puertas micro perforadas. Capacidad de 42U universal para equipos de telecomunicaciones. Las partes deberán ser tratadas por inmersión en caliente y electroforesis con tratamiento anti polvo.	Cumple, "B" Cisco R Series Racks : 2
1.5.7.2	Compatibilidad con estándares universales y equipos de telecomunicaciones	Cumple, "B" Cisco R Series Racks : 1
1.5.7.3	Dispositivo de fácil apertura de puertas, puertas frontal y posterior.	Cumple, "B" Cisco R Series Racks : 1
1.5.7.4	Paneles laterales desmontables con cerraduras, dos paneles independientes por cada lado	Cumple, "B" Cisco R Series Racks : 1
1.5.7.5	Profundidad 1100mm	Cumple, "B" Cisco R Series Racks : 2
1.5.7.6	Panel superior para entrada de cables, y para soporte de ventiladores, con sus accesorios: pernos, tornillos, etc.	Cumple, "B" Cisco R Series Racks : 2
1.5.7.7	Marcación de unidades en los rieles frontales y posteriores (recomendado)	Cumple, "B" Cisco R Series Racks : 2
1.5.7.8	Puertas laterales desmontables.	Cumple, "B" Cisco R Series Racks : 1
1.5.7.9	Puertas micro perforadas en un 70% como mínimo.	Cumple, "B" Cisco R Series Racks : 1
1.5.7.10	Las puertas traseras deberán ser de doble hoja para ahorrar espacio y facilitar trabajos de accesos en lado posterior.	Cumple, "B" Cisco R Series Racks : 1
1.5.7.11	Puerta frontal y posterior completamente perforadas	Cumple, "B" Cisco R Series Racks : 1
1.5.7.12	Dispositivos de cerraduras para las puertas frontales, posteriores, y puertas laterales.	Cumple, "B" Cisco R Series Racks : 1
1.5.7.13	Debe soportar hasta 1300Kg	Cumple, "B" Cisco R Series Racks : 2
1.5.7.14	Canaletas verticales incluidas en cada rack	Cumple, Fs. 179
1.5.7.15	Canaletas horizontales incluidas en cada rack	Cumple, Fs. 179
1.5.7.16	Deberá contar con sus accesorios de montaje, como set kit de tornillos, cintillos, velcro, soportes y demás.	Cumple, Fs. 179

Lic. Jesús Ma. Ramírez O.
Gcia. de Tecnología de Información

Guillermo Godoy Aldereta
Jefe Div. Redes y Comunicaciones

Amancio Dutra Ferreira
Jefe Departamento Soporte Técnico
GTI

1.5.7.17	Conectores eléctricos inteligentes de 24 tomas (mínimo) disponibles a lo largo del equipo, monitoreable, SNMP. Dos por cada Rack	Cumple, Fs. 179
1.5.7.18	El Oferente deberá realizar la instalación de los bienes ofertados considerando todas las especificaciones técnicas, a través de mano de obra especializada para instalación, conexión y puesta en marcha de los equipos	Cumple, Fs. 179
1.5.7.19	Todos los bienes deben ser nuevos, de fabricación reciente, encontrarse en comercialización	Cumple, Fs. 179

Sección VII.
Anexos

ANEXO Nº I

Cualquier otro documento adicional requerido.	
• Carta del fabricante en donde certifique la interoperabilidad de todos sus componentes para dar cumplimiento al punto 2.3 de la Sección III Especificaciones Técnicas.	Cumple Fs. 226
• Documentos o Cartas emitidas por clientes, al menos 3 referencias del fabricante a nivel regional (Paraguay, Argentina, Chile, Brasil y Uruguay) de implementaciones e instalaciones iguales o superiores que utilicen exactamente el mismo equipamiento propuesto en esta Licitación, a fin de dar cumplimiento a lo requerido en los punto 2.4 de la Sección III - Especificaciones Técnicas.	Cumple Fs. 127-133
• Experiencia en provisiones similares, la misma se demostrará mediante documentos o cartas emitidas por clientes que deberán ser con fecha actualizada aun cuando la provisión se haya hecho en años anteriores, además en el documento deberá constar el listado de los equipos provistos por la empresa oferente.	Cumple Fs. 60-125, 221
• Listado de Ingenieros Certificados por el Fabricante, 4 (cuatro) a Nivel Asociado y 4 (cuatro) a Nivel Profesional.	Cumple Fs. 210-125
• Certificación avanzada emitida por el fabricante en Data Center u otro igual o mejor.	Cumple Fs. 231
• Carta autorización del fabricante con fecha actual, dirigida a COPACO haciendo mención a la presente Licitación.	Cumple Fs. 187-192
• Carta del fabricante en la cual se garantiza que los equipos contarán con repuestos al menos por 5 años posteriores a la instalación de los equipos ofertados.	Cumple Fs. 195
• Garantías para todos los equipos y software deberán ser de 12 (doce) meses.	Cumple Fs. 248
• Copia autenticada del Certificado de Calidad ISO serie 9001:2008.	Cumple

Lic. Jesús Ma. Ramírez O.
Gerente de Tecnología de Información

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones

Amancio Daira Ferreira
Jefe Departamento Soporte Técnico
GTI

	Fs. 214-219
• Deberá presentar reportes expedidos por terceras partes (no por el fabricante) en donde se certifique que los equipos cumplen con el perfomance declarado.	Cumple 197-209
• Constancia de visitas emitida por la convocante o Declaración Jurada de Conocer los Locales de Copaco S.A.	Cumple Fs.58
• Plan de Capacitación, de conformidad a lo requerido en la *Sección III. Numeral 2 "Consideraciones Generales"*. en los puntos 2.19 y 2.20.	Cumple Nota 26/10/16
• Catálogos Técnicos de los suministros ofertados.	Cumple Fs. 249
• Certificado de Origen Nacional expedido por el Ministerio de Industria y Comercio.	N/A

Con relación a la observación realizada en el **Acta de Apertura de Ofertas Nro. 29/2016** por el representante de **LOGICALIS PARAGUAY S.A**, donde objeta que la firma **INFOCENTER S.A** no presenta la Certificación Avanzada en **DATA CENTER** o similar emitida por el fabricante; esta Comisión no puede apartarse de lo establecido en el Pliego de Bases y Condiciones donde se refiere a ***las Especificaciones Técnicas en su punto 2 - CONSIDERACIONES GENERALES y en sus puntos 2.6 y 2.7 respectivamente expresa lo siguiente:***

> **2.6** *-Debe contar con ingenieros certificados por el fabricante, al menos 4 en nivel asociado y 4 en nivel profesional, se deben incluir los certificados respectivos, la entidad tiene la posibilidad de exigir en caso sea necesaria las planillas de IPS para corroborar que dichos empleados pertenezcan a la empresa oferente.*
>
> **2.7** *-Debe tener la certificación avanzada por el fabricante en Datacenter o similar.*

Se distingue a prima facie que son los profesionales que pertenecen a las empresas los que deberán contar con la Certificación Avanzada, ya que se trata de una **Contratación de Servicios.** atendiendo a la naturaleza del servicio serán los Ingenieros de la empresa oferente los encargados de realizar los trabajos técnicos donde se pretende dotar a la Compañía de una nueva tecnología de comunicación para los Datacenter del Sitio uno, (Primario) de la Gerencia TI, como así también al de la Central Uno, Sitio dos (Secundario o de Contingencia) .- Y según se constata con las documentaciones presentadas por la Empresa **INFOCENTER S.A**, con relación a los Profesionales Certificados, este requisito es cumplido por la misma.

De conformidad a lo establecido en el Art. Nº 59 del Decreto Nº 21909/03, se ha procedido a solicitar a la empresa **INFOCENTER S.A**, la presentación de documentos de carácter formal:

a) Nota de fecha 19 de octubre de 2016, se ha solicitado la presentación de los siguientes documentos:

- Catálogo Switch Secundario, Marca: Cisco Systems, Modelo: Cisco Nexus 93180.
- Catálogo Servidor para Controlador SDN, Marca: Cisco Systems, Modelo: UCS C220.
- Catálogo Rack, Marca: Cisco Systems, Modelo: Cisco RACK-UCS2

Lic. Jesús Ma. Ramírez O.
Dpto. de Tecnología de Información

Respondiendo la misma en la Nota de fecha 21 de octubre de 2016 (Carpeta "A" DataSheets y WhitePapers).

b) Nota de fecha 21 de octubre de 2016, se ha solicitado la presentación de los siguientes documentos:

- Plan de Capacitación, de conformidad a lo requerido en la *Sección III. Numeral 2 "Consideraciones Generales"*. en los puntos 2.19 y 2.20.
- Certificado de Origen Nacional expedido por el Ministerio de Industria y Comercio.

Respondiendo la misma en la Nota de fecha 26 de octubre de 2016.

c) Nota de fecha 28 de octubre de 2016, se ha solicitado la ampliación de los siguientes documentos:

- Switches Principales
- Switches Secundarios
- Controlador SDN
- Firewalls

Respondiendo la misma en la Nota de fecha 31 de octubre de 2016 ("B" CD Infocenter Catálogo).

Por todo lo expuesto y en virtud al análisis de las Especificaciones Técnicas, la Sección VII - Anexo 1 y las documentaciones presentadas, concluimos que la Empresa **INFOCENTER S.A.** **cumple** con todos los requisitos de la evaluación técnica.

Lic. Guillermo Godoy
Jefe Div. Redes de Comunicación
Dpto. Técnico – GTI

Sr. Amancio Dutra
Jefe de Dpto. Soporte Técnico - GTI

Lic. Jesús Ramírez
Gcia. de Tecnología de Información
Coordinador

Foliado del 01 al 47, inclusive

Adjuntos:

- Carpeta "A" DataSheets y WhitePapers Pg.: 210.- 1 (Un) CD.-
- Nota Infocenter. Pg.: 3.-
- Memorándum Nº 4. Pg.: 4.- 1 (Un) CD ("B" Infocenter Catálogo).-

Guillermo Godoy Alderete
Jefe Div. Redes y Comunicaciones