Poder Judicial del Estado de Tabasco
Tribunal Superior de Justicia
Comité de Compras del Poder Judicial

"25 de Noviembre, Conmemoración del Día Internacional de la Eliminación de la Violencia contra la Mujer"

OFICIO No. TSJ/OM/DC/095/2015

Villahermosa, Tabasco, Junio 26, de 2015.

ASUNTO: INVITACIÓN A LICITACIÓN SIMPLIFICADA MENOR PARA EL FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012).

ASESORES EN SISTEMAS ELECTRÓNICOS DEL SURESTE, S.A. DE C.V.
ERNESTO MALDA NO. 431-63 COL. LINDA VISTA
VILLAHERMOSA, TABASCO C.P. 86038
TEL. 3 16 76 34.

Con fundamento en lo dispuesto por los artículos 22, fracción II, y 36, 1er. Párrafo de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios; 40, fracción I, 41, Fracciones I y I.1.- del reglamento de la Ley; y 13, fracción IV, 14, fracción III, del Reglamento del Comité de Compras el Poder Judicial en vigor.

El Comité de Compras del Poder Judicial le invita a participar en el Proceso de **Licitación Simplificada Menor No. TSJ/CC/FASP/LSME-001/2015**, relativo al **FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012)**; por lo cual enviamos a usted las condiciones generales del proceso; así como el Anexo "A"; en el que se describen los bienes materia de la presente licitación. En el entendido de que para participar en el citado procedimiento deberá enviar sus sobres de documentación legal, técnica y económica a más tardar el día **Viernes 03 de Julio de 2015;** antes de las **15:00 horas.**

La documentación deberá ser dirigida al suscrito presidente y entregarse en las oficinas de la Oficialía Mayor del Tribunal Superior de Justicia, ubicada en la Calle Independencia esquina Nicolás Bravo s/n, Tercer Piso, Colonia Centro, Villahermosa, Tabasco, en la fecha señalada.

Para el cabal cumplimiento de lo anterior, de manera adjunta y como parte integrante de este mismo oficio se le informan las Condiciones Generales del Proceso así como las Bases del mismo.

Sin más por el momento se les invita cordialmente a participar:

ATENTAMENTE

LIC. PEDRO ÁNGEL ZURITA SAHAGÚN **PRESIDENTE DEL COMITÉ Y OFICIAL MAYOR**	**L.C.P. GABRIEL RAMOS TORRES** **VICEPRESIDENTE Y ENCARGADO DEL DESPACHO DE LA TESORERÍA JUDICIAL**

C.c.p. LIC. PEDRO ÁNGEL ZURITA SAHAGÚN.- Oficial Mayor y Presidente del Comité de Compras.
L.C.P. GABRIEL RAMOS TORRES.- Vicepresidente y Encargado del Despacho de la Tesorería Judicial.
C.P. Y M.D.F. JOSÉ MARIO ORNELAS PÉREZ.-Secretario y Coordinador de Presupuesto.
L.C.P. JUAN CARLOS PÉREZ PÉREZ.- Primer Vocal y Director de Contraloría Judicial.
LIC. LEONEL CÁCERES HERNÁNDEZ.- Segundo Vocal.
LIC. ROSA ISELA GÓMEZ VÁZQUEZ.- Tercera Vocal.
L.A.E. RAQUEL AGUILERA ALEMÁN.-Suplente y Jefa del Departamento de Compras.
Minutario/Archivo Comité

Poder Judicial del Estado de Tabasco
Tribunal Superior de Justicia
Comité de Compras del Poder Judicial

"25 de Noviembre, Conmemoración del Día Internacional de la Eliminación de la Violencia contra la Mujer"

OFICIO No. TSJ/OM/DC/096/2015

Villahermosa, Tabasco, Junio 26, de 2015.

ASUNTO: INVITACIÓN A LICITACIÓN SIMPLIFICADA MENOR PARA EL FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012).

RADIKAL SYSTEMS, S.A. DE C.V.
CALLE 4, ESQ. CIRCUITO 1, LOTE 53
FRACC. BONAMPAK, RANCHERÍA MIGUEL HIDALGO
VILLAHERMOSA, TABASCO C.P. 86126
TEL. 3 51 99 78.

Con fundamento en lo dispuesto por los artículos 22, fracción II, y 36, 1er. Párrafo de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios; 40, fracción I, 41, Fracciones I y I.1.- del reglamento de la Ley; y 13, fracción IV, 14, fracción III, del Reglamento del Comité de Compras el Poder Judicial en vigor.

El Comité de Compras del Poder Judicial le invita a participar en el Proceso de **Licitación Simplificada Menor No. TSJ/CC/FASP/LSME-001/2015**, relativo al **FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012);** por lo cual enviamos a usted las condiciones generales del proceso; así como el Anexo "A"; en el que se describen los bienes materia de la presente licitación. En el entendido de que para participar en el citado procedimiento deberá enviar sus sobres de documentación legal, técnica y económica a más tardar el día **Viernes 03 de Julio de 2015;** antes de las **15:00 horas**.

La documentación deberá ser dirigida al suscrito presidente y entregarse en las oficinas de la Oficialía Mayor del Tribunal Superior de Justicia, ubicada en la Calle Independencia esquina Nicolás Bravo s/n, Tercer Piso, Colonia Centro, Villahermosa, Tabasco, en la fecha señalada.

Para el cabal cumplimiento de lo anterior, de manera adjunta y como parte integrante de este mismo oficio se le informan las Condiciones Generales del Proceso así como las Bases del mismo.

Sin más por el momento, se les invita cordialmente a participar:

A T E N T A M E N T E

LIC. PEDRO ÁNGEL ZURITA SAHAGÚN
PRESIDENTE DEL COMITÉ Y OFICIAL MAYOR

L.C.P. GABRIEL RAMOS TORRES
VICEPRESIDENTE Y ENCARGADO DEL DESPACHO DE LA TESORERÍA JUDICIAL

C.c.p. LIC. PEDRO ÁNGEL ZURITA SAHAGÚN.- Oficial Mayor y Presidente del Comité de Compras.
L.C.P. GABRIEL RAMOS TORRES.- Vicepresidente y Encargado del Despacho de la Tesorería Judicial.
C.P. Y M.D.F. JOSÉ MARIO ORNELAS PÉREZ.-Secretario y Coordinador de Presupuesto.
L.C.P. JUAN CARLOS PÉREZ PÉREZ.- Primer Vocal y Director de Contraloría Judicial.
LIC. LEONEL CÁCERES HERNÁNDEZ.- Segundo Vocal.
LIC. ROSA ISELA GÓMEZ VÁZQUEZ.- Tercera Vocal.
L.A.E. RAQUEL AGUILERA ALEMÁN.-Suplente y Jefa del Departamento de Compras.
Minutario/Archivo Comité

Recibí 30-06-2015
Miguel Angel Hernández

Radikal systems
RFC: RSY030728114
www.radikalsystems.com

Poder Judicial del Estado de Tabasco
Tribunal Superior de Justicia
Comité de Compras del Poder Judicial

"25 de Noviembre, Conmemoración del Día Internacional de la Eliminación de la Violencia contra la Mujer"

OFICIO No. TSJ/OM/DC/097/2015

Villahermosa, Tabasco, Junio 26, de 2015.

ASUNTO: INVITACIÓN A LICITACIÓN SIMPLIFICADA MENOR PARA EL FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012).

COMPULOGIC, S.A. DE C.V.
CALLE TRES NO. 122, FRACC. BOULEVARES
ZACATECAS, ZACATECAS, C.P. 98060
TEL. 01 492 924 0950.

Con fundamento en lo dispuesto por los artículos 22, fracción II, y 36, 1er. Párrafo de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios; 40, fracción I, 41, Fracciones I y I.1.- del reglamento de la Ley; y 13, fracción IV, 14, fracción III, del Reglamento del Comité de Compras el Poder Judicial en vigor.

El Comité de Compras del Poder Judicial le invita a participar en el Proceso de **Licitación Simplificada Menor No. TSJ/CC/FASP/LSME-001/2015**, relativo al **FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012);** por lo cual enviamos a usted las condiciones generales del proceso; así como el Anexo "A"; en el que se describen los bienes materia de la presente licitación. En el entendido de que para participar en el citado procedimiento deberá enviar sus sobres de documentación legal, técnica y económica a más tardar el día **Viernes 03 de Julio de 2015;** antes de las **15:00 horas**.

La documentación deberá ser dirigida al suscrito presidente y entregarse en las oficinas de la Oficialía Mayor del Tribunal Superior de Justicia, ubicada en la Calle Independencia esquina Nicolás Bravo s/n, Tercer Piso, Colonia Centro, Villahermosa, Tabasco, en la fecha señalada.

Para el cabal cumplimiento de lo anterior, de manera adjunta y como parte integrante de este mismo oficio se le informan las Condiciones Generales del Proceso así como las Bases del mismo.

Sin más por el momento, se les invita cordialmente a participar:

ATENTAMENTE

LIC. PEDRO ÁNGEL ZURITA SAHAGÚN
PRESIDENTE DEL COMITÉ Y OFICIAL MAYOR

L.C.P. GABRIEL RAMOS TORRES
VICEPRESIDENTE Y ENCARGADO DEL DESPACHO DE LA TESORERÍA JUDICIAL

C.c.p. LIC. PEDRO ÁNGEL ZURITA SAHAGÚN.- Oficial Mayor y Presidente del Comité de Compras.
L.C.P. GABRIEL RAMOS TORRES.- Vicepresidente y Encargado del Despacho de la Tesorería Judicial.
C.P. Y M.D.F. JOSÉ MARIO ORNELAS PÉREZ.-Secretario y Coordinador de Presupuesto.
L.C.P. JUAN CARLOS PÉREZ PÉREZ.- Primer Vocal y Director de Contraloría Judicial.
LIC. LEONEL CÁCERES HERNÁNDEZ.- Segundo Vocal.
LIC. ROSA ISELA GÓMEZ VÁZQUEZ.- Tercera Vocal.
L.A.E. RAQUEL AGUILERA ALEMÁN.-Suplente y Jefa del Departamento de Compras.
Minutario/Archivo Comité

powered by compulogic
Nelson Manuel Galvez
calle tres 122, fracc boulevares
zacatecas, zacatecas. 98065
COM940110JE2

INVITACIÓN A LICITACIÓN SIMPLIFICADA MENOR
No. TSJ/CC/FASP/LSME-001/2015
FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012).

CONDICIONES GENERALES DEL PROCESO

El Comité de Compras del Poder Judicial le invita a participar en el Proceso de Licitación Simplificada Menor No. **TSJ/CC/FASP/LSME-001/2015**, relativo al **FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012);** por lo cual adjunto enviamos a usted las condiciones generales del proceso; así como el Anexo "A"; en el que se describen los bienes materia de la presente licitación. En el entendido de que para participar en el citado procedimiento deberá enviar sus sobres de documentación legal, técnica y económica a más tardar el día **Viernes 03 de Julio de 2015; antes de las 15:00 horas.**

La documentación deberá ser dirigida al suscrito presidente y entregarse en las instalaciones de la Oficialía Mayor del Tribunal Superior de Justicia, ubicada en la Calle Independencia esquina Nicolás Bravo s/n, Tercer Piso, Colonia Centro, Villahermosa, Tabasco, en la fecha señalada.

Para el cabal cumplimiento de lo anterior, se informan las Condiciones Generales del Proceso.

Las Propuestas deberán elaborarse en papel membretado original de la empresa, con sello y firma autógrafa del representante legal de la empresa; venir en idioma español, y con precios cotizados en moneda nacional. Y deberán elaborarse conforme a lo siguiente:

Venir en 2 sobres sellados y lacrados, los cuáles deberán rotularse con los datos generales del licitante, así como con el Número del Proceso de Licitación Simplificada Menor No. **TSJ/CC/FASP/LSME-001/2015**, relativo a la **FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012);** y con el siguiente contenido:

EL SOBRE No. 1.- PROPUESTA LEGAL Y TECNICA, CONTENDRÁ:

A.- Documentación Legal:

1. Copia del acta constitutiva y sus reformas inscritas en el Registro Público de la Propiedad y del Comercio, **(sólo si es persona jurídica colectiva)**.
2. Copia del acta de nacimiento y de alguno de los siguientes documentos de identificación: credencial para votar, pasaporte o cartilla del servicio militar **(sólo si es persona física)**.
3. Copia de la cédula de identificación fiscal.

4. Copia del último aviso de cambio de domicilio fiscal **(en su caso).**
5. Copia de la declaración anual de impuestos (ISR, IVA e IA) del último ejercicio fiscal.
6. Copia de la declaración provisional de impuestos (ISR, IVA e IA) del periodo inmediato anterior.
7. Copia de la Identificación y del Poder notarial del representante legal que firma las cartas.
8. Carta, bajo "Protesta de Decir Verdad" de que no se encuentra en ninguno de los supuestos que señala el artículo 51, de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del estado.
9. Anexo B), debidamente requisitado o bien escrito libre que contenga los datos con los que acredita su personalidad.

B.- Propuesta Técnica.

a) Cedula técnica conforme al Anexo A.- (Listado de bienes); en original y copia.

En la que deberá de describir conforme a los requerido por renglón, las características del bien que nos oferta describiendo la cantidad, la marca, el modelo, el número de parte, y cualquier otra información que permita evaluar y conocer las características del bien.

b) Sin incluir precios

c) Tiempo, Lugar y forma de entrega: La entrega de los bienes será libre abordo destino en el almacén del poder judicial; y se realizará en una sola entrega, el tiempo máximo para realizar el suministro e instalación es de 4 semanas.

d) Catálogos, folletos y/o fichas técnicas, en los que se ilustre el modelo y las características del bien ofertado, los cuales podrán presentarse en el idioma del país de origen de los bienes, pero acompañados de una traducción simple al español. (requisito no indispensable).

De preferencia, la documentación deberá venir, acomodada en el orden indicado, con separadores y pestañas indicativas de cada documento que se anexa. La omisión de lo anterior, no se considerará un requisito indispensable para la participación; sin embargo, si se considera necesario para agilizar la adecuada consecución del proceso de revisión documental.

SOBRE No. 2.- PROPUESTA ECONÓMICA
C.- Propuesta Económica.

La propuesta económica se elaborará en original y copia, con sus listas de precios debidamente protegidas con cinta adhesiva transparente. Y señalar:

a) Precios unitarios sin incluir el IVA y que reflejen los descuentos que ofrezca.
b) Especificar en sus condiciones de pago 30 días naturales contados a partir de la entrega de los bienes y una vez de haber terminado los servicios solicitados, y

de la entrega de la factura, así como de toda la documentación requerida para trámites de pago.
c) El precio ofertado incluirá todos aquellos cargos por los servicios de fletes; la entrega será **LIBRE A BORDO** destino almacén del Poder Judicial.
d) Que los precios ofertados se encontraran vigentes cuando menos 15 días naturales contados a partir de la presentación de la oferta.

Nota.- Las descripciones de las partidas cotizadas por el licitante, deberán ser descritas conforme a las mismas características señaladas en las propuestas técnicas y no presentar variaciones y/o modificaciones. Toda vez, que derivado de las mismas, se elaborarán los contratos pedidos.

Aspectos a Considerar:

1.- Que previo a la firma del contrato se deberá entregar Cheque Cruzado Original a nombre del Tribunal Superior de Justicia; por el 10% del monto total adjudicado con IVA incluido, librado con cargo a una institución bancaria, con domicilio en el Estado de Tabasco. El cuál se mantendrá vigente durante el tiempo que dure el contrato. Las garantías que se ofrezcan serán liberadas por el Tribunal, una vez agotada la materia del contrato, es decir, cuando se haya cumplido con la entrega de bienes pactadas en el mismo y durante 1 año.

El cheque cruzado, se entregará con un escrito **"Bajo Protesta de Decir Verdad"** en papel membretado original con sello y firma autógrafa del representante legal, y con el siguiente texto:

"...Que el cheque cruzado original que se adjunta (mencionando los datos del mismo –No. de cheque, fecha, institución bancaria, importe)

A) Se otorga para garantizar todas y cada una de las obligaciones contenidas en el contrato de **fecha __ de _____ de 2015,** celebrado entre _____., y El Tribunal Superior de Justicia del estado de Tabasco; derivado de su participación en el Proceso de **Licitación Simplificada Menor No. TSJ/CC/FASP/LSME-001/2015**, relativo al **FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO (ECONOMÍAS FASP 2012);**

B) Que esta garantía tendrá una vigencia de 1 Año, contado a partir de la fecha de su expedición continuará vigente, aun cuando se otorguen prórrogas o esperas al deudor, para el cumplimiento de las obligaciones que se garantizan;

C) La presente carta permanecerá en vigor desde la fecha de su expedición y hasta dentro de 1 año, siguiente a la entrega de todos y cada uno de los bienes y servicios que se señalan en el contrato; o en su caso, durante la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por la autoridad competente.

2.- Considerar que en las fechas de entrega; el Tribunal no aceptará condonaciones de tiempo para el cumplimiento de las mismas. Toda **vez que los bienes y servicios señalados se requieren en el tiempo de entrega citado,** de no cumplirse con la puntual entrega de los mismos; **se procederá a aplicar una sanción por cada día de mora**. La que será en razón del **0.005** del importe total de aquellos bienes y servicios no entregados y realizados en la fecha ofrecida. Cantidad que se descontará de las cantidades pendientes por pagar**, o en su caso; se hará efectiva la garantía de cumplimiento al contrato otorgada.**

Por lo que deberá **de tener la capacidad de respuesta inmediata y suficiente como para cumplir con las obligaciones derivadas de la presente licitación; en cuanto precios y fechas de entrega ofertadas.**

Por lo anterior claramente se solicitan los tiempos de entrega requeridos, a partir de la fecha de notificación de la adjudicación y en una etapa, conforme a lo señalado en párrafos anteriores.

3.- Que los contratos serán abiertos, es decir que podrán incrementarse hasta un 10% sobre lo originalmente solicitado, previo acuerdo de ambas partes.

4.- Que la adjudicación será por renglón a él o los licitantes, que habiendo cumplido con toda la documentación legal y técnica ofrezcan las mejores condiciones en cuanto a precio, tiempo de entrega y especificaciones técnicas requeridas, por la convocante.

5.- Que los precios ofertados deberán ser firmes e incondicionados; por lo menos durante 15 días que será el tiempo estimado que durará el presente proceso licitatorio.

6.- Que deberán presentar información verídica, legítima y fehaciente, toda vez que de detectarse alguna imprecisión, alteración o falsedad, será motivo de descalificación; o bien de la presentación de la denuncia correspondiente ante las autoridades pertinentes, en razón de que conforme a la legislación vigente, la falsedad de testimonios ante una autoridad; aún en su carácter de administrativa, es privativa de la libertad.

La convocante se reserva el derecho de cancelar partidas o renglones, así como a disminuir las cantidades originalmente solicitadas a cotizar, en los casos en los que advierta que existe insuficiencia presupuestal. O bien, en el caso de que no se reciban al menos **3 sobres de propuestas**, se procederá a declarar desierta la licitación y se convocará nuevamente al proceso, en una fecha posterior.

La evaluación de las propuestas se sujetará a las siguientes:

BASES

I.- El Comité en pleno recibirá y revisará que los sobres entregados por los licitantes, vengan en perfecto estado, rotulados y sellados.

II.- En el orden que hayan sido recibidos o acomodados, se procederá a la apertura de cada una de las propuestas, verificándose en primer término; que se haya adjuntado toda la documentación legal que permita acreditar fehacientemente la personalidad jurídica y existencia legitima del licitante y de su poderdante. El resultado de esta evaluación se asentará en un tabla comparativa de evaluación bajo el resultado de "Cumple" o "No cumple".

III.- Seguidamente se dará cuenta al Secretario del Comité, de aquellas propuestas que sí cumplan con toda la documentación legal solicitada, procediéndose a revisar que la documentación técnica satisfaga todos y cada uno de los requisitos solicitados por la convocante. Por ello, las propuestas que omitan, o incluyan documentos que no cumplan con los requisitos señalados en estas bases; o los mismos contengan información falsa, serán desechadas. Es indispensable que las propuestas técnicas satisfagan todos y cada uno de los requisitos solicitados en estas bases, en cuanto a características técnicas, especificaciones y tecnología requerida en los bienes en cuanto a **DESCRIPCIÓN, UNIDAD Y CANTIDAD.** La propuesta que no cumpla lo anterior será desechada.

IV.- Realizado el análisis correspondiente, los resultados serán asentados en un acta, misma que deberá ser firmada por los responsables de la revisión, en la que se hará constar todas y cada una de las observaciones efectuadas. Así como las propuestas aceptadas para su evaluación económica.

V.- Agotada la revisión técnica, se procederá a la apertura exclusiva de aquellos sobres cuya documentación legal y técnica, cumplió con todos y cada uno de los requisitos de la convocante.

VI.- Una vez abiertos los sobres económicos se procederá a revisar que estos contengan la información en la forma y términos en que fueron solicitados por la convocante; debiendo ser rubricadas estas por todos los miembros del Comité, quienes harán constar aquellas que si cumplan con los mismos, y por lo tanto, las entregarán al Secretario, quién elaborará los cuadros comparativos de los mismos.

VII.- Durante el análisis efectuado a las propuestas económicas se verificará que las propuestas vengan en pesos mexicanos, con precios firmes e incondicionados, IVA desglosado, subtotales y cantidades totales. Así como que se incluya la leyenda en la que se establezcan la vigencia de precios requerida y las condiciones de crédito.

Si durante el análisis económico se advirtiera que los precios ofertados en algunos o algunos de los renglones, es demasiado bajo, en relación con los del mercado; la propuesta en ese renglón en particular se considerará como insolvente, en razón de que el precio ofertado sea inferior al costo de fabricación y comercialización del bien de que se trate.

Dicha situación será informada al Comité, y este, en pleno verificará tal situación.

VIII.- La adjudicación se realizará a un solo licitante, que habiendo cumplido con toda la documentación legal y técnica ofrezca las mejores condiciones en cuanto **a precio, tiempo de entrega, garantía y especificaciones requeridas,** por la convocante.

IX.- Finalmente, el resultado de proceso de Licitación será publicado en los tableros de avisos del Tribunal Superior de Justicia, girándose un aviso de adjudicación a aquel licitante que haya resultado adjudicado.

Poder Judicial del Estado de Tabasco

Tribunal Superior de Justicia

DEPARTAMENTO DE COMPRAS

ANEXO "A"

LICITACIÓN SIMPLIFICADA MENOR NO. TSJ/CC/FASP/LSME-001/2015

PROYECTO PJ080 FORTALECIMIENTO DE ESTRUCTURA DE VOZ Y DATOS DE LOS JUZGADOS PENALES DEL MUNICIPIO DE CENTRO ECONOMÍAS FASP 2012

PARTIDA 51501 BIENES INFORMÁTICOS

ESPECIFICACIONES TÉCNICAS DE LOS BIENES Y SERVICIOS REQUERIDOS			
PARTIDA	**CANTIDAD**	**UNIDAD**	**DESCRIPCIÓN**
1	**1**	**LOTE**	SUMINISTRO E INSTALACIÓN DE SISTEMA DE CABLEADO ESTRUCTURADO SUMINISTRO E INSTALACIÓN DE SISTEMA DE CABLEADO ESTRUCTURADO COMPUESTOS DE 50 NODOS DE RED DE LA CATEGORIA 6 EL CUAL DEBERÁ DE CUMPLIR CON LA NORMATIVA ESPECÍFICA PARA EL CUMPLIMIENTO DEL DESEMPEÑO DEL CANAL. EL SISTEMA DE CABLEADO ESTRUCTURADO DE VOZ Y DATOS PARA EL CABLEADO HORIZONTAL DEBERÁ CUMPLIR CON LAS ESPECIFICACIONES DE LA CATEGORIA 6 (TIA/EIA 568-B.2-1). ADEMÁS ESTE SISTEMA DEBERÁ DE CUMPLIR CON LAS SIGUIENTES NORMAS: • ANSI/TIA/EIA–568 GENERIC TELECOMUNICATIONS CABLING FOR CUSTOMER PREMISES, QUE PERMITE LA PLANEACIÓN E INSTALACIÓN DE UN SISTEMA DE CABLEADO ESTRUCTURADO QUE SOPORTA INDEPENDIENTEMENTE DEL PROVEEDOR Y SIN CONOCIMIENTO PREVIO, LOS SERVICIOS Y DISPOSITIVOS DE TELECOMUNICACIONES QUE SERÁN INSTALADOS DURANTE LA VIDA ÚTIL DEL EDIFICIO. • EIA/TIA-568-C.0 (REQUERIMIENTOS GENERALES) • EIA/TIA-568-C.1 (EDIFICIOS COMERCIALES) • EIA/TIA-568-C.2 (COMPONENTES DE CABLEADO – CATEGORÍA 6 PAR TRENZADO BALANCEADO) • ANSI/TIA/EIA-569-B COMMERCIAL BUILDING STANDARD FOR TELECOMUNICATIONS PATHWAYS AND SPACES, QUE ESTANDARIZA PRÁCTICAS DE DISEÑO Y CONSTRUCCIÓN DENTRO Y ENTRE EDIFICIOS, QUE SON HECHAS EN SOPORTE DE MEDIOS Y/O EQUIPOS DE TELECOMUNICACIONES TALES COMO CANALETAS Y GUÍAS, FACILIDADES DE ENTRADA AL EDIFICIO, ARMARIOS Y/O CLOSET DE COMUNICACIONES Y CUARTO DE EQUIPOS. • ANSI/EIA/TIA-606A ADMINISTRATION STANDARD FOR THE TELECOMUNICATIONS COMMERCIAL BUILDING, QUE DA LAS GUÍAS PARA MARCAR Y ADMINISTRAR LOS COMPONENTES DE UN SISTEMA DE CABLEADO ESTRUCTURADO. • J-STD-607A COMMERCIAL BUILDING GROUNDING (EARTHING) AND BONDING REQUERIMENTS FOR TELECOMUNICATIONS, QUE DESCRIBE LOS MÉTODOS ESTÁNDARES PARA DISTRIBUIR LAS SEÑALES DE TIERRA

			A TRAVÉS DE UN EDIFICIO. TODOS LOS COMPONENTES DEL SISTEMA DEBERÁN SER PARA LA CATEGORÍA 6, TOMANDO EN CUENTA LA DISTRIBUCIÓN DE LOS NODOS DE ACUERDO A CADA PUESTO DE TRABAJO DISTRIBUIDOS EN LAS DIFERENTES PLANTAS DEL EDIFICIO (50 NODOS DE RED). ESTE SISTEMA INCLUIRÁ EL SUMINISTRO DE LA INFRAESTRUCTURA DEL CUARTO DE TELECOMUNICACIONES (MDF) CUARTO DE TELECOMUNICACIONES EN EL CUARTO DE TELECOMUNICACIONES PARA EL EDIFICIO SE INSTALARÁ LOS BASTIDORES QUE CONTENDRÁN LA ADMINISTRACIÓN DEL CABLEADO PARA LA ACOMETIDA, TANTO INALÁMBRICA COMO OTROS SERVICIOS DE TELECOMUNICACIONES; ADEMÁS DE LOS CABLEADOS HORIZONTAL Y VERTICAL, TANTO COMO LOS EQUIPOS ACTIVOS PARA LA RED Y CALIDAD DE ENERGÍA NECESARIOS. ESTOS BASTIDORES DEBERÁN DE TENER LAS SIGUIENTES CARACTERÍSTICAS: EL SISTEMA DE ADMINISTRACIÓN DE CABLEADO SERÁ PROVISTO USANDO DOS (2) BASTIDORES CAPACES DE SOPORTAR EQUIPAMIENTO PESADO PARA CONEXIONES CRUZADAS O APLICACIONES DE INTERCONEXIÓN EN CUARTOS DE TELECOMUNICACIONES. LOS SISTEMAS DE SOPORTE DE LOS BASTIDORES (RACK) DEBERÁN SER MODULARES Y SOPORTARÁN APLICACIONES TANTO CABLEADO DE COBRE Y FIBRA. LA SOLUCIÓN CON SISTEMAS DE RACK DEBERÁ ESTAR CONSTRUIDA DE ACERO Y SOPORTAR COMPONENTES DE 19". LOS RACK (BASTIDORES) DEBERÁN ESTAR LISTADO UL CON CLASIFICACIÓN DE CARGA DE 1500 LIBRAS PARA SOPORTAR EQUIPO DE NETWORKING ROBUSTO. ESTA SOLUCIÓN DE BASTIDORES DEBEN PROVEER UN SISTEMA INTEGRAL DE ADMINISTRACIÓN DE CABLEADO INCLUYENDO CANALES VERTICALES, ORIFICIOS DE ACCESO PARA CRUCE Y CANALES QUE PROVEAN CAPACIDAD ADICIONAL EN EL ACOPLAMIENTO DE OTROS ACCESORIOS PARA ADMINISTRACIÓN DE CABLEADO. LOS ORIFICIOS DE PASO DEBEN LOCALIZARSE AL FRENTE, ATRÁS Y A LOS LADOS PARA MÁXIMA FLEXIBILIDAD. ADEMÁS TENDRÁN AL MENOS 7 FT DE ALTURA; LOS ACCESORIOS QUE SE INSTALARÁN EN LA PARTE SUPERIOR CUIDARAN LOS RADIOS DE CURVATURA DE LOS CABLES, DEBEN SER MODULARES Y SOPORTAR APLICACIONES DE CABLEADO PARA COBRE Y FIBRA; LOS RACKS DEBEN ACEPTAR PUERTAS REMOVIBLES Y ABATIBLES ASÍ COMO LOS ANILLOS PLÁSTICOS PARA ADMINISTRACIÓN. DEBEN DE PROVEERSE JUNTO CON LA SOLUCIÓN DE BASTIDORES DEL CUARTO DE EQUIPO DE TODOS LOS ACCESORIOS NECESARIOS PARA LA ADMINISTRACIÓN DEL CABLEADO, DE ACUERDO A LA CANTIDAD DE NODOS QUE SE PROVEERÁN. CANALIZACIÓN

			EL SISTEMA DE CANALIZACIÓN PRINCIPAL, ASÍ COMO LAS RAMIFICACIONES HASTA EL NIVEL ESCRITORIO YA EXISTE EN EL EDIFICIO COMO PARTE DE LA OBRA CIVIL, EN CASO DE QUE LLEGASE A FALTAR UN SEGMENTO DE DICHA CANALIZACIÓN REQUERIDA, EL CONCURSANTE DEBERÁ DE CONSIDERARLA DENTRO DE SU PROPUESTA. ADEMÁS DEBERÁ DE INCLUIR LOS DISPAROS NECESARIOS BASADOS EN TUBERÍA CONDUIT DE ¾ DE PULGADA DESDE LA CANALIZACIÓN PRINCIPAL (ESCALERILLA) HASTA EL MURO DONDE SE ENCUENTRAN LOS REGISTROS PARA LAS ÁREAS DE TRABAJO, DEBERÁ DE CONSIDERARSE TODOS LOS MATERIALES Y ACCESORIOS NECESARIOS PARA LA CORRECTA INSTALACIÓN DE ESTE DUCTO. LA INGENIERÍA PROPUESTA DEBERÁ DE GARANTIZAR UNA HOLGURA MÍNIMA DE 60% DE LLENADO EXIGIDO SEGÚN LA ANSI/TIA/EIA-569-B. LOS DUCTOS PRIMARIOS ESTÁN BASADOS EN ESCALERILLA ELECTROZINCADA CON CAPACIDAD SUFICIENTE PARA EL TRANSPORTE DE CABLES; CONSIDERANDOSE QUE SE INSTALARÁ SOBRE EL PLAFÓN, O BIEN OTRO SISTEMA DE TRANSPORTE PREVISTO. INCLUIRÁ EL SUMINISTRO Y TENDIDO DE CABLE UTP CATEGORÍA 6, Y LOS CONECTORES RESPECTIVOS. PARA LA SOLUCIÓN UTP, EL CANAL COMPLETO CATEGORÍA 6 DEBERÁ CUMPLIR CON LAS PRUEBAS DE RENDIMIENTO Y DESEMPEÑO DE LA EIA/TIA 568B.2-1 PARA 90 METROS DE CABLE UTP, 10 METROS DE PATCH CORDS Y CUATRO (4) CONECTORES EN EL CANAL. TODOS LOS COMPONENTES DEL CABLEADO ESTRUCTURADO HORIZONTAL DEBERÁN SER DEL MISMO FABRICANTE TALES COMO PATCH CORDS, CABLE UTP, JACKS RJ45, PANEL DE PARCHEO, ORGANIZADORES HORIZONTALES, BASTIDORES, GABINETES Y SUS RESPECTIVOS ACCESORIOS PARA LA ADMINISTRACIÓN DEL SISTEMA DE CABLEADO. CARACTERÍSITCAS MÍNIMAS QUE DEBERÁ TENER EL CABLE UTP: • EL CABLE UTP ES EL USADO PARA EL TENDIDO DEL CABLEADO HORIZONTAL, NO DEBE EXCEDER DE 90 METROS DESDE LA PLACA HASTA EL PANEL DE PARCHEO POR CADA ENLACE. • CABLE DE COBRE UNSHIELD TWISTED PAIR DE 4 PARES TRENZADOS, 23-24 AWG, 100 OHM, EN PRESENTACIÓN DE CAJAS SELLADAS. • DEBE CUMPLIR O SUPERAR LAS ESPECIFICACIONES DE LA NORMA TIA/EIA 568-B.2-1 TRANSMISSION PERFORMANCE SPECIFICATIONS FOR 4 PAR 100 Ω CATEGORY 6 CABLING Y LOS REQUISITOS DE CABLE CATEGORÍA 6 (CLASE E) DE LA NORMA ISO/IEC 11801. • EL CABLE DEBE TENER AISLANTE DE POLIETILENO Y LA CHAQUETA DEL CABLE UTP DEBE SER DEL TIPO CMR, TIPO NO PLENUM. • EL CABLE DEBE TENER UN SEPARADOR DE PARES DEL TIPO CRUZ Y DEBE SER RETARDANTE A LA FLAMA.

			CARACTERÍSTICAS MÍNIMAS QUE DEBERÁ DE TENER LOS LINE CORDS: • EL LINE CORD ES EL CABLE UTILIZADO PARA CONECTAR EL EQUIPO PERIFÉRICO (PC, SERVIDOR, IMPRESORA, U OTRO DISPOSITIVO) CON LA TOMA PARA DATOS CONFORMADA POR EL JACK Y LA PLACA. • EL LINE CORD DEBE ESTAR CONFORMADO SOLAMENTE POR CABLE DE COBRE MULTIFILAR UNSHIELD TWISTED PAIR DE 4 PARES TRENZADOS 24 AWG, Y CON UN PLUG RJ45 CATEGORÍA-6 DE 8 POSICIONES EN CADA EXTREMO. DEBE ESTAR CONFECCIONADO INTEGRALMENTE POR EL FABRICANTE EN CONFIGURACIÓN SEGÚN EL ESQUEMA T568. • LOS LINE CORDS DEBERÁN SER ENSAMBLADOS Y CERTIFICADOS DE FÁBRICA. • DEBIDO A QUE ES UTP NO DEBERÁN CONTAR CON NINGÚN BLINDAJE O MALLA ELÉCTRICA ALREDEDOR EL PLUG. • DEBE TENER UNA VARIEDAD DE 8 COLORES PARA PODER IDENTIFICAR EL SERVICIO SEGÚN LA TIA/EIA 606A. • LOS PLUG RJ45 DE CADA LINE CORD DEBEN TENER UN SISTEMA ANTI ENREDO O CAPUCHAS COMO PARTE DEL PLUG RJ45 PARA EVITAR ATASCOS DURANTE MOVIMIENTOS O REORDENAMIENTO Y NO DEBERÁN TENER ALGÚN ACCESORIO QUE AMPLÍE SUS DIMENSIONES LATERALES. • LA LONGITUD DEL LINE CORD DEBE SER NO MAYOR A 3 METROS. CARACTERÍSTICAS MÍNIMAS QUE DEBERÁ DE TENER LOS PATCH CORDS: • EL PATH CORD ES EL CABLE UTILIZADO PARA CONECTAR EL PATCH PANEL CON EL EQUIPO ACTIVO DE RED (SWITCH O SIMILAR) EN CONFIGURACIÓN DIRECTA O EN CONFIGURACIÓN CROSS-CONNECT. • EL PATCH CORD CATEGORÍA-6 DEBE ESTAR CONFORMADO SOLAMENTE POR CABLE DE COBRE MULTIFILAR UNSHIELD TWISTED PAIR DE 4 PARES TRENZADOS 24 AWG Y CON UN PLUG RJ45 CATEGORÍA-6 DE 8 POSICIONES EN CADA EXTREMO. DEBE ESTAR CONFECCIONADO INTEGRALMENTE POR EL FABRICANTE EN CONFIGURACIÓN SEGÚN EL ESQUEMA T568. • LOS PATCH CORDS DEBERÁN SER ENSAMBLADOS Y CERTIFICADOS DE FÁBRICA. • DEBE TENER UNA VARIEDAD DE 8 COLORES PARA PODER IDENTIFICAR EL SERVICIO SEGÚN LA TIA/EIA 606A. • DEBIDO A QUE ES UTP NO DEBERÁN CONTAR CON NINGÚN BLINDAJE O MALLA ELÉCTRICA ALREDEDOR EL PLUG. • LOS PLUG RJ45 DE CADA PATCH CORD DEBEN TENER UN SISTEMA ANTI ENREDO O CAPUCHAS COMO PARTE DEL PLUG RJ45 PARA EVITAR ATASCOS DURANTE MOVIMIENTOS O REORDENAMIENTO Y NO DEBERÁN TENER ALGÚN ACCESORIO QUE AMPLIÉ SUS DIMENSIONES LATERALES. • DEBE CUMPLIR CON LAS PRUEBAS DE DESEMPEÑO DE LA EIA/TIA 568B.2-1 CATEGORÍA-6.

			• LA CHAQUETA DEL CABLE UTP DEBE SER DE PVC, TIPO NO PLENUM. • LA LONGITUD DEL PATCH CORD OSCILARÁ ENTRE LOS 3 Y 10 FT, ADEMÁS LA LONGITUD EXACTA PARA CADA UNO DE LOS COMPONENTES SOLICITADOS SE DETERMINARÁN EN UNA MESA DE TRABAJO. GARANTIZANDO UN CORRECTO ORDENAMIENTO DE CABLES CON LOS ORGANIZADORES SOLICITADOS PARA EL PATCH PANEL Y LOS BASTIDORES Y GABINETES. CARACTERÍSTICAS MÍNIMAS QUE DEBERÁ DE TENER LOS PATCH PANEL: • DEBE PERMITIR LA INSERCIÓN DE: 24 JACKS DE CATEGORÍA 6 O 24 JACKS DE CATEGORÍA 6A UTP O 24 ACOPLADORES LC DÚPLEX, A FIN DE GARANTIZAR UPGRADES FUTUROS. • DEBEN SER MODULARES Y PERMITIR LA INSTALACIÓN DE DIFERENTES CONECTORES: UTP CATEGORÍA 6, COAXIAL, TIPO F DE AUDIO, RCA, FIBRA ÓPTICA: ST, SC, LC Y MTRJ, ETC. A FIN DE ASEGURAR LA INVERSIÓN A FUTURO RESPECTO A LAS TENDENCIAS EN TECNOLOGÍAS. • CADA JACK DEL PATCH PANEL DEBE CUMPLIR CON LAS PRUEBAS DE DESEMPEÑO DE LA EIA/TIA 568B.2-1 CATEGORÍA-6. • DEBEN SER MODULARES PUERTO POR PUERTO DE TAL FORMA QUE PUEDA SER POSIBLE CAMBIAR UN JACK INDIVIDUALMENTE EN CASO DE FALLAS Y NO SE REQUIERA TENER QUE ADQUIRIR UN BLOQUE O MODULO DE 04 O 06 JACKS NI TENER QUE CAMBIAR TODO EL PATCH PANEL. • LOS CONECTORES RJ45 OFERTADOS PARA LOS PATCH PANEL DEBEN PERMITIR TRABAJAR CON EL MAPA DE CABLES T568A O EL T568B. • LA MÁSCARA EL PATCH PANEL DEBE SER DE MATERIAL METÁLICO. • DEBE TENER 19 PULGADAS DE ANCHO PARA SER INSTALADOS EN LOS RACKS O GABINETES. • DEBEN PERMITIR LA CONEXIÓN TOTAL DE LAS SALIDAS DE INFORMACIÓN DE TODAS LAS APLICACIONES (DATOS, VOZ, ETC.), PERFECTAMENTE IDENTIFICADOS EN EL PANEL, Y CON TODOS LOS REQUERIMIENTOS PARA FACILITAR LA ADMINISTRACIÓN Y MANEJO DE LA RED, DE ACUERDO CON LA NORMA ANSI/TIA/EIA 606A. • DEBEN CONTAR CON UNA PROTECCIÓN PLÁSTICA TRANSPARENTE QUE IMPIDA EL CONTACTO DIRECTO DE LAS MANOS U OTROS OBJETOS CON LAS ETIQUETAS GARANTIZANDO CON ELLO SU LONGEVIDAD DE ACUERDO A LA ANSI/TIA/EIA 606A. • LOS PATCH PANEL DEBEN PERMITIR LA INSTALACIÓN DE LOS JACKS OFERTADOS. • SE DEBERÁN COLOCAR MODULO INDIVIDUALES / TAPAS DE COLOR NEGRO EN TODOS LOS PUERTOS NO UTILIZADOS DEL PATCH PANEL. CARACTERÍSTICAS MÍNIMAS QUE DEBERÁ DE TENER LOS JACKS RJ45 CATEGORÍA 6 • DEBEN SER DE CATEGORÍA 6 DE ACUERDO A LA TIA/EIA 568-B.2-1.

			• DEBE SER DE 8 POSICIONES TIPO IDC, PARA CONECTORIZACIÓN SIN HERRAMIENTA DE IMPACTO. • DEBE PERMITIR LA CONECTORIZACIÓN TIPO T568A O T568B CONTANDO CON UNA ETIQUETA QUE INDIQUE EL MÉTODO PARA ELLO. • DEBEN ASEGURAR LA NO DESCONEXIÓN DEL CABLE UTP SÓLIDO AL SER EXPUESTO A JALONES, CONTANDO PARA ELLO CON UNA TAPA O SEGURO SOBRE LAS CONEXIONES DEL CABLE UTP Y LAS CONEXIONES IDC. • DEBE PERMITIR LA INSERCIÓN DE ICONOS PLÁSTICOS. • EL FABRICANTE DEBE CONTAR CON AL MENOS 8 COLORES DISTINTOS (TIA/EIA 606A) A FIN DE FACILITAR LA ADMINISTRACIÓN. • DEBE CUMPLIR CON LOS REQUERIMIENTOS DE IEC60603-7 DE ACUERDO A LA TIA/EIA 568B. • DEBE PODER SER INSTALADO EN LAS PLACAS COMO EN LOS PATCH PANEL SUMINISTRADOS. • DEBE PERMITIR LA INSERCIÓN DE PATCH CORD DE 2 Y 4 PARES SIN DEGRADARSE. INCLUIRÁ DISPAROS DE LA ESCALERILLA HACIA EL PUESTO DE TRABAJO. SE DOTARÁ DE UNA PLACA CON EL NÚMERO DE VÍAS NECESARIO PARA CADA PUESTO DE TRABAJO, ASÍ COMO CAPACIDAD DE CRECIMIENTO. DE ACUERDO A LAS SIGUIENTES CARACTERÍSTICAS MÍNIMAS: • DEBERÁN INSTALARSE PLACAS DOBLES POR ÁREA DE TRABAJO, LA SALIDA NO UTILIZADA DEBERÁ IR CON TAPA CIEGA. • DEBERÁ PERMITIR LA INSERCIÓN DE UN ICONO DE IDENTIFICACIÓN SOBRE CADA SALIDA RJ45 PARA IDENTIFICAR SI EL SERVICIO ES DE TELEFONÍA O DATOS. • DEBE PERMITIR LA INSERCIÓN DE: JACKS DE CATEGORÍA 6 O JACKS DE CATEGORÍA 6A UTP O ACOPLADORES LC DÚPLEX, A FIN DE GARANTIZAR UPGRADES FUTUROS. • LAS SALIDAS DE LA PLACA DEBERÁN TENER UN ÁNGULO DE INCLINACIÓN DE 45º PARA ASEGURAR EL RADIO DE GIRO DE LOS PATCH CORPS. • DEBE INCLUIR SUS TORNILLOS DE SUJECIÓN Y ETIQUETAS DE IDENTIFICACIÓN PARA CADA PUERTO DE LA PLACA, CON COBERTOR TRANSPARENTE. SE REALIZARÁ EL TERMINADO MECÁNICO TANTO EN PÁNELES DE PARCHEO EN EL CUARTO DE TELECOMUNICACIONES Y CABLEADO POR ZONA Y PLACA EN LOS PUESTOS DE TRABAJO. IDENTIFICACIÓN, SEÑALIZACIÓN Y ORDENAMIENTO TODOS LOS NODOS SE IDENTIFICARÁN DE ACUERDO A LA NORMATIVIDAD, ADEMÁS CONTARÁN CON CORDONES DE PARCHEO DE FABRICA. DEBERÁ DE

			CONSIDERARSE DOS CONEXIONES DE CABLE DE COBRE (GIGAETHERNET) DEL MDF A LOS IDFS DEBERÁ DE ENTREGARSE UNA MEMORIA TÉCNICA DEL LOS TRABAJOS REALIZADOS; INCLUYENDO LA CERTIFICACIÓN DE LOS NODOS, ADEMÁS DE LOS PLANOS DE DISTRIBUCIÓN Y DEBERÁ CONTENER UN RESPALDO EN MEDIO ÓPTICO. SE DEBERÁ INCLUIR UN INFORME IMPRESO Y ELECTRÓNICO DE VERIFICACIÓN POR CADA PUNTO DE LOS PARÁMETROS DE DESEMPEÑO SEGÚN LA TIA/EIA-568B SEGÚN LA CATEGORÍA REQUERIDA PARA EL PRESENTE PROCESO, ESTO SE REALIZARÁ CON UN EQUIPO CERTIFICADOR PARA MEDIR ESTOS PARÁMETROS DE DESEMPEÑO, LOS CUALES FORMARÁN PARTE DEL DOCUMENTO "MEMORIA TÉCNICA DE LA INSTALACIÓN" LA CUAL DEBERÁ DE DESCRIBIR LOS TRABAJOS REALIZADOS EN LA EJECUCIÓN DEL PROYECTO, ASÍ COMO TODOS LOS PLANOS DE LOCALIZACIÓN DE NODOS Y DEL SISTEMA DE CANALIZACIÓN. ESTE DOCUMENTO SE DEBERÁ DE ENTREGAR EN FORMA IMPRESA Y EN RESPALDO ELECTRÓNICO. TODOS LOS ELEMENTOS DEL SISTEMA DE CABLEADO ESTRUCTURADO INCLUYENDO: CABLES, PLACAS, JACK DE LA PLACA, PATCH PANEL, JACK DE PATCH PANEL, RACKS, CUARTOS DE TELECOMUNICACIONES Y CUARTOS DE EQUIPOS, DEBERÁN CONTAR CON UNA IDENTIFICACIÓN ÚNICA DE ACUERDO A LO INDICADO POR LA ANSI/TIA/EIA 606A. TODAS LAS IDENTIFICACIONES DEBERÁN SER IMPRESAS CON IMPRESORA LÁSER (O IMPRESORAS ESPECIFICAS PARA ETIQUETAR), NO SE ACEPTARÁN IMPRESIONES EN IMPRESORA DE TINTA, MATRICIAL O A MANO. EN TODOS LOS CASOS LA IDENTIFICACIÓN DEBERÁ SER FÁCILMENTE VISIBLE Y DEBERÁ ESTAR BASADA EN ETIQUETAS ADHESIVAS SIENDO NECESARIA QUE ADICIONALMENTE CUENTEN CON ALGUNA PROTECCIÓN PLÁSTICA QUE IMPIDA EL CONTACTO DIRECTO DE LAS MANOS CON LA IMPRESIÓN. LAS ETIQUETAS PARA CABLES Y TUBOS PODRÁN SER AUTOLAMINABLES. TODOS LOS CABLES DEBERÁN AGRUPARSE POR ZONAS USANDO CINTAS TAK-TIES (CINTAS TIPO VELCRO) LOS MISMOS QUE DEBERÁN INCLUSO COLOCARSE DENTRO DE LOS ORGANIZADORES DE CABLES VERTICALES ANTES DEL INGRESO DE CABLES A LOS ORGANIZADORES HORIZONTALES, NO SE PERMITIRÁ EL USO DE CINTILLOS PLÁSTICOS PARA ESTA LABOR. INGENIERÍA EL ALCANCE DE LA INGENIERÍA PARA EL SISTEMA DE CABLEADO ESTRUCTURADO INCLUIRÁ, DE MANERA ENUNCIATIVA, MÁS NO LIMITATIVA, LO SIGUIENTE: • IMPLEMENTACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO DE ACUERDO A LO SOLICITADO EN EL PRESENTE ANEXO Y DOCUMENTACIÓN DIGITAL QUE SE ENTREGARÁ AL CONCURSANTE, • PRUEBAS DE OPERACIÓN DE LOS SISTEMAS, ASÍ COMO PRUEBAS DE

			COMPATIBILIDAD SOPORTADAS, • DOCUMENTACIÓN TÉCNICA DEL PROYECTO, • MEMORIA TÉCNICA DEL PROYECTO, ADEMÁS DE LA INFORMACIÓN NECESARIA PARA REALIZAR CAMBIOS Y O ACTUALIZACIONES A FUTURO, • ASISTENCIA TÉCNICA, CAPACITACIÓN Y SERVICIOS DE GARANTÍAS DE OPERACIÓN, LOS CUALES DEBERÁN QUEDAR PLASMADOS EN UN DOCUMENTO Y SU RESPECTIVO ALCANCE, PARA DAR CUMPLIMIENTO CON LAS GARANTÍAS SOLICITADAS • CERTIFICACIÓN DE CADA NODO DE ACUERDO A LAS NORMAS DE LA CATEGORÍA 6 SOLICITADA, • INSTALACIÓN DE TODOS LOS COMPONENTES DE LOS SUBSISTEMAS DE CABLEADO ESTRUCTURADO: CUARTO DE TELECOMUNICACIONES (BASTIDORES, GABINETES DE PARED, GABINETES PARA PUNTOS DE CONSOLIDACIÓN, PANELES DE PARCHEO DE ALTA DENSIDAD, CONEXIÓN DE LOS BASTIDORES Y GABINETES AL SISTEMA DE TIERRA FÍSICA, ACCESORIOS PARA LA ADMINISTRACIÓN DE CABLE, PATCH CORD); CABLEADO HORIZONTAL: INSTALACIÓN DE CABLE UTP, CONEXIÓN MECÁNICA EN PANEL DE PARCHEO Y PLACA DE SERVICIO; LINE CORDS); LA GARANTÍA DE INSTALACIÓN QUE DEBERÁ PRESENTAR LA EMPRESA ADJUDICADA DEBE SER EMITIDA POR EL FABRICANTE DE LA SOLUCIÓN DE CABLEADO ESTRUCTURADO POR UN TIEMPO MÍNIMO DE 5 AÑOS, EN LA QUE SE ESPECIFIQUE UNA GARANTÍA DE FABRICACIÓN DE LOS COMPONENTES, DESEMPEÑO, Y APLICACIONES. Y MANO DE OBRA POR UN TIEMPO DE MÍNIMO DE 5 AÑOS. LA GARANTÍA POR MANO DE OBRA POR PARTE DEL FABRICANTE SIGNIFICA QUE EN CASO DE QUE ALGÚN PRODUCTO CON FALLA DE FÁBRICA APLICACIÓN PRESENTE O FUTURA QUE SE DESARROLLE PARA TRABAJAR SOBRE LA CATEGORÍA SOLICITADA, NO CUMPLA CON LO SOLICITADO TENGA QUE SER CAMBIADA, EL FABRICANTE SE COMPROMETERÁ A CUBRIR CON EL TOTAL DE COSTOS (MANO DE OBRA POR RE-INSTALACIÓN, VIÁTICOS, PASAJES, ETC., LOS GASTOS QUE FUERAN NECESARIOS) QUE DEMANDE DICHOS CAMBIOS ADICIONALMENTE AL CAMBIO DE PRODUCTOS, INDEPENDIENTEMENTE SI ES QUE EL POSTOR EXISTIERA O NO A LA FECHA DE PRESENTADO EL PROBLEMA, SIN PERJUICIO ALGUNO PARA EL CENTRO ASISTENCIAL.
2	**1**	**PIEZA**	SUMINISTRO E INSTALACIÓN DE UN (1) EQUIPO DE SEGURIDAD DE RED QUE SEA DEL TIPO ADMINISTRACIÓN UNIFICADA DE AMENAZAS, DONDE SE DEBERÁN OFRECER LAS FUNCIONALIDADES QUE ABAJO SE DETALLAN, Y DEBERÁN DE ESTAR INCLUIDAS Y LISTAS PARA SER UTILIZADAS. FUNCIONALIDADES Y CARACTERÍSTICAS DEL SISTEMA: CARACTERÍSTICAS QUE DEBERÁ TENER EL DISPOSITIVO

			• EL DISPOSITIVO DEBE SER UNA APPLIANCE DE PROPÓSITO ESPECÍFICO • BASADO EN TECNOLOGÍA ASIC Y QUE SEA CAPAZ DE BRINDAR UNA SOLUCIÓN DE "COMPLETE CONTENT PROTECTION". POR SEGURIDAD Y FACILIDAD DE ADMINISTRACIÓN, NO SE ACEPTAN EQUIPOS DE PROPÓSITO GENÉRICO (PCS O SERVERS) SOBRE LOS CUALES PUEDA INSTALARSE Y/O EJECUTAR UN SISTEMA OPERATIVO REGULAR COMO MICROSOFT WINDOWS, FREEBSD, SUN SOLARIS, APPLE OS-X O GNU/LINUX. • CAPACIDAD DE REENSAMBLADO DE PAQUETES EN CONTENIDO PARA BUSCAR ATAQUES O CONTENIDO PROHIBIDO, BASADO EN HARDWARE (MEDIANTE EL USO DE UN ASIC). • EL EQUIPO DEBERÁ PODER SER CONFIGURADO EN MODO GATEWAY O EN MODO TRANSPARENTE EN LA RED. • EN MODO TRANSPARENTE, EL EQUIPO NO REQUERIRÁ DE HACER MODIFICACIONES EN LA RED EN CUANTO A RUTEO O DIRECCIONAMIENTO IP. CARACTERÍSTICAS QUE DEBERÁ TENER EL SISTEMA OPERATIVO INCLUIDO: • SISTEMA OPERATIVO BLINDADO, ESPECÍFICO PARA SEGURIDAD, QUE SEA COMPATIBLE CON EL APPLIANCE. POR SEGURIDAD Y FACILIDAD DE ADMINISTRACIÓN Y OPERACIÓN, NO SE ACEPTAN SOLUCIONES SOBRE SISTEMAS OPERATIVOS GENÉRICOS TALES COMO GNU/LINUX, FREEBSD, SUN SOLARIS, HP-UX DE HP, AIX DE IBM O MICROSOFT WINDOWS • EL SISTEMA OPERATIVO DEBE INCLUIR UN SERVIDOR DE DNS QUE PERMITA RESOLVER DE FORMA LOCAL CIERTAS CONSULTAS DE ACUERDO A LA CONFIGURACIÓN DEL ADMINISTRADOR. FIREWALL • LAS REGLAS DE FIREWALL DEBEN ANALIZAR LAS CONEXIONES QUE ATRAVIESEN EN EL EQUIPO, ENTRE INTERFACES, GRUPOS DE INTERFACES (O ZONAS) Y VLANS • POR GRANULARIDAD Y SEGURIDAD, EL FIREWALL DEBERÁ PODER ESPECIFICAR POLÍTICAS TOMANDO EN CUENTA PUERTO FÍSICO FUENTE Y DESTINO. ESTO ES, EL PUERTO FÍSICO FUENTE Y EL PUERTO FÍSICO DESTINO DEBERÁN FORMAR PARTE DE LA ESPECIFICACIÓN DE LA REGLA DE FIREWALL. • SERÁ POSIBLE DEFINIR POLÍTICAS DE FIREWALL QUE SEAN INDEPENDIENTES DEL PUERTO DE ORIGEN Y PUERTO DE DESTINO. • LAS REGLAS DEL FIREWALL DEBERÁN TOMAR EN CUENTA DIRECCIÓN IP ORIGEN (QUE PUEDE SER UN GRUPO DE DIRECCIONES IP), DIRECCIÓN IP DESTINO (QUE PUEDE SER UN GRUPO DE DIRECCIONES IP) Y SERVICIO (O GRUPO DE SERVICIOS) DE LA COMUNICACIÓN QUE SE ESTÁ ANALIZANDO • DEBERÁN PODER DEFINIRSE REGLAS DE FIREWALL PARA SERVICIOS SOBRE PROTOCOLO SCTP. • LAS ACCIONES DE LAS REGLAS DEBERÁN CONTENER AL MENOS EL ACEPTAR O RECHAZAR LA COMUNICACIÓN • DEBERA TENER SOPORTE A REGLAS DE FIREWALL PARA TRÁFICO DE MULTICAST, PUDIENDO ESPECIFICAR PUERTO FÍSICO FUENTE, PUERTO FÍSICO DESTINO, DIRECCIONES IP FUENTE, DIRECCIÓN IP DESTINO. • LAS REGLAS DE FIREWALL DEBERÁN PODER TENER LIMITANTES Y/O

			VIGENCIA EN BASE A TIEMPO • LAS REGLAS DE FIREWALL DEBERÁN PODER TENER LIMITANTES Y/O VIGENCIA EN BASE A FECHAS (INCLUYENDO DÍA, MES Y AÑO) • DEBE SOPORTAR LA CAPACIDAD DE DEFINIR NUEVOS SERVICIOS TCP Y UDP QUE NO ESTÉN CONTEMPLADOS EN LOS PREDEFINIDOS. • DEBE PODER DEFINIRSE EL TIEMPO DE VIDA DE UNA SESIÓN INACTIVA DE FORMA INDEPENDIENTE POR PUERTO Y PROTOCOLO (TCP Y UDP) • DEBERA TENER LA CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES ESTÁTICO, UNO A UNO, NAT. • DEBERA TENER LA CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES DINÁMICO, MUCHOS A UNO, PAT. • DEBERÁ SOPORTAR REGLAS DE FIREWALL EN IPV6 CONFIGURABLES TANTO POR CLI (COMMAND LINE INTERFACE, INTERFACE DE LÍNEA DE COMANDO) COMO POR GUI (GRAPHICAL USER INTERFACE, INTERFACE GRÁFICA DE USUARIO) • LA SOLUCIÓN DEBERÁ TENER LA CAPACIDAD DE BALANCEAR CARGA ENTRE SERVIDORES. ESTO ES REALIZAR UNA TRASLACIÓN DE UNA ÚNICA DIRECCIÓN A MÚLTIPLES DIRECCIONES DE FORMA TAL QUE SE DISTRIBUYA EL TRÁFICO ENTRE ELLAS • EN LA SOLUCIÓN DE BALANCEO DE CARGA ENTRE SERVIDORES, DEBE SOPORTARSE PERSITENCIA DE SESIÓN AL MENOS MEDIANTE HTTP COOKIE O SSL SESSION ID • EN LA SOLUCIÓN DE BALANCEO DE CARGA DE ENTRE SERVIDORES DEBEN SOPORTARSE MECANISMOS PARA DETECTAR LA DISPONIBILIDAD DE LOS SERVIDORES, DE FORMA TAL DE PODER EVITAR ENVIAR TRÁFICO A UN SERVIDOR NO DISPONIBLE. CONECTIVIDAD Y SISTEMA DE RUTEO • EL EQUIPO DEBERA TENER AL MENOS CUATRO PUERTOS 1GE SFP INTERFAZ/PUERTO. • DEBERA TENER LA FUNCIONALIDAD DE DHCP: COMO CLIENTE DHCP, SERVIDOR DHCP Y REENVÍO (RELAY) DE SOLICITUDES DHCP • DEBERA SOPORTAR ETIQUETAS DE VLAN (802.1Q) Y CREACIÓN DE ZONAS DE SEGURIDAD EN BASE A VLANS • DEBERA DE TENER SOPORTE A RUTEO ESTÁTICO, INCLUYENDO PESOS Y/O DISTANCIAS Y/O PRIORIDADES DE RUTAS ESTÁTICAS • SOPORTE A POLÍTICAS DE RUTEO (POLICY ROUTING) • DEBERA DE SOPORTAR POLÍTICAS DE RUTEO, QUE PERMINATN QUE ANTE LA PRESENCIA DE DOS ENLACES A INTERNET, SE PUEDA DECIDIR CUÁL TRÁFICO SALE POR UN ENLACE Y QUÉ TRÁFICO SALE POR OTRO ENLACE • SOPORTE A RUTEO DINÁMICO RIP V1, V2, OSPF, BGP Y IS-IS • SOPORTE A RUTEO DINÁMICO RIPNG, OSPFV3, BGP4+ • LA CONFIGURACIÓN DE BGP DEBE SOPORTAR AUTONOMOUS SYSTEM PATH (AS-PATH) DE 4 BYTES. • DEBERA DE SOPORTAR ECMP (EQUAL COST MULTI-PATH) • DEBERA DE SOPORTAR ECMP CON PESO. EN ESTE MODO EL TRÁFICO SERÁ DISTRIBUIDO ENTRE MÚLTIPLES RUTAS PERO NO EN FORMA EQUITATIVA, SINO EN BASE A LOS PESOS Y PREFERENCIAS DEFINIDAS POR EL

			ADMINISTRADOR. • DEBERA DE TENER SOPORTE DE ECMP BASADO EN COMPORTAMIENTO. EN ESTE MODO, EL TRÁFICO SERÁ ENVIADO DE ACUERDO A LA DEFINICIÓN DE UNA RUTA HASTA QUE SE ALCANCE UN UMBRAL DE TRÁFICO. EN ESTE PUNTO SE COMENZARÁ A UTILIZAR EN PARALELO UNA RUTA ALTERNATIVA. • DEBERA DE TENER SOPORTE RUTEO DE MULTICAST • LA SOLUCIÓN PERMITIRÁ LA INTEGRACIÓN CON ANALIZADORES DE TRÁFICO MEDIANTE EL PROTOCOLO SFLOW. VPN IPSEC/L2TP/PPTP DEBERA DE CONTAR CON LAS SIGUIENTES CARACTERISTICAS: • SOPORTE A CERTIFICADOS PKI X.509 PARA CONSTRUCCIÓN DE VPNS CLIENTE A SITIO (CLIENT-TO-SITE) • SOPORTE A CONFIGURACIÓN DE VPNS CON IKE E IKEV2 • DEBE SOPORTAR LA CONFIGURACIÓN DE TÚNELES L2TP • DEBE SOPORTAR LA CONFIGURACIÓN DE TÚNELES PPTP • SOPORTE DE VPNS CON ALGORITMOS DE CIFRADO: AES, DES, 3DES. • SE DEBE SOPORTAR LONGITUDES DE LLAVE PARA AES DE 128, 192 Y 256 BITS • SE DEBE SOPORTAR AL MENOS LOS GRUPOS DE DIFFIE-HELLMAN 1, 2, 5 Y 14. • SE DEBE SOPORTAR LOS SIGUIENTES ALGORITMOS DE INTEGRIDAD: MD5, SHA-1 Y SHA256. • DEBE TENER LA POSIBILIDAD DE CREAR VPN'S ENTRE GATEWAYS Y CLIENTES CON IPSEC. ESTO ES, VPNS IPSEC SITE-TO-SITE Y VPNS IPSEC CLIENT-TO-SITE. • LA VPN IPSEC DEBERÁ PODER SER CONFIGURADA EN MODO INTERFAZ (INTERFACE-MODE VPN) • EN MODO INTERFAZ, LA VPN IPSEC DEBERÁ PODER TENER ASIGNADA UNA DIRECCIÓN IP, TENER RUTAS ASIGNADAS PARA SER ENCAMINADAS POR ESTA INTERFACE Y DEBERÁ SER CAPAZ DE ESTAR PRESENTE COMO INTERFACE FUENTE O DESTINO EN POLÍTICAS DE FIREWALL. • TANTO PARA IPSEC COMO PARA L2TP DEBE SOPORTARSE LOS CLIENTES TERMINADORES DE TÚNELES NATIVOS DE WINDOWS Y MACOS X. VPN SSL • DEBERA DE TENER LA CAPACIDAD DE REALIZAR SSL VPNS. • DEBERA SOPORTAR CERTIFICADOS PKI X.509 PARA CONSTRUCCIÓN DE VPNS SSL. • DEBERA SOPORTAR AUTENTICACIÓN DE DOS FACTORES. EN ESTE MODO, EL USUARIO DEBERÁ PRESENTAR UN CERTIFICADO DIGITAL ADEMÁS DE UNA CONTRASEÑA PARA LOGRAR ACCESO AL PORTAL DE VPN. • DEBERA SOPORTAR RENOVACIÓN DE CONTRASEÑAS PARA LDAP Y RADIUS. • DEBERA SOPORTAR ASIGNACIÓN DE APLICACIONES PERMITIDAS POR

			GRUPO DE USUARIOS • DEBERA DAR SOPORTE NATIVO PARA AL MENOS HTTP, FTP, SMB/CIFS, VNC, SSH, RDP Y TELNET. • DEBERÁ PODER VERIFICAR LA PRESENCIA DE ANTIVIRUS (PROPIO Y/O DE TERCEROS Y DE UN FIREWALL PERSONAL (PROPIO Y/O DE TERCEROS) EN LA MÁQUINA QUE ESTABLECE LA COMUNICACIÓN VPN SSL. • DEBERA TENER LA CAPACIDAD INTEGRADA PARA ELIMINAR Y/O CIFRAR EL CONTENIDO DESCARGADO AL CACHÉ DE LA MÁQUINA CLIENTE (CACHÉ CLEANING) • DEBERA DAR SOPORTE A LA VPN SSL INTEGRADA A TRAVÉS DE ALGUN PLUG-IN ACTIVEX Y/O JAVA, LA CAPACIDAD DE METER DENTRO DEL TÚNEL SSL TRÁFICO QUE NO SEA HTTP/HTTPS • DEBERÁ TENER SOPORTE AL CONCEPTO DE REGISTROS FAVORITOS (BOOKMARKS) PARA CUANDO EL USUARIO SE REGISTRE DENTRO DE LA VPN SSL • DEBERÁ SOPORTAR LA REDIRECCIÓN DE PÁGINA HTTP A LOS USUARIOS QUE SE REGISTREN EN LA VPN SSL, UNA VEZ QUE SE HAYAN AUTENTICADO EXITOSAMENTE • DEBE SER POSIBLE DEFINIR DISTINTOS PORTALES SSL QUE SERVIRÁN COMO INTERFAZ GRÁFICA A LOS USUARIOS DE VPN SSL LUEGO DE SER AUTENTICADOS POR LA HERRAMIENTA. DICHOS PORTALES DEBEN PODER ASIGNARSE DE ACUERDO AL GRUPO DE PERTENENCIA DE DICHOS USUARIOS. • LOS PORTALES PERSONALIZADOS DEBERÁN SOPORTAR AL MENOS LA DEFINICIÓN DE: • WIDGETS A MOSTRAR • APLICACIONES NATIVAS PERMITIDAS. AL MENOS: HTTP, CIFS/SMB, FTP, VNC • ESQUEMA DE COLORES • SOPORTE PARA ESCRITORIO VIRTUAL • DEBE SOPORTAR POLÍTICA DE VERIFICACIÓN DE LA ESTACIÓN DE TRABAJO. • LA VPN SSL INTEGRADA DEBE SOPORTAR LA FUNCIONALIDAD DE ESCRITORIO VIRTUAL, ENTENDIÉNDOSE COMO UN ENTORNO DE TRABAJO SEGURO QUE PREVIENE CONTRA CIERTOS ATAQUES ADEMÁS DE EVITAR LA DIVULGACIÓN DE INFORMACIÓN. TRAFFIC SHAPPING / QOS • DEBERA TENER LA CAPACIDAD DE PODER ASIGNAR PARÁMETROS DE TRAFFIC SHAPPING SOBRE REGLAS DE FIREWALL • DEBERA TENER LA CAPACIDAD DE PODER ASIGNAR PARÁMETROS DE TRAFFIC SHAPING DIFERENCIADAS PARA EL TRÁFICO EN DISTINTOS SENTIDOS DE UNA MISMA SESIÓN • DEBERA TENER LA CAPACIDAD DE DEFINIR PARÁMETROS DE TRAFFIC SHAPING QUE APLIQUEN PARA CADA DIRECCIÓN IP EN FORMA INDEPENDIENTE, EN CONTRASTE CON LA APLICACIÓN DE LAS MISMAS PARA LA REGLA EN GENERAL. CAPACIDAD DE PODER DEFINIR ANCHO DE BANDA GARANTIZADO EN

			KILOBYTES POR SEGUNDO • DEBERA TENER LA CAPACIDAD DE PODER DEFINIR LÍMITE DE ANCHO DE BANDA (ANCHO DE BANDA MÁXIMO) EN KILOBYTES POR SEGUNDO • DEBERA TENER LA CAPACIDAD DE PARA DEFINIR PRIORIDAD DE TRÁFICO, EN AL MENOS TRES NIVELES DE IMPORTANCIA AUTENTICACIÓN Y CERTIFICACIÓN DIGITAL • DEBERA TENER LA CAPACIDAD DE INTEGRARSE CON SERVIDORES DE AUTENTICACIÓN RADIUS. • DEBERA TENER LA CAPACIDAD NATIVA DE INTEGRARSE CON DIRECTORIOS LDAP • DEBERA TENER LA CAPACIDAD INCLUIDA, AL INTEGRARSE CON MICROSOFT WINDOWS ACTIVE DIRECTORY O NOVELL EDIRECTORY, DE AUTENTICAR TRANSPARENTEMENTE USUARIOS SIN PREGUNTARLES USERNAME O PASSWORD. ESTO ES, APROVECHAR LAS CREDENCIALES DEL DOMINIO DE WINDOWS BAJO UN CONCEPTO "SINGLE-SIGN-ON" • DEBERA TENER LA CAPACIDAD DE AUTENTICAR USUARIOS PARA CUALQUIER APLICACIÓN QUE SE EJECUTE BAJO LOS PROTOCOLOS TCP/UDP/ICMP. DEBE DE MOSTRAR SOLICITUD DE AUTENTICACIÓN (PROMPT) AL MENOS PARA WEB (HTTP), FTP Y TELNET. • DEBERA DE SER POSIBLE DEFINIR PUERTOS ALTERNATIVOS DE AUTENTICACIÓN PARA LOS PROTOCOLOS HTTP, FTP Y TELNET. • DEBERA TENER SOPORTE A CERTIFICADOS PKI X.509 PARA CONSTRUCCIÓN DE VPNS CLIENTE A SITIO (CLIENT-TO-SITE) • DEBERA DAR SOPORTE A INCLUSIÓN EN AUTORIDADES CERTIFICADORAS (ENROLLMENT) MEDIANTE SCEP (SIMPLE CERTIFICATE ENROLLMENT PROTOCOL) Y MEDIANTE ARCHIVOS. • DEBERA DAR SOPORTE DE VERIFICACIÓN DE VALIDACIÓN DE CERTIFICADOS DIGITALES MEDIANTE EL PROTOCOLO OSCP (ONLINE SIMPLE ENRROLLMENT PROTOCOL) • DEBERA SOPORTAR POLÍTICAS BASADAS EN IDENTIDAD. ESTO SIGNIFICA QUE PODRÁN DEFINIRSE POLÍTICAS DE SEGURIDAD DE ACUERDO AL GRUPO DE PERTENENCIA DE LOS USUARIOS. • DEBERA PODER DEFINIR USUARIOS Y GRUPOS EN UN REPOSITORIO LOCAL DEL DISPOSITIVO. • PARA LOS ADMINISTRADORES LOCALES DEBE PODER DEFINIRSE LA POLÍTICA DE CONTRASEÑAS QUE ESPECIFICARÁ COMO MÍNIMO: • LONGITUD MÍNIMA PERMITIDA • RESTRICCIONES DE TIPO DE CARACTERES: NUMÉRICOS, ALFANUMÉRICOS, ETC. • EXPIRACIÓN DE CONTRASEÑA. • DEBE PODER LIMITARSE LA POSIBILIDAD DE QUE DOS USUARIOS O ADMINISTRADORES TENGAN SESIONES SIMULTÁNEAS DESDE DISTINTAS DIRECCIONES IP. ANTIVIRUS • DEBE SER CAPAZ DE ANALIZAR, ESTABLECER CONTROL DE ACCESO Y

			DETENER ATAQUES Y HACER ANTIVIRUS EN TIEMPO REAL EN AL MENOS LOS SIGUIENTES PROTOCOLOS APLICATIVOS: HTTP, SMTP, IMAP, POP3, FTP. • EL ANTIVIRUS DEBERÁ PODER CONFIGURARSE EN MODO PROXY COMO EN MODO DE FLUJO. EN EL PRIMER CASO, LOS ARCHIVOS SERÁN TOTALMENTE RECONSTRUÍDOS POR EL MOTOR ANTES DE HACER LA INSPECCIÓN. EN EL SEGUNDO CASO, LA INSPECCIÓN DE ANTIVIRUS SE HARÁ POR CADA PAQUETE DE FORMA INDEPENDIENTE. • DEBERA EL ANTIVIRUS EN TIEMPO REAL, INTEGRADO A LA PLATAFORMA DE SEGURIDAD "APPLIANCE". SIN NECESIDAD DE INSTALAR UN SERVIDOR O APPLIANCE EXTERNO, LICENCIAMIENTO DE UN PRODUCTO EXTERNO O SOFTWARE ADICIONAL PARA REALIZAR LA CATEGORIZACIÓN DEL CONTENIDO. • EL ANTIVIRUS INTEGRADO DEBE SOPORTAR LA CAPACIDAD DE INSPECCIONAR Y DETECTAR VIRUS EN TRÁFICO IPV6. • DEBERA SOPORTAR LA CONFIGURACIÓN DE ANTIVIRUS EN TIEMPO REAL SOBRE LOS PROTOCOLOS HTTP, SMTP, IMAP, POP3 Y FTP DEBERÁ ESTAR COMPLETAMENTE INTEGRADA A LA ADMINISTRACIÓN DEL DISPOSITIVO APPLIANCE, QUE PERMITA LA APLICACIÓN DE ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. • EL ANTIVIRUS DEBERÁ SOPORTAR MÚLTIPLES BASES DE DATOS DE VIRUS DE FORMA TAL DE QUE EL ADMINISTRADOR DEFINA CUÁL ES CONVENIENTE UTILIZAR PARA SU IMPLEMENTACIÓN EVALUANDO DESEMPEÑO Y SEGURIDAD. • EL APPLIANCE DEBERÁ DE MANERA OPCIONAL PODER INSPECCIONAR POR TODOS LOS VIRUS CONOCIDOS (ZOO LIST) • EL ANTIVIRUS INTEGRADO DEBERÁ TENER LA CAPACIDAD DE PONER EN CUARENTENA ARCHIVOS ENCONTRADOS INFECTADOS QUE ESTÉN CIRCULANDO A TRAVÉS DE LOS PROTOCOLOS HTTP, FTP, IMAP, POP3, SMTP • EL ANTIVIRUS INTEGRADO TENDRÁ LA CAPACIDAD DE PONER EN CUARENTENA A LOS CLIENTES CUANDO SE HAYA DETECTADO QUE LOS MISMOS ENVÍAN ARCHIVOS INFECTADOS CON VIRUS. • EL ANTIVIRUS DEBERÁ INCLUÍR CAPACIDADES DE DETECCIÓN Y DETENCIÓN DE TRÁFICO SPYWARE, ADWARE Y OTROS TIPOS DE MALWARE/GRAYWARE QUE PUDIERAN CIRCULAR POR LA RED. • EL ANTIVIRUS DEBERÁ PODER HACER INSPECCIÓN Y CUARENTENA DE ARCHIVOS TRANSFERIDOS POR MENSAJERÍA INSTANTÁNEA (INSTANT MESSAGING) PARA AL MENOS MSN MESSENGER. • EL ANTIVIRUS DEBERÁ SER CAPAZ DE FILTRAR ARCHIVOS POR EXTENSIÓN • EL ANTIVIRUS DEBERÁ SER CAPAZ DE FILTRAR ARCHIVOS POR TIPO DE ARCHIVO (EJECUTABLES POR EJEMPLO) SIN IMPORTAR LA EXTENSIÓN QUE TENGA EL ARCHIVO • DEBERA TENER LA CAPACIDAD DE ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS ANTIVIRUS MEDIANTE TECNOLOGÍA DE TIPO "PUSH" (PERMITIR RECIBIR LAS ACTUALIZACIONES CUANDO LOS CENTROS DE ACTUALIZACIÓN ENVÍEN NOTIFICACIONES SIN PROGRAMACIÓN PREVIA), ADICIONAL A TECNOLOGÍAS TIPO "PULL" (CONSULTAR LOS CENTROS DE ACTUALIZACIÓN POR VERSIONES NUEVAS)

			ANTISPAM • DEBERA TENER LA CAPACIDAD ANTISPAM INCLUÍDA DEBERÁ SER CAPAZ DE DETECTAR PALABRAS DENTRO DEL CUERPO DEL MENSAJE DE CORREO, Y EN BASE A LA PRESENCIA/AUSENCIA DE COMBINACIONES DE PALABRAS, DECIDIR RECHAZAR EL MENSAJE. • DEBERA TENER LA CAPACIDAD ANTISPAM INCLUÍDA DEBERÁ PERMITIR ESPECIFICAR LISTAS BLANCAS (CONFIABLES, A LOS CUALES SIEMPRE SE LES DEBERÁ PASAR) Y LISTAS NEGRAS (NO CONFIABLES, A LOS CUALES SIEMPRE LES DEBERÁ BLOQUEAR). LAS LISTAS BLANCAS Y LISTAS NEGRAS PODRÁN SER POR DIRECCIÓN IP O POR DIRECCIÓN DE CORREO ELECTRÓNICO (E-MAIL ADDRESS) • DEBERA TENER LA CAPACIDAD ANTISPAM DEBERÁ PODER CONSULTAR UNA BASE DE DATOS DONDE SE REVISE POR LO MENOS DIRECCIÓN IP DEL EMISOR DEL MENSAJE, URLS CONTENIDOS DENTRO DEL MENSAJE Y CHECKSUM DEL MENSAJE, COMO MECANISMOS PARA DETECCIÓN DE SPAM • EN EL CASO DE ANÁLISIS DE SMTP, LOS MENSAJES ENCONTRADOS COMO SPAM PODRÁN SER ETIQUETADOS O RECHAZADOS (DESCARTADOS). EN EL CASO DE ETIQUETAMIENTO DEL MENSAJE, DEBE TENERSE LA FLEXIBILIDAD PARA ETIQUETARSE EN EL MOTIVO (SUBJECT) DEL MENSAJE O A TRAVÉS UN ENCABEZADO MIME EN EL MENSAJE. FILTRAJE DE URLS (URL FILTERING) • DEBERA DE CONTAR CON FACILIDAD PARA INCORPORAR CONTROL DE SITIOS A LOS CUALES NAVEGUEN LOS USUARIOS, MEDIANTE CATEGORÍAS. POR FLEXIBILIDAD, EL FILTRO DE URLS DEBE TENER POR LO MENOS 75 CATEGORÍAS Y POR LO MENOS 54 MILLONES DE SITIOS WEB EN LA BASE DE DATOS. • DEBE PODER CATEGORIZAR CONTENIDO WEB REQUERIDO MEDIANTE IPV6. • DEBERA DE SOPORTAR EL FILTRADO DE CONTENIDO BASADO EN CATEGORÍAS EN TIEMPO REAL, INTEGRADO A LA PLATAFORMA DE SEGURIDAD "APPLIANCE". SIN NECESIDAD DE INSTALAR UN SERVIDOR O APPLIANCE EXTERNO, LICENCIAMIENTO DE UN PRODUCTO EXTERNO O SOFTWARE ADICIONAL PARA REALIZAR LA CATEGORIZACIÓN DEL CONTENIDO. • DEBERA DE SER CONFIGURABLE DIRECTAMENTE DESDE LA INTERFAZ DE ADMINISTRACIÓN DEL DISPOSITIVO APPLIANCE. CON CAPACIDAD PARA PERMITIR ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. • DEBERÁ PERMITIR DIFERENTES PERFILES DE UTILIZACIÓN DE LA WEB (PERMISOS DIFERENTES PARA CATEGORÍAS) DEPENDIENDO DE FUENTE DE LA CONEXIÓN O GRUPO DE USUARIO AL QUE PERTENEZCA LA CONEXIÓN SIENDO ESTABLECIDA • DEBERA PERMITIR QUE LOS MENSAJES ENTREGADOS AL USUARIO POR PARTE DEL URL FILTER (POR EJEMPLO, EN CASO DE QUE UN USUARIO INTENTE NAVEGAR A UN SITIO CORRESPONDIENTE A UNA CATEGORÍA NO PERMITIDA) DEBERÁN SER PERSONALIZABLES.

			• DEBERA DE SOPORTAR LA CAPACIDAD DE FILTRADO DE SCRIPTS EN PÁGINAS WEB (JAVA/ACTIVE X). • LA SOLUCIÓN DE FILTRAJE DE CONTENIDO DEBE SOPORTAR EL FORZAMIENTO DE "SAFE SEARCH" O "BÚSQUEDA SEGURA" INDEPENDIENTEMENTE DE LA CONFIGURACIÓN EN EL BROWSER DEL USUARIO. ESTA FUNCIONALIDAD NO PERMITIRÁ QUE LOS BUSCADORES RETORNEN RESULTADOS CONSIDERADOS COMO CONTROVERSIALES. ESTA FUNCIONALIDAD SE SOPORTARÁ AL MENOS PARA GOOGLE, YAHOO! Y BING. • DEBERA SER POSIBLE DEFINIR CUOTAS DE TIEMPO PARA LA NAVEGACIÓN. DICHAS CUOTAS DEBEN PODER ASIGNARSE POR CADA CATEGORÍA Y POR GRUPOS. • DEBERA SER POSIBLE EXCEPTUAR LA INSPECCIÓN DE HTTPS POR CATEGORÍA. PROTECCIÓN CONTRA INTRUSOS (IPS) • EL DETECTOR Y PREVENTOR DE INTRUSOS DEBEN PODER IMPLEMENTARSE TANTO EN LÍNEA COMO FUERA DE LINEA. EN LÍNEA, EL TRÁFICO A SER INSPECCIONADO PASARÁ A TRAVÉS DEL EQUIPO. FUERA DE LÍNEA, EL EQUIPO RECIBIRÁ EL TRÁFICO A INSPECCIONAR DESDE UN SWITCH CON UN PUERTO CONFIGURADO EN SPAN O MIRROR • EL DETECTOR Y PREVENTOR DE INTRUSOS DEBERÁ IMPLEMENTARSE EN LINEA Y FUERA DE LINEA EN FORMA SIMULTÁNEA PARA DISTINTOS SEGMENTOS. • DEBERÁ SER POSIBLE DEFINIR POLÍTICAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES PARA TRÁFICO IPV6 • DEBERA TENER LA CAPACIDAD DE DETECCIÓN DE MÁS DE 5000 ATAQUES. • DEBERA TENER LA CAPACIDAD DE ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS IPS MEDIANTE TECNOLOGÍA DE TIPO "PUSH" (PERMITIR RECIBIR LAS ACTUALIZACIONES CUANDO LOS CENTROS DE ACTUALIZACIÓN ENVÍEN NOTIFICACIONES SIN PROGRAMACIÓN PREVIA), ADICIONAL A TECNOLOGÍAS TIPO "PULL" (CONSULTAR LOS CENTROS DE ACTUALIZACIÓN POR VERSIONES NUEVAS) • EL DETECTOR Y PREVENTOR DE INTRUSOS DEBERÁ DE ESTAR ORIENTADO PARA LA PROTECCIÓN DE REDES. • EL DETECTOR Y PREVENTOR DE INTRUSOS DEBERÁ ESTAR INTEGRADO A LA PLATAFORMA DE SEGURIDAD "APPLIANCE". SIN NECESIDAD DE INSTALAR UN SERVIDOR O APPLIANCE EXTERNO, LICENCIAMIENTO DE UN PRODUCTO EXTERNO O SOFTWARE ADICIONAL PARA REALIZAR LA PREVENCIÓN DE INTRUSOS. LA INTERFAZ DE ADMINISTRACIÓN DEL DETECTOR Y PREVENTOR DE INTRUSOS DEBERÁ DE ESTAR PERFECTAMENTE INTEGRADA A LA INTERFAZ DE ADMINISTRACIÓN DEL DISPOSITIVO DE SEGURIDAD APPLIANCE, SIN NECESIDAD DE INTEGRAR OTRO TIPO DE CONSOLA PARA PODER ADMINISTRAR ESTE SERVICIO. ESTA DEBERÁ PERMITIR LA PROTECCIÓN DE ESTE SERVICIO POR POLÍTICA DE CONTROL DE ACCESO. • EL DETECTOR Y PREVENTOR DE INTRUSOS DEBERÁ SOPORTAR CAPTAR ATAQUES POR ANOMALÍA (ANOMALY DETECTION) ADEMÁS DE FIRMAS (SIGNATURE BASED / MISUSE DETECTION).

			• BASADO EN ANÁLISIS DE FIRMAS EN EL FLUJO DE DATOS EN LA RED, Y DEBERÁ PERMITIR CONFIGURAR FIRMAS NUEVAS PARA CUALQUIER PROTOCOLO. • TECNOLOGÍA DE DETECCIÓN TIPO STATEFUL BASADA EN FIRMAS (SIGNATURES). • DEBERA DE SOPORTAR LA ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS PARA EL DETECTOR DE INTRUSOS • EL DETECTOR DE INTRUSOS DEBERÁ MITIGAR LOS EFECTOS DE LOS ATAQUES DE NEGACIÓN DE SERVICIOS. • DEBERA DE CONTAR CON MECANISMOS DE DETECCIÓN DE ATAQUES Y RECONOCIMIENTO DE PATRONES, ANÁLISIS DE PROTOCOLOS, DETECCIÓN DE ANOMALÍAS , DETECCIÓN DE ATAQUES DE RPC (REMOTE PROCEDURE CALL) • DEBERA DE CONTAR CON PROTECCIÓN CONTRA ATAQUES DE WINDOWS O NETBIOS • DEBERA DE CONTAR CON PROTECCIÓN CONTRA ATAQUES DE SMTP (SIMPLE MESSAGE TRANSFER PROTOCOL) IMAP (INTERNET MESSAGE ACCESS PROTOCOL, SENDMAIL O POP (POST OFFICE PROTOCOL) • DEBERA DE CONTAR CON PROTECCIÓN CONTRA ATAQUES DNS (DOMAIN NAME SYSTEM) • DEBERA DE CONTAR CON PROTECCIÓN CONTRA ATAQUES A FTP, SSH , TELNET Y RLOGIN • DEBERA DE CONTAR CON PROTECCIÓN CONTRA ATAQUES DE ICMP (INTERNET CONTROL MESSAGE PROTOCOL). • DEBERA DE CONTAR CON MÉTODOS DE NOTIFICACIÓN: • ALARMAS MOSTRADAS EN LA CONSOLA DE ADMINISTRACIÓN DEL APPLIANCE. • ALERTAS VÍA CORREO ELECTRÓNICO. • DEBERÁ TENER LA CAPACIDAD DE CUARENTENA, ES DECIR PROHIBIR EL TRÁFICO SUBSIGUIENTE A LA DETECCIÓN DE UN POSIBLE ATAQUE. ESTA CUARENTENA DEBE PODER DEFINIRSE AL MENOS PARA EL TRÁFICO PROVENIENTE DEL ATACANTE O PARA EL TRÁFICO DEL ATACANTE AL ATACADO. • LA CAPACIDAD DE CUARENTENA DEBERÁ OFRECER LA POSIBILIDAD DE DEFINIR EL TIEMPO EN QUE SE BLOQUEARÁ EL TRÁFICO. TAMBIÉN PODRÁ DEFINIRSE EL BLOQUEO DE FORMA "INDEFINIDA", HASTA QUE UN ADMINISTRADOR TOME UNA ACCIÓN AL RESPECTO. • DEBERÁ DE OFRECER LA POSIBILIDAD DE GUARDAR INFORMACIÓN SOBRE EL PAQUETE DE RED QUE DETONÓ LA DETECCIÓN DEL ATAQUE ASÍ COMO AL MENOS LOS 5 PAQUETES SUCESIVOS. ESTOS PAQUETES DEBEN PODER SER VISUALIZADOS POR UNA HERRAMIENTA QUE SOPORTE EL FORMATO PCAP. PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP) • LA SOLUCIÓN DEBERÁ OFRECER LA POSIBILIDAD DE DEFINIR REGLAS QUE PERMITAN ANALIZAR LOS DISTINTOS ARCHIVOS QUE CIRCULAN A TRAVÉS DE LA RED EN BÚSQUEDA DE INFORMACIÓN CONFIDENCIAL. • LA FUNCIONALIDAD DEBERÁ SOPORTAR EL ANÁLISIS DE ARCHIVOS

			DEL TIPO: MS-WORD, PDF, TEXTO, ARCHIVOS COMPRIMIDOS. • DEBERÁ SOPORTARSE EL ESCANEO DE ARCHIVOS EN AL MENOS LOS SIGUIENTES PROTOCOLOS: HTTP, POP3, SMTP, IMAP, NNTP Y FTP. • ANTE LA DETECCIÓN DE UNA POSIBLE FUGA DE INFORMACIÓN DEBERÁ PODER APLICARSE EL MENOS LAS SIGUIENTES ACCIONES: BLOQUEAR EL TRÁFICO DEL USUARIO, BLOQUEAR EL TRÁFICO DE LA DIRECCIÓN IP DE ORIGEN, REGISTRAR EL EVENTO, • EN CASO DEL BLOQUEO DE USUARIOS, LA SOLUCIÓN DEBERÁ PERMITIR DEFINIR POR CUÁNTO TIEMPO SE HARÁ EL BLOQUEO O EN SU DEFECTO BLOQUEAR POR TIEMPO INDEFINIDO HASTA QUE EL ADMINISTRADOR TOME UNA ACCIÓN. • LA SOLUCIÓN DEBERÁ SOPORTAR LA CAPACIDAD DE GUARDAR UNA COPIA DEL ARCHIVO IDENTIFICADO COMO POSIBLE FUGA DE INFORMACIÓN. ESTA COPIA PODRÍA SER ARCHIVADA LOCALMENTE O EN OTRO DISPOSITIVO. • LA SOLUCIÓN DEBERÁ PERMITIR LA BÚSQUEDA DE PATRONES EN ARCHIVOS MEDIANTE LA DEFINICIÓN DE EXPRESIONES REGULARES. CONTROL DE APLICACIONES • LO SOLUCIÓN DEBERÁ SOPORTAR LA CAPACIDAD DE IDENTIFICAR LA APLICACIÓN QUE ORIGINA CIERTO TRÁFICO A PARTIR DE LA INSPECCIÓN DEL MISMO. • LA IDENTIFICACIÓN DE LA APLICACIÓN DEBERÁ SER INDEPENDIENTE DEL PUERTO Y PROTOCOLO HACIA EL CUAL ESTÉ DIRECCIONADO DICHO TRÁFICO. • LA SOLUCIÓN DEBERÁ TENER UN LISTADO DE AL MENOS 1000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE. • EL LISTADO DE APLICACIONES DEBERÁ ACTUALIZARSE PERIÓDICAMENTE. • PARA APLICACIONES IDENTIFICADAS DEBERÁN PODER DEFINIRSE AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) DEBERÁN PODER DEFINIRSE AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES DE TIPO P2P DEBERÁ PODER DEFINIRSE ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING. • PREFERENTEMENTE DEBERÁN SOPORTAR MAYOR GRANULARIDAD EN LAS ACCIONES. INSPECCIÓN DE CONTENIDO SSL • LA SOLUCIÓN DEBERÁ SOPORTAR LA CAPACIDAD DE INSPECCIONAR TRÁFICO QUE ESTÉ SIENDO ENCRIPTADO MEDIANTE TLS AL MENOS PARA LOS SIGUIENTES PROTOCOLOS: HTTPS, IMAPS, SMTPS, POP3S. • LA INSPECCIÓN DEBERÁ REALIZARSE MEDIANTE LA TÉCNICA CONOCIDA COMO HOMBRE EN EL MEDIO (MITM – MAN IN THE MIDDLE). • LA INSPECCIÓN DE CONTENIDO ENCRIPTADO NO DEBERÁ REQUERIR NINGÚN CAMBIO DE CONFIGURACIÓN EN LAS APLICACIONES O SISTEMA

			OPERATIVO DEL USUARIO. • PARA EL CASO DE URL FILTERING, DEBERÁ SER POSIBLE CONFIGURAR EXCEPCIONES DE INSPECCIÓN DE HTTPS. DICHAS EXCEPCIONES EVITAN QUE EL TRÁFICO SEA INSPECCIONADO PARA LOS SITIOS CONFIGURADOS. LAS EXCEPCIONES DEBEN PODER DETERMINARSE AL MENOS POR CATEGORÍA DE FILTRADO. FILTRAJE DE TRÁFICO VOIP, PEER-TO-PEER Y MENSAJERÍA INSTANTÁNEA • DEBERA DAR SOPORTE A APLICACIONES MULTIMEDIA TALES COMO (INCLUYENDO): SCCP (SKINNY), H.323, SIP, REAL TIME STREAMING PROTOCOL (RTSP). • EL DISPOSITIVO DEBERÁ CONTAR CON TÉCNICAS DE DETECCIÓN DE P2P Y PROGRAMAS DE ARCHIVOS COMPARTIDOS (PEER-TO-PEER), SOPORTANDO AL MENOS YAHOO! MESSENGER, MSN MESSENGER, ICQ Y AOL MESSENGER PARA MESSENGER, Y BITTORRENT, EDONKEY, GNUTELLA, KAZAA, SKYPE Y WINNY PARA PEER-TO-PEER. • EN EL CASO DE LOS PROGRAMAS PARA COMPARTIR ARCHIVOS (PEER-TO-PEER) DEBERÁ PODER LIMITAR EL ANCHO DE BANDA UTILIZADO POR ELLOS, DE MANERA INDIVIDUAL. • LA SOLUCIÓN DEBERÁ DE CONTAR CON UN ALG (APPLICATION LAYER GATEWAY) DE SIP • DEBERÁ PODER HACERSE INSPECCIÓN DE ENCABEZADOS DE SIP • DEBERÁN PODER LIMITARSE LA CANTIDAD DE REQUERIMIENTOS SIP QUE SE HACEN POR SEGUNDO. ESTO DEBE PODER DEFINIRSE POR CADA MÉTODO SIP. • LA SOLUCIÓN DEBERÁ SOPORTAR SIP HNT (HOSTED NAT TRANSVERSAL). ALTA DISPONIBILIDAD • DEBERÁ DE CONTAR CON LA POSIBILIDAD DE DAR SOPORTNE EN FIREWALL, A ALTA DISPONIBILIDAD TRANSPARENTE, ES DECIR, SIN PÉRDIDA DE CONEXIONES EN CASO DE QUE UN NODO FALLE. • DEBERÁ DE SOPORTAR ALTA DISPONIBILIDAD EN MODO ACTIVO-PASIVO • DEBERÁ DE SOPORTAR ALTA DISPONIBILIDAD EN MODO ACTIVO-ACTIVO • DEBERÁ DE TENER LA POSIBILIDAD DE DEFINIR AL MENOS DOS INTERFACES PARA SINCRONÍA • EL ALTA DISPONIBILIDAD PODRÁ HACERSE DE FORMA QUE EL USO DE MULTICAST NO SEA NECESARIO EN LA RED • DEBERÁ DE SER POSIBLE DEFINIR INTERFACES DE GESTIÓN INDEPENDIENTES PARA CADA MIEMBRO EN UN CLUSTER. CARACTERÍSTICAS DE GERENCIA

			• DEBERÁ TENER UNA INTERFAZ GRÁFICA DE USUARIO (GUI), VÍA WEB POR HTTP Y HTTPS PARA HACER ADMINISTRACIÓN DE LAS POLÍTICAS DE SEGURIDAD Y QUE FORME PARTE DE LA ARQUITECTURA NATIVA DE LA SOLUCIÓN PARA ADMINISTRAR LA SOLUCIÓN LOCALMENTE. POR SEGURIDAD LA INTERFAZ DEBERÁ SOPORTAR SSL SOBRE HTTP (HTTPS) • LA INTERFAZ GRÁFICA DE USUARIO (GUI) VÍA WEB DEBERÁ PODER ESTAR EN ESPAÑOL Y EN INGLÉS, CONFIGURABLE POR EL USUARIO. • DEBERÁ TENER UNA INTERFAZ BASADA EN LÍNEA DE COMANDO (CLI) PARA ADMINISTRACIÓN DE LA SOLUCIÓN. • DEBERÁ DE TENER UN PUERTO SERIAL DEDICADO PARA ADMINISTRACIÓN. ESTE PUERTO DEBE ESTAR ETIQUETADO E IDENTIFICADO PARA TAL EFECTO. • LA COMUNICACIÓN DEBERÁ DE ESTAR CIFRADA Y AUTENTICADA CON USERNAME Y PASSWORD, TANTO COMO PARA LA INTERFAZ GRÁFICA DE USUARIO COMO LA CONSOLA DE ADMINISTRACIÓN DE LÍNEA DE COMANDOS (SSH O TELNET) • EL ADMINISTRADOR DEL SISTEMA PODRÁ TENER LAS OPCIONES INCLUÍDAS DE AUTENTICARSE VÍA PASSWORD Y VÍA CERTIFICADOS DIGITALES. • LOS ADMINISTRADORES PODRÁN TENER ASIGNADO UN PERFIL DE ADMINISTRACIÓN QUE PERMITA DELIMITAR LAS FUNCIONES DEL EQUIPO QUE PUEDEN GERENCIAR Y AFECTAR. • EL EQUIPO OFRECERÁ LA FLEXIBILIDAD PARA ESPECIFICAR QUE LOS ADMINISTRADORES PUEDAN ESTAR RESTRINGIDOS A CONECTARSE DESDE CIERTAS DIRECCIONES IP CUANDO SE UTILICE SSH, TELNET, HTTP O HTTPS. • EL EQUIPO DEBERÁ PODER ADMINISTRARSE EN SU TOTALIDAD (INCLUYENDO FUNCIONES DE SEGURIDAD, RUTEO Y BITÁCORAS) DESDE CUALQUIER EQUIPO CONECTADO A INTERNET QUE TENGA UN BROWSER (INTERNET EXPLORER, MOZILLA, FIREFOX) INSTALADO SIN NECESIDAD DE INSTALACIÓN DE NINGUN SOFTWARE ADICIONAL. • DEBERÁ DE DAR SOPORTE DE SNMP VERSIÓN 2 • DEBERÁ DE DAR SOPORTE DE SNMP VERSIÓN 3 • DEBERÁ DE DAR SOPORTE DE AL MENOS 3 SERVIDORES SYSLOG PARA PODER ENVIAR BITÁCORAS A SERVIDORES DE SYSLOG REMOTOS • DEBERÁ DE DAR SOPORTAR PARA ALMACENAMIENTO DE EVENTOS EN UN REPOSITORIO QUE PUEDA CONSULTARSE LUEGO CON SQL. • DEBERÁ DE DAR SOPORTE DE CONTROL DE ACCESO BASADO EN ROLES, CON CAPACIDAD DE CREAR AL MENOS 6 PERFILES PARA ADMINISTRACIÓN Y MONITOREO DEL FIREWALL. • EL MONITOREO DE COMPORTAMIENTO DEL APPLIANCE MEDIANTE SNMP, EL DISPOSITIVO DEBERÁ SER CAPAZ DE ENVIAR TRAPS DE SNMP CUANDO OCURRA UN EVENTO RELEVANTE PARA LA CORRECTA OPERACIÓN DE LA RED. • DEBERÁ SER POSIBLE DEFINIR LA DIRECCIÓN IP QUE SE UTILIZARÁ COMO ORIGEN PARA EL TRÁFICO INICIADO DESDE EL MISMO DISPOSITIVO. ESTO DEBE PODER HACERSE AL MENOS PARA EL TRÁFICO DE ALERTAS, SNMP, LOG Y GESTIÓN. VIRTUALIZACIÓN

			• EL DISPOSITIVO DEBERÁ PODER VIRTUALIZAR LOS SERVICIOS DE SEGURIDAD MEDIANTE "VIRTUAL SYSTEMS", "VIRTUAL FIREWALLS" O "VIRTUAL DOMAINS" • LA INSTANCIA VIRTUAL DEBE SOPORTAR POR LO MENOS FIREWALL, VPN, URL FILTERING, IPS Y ANTIVIRUS • CADA INSTANCIA VIRTUAL DEBERÁ PODER TENER UN ADMINISTRADOR INDEPENDIENTE • LA CONFIGURACIÓN DE CADA INSTANCIA VIRTUAL DEBERÁ PODER ESTAR AISLADA DE MANERA LÓGICA DEL RESTO DE LAS INSTANCIAS VIRTUALES. • CADA INSTANCIA VIRTUAL DEBERÁ PODER ESTAR EN MODO GATEWAY O EN MODO TRANSPARENTE A LA RED • DEBERÁ SER POSIBLE LA DEFINICIÓN Y ASIGNACIÓN DE RECURSOS DE FORMA INDEPENDIENTE PARA CADA INSTANCIA VIRTUAL • DEBERÁ SER POSIBLE DEFINIR DISTINTOS SERVIDORES DE LOG (SYSLOG) PARA CADA INSTANCIA VIRTUAL. • DEBERÁ SER POSIBLE DEFINIR Y MODIFICAR LOS MENSAJES MOSTRADOS POR EL DISPOSITIVO DE FORMA INDEPENDIENTE PARA CADA INSTANCIA VIRTUAL. ESTÁNDARES Y CERTIFICACIONES • LA SOLUCIÓN DEBERÁ CONTAR CON AL MENOS LAS SIGUIENTES CERTIFICACIONES Y CUMPLIR CON LOS SIGUIENTES ESTÁNDARES • * CERTIFICACIONES • CERTIFICACIÓN ICSA PARA EL FIREWALL. • CERTIFICACIÓN ICSA IPSEC. (VPN IPSEC) • CERTIFICACIÓN ICSA PARA SSL-TLS (VPN SSL) • CERTIFICACIÓN ICSA PARA EL DETECTOR DE INTRUSOS (IPS) • CERTIFICACIÓN ICSA PARA EL ANTIVIRUS • CERTIFICACIÓN NSS COMO UTM • CERTIFICACIÓN COMMON CRITERIA COMO EAL4+ * ESTÁNDARES SOPORTE DOCUMENTADO DE LOS SIGUIENTES RFCS: RFC 0768, RFC 0791, RFC 0792, RFC 0793, RFC 0822, RFC 1035, RFC 1112, RFC 1119, RFC 1123, RFC 1191, RFC 1323, RFC 1340, RFC 1349, RFC 1519, RFC 1577, RFC 1700, RFC 1812, RFC 1918, RFC 2131, RFC 2181, RFC 2225, RFC 2236, RFC 2373, RFC 2460, RFC 2461, RFC 2462, RFC 2474, RFC 2822, RFC 3232, RFC 3456, RFC 3513, RFC 4291, RFC 1866, RFC 1867, RFC 1945, RFC 2068, RFC 2616, RFC 2817, RFC 2854, RFC 1321, RFC 1631, RFC 1829, RFC 2104, RFC 2401, RFC 2403, RFC 2404, RFC 2405, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2410, RFC 2411, RFC 2412, RFC 2459, RFC 2631, RFC 2637, RFC 2661, RFC 3706. SOPORTE DOCUMENTADO A LOS SIGUIENTES ESTÁNDARES DE CRIPTOGRAFÍA: PKCS #7 (RFC 2315), PKCS #10 (RFC 2986), PKCS #12

			LICENCIAMIENTO Y ACTUALIZACIONES EL LICENCIAMIENTO DE TODAS LAS FUNCIONALIDADES DEBE SER ILIMITADO EN CUANTO A USUARIOS, CAJAS DE CORREO, CONEXIONES, EQUIPOS QUE PASAN A TRAVÉS DE VIGENCIA DE LICENCIA DE ACTUALIZACIÓN LA VIGENCIA DE LAS ACTUALIZACIONES PARA LOS SERVICIOS DE ANTIVIRUS, ANTISPAM, IPS Y URL FILTERING DEBE PROVEERSE POR AL MENOS 1 AÑO. DESEMPEÑO / CONECTIVIDAD EL EQUIPO DEBE POR LO MENOS OFRECER LAS SIGUIENTES CARACTERÍSTICAS DE DESEMPEÑO Y CONECTIVIDAD A) THROUGHPUT - FIREWALL: 2.5 GBPS - VPN (3DES): 8 GBPS - ANTIVIRUS: 950 MBPS - IPS: 450 MBPS B) CONEXIONES CONCURRENTES TOTALES • 3 MILLONES C) NUEVAS CONEXIONES POR SEGUNDO • 22,000 D) INTERFACES DE RED UNO (1) 10/100/1000 INTERFAZ/PUERTO PARA ADMINISTRACION. • VEINTE (20) 10/100/1000 INTERFAZ/PUERTO (RG-45). • DOS (2) INTERFAZ/PUERTO COMPARTIDO 10/100/1000 GE SFP / RJ45 10/100/1000 EL EQUIPO DEBERÁ INCLUIR GARANTÍA LIMITADA POR UN AÑO PROPORCIONADA DIRECTAMENTE POR EL FABRICANTE, CON ATENCIÓN 8X5 Y SUSCRIPCIÓN A ACTUALIZACIONES DE SEGURIDAD POR 1 AÑO. LOS COMPONENTES DEL INCISO A) B) DEBERÁN SER DEL MISMO FABRICANTE PARA GARANTIZAR EL 100% DE COMPATIBILIDAD Y TODAS LAS FUNCIONES DE INTEROPERABILIDAD.

ANEXO B
FORMATO PARA ACREDITAR LA PERSONALIDAD

Comité de Compras del Poder Judicial del Estado de Tabasco; (NOMBRE DE QUIEN FIRMA) manifiesto bajo protesta de decir verdad, que los datos aquí asentados son ciertos y han sido debidamente verificados, así como de que cuento con facultades suficientes para suscribir la propuesta en la presente licitación, a nombre y representación de: (PERSONA FISICA O JURIDICA COLECTIVA).

DATOS DE LICITACION: LICITACION SIMPLIFICADA (MAYOR/MENOR)
No.
ADQUISICIÓN DE_____

Registro Federal de Contribuyentes:
Domicilio:
Calle y Número:
Colonia: **Delegación o Municipio:**
Código Postal: **Entidad Federativa:**
Correo Electrónico:
No. de la Escritura en la que consta su acta Constitutiva:
Fecha:
Nombre, Número y Lugar del Notario Público ante quien se dió fé de la misma:
Relación de Accionistas:
Apellido Paterno, Apellido Materno, Nombre(s).
Descripción del Objeto Social:
Reformas al Acta Constitutiva:

Nombre del apoderado o representante:
Datos del documento mediante el cuál acredita su personalidad y facultades:
Escritura Pública Número: **Fecha:**
Nombre, Número y Lugar del Notario Público ante el cuál se otorgó: