Poder Judicial del Estado de Tabasco

Tribunal Superior de Justicia

Comité de Compras

LICITACIÓN PÚBLICA NACIONAL

No. 56063001-003-13

PRESENTACIÓN

El Tribunal Superior de Justicia del Estado de Tabasco, en cumplimiento a las disposiciones legales que rigen la materia, convoca a personas físicas y jurídicas colectivas, a participar en la presente licitación pública de carácter nacional, para la adjudicación de un contrato de adquisición de **Equipos de Comunicación y Teleradio-comunicación**, bajo las siguientes:

B A S E S

Junio de 2013.

1. Glosario de términos.

Para efectos de estas bases, se entenderá por:

TRIBUNAL:	El Tribunal Superior de Justicia del Estado de Tabasco
CONTRALORÍA:	La Dirección de Contraloría Judicial
OFICIALIA:	La Oficialía Mayor del Poder Judicial
TESORERÍA:	La Tesorería del Poder Judicial.
COMITÉ:	El Comité de Compras del Poder Judicial
LEY:	Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del estado de Tabasco.
REGLAMENTO:	Reglamento de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del estado de Tabasco
BASES:	Documento que contiene los conceptos y criterios que regirán y serán aplicados para la adjudicación del o los contratos.
CONTRATO:	Documento que establece los derechos y obligaciones entre la convocante y proveedor
PROPUESTA O PROPOSICIÓN	Oferta técnica y económica que presenten los licitantes
CONVOCANTE:	El Tribunal Superior de Justicia del estado de Tabasco, quien en apego a la Ley de la materia, realiza la licitación
PROVEEDOR:	La persona física o jurídica colectiva, que celebre contratos de adquisiciones, arrendamientos o de servicios relacionados con las mismas

LICITANTE:	La persona que participe en este procedimiento de licitación pública
BIENES:	Los productos a adquirir, motivo de esta licitación
RENGLON O PARTIDA	Descripción y clasificación específica de los bienes
IFOS	Ingresos Fiscales Ordinarios
DIAS Y HORAS HABILES	Se entenderán como días y horas hábiles Los días Lunes, Martes, Miércoles, Jueves y Viernes, y el horario que comprenden será de las 8:00 a las 15:00 horas.

2. INFORMACIÓN GENERAL DE LA LICITACIÓN.

2.1. OFICINAS RELACIONADAS CON EL PROCEDIMIENTO.

OFICIALIA MAYOR JUDICIAL:

At'n. LIC. Alberto Caso Becerra

Presidente del Comité de Compras y Oficial Mayor

Tel. 3 58 2000 ext. 2026

TESORERIA JUDICIAL

At'n. L.C.P. Alberto Vidal Castillo

Vice-Presidente del Comité de Compras y Tesorero Judicial

Tel. 3 58 2000 ext. 2027

COORDINACION DE CONTROL PRESUPUESTAL

At'n. Lic. Romeo Notario Marcín

Secretario del Comité de Compras y Coordinador de Control Presupuestal

Tel. 3 58 2000 ext. 2087 y 2088

CONTRALORÍA JUDICIAL

At'n. L.C.P. Adriana María González Aranda

1er. Vocal del Comité de Compras y Encargada de la Dirección de Contraloría.

Tel. 358-20-00 Ext. 2028

DIRECCION DE ESTADISTICA, INFORMATICA Y COMPUTACION

At´n Ing. Voltaire Jesus Torre

Director.

Tel: 3 582000 ext. 2029

UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN

At´n. L.C.P. Ada Patricia Herrera González

Titular de la Unidad de Transparencia y Acceso a la Información

Tel: 3 58 2000 ext. 2128 Fax: 2072

Sitio Web: http://www.tsj-tabasco.gob.mx

Correo: transparencia@tsj-tabasco.gob.mx

UBICACIÓN DE LAS OFICINAS RELACIONADAS:

Domicilio: Edificio Sede del Tribunal Superior de Justicia.

Calle Independencia esquina Nicolás Bravo s/n

Col. Centro C.P. 86000

Villahermosa, Tabasco

3. VENTA DE LAS BASES.

Derivado del oficio No. SC/DGNECS/0136/2010; suscrito por el C.P. Roger Pérez Evoli, Secretario de Contraloría del Gobierno del estado de Tabasco; quien en fecha 02 de marzo de 2010, informó al titular del Poder Judicial; la disposición normativa del sistema Compranet; mediante la cual se notifica que es facultad de las dependencias y entidades del estado de Tabasco; el decidir el cobro por obtención de Bases de Licitaciones Públicas; así como comunicar a los interesados en participar de las mismas el costo y forma de pago de dichas bases; toda vez que a partir del 15 de

marzo de 2010; el sistema Compranet dejó de emitir los formatos de Pagos de Bases; se comunica a todos los interesados lo siguiente:

Que de conformidad a lo que disponen los artículos 26, fracción III, de la Ley y 36 fracción II del Reglamento de la Ley; las bases estarán a disposición de los interesados para consulta y/o venta en la Oficialía Mayor, ubicada en el 3er. Piso del edificio sede del Tribunal Superior de Justicia, ubicado en la Calle Independencia esq. Nicolás Bravo s/n; Col. Centro Villahermosa, Tabasco, C.P. 86000 Tel/Fax. (01993) 358-2000, ext. 2026 en días y horas hábiles, desde la publicación de la convocatoria y hasta el 14 de Junio de 2013; en horario de 9:00 a 15:00 horas.

En el entendido de que el horario señalado para venta de bases, concluye el día 14 de Junio de 2013 a las 15:00 horas. Y por ninguna otra causa se extenderá dicho plazo. Por lo que no se aceptarán propuestas de los licitantes que presenten fichas de depósitos con sello de Banco después de la fecha y hora indicada como límite para adquirir bases.

El costo de las bases es la cantidad de **$2,500.00 (Dos Mil Quinientos Pesos, 00/100 MN)** (IVA incluido), cantidad que podrá ser pagada mediante efectivo; depósitos o transferencia bancaria, a favor del Tribunal Superior de Justicia del estado de Tabasco, en la institución **HSBC** al número de cuenta **400323033-1**, con clave interbancaria: 021790040032303312 cuyo Registro Federal de Contribuyentes es TSJ-250202-PH0. O bien directamente en la Tesorería Judicial del Tribunal Superior de Justicia.

Aquellas empresas o personas físicas con actividad comercial que opten por realizar el pago de sus bases directamente en instituciones bancarias, indefectiblemente deberán acudir a la Tesorería judicial, a fin de que mediante el canje de la ficha de depósito, se les entregará el recibo oficial de pago de bases que emite la Tesorería Judicial; toda vez, que será este recibo el que se deberá de adjuntar a las proposiciones técnicas de cada licitante. (DOCUMENTO No. 1). Lo anterior en virtud de que esta convocante, requiere las fichas de depósito de quienes hayan pagado sus

bases a través de instituciones bancarias a fin de poder rastrear estos depósitos en la cuenta.

Los interesados que así lo deseen, podrán revisar gratuitamente, las bases de manera electrónica o física en la Unidad de Transparencia y Acceso a la Información del Poder Judicial, sito en el sótano del Tribunal Superior de Justicia, o en nuestro sitio web http://www.tsj-tabasco.gob.mx Así también, las bases estarán disponibles para consulta en el sistema electrónico de contrataciones gubernamentales del gobierno del Estado de Tabasco, (CompraNet), en la dirección electrónica http://contraloria.tabasco.gob.mx/content/licitaciones-2013, Licitación Pública con Normatividad Estatal.

3.1. MARCO JURIDICO.

- **Constitución Política de los Estados Unidos Mexicanos: Artículo 134.**
- **Constitución Política del estado libre y soberano de Tabasco, artículo 76.**
- **Ley Orgánica del Poder Judicial del estado de Tabasco.**
- **Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del estado de Tabasco.**
- **Ley Estatal de Presupuesto, Contabilidad y Gasto Público**
- **Código Fiscal de la Federación**
- **Ley Federal de Instituciones de Fianzas: Artículos 93, 93 Bis, 95 y 95 Bis, 118 y 120.**
- **Reglamento de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del estado de Tabasco.**
- **Código Civil Vigente en el estado de Tabasco.**
- **Código de Procedimientos Civiles para el estado libre y soberano de Tabasco.**
- **Reglamento del Comité de Compras del Poder Judicial del estado.**
- **Manual de Normas y Lineamientos Presupuestarios para la Administración Pública del Poder Judicial**

3.2. ORIGEN DE LOS RECURSOS.

Los recursos económicos para la Adquisición de los bienes materia de esta licitación, provienen de los Ingresos Fiscales Ordinarios IFOS 2013, y su utilización ha sido debidamente autorizada mediante Oficio No. SPF-0002/2013, de fecha 2 de Enero de 2013.

4.- OBJETO DE LA LICITACIÓN, JUSTIFICACIÓN Y CARÁCTER DE LA MISMA.

4.1. OBJETO

La presente licitación tiene por objeto la Adquisición de Bienes de Telefonía y Teleradio-Comunicaciones, para el cumplimiento de las actividades de todos los juzgados establecidos en la entidad, proporcionando un enlace de comunicación interinstitucional con altos niveles de seguridad, resilencia, confianza y robustes necesarias para dar respuesta pronta, confiable y segura a las necesidades de comunicación a nivel interno y externo.

4.2 JUSTIFICACIÓN

Proveer bienes de Telefonía y Teleradio-Comunicaciones que permitan a las áreas jurisdiccionales, realizar con mayor confianza y claridad la transmisión de información vía telefónica de las actividades diarias; brindando mayores niveles de confiabilidad, estabilidad y seguridad a las comunicaciones del poder judicial a fin de que pueda prestarse un servicio más expedito a la ciudadanía que acude diariamente a solicitar la impartición de justicia.

1) En tal virtud, se han establecido las características y especificaciones técnicas que los bienes a ofertar en el presente proceso licitatorio deben de cumplir de manera indefectible; a fin de que estos puedan garantizar los niveles de seguridad y confianza lógicos y físicos para las comunicaciones interinstitucionales y hacia el exterior en el Poder Judicial. En ese mismo sentido los bienes sujetos al procedimiento de cuenta, deberán de cumplir a cabalidad con las características y especificaciones técnicas establecidas en

estas bases; y por tal motivo no serán admisibles ofertas de bienes que no satisfagan de manera precisa y exacta dichas especificaciones.

2) Lo anterior, considerando que las especificaciones solicitadas en los bienes materia del presente proceso licitatorio no limitan ni vulneran el derecho a la libre concurrencia de ofertas; en virtud de que existen en el país numerosas empresas registradas como distribuidores autorizados de bienes con las especificaciones y características solicitadas en estas bases; y en tal sentido no se afecta el principio de libre participación de las empresas y/o personas dedicadas al comercio de bienes de tecnología de la información.

Por lo anterior, los bienes considerados en el presente proceso se convocan a concurso de manera específica de acuerdo a las necesidades tecnológicas y en concordancia con las condiciones presupuestales de la institución, ya que de no hacerlo se causaría perjuicio grave al sistema de impartición de justicia, al vulnerar su presupuesto; y por ende, se verían seriamente afectados los servicios que diariamente se prestan a la ciudadanía en los 73 juzgados con los que se cuenta en la entidad.

Por los motivos expuestos se autorizó en el seno del Comité de Compras del Poder Judicial, en su sesión de fecha 20 de Mayo de 2013, que se lleve a cabo el procedimiento de licitación por convocatoria pública; conforme a lo previsto en el artículo 23, 1er. Párrafo, de la Ley de la materia; así también las presentes bases fueron revisadas y autorizadas en la misma sesión por el citado cuerpo colegiado, en concordancia a lo dispuesto por el articulo 34 del Reglamento de la Ley.

En el mismo sentido, se contempla un período de entrega para los equipos licitados de 45 días naturales contados a partir de la emisión del fallo, toda vez que se requiere disponer de los mismos en el transcurso del mes de agosto de este año, para

no retrasar los programas de ejecución en materia de equipamiento a que serán destinados, a efecto de cumplir en tiempo y forma con las metas planteadas durante el presente ejercicio.

4.3 CARÁCTER NACIONAL DE LA LICITACIÓN

Se determina de conformidad a lo establecido en los artículos 22, fracción I, 23, y 24, fracción II; de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios del Estado de Tabasco; y observando el ***Acuerdo por el que se Establecen las Reglas para la Determinación y Acreditación del Grado de Contenido Nacional, Publicado el 3 de Marzo de 2000***, y porque además, el Poder Judicial del estado de Tabasco no se encuentra contemplado en las listas de México ubicadas en los Anexos 1001.1ª-1 y 1001.1ª-2 del Capítulo X Denominado ***"Compras del Sector Público" del Tratado de Libre Comercio de América del Norte***, y en concordancia a lo que establece el artículo 1ro. Último párrafo de la Ley.

Para lo anterior, los licitantes deberán de exhibir:

1) Carta en papel membretado bajo protesta de decir verdad, de acuerdo a las partidas que oferten a esta institución: el grado de contenido nacional con el que cuenta su producto sin importar el número, es decir puede ir de 0% (en caso de productos cien por ciento importación) hasta 100% (en caso de productos nacionales). Quedando siempre bajo la estricta responsabilidad del proveedor, la obligación de garantizar en todo momento la legal importación de los productos, su permanencia y utilización en el país, así como la de contar en todo momento con las autorizaciones y permisos requeridos por la Secretaria de Relaciones Exteriores. (DOCUMENTO No. 2)

2) Carta en la que indique el licitante del equipo; el País de Procedencia de los productos que se ofertan en la licitación, expedida en términos de lo previsto en el ***Acuerdo por el que se Establecen las Reglas para la Determinación y Acreditación del Grado de Contenido Nacional, Publicado el 3 de Marzo de 2000***, conforme a los tratados de libre comercio para la adquisición de bienes, de conformidad con las disposiciones establecidas en los capítulos relativos a compras del sector público de los tratados de libre comercio que México tiene celebrados con diferentes países. Dicha carta, deberá ser expedida por el

fabricante del equipo en papel membretado original, con firma autógrafa de persona legalmente facultada; y Bajo protesta de decir verdad. **(DOCUMENTO No. 3)**

5. DESCRIPCIÓN DE BIENES REQUERIDOS Y GARANTÍAS

5.1. DESCRIPCIÓN Y CANTIDAD.

Los bienes a adquirir son **Equipos de Telefonia y Teleradio-comunicación**, con las características y especificaciones técnicas que a continuación se describen:

ANEXO 1

PARTIDA ÚNICA

LOS BIENES DE LOS INCISOS A), B), C), D), E), F), G), H), I), DEBERÁN DE SER DE UN MISMO FABRICANTE, SI NO SE INDICA LO CONTRARIO, ADEMÁS SERÁN 100% COMPATIBLES Y FUNCIONALES ENTRE SÍ; SIN NECESIDAD DE UTILIZAR YA SEA MÓDULOS, SOFTWARE Y LICENCIAMIENTO ADICIONAL.

DE IGUAL MANERA LOS BIENES DE LOS INCISOS J), K), DEBERÁN DE SER DE UN MISMO FABRICANTE, SI NO SE INDICA LO CONTRARIO, ADEMÁS SERÁN 100% COMPATIBLES Y FUNCIONALES ENTRE SÍ; SIN NECESIDAD DE UTILIZAR YA SEA MÓDULOS, SOFTWARE Y LICENCIAMIENTO ADICIONAL.

PARA TODOS LOS EQUIPOS MONTADOS EN RACK SE INCLUIRÁN LOS CABLES NECESARIOS PARA LA CONEXIÓN A LAS UNIDADES DE DISTRIBUCIÓN DE ENERGÍA, ASÍ COMO LOS ACCESORIOS NECESARIOS.

LA GARANTÍA DE LOS BIENES DE LOS INCISOS A), B), C), D), E), F), G), H), I), J), K), SERÁ DE UN (1) AÑO LIMITADA POR EL FABRICANTE.

INCISO	DESCRIPCIÓN	UNIDAD	CANTIDAD
A)	**SUMINISTRO E INSTALACIÓN DE SERVIDOR DE SISTEMA DE TELEFONIA IP** DEBERÁ CUMPLIR CON LAS SIGUIENTES ESPECIFICACIONES FISICAS Y FUNCIONALES: • SERÁ PROPORCIONADO POR EL MISMO FABRICANTE DEL SOFTWARE DE TELEFONÍA INDICADO EN EL INCISO B) • DEBERA SER COMPATIBLE PARA LA INSTALACION DE SISTEMAS DE COMUNICACIONES UNIFICADAS PARA SOPORTAR LAS DIFERENTES PLATAFORMAS DE COLABORACION COMO SISTEMAS DE TELEFONIA IP, SISTEMAS DE CENTROS DE CONTACTO, SISTEMAS DE RESPUESTA DE VOZ INTERACTIVA • PARA EL SISTEMA DE TELEFONIA IP DEBERA SOPORTAR HASTA 500 DISPOSITIVOS • DEBEN DE SUMINISTRARSE DOS SERVIDORES CONFIGURADOS EN UN CLÚSTER DE ALTA DISPONIBILIDAD 1:1 (*PUBLISHER, SUBSCRIBER)* • DEBERÁ INCLUIRSE POLIZA DE SOPORTE DE GARANTIA EXTENDIDA	LOTE	1

POR 1 AÑO 8X5XNBD

DEBERA CONTAR, COMO MÍNIMO, CON LAS SIGUIENTES ESPECIFICACIONES FISICAS Y FUNCIONALES:

COMPONENTE	VALOR
PROCESADOR	SINGLE INTEL X3430 QUAD-CORE 2.40-GHZ; LAST LEVEL CACHE: 8 MB
MEMORIA INCLUIDA	4-GB (TWO 2-GB DUAL IN-LINE MEMORY MODULE [DIMM]) DUAL-RANK PC3-10600R-999 1333 MHZ, FULLY BUFFERED DOUBLE DATA RATE 3 (DDR3) REGISTERED DIMM (RDIMM)
MEMORIA MAXIMA	32 GB
MEMORY BUS CLOCK	UP TO 1333 MHZ
MEMORY TECHNOLOGY	REGISTERED PC3-10600 DDR3 1333-MHZ DUAL-RANK DIMM
TOTAL DIMM SLOTS	6
DISCO DURO	ONE 250-GB SERIAL ADVANCED TECHNOLOGY ATTACHMENT (SATA) 3.5-IN. SIMPLE SWAP
SIMPLE SWAP BAYS	2
HARD DISK INTERFACE TYPE	SATA
HARD DISK SPINDLE SPEED	7,200 RPM (REVOLUTIONS PER MINUTE)
HARD DISK SEEK TIME	1.9 MS (AVERAGE)
HARD DISK LATENCY	4.2 MS (NOMINAL)
DATA-TRANSFER RATE	CAPABLE OF 3 GBPS
HARD DISK FORM SIZE	3.5-INCH SMALL FORM FACTOR (SFF)
ETHERNET NETWORK INTERFACE CARD (NIC)	DUAL ONBOARD 10/100/1000
ETHERNET CONNECTORS	2 RJ-45 CONNECTORS ON BACK OF SERVER
10BASE-T CABLE SUPPORT	EIA CATEGORY 3, 4, OR 5 UNSHIELDED TWISTED PAIR (UTP) (2 OR 4 PAIR) UP TO 328 FT (100M)
100BASE-TX CABLE SUPPORT	EIA CATEGORY 5 UTP (2 PAIR) UP TO 328 FT (100M)
1000BASE-T CABLE SUPPORT	EIA CATEGORY 6 UTP (RECOMMENDED), 5E UTP, 5 UTP (2 PAIR) UP TO 328 FT (100M)
SERIAL PORTS	1
USB 2.0 PORTS	7 (2 FRONT, 4 REAR, AND 1 INTERNAL)
KEYBOARD PORTS	USE ONE OF THE USB PORTS (PS/2 PORTS ARE NOT PROVIDED)

MOUSE PORTS	USE ONE OF THE USB PORTS (PS/2 PORTS ARE NOT PROVIDED)
AUDIO PORTS	NONE
VIDEO GRAPHICS ARRAY (VGA) PORTS	ONE (REAR)
DIMENSIONES	1 RU (UNIDAD DE RACK), ALTO 43 MM / ANCHO 440 MM / PRODUNDIDAD 559 MM

ESPECIFICACIONES DE ENERGÍA:

RATED LINE VOLTAGE: 100-127 VAC; 50 OR 60 HZ

- INPUT CURRENT (AMPS)
    - 0.58 (IDLE)
    - 1.53 (MAXIMUM MEASURED)
    - 6.0 (SYSTEM RATED)
    - 40 (PEAK INRUSH CURRENT; 4 MS)
- LEAKAGE CURRENT (MA)
    - 0.47 (IDLE; MAXIMUM MEASURED; SYSTEM RATED)
- POWER (WATTS)
    - 68 (IDLE)
    - 174 (MAXIMUM MEASURED)
    - 351 (SYSTEM RATED)
- VA RATING (VA)
    - 70 (IDLE)
    - 178 (MAXIMUM MEASURED)
    - 351 (SYSTEM RATED)
- BTU RATING (BTU/HR)
    - 232 (IDLE)
    - 594 (MAXIMUM MEASURED)
    - 2047 (SYSTEM RATED)

RATED LINE VOLTAGE: 200-240 VAC; 50 OR 60 HZ

- INPUT CURRENT (AMPS)
    - 0.33 (IDLE)
    - 0.82 (MAXIMUM MEASURED)
    - 3.0 (SYSTEM RATED)
    - 40 (PEAK INRUSH CURRENT; 4 MS)

	• LEAKAGE CURRENT (MA)
	  o 0.47 (IDLE; MAXIMUM MEASURED; SYSTEM RATED)
	• POWER (WATTS)
	  o 67 (IDLE)
	  o 171 (MAXIMUM MEASURED)
	  o 351 (SYSTEM RATED)
	• VA RATING (VA)
	  o 68 (IDLE)
	  o 175 (MAXIMUM MEASURED)
	  o 351 (SYSTEM RATED)
	• BTU RATING (BTU/HR)
	  o 229 (IDLE)
	  o 583 (MAXIMUM
	  o 2047 (SYSTEM RATED)
	POWER SUPPLY OUTPUT POWER RATED STEADY-STATE POWER 351W
	CERTIFICACIONES DEL PRODUCTO:
	• FCC - VERIFIED TO COMPLY WITH PART 15 OF THE FCC RULES, CLASS A
	• ICES-003 CLASS A
	• AS/NZS CISPR22 CLASS A
	• CISPR22 CLASS A
	• CISPR24 CLASS A
	• EN55022 CLASS A
	• EN55024
	• IEC 61000-3-2
	• IEC 61000-3-3
	• KN22 CLASS A
	• CNS13438 CLASS A
	• GB9254 CLASS A
	• GB4943
	• VCCI-03 CLASS A		

	• CSA C22.2 NO. 60950-1-07 • UL 60950-1 2ND EDITION • IEC/EN 60950-1 2ND EDITION • CE MARK (LOW VOLTAGE DIRECTIVE 2006/95/EC, EMC DIRECTIVE 2004/108/EC • KN24		
B)	**SUMINISTRO E INSTALACIÓN DE SISTEMA GESTOR DE TELEFONÍA IP, LICENCIAMIENTO DE SISTEMA Y DE DISPOSITIVOS TELEFÓNICOS** **LICENCIAMIENTO:** LA NECESARIA PARA GARANTIZAR UN ESQUEMA DE ALTA DISPONIBILIDAD 1:1 DESCRITO EN LOS REQUERIMIENTOS GENERALES. • EL SISTEMA PROPUESTO DEBE SOPORTAR EL MANEJO DE TELEFONÍA Y VIDEOTELEFONÍA IP PARA IMPLEMENTAR UNA ARQUITECTURA DE VOZ Y VIDEO INTEGRADOS. • CON EL FIN DE GARANTIZAR UN SERVICIO HOMOGÉNEO Y ESTÁNDAR SE SOLICITA QUE LA PROPUESTA DEL SERVICIO DE COMUNICACIONES IP SOLICITADO SE INTEGRE CON COMPONENTES DE UNA MISMA MARCA, PARA AL MENOS LOS SIGUIENTES ELEMENTOS DE LA SOLUCIÓN: SERVIDORES GESTORES DE LLAMADA, GATEWAY DE TRONCALES DIGITALES (E1S), TELÉFONOS IP, VIDEOTELÉFONOS, HERRAMIENTAS DE COLABORACIÓN WEB Y CORREO DE VOZ **PREMISAS GENERALES:** • EL SISTEMA DEBERÁ SER LA ÚLTIMA VERSIÓN LIBERADA DEL SISTEMA OPERATIVO CON QUE CUENTE EL FABRICANTE AL MOMENTO DE LA ENTREGA DEL SISTEMA EN OPERACIÓN. • DEBERÁ INCLUIR LICENCIAMIENTO PARA EL SISTEMA EN ALTA DISPONIBILIDAD EN UN ESQUEMA DE 1:1 • DEBERÁ INCLUIR LICENCIAMIENTO PARA SOPORTAR LA CANTIDAD DE DISPOSITIVOS SEÑALADOS EN LOS C Y D. • INCLUIRÁ SOPORTE PROPORCIONADO POR EL FABRICANTE PARA EL SOFTWARE, ASÍ COMO ACTUALIZACIONES MENORES Y MAYORES, DURANTE UN AÑO. **REQUERIMIENTOS GENERALES:** • DEBIDO A QUE LA TELEFONÍA ES UN PUNTO IMPORTANTE PARA **EL TRIBUNAL SUPERIOR DE JUSTICIA DEL ESTADO DE TABASCO**, EL SISTEMA DEBE CONFORMARSE POR UNA ARREGLO EN ALTA DISPONIBILIDAD PARA **250 USUARIOS** EN EL CUAL EL ESQUEMA SE DEBERÁ REPARTIR DE MANERA EQUITATIVA EN CADA SERVIDOR PROPUESTO Y A SU VEZ SE DEBERÁ CONSIDERAR QUE ESTA REDUNDANCIA SE COMPLEMENTARÁ ADICIONANDO AL ESQUEMA DE ALTA DISPONIBILIDAD UN ARREGLO 1:1, TENIENDO EN CUENTA QUE ESTE ARREGLO SE PODRÁ DISTRIBUIR EN UN PUNTO DE LA RED, ASÍ COMO PERMITIR LA INTERCONEXIÓN A SITIOS REMOTOS A TRAVÉS DE TRONCALES H.323 Y SIP. • EL SISTEMA DEBE CONTAR CON LA CAPACIDAD DE RESPALDO AUTOMÁTICO. ESTO SE REFIERE A QUE LA CAÍDA DE UNO DE LOS SERVIDORES DE PROCESAMIENTO DE LLAMADAS ACTIVARÁ QUE LOS DISPOSITIVOS A SU CARGO SEAN ATENDIDOS POR EL OTRO SERVIDOR EN EL ARREGLO.	LOTE	1

	• EL SOFTWARE Y EL HARDWARE INDICADO EN EL INCISO A DEBEN SER DE LA MISMA MARCA PARA GARANTIZAR LA ADECUADA EJECUCIÓN DE LA APLICACIÓN. • DEBE CONTAR CON LA CAPACIDAD PARA HACER COPIAS DE SEGURIDAD DE LOS DATOS MÁS IMPORTANTES Y LA FLEXIBILIDAD DE GUARDAR LOS DATOS IMPORTANTES DE LOS USUARIOS EN OTRO SERVIDOR SITUADO EN CUALQUIER LUGAR DE LA RED IP. • DEBE PERMITIR EXTENDER LOS SERVICIOS COMPLEMENTARIOS Y MEJORADOS, COMO RETENCIÓN, TRANSFERENCIA, REENVÍO, CONFERENCIA, LA APARICIÓN DE VARIAS LÍNEAS, LA SELECCIÓN AUTOMÁTICA DE RUTA, LA MARCACIÓN RÁPIDA, LLAMADA AL ÚLTIMO NÚMERO Y OTRAS CARACTERÍSTICAS A TELÉFONOS IP Y GATEWAYS. • PERMITIR DISTRIBUIR TODOS LOS TELÉFONOS, GATEWAYS Y APLICACIONES EN UNA RED IP ÚNICA CONTANDO CON SERVICIO DE DHCP PARA LA TOTALIDAD DE TELÉFONOS SOLICITADOS. • SE DEBERÁ PROVEER UN MECANISMO DE SUPERVIVENCIA QUE ANTE LA EVENTUALIDAD DE PÉRDIDA DE COMUNICACIÓN AL SITIO DE PROCESAMIENTO DE LLAMADAS CENTRAL, LOS SERVICIOS TELEFÓNICOS PUEDAN SEGUIR PROPORCIONÁNDOSE DE MANERA LOCAL MEDIANTE LOS GATEWAYS DISTRIBUIDOS POR LA RED. EL ESQUEMA DE SUPERVIVENCIA DEBERÁ ESTAR PRESENTE TANTO PARA LOS TELÉFONOS IP CON SEÑALIZACIÓN EN SIP COMO PARA LOS VIDEOTELÉFONOS TAMBIÉN CON SEÑALIZACIÓN SIP SIN IMPORTAR LA UBICACIÓN GEOGRÁFICA DE LOS MISMOS. • TODOS LOS TELÉFONOS IP PROPUESTOS (TELÉFONO DE HARDWARE, VIDEOTELÉFONO, TELÉFONO EN SOFTWARE) DEBERÁN SOPORTAR IMPLEMENTAR APLICACIONES QUE PUEDAN SER DESARROLLADAS CON LA AYUDA DEL LENGUAJE DE PROGRAMACIÓN XML. • CADA SERVIDOR DEL SISTEMA DE PROCESAMIENTO DE LLAMADAS, APLICACIONES Y PLATAFORMAS DE ADMINISTRACIÓN DEBERÁN CONTAR CON AGENTES DE IDS DE HOST INSTALADOS EN ELLOS INDEPENDIENTEMENTE DEL SISTEMA OPERATIVO DE LA PLATAFORMA A OFERTAR. • EL SISTEMA DE COMUNICACIONES IP DEBERÁ MANEJAR CONFERENCIAS DE UN MÍNIMO DE 8 PARTICIPANTES EN CADA UNA DE ELLAS (SIN CASCADEO DE CONFERENCIAS). LAS CONFERENCIAS TELEFÓNICAS DEBERÁN LLEVARSE A CABO MEDIANTE RECURSOS DE HARDWARE Y NO DE SOFTWARE. EL SISTEMA DE ADMINISTRACIÓN DE TELEFONÍA IP DEBE SER CAPAZ DE SOPORTAR CAPACIDADES PROPIAS DEL SISTEMA TALES COMO: • INTERFACES DE PROGRAMACIÓN DE APLICACIONES (API) DE TELEFONÍA ABIERTA PARA PROPORCIONAR SERVICIOS ADICIONALES DE DATOS, VOZ Y VIDEO, MENSAJERÍA UNIFICADA, CONFERENCIA MULTIMEDIA, CENTROS DE CONTACTO COOPERATIVOS Y SISTEMAS MULTIMEDIA DE RESPUESTA INTERACTIVA CON SOLUCIONES DE TELEFONÍA IP. • AJUSTE DE ATENUACIÓN / GANANCIA EN CADA DISPOSITIVO (TELÉFONO Y GATEWAY). • AJUSTE AUTOMATIZADO DE ANCHO DE BANDA. • SOPORTE PARA CIFRADO PARA EL STREAM DE AUDIO DE LLAMADAS Y CONFERENCIAS • SELECCIÓN AUTOMÁTICA DE RUTA. • CONTROL DE ADMINISTRACIÓN DE LLAMADAS. • GENERACIÓN DE MÚSICA EN ESPERA. • TRATAMIENTO Y ANÁLISIS DIGITAL DE LA LLAMADA (INSERCIÓN, BORRADO Y EXTRACCIÓN DE CADENA DE		

	DÍGITOS, Y CÓDIGOS DE ACCESO DE LLAMADA). • PROCESAMIENTO DISTRIBUIDO DE LA LLAMADA. • FAX A TRAVÉS DE IP---G.711 “PASS-THROUGH”. • INTERFAZ H.323 V1 Y V2 A DISPOSITIVOS SELECCIONADOS. • LLAMADA AUTOMÁTICA (POR SUS SIGLAS EN INGLÉS PRIVATE LINE AUTOMATIC RESPONSE). • INTERFAZ AL GATEKEEPER A TRAVÉS DE H.323 PARA LA CAPACIDAD DE AMPLIACIÓN Y CONTROL DE ACEPTACIÓN DE LLAMADAS. • SOPORTE NATIVO DEL PROTOCOLO SIP PARA EL CONTROL DE LOS TELÉFONOS IP Y SIP T.38 PARA SERVICIOS DE FAX SIN NECESIDAD DE AGREGAR SERVIDORES O ELEMENTOS EXTERNOS • EL SISTEMA PROPUESTO DEBE CONTAR CON MANEJO DE VIDEO-TELEFONÍA PUNTO A PUNTO Y MEDIANTE EL ALGORITMO DE CODIFICACIÓN H.264 • EL SISTEMA DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER CONFIGURAR UN NÚMERO ÚNICO DE USUARIO A PARTIR DEL CUAL SE PUEDEN ASOCIAR LOS NÚMEROS TELEFÓNICOS DE EXTENSIONES, TELÉFONOS EXTERNOS Y CELULARES PARA PODER RECIBIR LA LLAMADA EN CUALQUIERA DE ESAS OPCIONES. CON ESTA FUNCIÓN DEBERÁN TIMBRAR DE MANERA SIMULTÁNEA TODOS LOS NÚMEROS DE LOS DISPOSITIVOS ASOCIADOS EN EL MOMENTO DE RECEPCIÓN DE UNA LLAMADA. • MANEJO DE AUTENTICACIÓN DE TELÉFONOS IP MEDIANTE CERTIFICADOS DIGITALES. ESTA CARACTERÍSTICA PERMITIRÁ AUTENTICAR CADA TELÉFONO IP QUE SE CONECTE A LA RED DE TAL FORMA QUE NO PUEDAN SER CONECTADOS Y UTILIZADOS TELÉFONOS NO PERMITIDOS POR EL ADMINISTRADOR DEL SISTEMA. • SOPORTE DE LAS "SIGNED FIRMWARE IMAGES". FUNCIÓN PERMITIRÁ PROTEGER AL TELÉFONO IP PARA QUE NINGÚN ATACANTE INSTALE FIRMWARE INSEGURO O NO VÁLIDO EN EL TELÉFONO QUE EVITE TENER LA IMAGEN EN EL TELÉFONO PARA LLEVAR A CABO LLAMADAS ENCRIPTADAS. • MANEJO DE ENCRIPTACIÓN DE LA SEÑALIZACIÓN EN LOS TELÉFONOS IP DE ESCRITORIO POR MEDIO DE TLS. • MANEJO DE SRTP PARA ENCRIPTAR EL AUDIO Y GARANTIZAR LA CONFIDENCIALIDAD DE LAS LLAMADAS CON AES-128. • LOCALIZACIÓN MÚLTIPLE---PARTICIÓN DEL PLAN DE MARCACIÓN. • UTILIDADES DE DEPURACIÓN Y ADMINISTRACIÓN DE MÚLTIPLES PLATAFORMAS REMOTAS DEL PROPIO SISTEMA. • CAPACIDAD DE MULTI-UBICACIÓN (CROSS-WAN) CON CONTROL DE ACEPTACIÓN DE LLAMADAS. • ESTACIÓN FUERA DE LAS INSTALACIONES (OFF-PREMISE STATION, OPX). • BLOQUEO DE LLAMADAS SALIENTES---SISTEMA. • SEÑALIZACIÓN DTMF FUERA DE BANDA A TRAVÉS DE IP. • RECUPERACIÓN DE FALLOS PSTN. • COMPATIBILIDAD CON APLICACIONES DE OTROS FABRICANTES (TARIFICACIÓN, SISTEMAS DE GRABACIÓN) • AVISO DE DIFUSIÓN A TRAVÉS DE FXS. • INDICACIÓN DE MENSAJES DE ESPERA. • SOPORTE PARA “HOOK-FLASH” EN LOS GATEWAYS FXS. • INTERFAZ DE PROVEEDOR DE SERVICIO TAPI 2.1(TSP). • INTERFAZ DE PROVEEDOR DE SERVICIO JTAPI 1.2. • ESTADÍSTICAS DE FACTURACIÓN Y LLAMADAS. • CONFIGURACIÓN Y ADMINISTRACIÓN DE RECURSOS/APLICACIONES COMPARTIDAS: • RECURSO TRANSCODIFICADOR. • RECURSO “BRIDGE” DE CONFERENCIAS.		

	• SUPRESIÓN DE SILENCIO, DETECCIÓN DE ACTIVIDAD DE VOZ. • CONFIGURACIÓN UNIFICADA DE SISTEMA Y DISPOSITIVO. • PLAN DE MARCACIÓN UNIFICADO. DEBE SOPORTAR COMO MÍNIMO LAS SIGUIENTES CARACTERÍSTICAS PARA USUARIOS: • RESPUESTA/LIBERACIÓN DE RESPUESTA. • RESPUESTA AUTOMÁTICA. • CONEXIÓN DE LLAMADA. • DESVÍO DE TODAS LAS LLAMADAS (FUERA DE LA RED/EN LA RED). • DESVÍO DE LLAMADA-DESPUÉS DE TIMBRAR, DESVÍO DE LLAMADA-SIN RESPUESTA. • SUSPENSIÓN TEMPORAL/RECUPERACIÓN DE LLAMADAS. • FUNCIÓN DE NO MOLESTAR (DO NOT DISTURB) • APARCAMIENTO/RECOGIDA DE LLAMADAS. • RECEPCIÓN DE LLAMADAS DE GRUPO-UNIVERSAL. • ESTADO DE LA LLAMADA POR LÍNEA (ESTADO, DURACIÓN Y NÚMERO) • LLAMADA EN ESPERA/RECUPERACIÓN DE LLAMADAS. • IDENTIFICACIÓN DE LA LÍNEA DE LLAMADA---CLID. • IDENTIFICACIÓN DEL NOMBRE DEL GRUPO QUE LLAMA---CNID. • MARCACIÓN ENTRANTE DIRECTA---DID. • MARCACIÓN SALIENTE DIRECTA---DOD. • TIMBRADO DISTINTIVO (INTERNO VS. EXTERNO). • TIMBRADO DISTINTIVO POR TELÉFONO. • ALTAVOZ FULL DÚPLEX Y MANOS LIBRES. • ACCESO A LA AYUDA HTML DESDE EL TELÉFONO. • RELLAMADA DE ÚLTIMO NÚMERO (FUERA DE LA RED/EN LA RED). • INDICADOR DE MENSAJE EN ESPERA. • CONFERENCIA MÚLTIPLE---INSTANTÁNEA CON COMPLEMENTOS, MEET-ME. • APARICIÓN DE VARIAS LÍNEAS POR TELÉFONO. • SILENCIADOR---ALTAVOZ Y AURICULAR. • MARCACIÓN ON-HOOK. • MÚSICA EN ESPERA. • ASISTENCIA DEL OPERADOR INTERFAZ DE NAVEGADOR WEB, NOTIFICACIÓN DE LOOP PRINCIPAL, CONEXIÓN/DESCONEXIÓN, OCUPADO/DISPONIBLE, ACCESO MANUAL IZQUIERDA/DERECHA, ACCESO A AURICULAR, LUCES DE OCUPADO, SELECCIÓN DIRECTA DE ESTACIÓN, TRANSFERENCIA “DRAG AND DROP”, ESTADO DE LA LLAMADA (ESTADO, DURACIÓN Y NÚMERO). • CAPACIDAD PARA QUE MEDIANTE UN ICONO EL USUARIO SEPA QUE SU LLAMADA ESTÁ SIENDO ENCRIPTADA Y QUE NO SERÁ ESCUCHADA PESE A QUE SEAN CAPTURADOS LOS PAQUETES DE VOZ. • PRIVACIDAD. • ESTADÍSTICAS QOS EN EL TELÉFONO. • LISTA DE MARCACIÓN RECIENTES---LLAMADAS AL TELÉFONO, LLAMADAS DESDE EL TELÉFONO, AUTO MARCACIÓN, EDICIÓN DE LA MARCACIÓN. • MARCACIÓN RÁPIDA---VARIAS MARCACIONES RÁPIDAS POR TELÉFONO. • CONTROLES DE VOLUMEN DE LA ESTACIÓN (AUDIO Y TONO). • TRANSFERENCIA---CON SUSPENSIÓN TEMPORAL DE CONSULTA. • MARCACIÓN RÁPIDA CONFIGURADA POR EL USUARIO, DESVÍO DE TODAS LAS LLAMADAS A TRAVÉS DE UN ACCESO WEB. • SERVICIOS WEB ACCESIBLES DESDE EL TELÉFONO.		

	CARACTERISTICAS ADMINISTRATIVAS: • DESCUBRIMIENTO Y REGISTRO DE APLICACIONES AL ADMINISTRADOR SNMP. • REGISTRO DE DETALLES DE LAS LLAMADAS. • BASE DE DATOS DE CONFIGURACIÓN CENTRALIZADA Y REPLICA, CONSOLAS DE ADMINISTRACIÓN DISTRIBUIDAS BASADAS EN WEB. • TONO DE TIMBRE DE ARCHIVOS WAV CONFIGURABLE Y POR DEFECTO POR TELÉFONO. • NOTIFICACIÓN AUTOMATIZADA DE CAMBIOS EN LA BASE DE DATOS. • FORMATO DE PRESENTACIÓN FECHA/HORA CONFIGURABLE POR TELÉFONO. • INFORMACIÓN DE DEPURACIÓN AL ARCHIVO SYSLOG COMÚN. • ACTUALIZACIÓN DESCARGABLES DE CARACTERÍSTICAS DE DISPOSITIVOS TELÉFONOS, HARDWARE, RECURSO TRANSCODIFICADOR, RECURSO HARDWARE DE BRIDGE DE CONFERENCIA, RECURSO GATEWAY VOIP. • GRUPOS Y CONJUNTOS DE DISPOSITIVOS PARA LA ADMINISTRACIÓN DE GRANDES SISTEMAS. • HERRAMIENTAS DE CORRESPONDENCIA DE DISPOSITIVOS DE DIRECCIONES IP A DIRECCIONES MAC. • TABLA DE CONVERSIÓN DE NÚMEROS MARCADOS (CONVERSIÓN ENTRADA/SALLIDA). • SERVICIO DE IDENTIFICACIÓN DE NÚMERO MARCADO. • INTERFAZ HOMOLOGADO H.323 PARA LOS CLIENTES, GATEWAYS Y GATEKEEPERS H.323.(NOMBRAR EL ORGANISMO QUE LA HOMOLOGA). • CONTROL DE RENDIMIENTO ESTADÍSTICAS SNMP DESDE LAS APLICACIONES AL ADMINISTRADOR SNMP O AL SISTEMA OPERATIVO. • MONITOREO DEL DESEMPEÑO. • SE DEBERÁ INCLUIR EL SERVICIO DE TFTP PARA LA TOTALIDAD DE TELÉFONOS SOLICITADOS • LAS ESTADÍSTICAS QOS SE OFRECEN POR LLAMADA. • SELECCIÓN DE LA APARICIÓN DE UNA LÍNEA DETERMINADA PARA TIMBRAR. • SELECCIÓN DE UN TELÉFONO ESPECÍFICO PARA EL TIMBRADO. • UN SÓLO CDR (CALL DETAIL RECORD) POR GRUPO. • UN SÓLO PUNTO DE CONFIGURACIÓN SISTEMA/DISPOSITIVO. • LISTA ORDENABLE DE COMPONENTES POR DISPOSITIVO, USUARIO O LÍNEA. • INFORME SOBRE LOS EVENTOS DEL SISTEMA PARA EL VISOR DE EVENTOS DEL SISTEMA OPERATIVO O EL SYSLOG COMÚN. • INTERFAZ DE TELEFONÍA INFORMÁTICA TAPI 2.1. • ZONA HORARIA CONFIGURABLE POR TELÉFONO.		
C)	**SUMINISTRO E INSTALACIÓN DE TELÉFONO TIPO-1** EL EQUIPO DEBERÁ CUMPLIR CON LAS SIGUIENTES CARACTERÍSTICAS: • CONTAR CON UNA PANTALLA DE CRISTAL LÍQUIDO TFT A COLORES CON LUZ DE FONDO, SENSIBLE AL TACTO Y CON UNA RESOLUCIÓN MÍNIMA DE 320 X 240 PIXELES. DICHA PANTALLA DEBE MOSTRAR LA FECHA Y LA HORA, EL NOMBRE Y EL NÚMERO DE LA PERSONA QUE REALIZA LA LLAMADA Y LOS DÍGITOS MARCADOS. LA CAPACIDAD GRÁFICA DE LA PANTALLA DEBE PERMITIR LA INCLUSIÓN DE LAS	PIEZA	8

	CARACTERÍSTICAS ACTUALES Y FUTURAS. • EL TELÉFONO DEBE PODER SOPORTAR CONFIGURACIÓN DE IP DE MANERA ESTÁTICA O DE MANERA DINÁMICA A TRAVÉS DEL PROTOCOLO DHCP • DEBE CONTAR CON SOPORTE PARA 8 LÍNEAS TELEFÓNICAS • DEBE DE CONTAR CON UN ALTAVOZ CON CAPACIDAD DE COMUNICACIÓN A MANOS LIBRES CON SUPRESIÓN DE ECO ACÚSTICO. • DEBE CONTAR CON UN MICRÓFONO PARA LA COMUNICACIÓN A MANOS LIBRES. • DEBERÁ CONTAR CON AL MENOS 2 PUERTOS DE RED 10/100/1000 MBPS QUE PERMITAN REALIZAR CONEXIONES DIRECTAS CON REDES GIGABITETHERNET 1000BASET A TRAVÉS DE UNA INTERFAZ RJ-45 PARA UNA SENCILLA CONEXIÓN LAN, TANTO DEL TELÉFONO COMO DE UN PC EN LA MISMA UBICACIÓN. EL ADMINISTRADOR DEL SISTEMA PUEDA DESIGNAR LAN VIRTUALES INDEPENDIENTES (VLAN) (802.1Q) PARA EL PC Y LOS TELÉFONOS IP. • SOPORTE PARA AUDIO EN BANDA ANCHA MEDIANTE EL ESTÁNDAR TIA 920. CON LA FINALIDAD DE INCREMENTAR EL ESPECTRO DE FRECUENCIAS DE LA VOZ Y PERMITIR UNA MAYOR CLARIDAD DE LA MISMA. • EL TELÉFONO IP DEBE SOPORTAR EL PROTOCOLO SIP Y SKINNY CLIENT CONTROL PROTOCOL (SCCP).. • INDICADOR LUMINOSO DE CORREO DE VOZ. • MANEJO DE AUTENTICACIÓN MEDIANTE CERTIFICADOS DIGITALES X.509V3 DE ACUERDO A LA RECOMENDACIÓN DE LA ITU-T EN LOS TELÉFONOS IP PARA EVITAR ACCESOS NO AUTORIZADOS POR EL ADMINISTRADOR DEL SISTEMA DE TELEFONÍA. SEÑALIZACIÓN Y MEDIOS SEGUROS POR MEDIO AES 128. • DEBERÁN DE CONTAR CON UN PUERTO PARA AUDÍFONOS O DIADEMA • DEBERÁ DE PERMITIR EL OCULTAR LOS TONOS DE MARCACIÓN MULTIFRECUENCIA (DTMF) EN MODO ALTAVOZ PARA QUE HAYA UNA MAYOR SEGURIDAD. • DEBERÁ OFRECER MÍNIMO 24 DIFERENTES TONOS DE TIMBRE SELECCIONABLES POR EL USUARIO. • EL MENÚ DEBERÁ DE SOPORTAR EL LENGUAJE EN ESPAÑOL. • DEBE SOPORTAR LOS PROTOCOLOS DE AUDIO G.711A, G711U, G.729A, G.729AB, G.722 Y ILBC. • PROGRAMACIÓN DE LA GENERACIÓN DE RUIDO DE APACIGUAMIENTO Y DETECCIÓN DE ACTIVIDAD DE VOZ A TRAVÉS DEL SISTEMA.		

	• CERTIFICADO DIGITAL ÍNTER CONSTRUIDO DE FÁBRICA EN EL TELÉFONO IP SOLICITADO. • MANEJO DE APLICACIONES XML. • LOS TELÉFONOS IP DEBEN TENER LA CAPACIDAD PARA RECIBIR LA ALIMENTACIÓN ELÉCTRICA A TRAVÉS DEL PUERTO DE RED LAN MEDIANTE EL PROTOCOLO ESTÁNDAR 802.3AF (POE) Ó BIEN DE UNA FUENTE DE ALIMENTACIÓN EXTERNA EN AC EN CASO DE SER REQUERIDA EL TELÉFONO DEBE DE OFRECER LAS SIGUIENTES FUNCIONALIDADES MÍNIMAS: • AJUSTE DE CONTRASTE DE LA PANTALLA • AJUSTE DE TIPO DE TIMBRE • CONFIGURACIÓN Y ESTADO DE LA RED A TRAVÉS DE MENÚS. • ESTADO DE LAS LLAMADAS EL TELÉFONO SERÁ DEL MISMO FABRICANTE QUE EL SOFTWARE DE TELEFONÍA IP (INCISO B)		
D)	**SUMINISTRO E INSTALACIÓN DE DISPOSITIVO TELEFONICO IP, TIPO 2** DEBERÁ DE CONSIDERARSE EL SUMINISTRO DE SESENTA Y UNA (61) FUENTE DE PODER Y CABLE DEL MISMO FABRICANTE DEL TELÉFONO IP DE ESTE INCISO, LOS CUALES SERÁN INSTALADOS EN LAS OFICINAS REMOTAS . • EL TELÉFONO DEBE SOPORTAR CONFIGURACIÓN DE IP DE MANERA ESTÁTICA O DE MANERA DINÁMICA A TRAVÉS DEL PROTOCOLO DHCP. • DEBERÁ SOPORTAR AL MENOS CUATRO LÍNEAS. • DEBERÁ CONTAR CON PANTALLA MONOCROMÁTICA DE LCD ANTI REFLEJANTE, CON LUZ DE FONDO Y UNA RESOLUCIÓN MÍNIMA DE 396 X 162 PIXELES. • DEBERÁ CONTAR CON AL MENOS 4 BOTONES MULTIFUNCIONALES. • DEBERÁ CONTAR CON BOTÓN DEDICADO PARA FUNCIONES DE TRANSFERENCIA. • DEBERÁ CONTAR CON BOTÓN DEDICADO PARA FUNCIONES DE CONFERENCIA. • DEBERÁ CONTAR CON BOTÓN DEDICADO PARA FUNCIONES DE ESPERA. • DEBERÁ SOPORTAR EXTENSIBLE MARKUP LANGUAGE (XML). • DEBERÁ CONTAR CON ALTAVOZ BIDIRECCIONAL A MANOS LIBRES. • DEBERÁ CONTAR CON UN PUERTO PARA AUDÍFONOS (O DIADEMA	PIEZA	192

	PREFERENTEMENTE) CONECTOR RJ9. • DEBERÁ CONTAR CON DOS PUERTOS ETHERNET A 10/100 MBPS CON CONECTOR RJ45, UNO DE ESTOS PUERTOS SERÁ DE INTERCONEXIÓN A PUERTO DE SWITCH Y EL OTRO PUERTO DEBERÁ PERMITIR CONEXIÓN DE UNA COMPUTADORA. • DEBERÁ SOPORTAR EL ESTÁNDAR 802.1Q/P • DEBERÁ SOPORTAR EL AJUSTE DE VOLUMEN DE TIMBRADO, EL VOLUMEN EN EL AURICULAR Y DE LA DIADEMA. • EL TELÉFONO DEBERÁ SOPORTAR HACER EL MONTAJE SOBRE LA PARED. • DEBERÁ SOPORTAR EL CAMBIO DE TIMBRADO E INCLUIR AL MENOS 7 DISTINTOS TIPOS. • DEBERÁ SOPORTAR LOS CODECS G.711A, G.711, G.729A, G.729B, G.729AB E ILBC • DEBERÁ SOPORTAR DETECCIÓN DE ACTIVIDAD DE VOZ. • DEBERÁ SOPORTAR VIDEO LLAMADAS CON CÁMARA EXTERNA A TRAVÉS DE LA PC. • DEBERÁ SOPORTAR CORREO DE VOZ CON NOTIFICACIÓN VISUAL. • DEBERÁ SOPORTAR IDENTIFICADOR DE NUMERO QUE LLAMA, SI LA LLAMADA ES INTERNA DEBERÁ APARECER CON NOMBRE. • DEBERÁ CONTAR CON UNA TECLA DE SILENCIO DE MICRÓFONO. • DEBERÁ SOPORTAR CÓDIGOS DE AUTORIZACIÓN DE ACCESO. • DEBERÁ SOPORTAR GENERAR UNA CONFERENCIA TRIPARTITA. • DEBERÁ SOPORTAR ACCESO AL DIRECTORIO TELEFÓNICO A TRAVÉS DE LA PANTALLA DEL TELÉFONO • DEBERÁ SOPORTAR GENERACIÓN DE TONOS. • DEBERÁ SOPORTAR DESVÍO DE LLAMADA AL NO CONTESTAR. • DEBERÁ SOPORTAR DESVÍO DE LLAMADA NOCTURNO • DEBERÁ SOPORTAR DESVÍO DE LLAMADA INMEDIATO. • DEBERÁ SOPORTAR DESVÍO DE LLAMADA AL TIMBRAR. • DEBERÁ CONTAR CON LA FUNCIONALIDAD DE RETENCIÓN DE LLAMADA • DEBERÁ CONTAR CON LA FUNCIONALIDAD DE RE LLAMADA. • DEBERÁ SOPORTAR LLAMADA EN ESPERA. • DEBERÁ SOPORTAR MÚSICA ENE ESPERA.		

	• DEBERÁ SOPORTAR LA FACILIDAD DE TRANSFERENCIA DE LLAMADA. • DEBERÁ SOPORTAR LA VISUALIZACIÓN A TRAVÉS DE LA PANTALLA LA LISTA DE PARTICIPANTES EN LA CONFERENCIA. • DEBERÁ PERMITIR PARTICIPAR EN CONFERENCIAS TIPO AD-HOC O MEETME. • DEBERÁ PODER VISUALIZAR EN LA PANTALLA EL REGISTRO DE LLAMADAS PERDIDAS Y LLAMADAS REALIZADAS. • DEBERÁ SOPORTAR ENCRIPCIÓN DE LLAMADA Y AUTENTICACIÓN DE SEÑALIZACIÓN CON NOTIFICACIÓN VISUAL. • DEBERÁ SOPORTAR ALIMENTACIÓN DE VOLTAJE A TRAVÉS DEL ESTÁNDAR IEEE802.3AF, ASÍ COMO ALIMENTACIÓN A TRAVÉS DE TOMA CORRIENTE. • DEBERÁ TENER LA CAPACIDAD DE OPERAR DE 0 A 40°C. EL TELÉFONO SERÁ DEL MISMO FABRICANTE QUE EL SOFTWARE DE TELEFONÍA IP (INCISO B)		
E)	**SUMINISTRO E INSTALACIÓN DE ADAPTADOR TELEFÓNICO PARA DISPOSITIVOS ANALÓGICOS** DEBERA SER DE LA MISMA MARCA QUE EL SISTEMA DE TELEFONIA IP (INCISO B) ACTUALIZADO PARA ASEGURAR COMPATIBILIDAD. DEBERÁ CONTAR CON LAS SIGUIENTES ESPECIFICACIONES FÍSICAS Y FUNCIONALES: • DOS PUERTOS DE VOZ RJ11 QUE SOPORTEN TELÉFONOS ANÁLOGOS. • PUERTO DE CONEXIÓN DE RED TIPO RJ45 • AUTO PROVISIONAMIENTO CON SERVIDORES TFTP. • ASIGNACIÓN DE DIRECCIONES IP POR MEDIO DE DHCP O ASIGNACIÓN ESTÁTICA. • CONFIGURACIÓN WEB A TRAVÉS DE UN SERVIDOR WEB INTERCONSTRUIDO. • CONFIGURACIÓN DE TELÉFONO POR MEDIO DE TELÉFONO DE TONOS A TRAVÉS DE MENSAJE DE VOZ. • PASSWORD DE ADMINISTRADOR PARA PROTEGER EL ACCESO A LA CONFIGURACIÓN DEL ADAPTADOR. • ACTUALIZACIONES REMOTAS A TRAVÉS DE LA RED. • PRE-PROCESAMIENTO AVANZADO PARA OPTIMIZAR LA COMPRESIÓN DE VOZ FULL-DULPLEX. • DEBE PERMITIR CONTAR CON SUPRESIÓN DE RUIDO Y DE	PIEZA	6

	ECO ACÚSTICO. • DEBE PERMITIR EL APACIGUAMIENTO DE RUIDO Y DETECCIÓN DE ACTIVIDAD DE VOZ A TRAVÉS DEL SISTEMA PARA AHORRO EN EL ANCHO DE BANDA. • MONITOREO DINÁMICO DE LA RED PARA REDUCIR LA PÉRDIDA DE PAQUETES. • PROTOCOLO DE SEÑALIZACIÓN SIP • DEBE SOPORTAR LOS CODECS G.711M-LAW, G.711A-LAW, G.729, G.729A, G.729B, G.729AB • DEBE ACEPTAR PROVISIONAMIENTO DE PLAN DE MARCACIÓN. • DEBERÁ DE OCULTAR LOS TONOS DE MARCACIÓN MULTIFRECUENCIA (DTMF) • CANCELACIÓN DE ECO POR CADA PUERTO • SUPRESIÓN NO LINEAR DE ECO. • TIEMPO DE CONVERGENCIA DE 25MS • SOPORTE A FAX EN MODO G.711 FAX Y G.711 PASS-THROUGH Y T.38 DEBERÁ SOPORTAR LOS PROTOCOLOS: • IEEE 802.1Q VLAN TAGGING • CISCO DISCOVERY PROTOCOL • DNS • DHCP • INTERNET CONTROL MESSAGE PROTOCOL (ICMP) • IP • REAL-TIME TRANSPORT PROTOCOL (RTP) • TCP • TRIVIAL FILE TRANSFER PROTOCOL (TFTP) • USER DATAGRAM PROTOCOL (UDP) DEBERÁ SOPORTAR LOS SERVICIOS SIP DE: • REGISTER • REFER • INVITE		

	• BYE • CANCEL • NOTIFY • OPTIONS • ACK • SUBSCRIBE • CALLER ID • CALL-WAITING CALLER ID • VOICE-MAIL INDICATION • CONFERENCE CALL • CALL WAITING • CALL FORWARDING • CALLING-LINE IDENTIFICATION • UNATTENDED TRANSFER • ATTENDED TRANSFER • SHARED LINE • SPEED DIAL • MEET ME • PICK UP • REDIAL 1.1.1 1.1.2		
F)	**SUMINISTRO DE EQUIPO GATEWAY DE VOZ PARA LOS SERVICIOS DE TELEFONIA IP (INCLUYE 1 PUERTOS E1 PARA TRONCALES DIGITALES, 4 PARA LÍNEAS ANALÓGICAS, MODULO DE SERVICIOS INTEGRADOS PARA SOPORTE DE SISTEMA DE MENSAJERIA Y AUTOCONTESADORA CON LICENCIAMIENTO PARA 50 BUZONES).** EL EQUIPO OFERTADO DEBERÁ CUMPLIR CON LAS SIGUIENTES ESPECIFICACIONES: • EL EQUIPO DEBERÁ CONTAR CON LA VERSIÓN MÁS RECIENTE LIBERADA DEL SISTEMA OPERATIVO CON QUE CUENTE EL FABRICANTE. • DEBERÁ INCLUIR MEMORIA COMPRESORA DE VOZ PARA 32 CANALES DE ÚLTIMA GENERACIÓN	PIEZA	1

	• DEBER INCLUIR 1 PUERTO E1 PARA RECEPCIÓN DE TRONCALES DIGITALES DE ULTIMA GENERACION • DEBERÁ INCLUIR 4 PUERTOS FXO PARA RECEPCIÓN DE TRONCALES ANALÓGICAS • DEBERÁ INCLUIR LICENCIA DE USO DE APLICACIONES DE COMUNICACIONES UNIFICADAS. • DEBERÁ INCLUIRSE MODULO INTERNO PARA SERVICIOS Y LICENCIAMIENTO DE COMUNICACIONES UNIFICADAS DE CORREO DE VOZ, SISTEMA DE AUTOCONTESTADORA COMPATIBLE CON EQUIPO GATEWAY DE VOZ PROPUESTO PARA EN ESTE MISMO INCISO QUE A SU VEZ DEBERÁ SER COMPATIBLE CON LA VERSION ACTUALIZADA DEL SISTEMA DE TELEFONIA IP SOLICITADA EN ESTE MISMO INCISO, DEBERA REUNIR LAS SIGUIENTES ESPECIFICACIONES TECNICAS Y FUNCIONALES: o EL EQUIPO DEBERÁ CONTAR CON LA VERSIÓN DE SISTEMA OPERATIVO MÁS ACTUAL LIBERADA POR EL FABRICANTE o DEBERÁ INCLUIR LICENCIAMIENTO PARA 50 BUZONES DE VOZ (CON CAPACIDAD DE AMPLIACION MEDIANTE SOFTWARE HASTA 500 BUZONES) o DEBERÁ INCLUIR LICENCIAMIENTO PARA UN TOTAL DE 8 PUERTOS DE CONEXIÓN A CORREO DE VOZ O SISTEMA DE AUTOCONTESTADORA (CON CAPACIDAD DE AMPLIACION MEDIANTE SOFTWARE HASTA 32 BUZONES) o CAPACIDAD DE ALMACENAMIENTO DE HASTA 600 HRS o CON IDIOMA EN ESPAÑOL PARA SISTEMA DE CORREO DE VOZ o ESPECIFICACIONES TECNICAS: ▪ PROCESADOR INTEL 1.06 GHZ ▪ MEMORIA SDRAM 2 GB ▪ 1 INTERFACE DE RED TIPO RJ45 ▪ 1 INTERFACE USB ▪ 1 DISCO DURO DE 500 GB PARA ALMACENAMIENTO LAS CARACTERÍSTICAS FÍSICAS MÍNIMAS A OFERTAR SON: • SOPORTE DE ACELERACIÓN DE CIFRADO INTEGRADA EN HARDWARE (IPSEC + SSL) • DEBERÁ SOPORTAR UN MÁXIMO DE 25 DISPOSITIVOS TELEFÓNICOS IP EN MODO SRST. • DEBERÁ INCLUIR LICENCIAMIENTO PARA SOPORTAR LOS 25 DISPOSITIVOS.		

	• 3 PUERTOS 10/100/1000 INTEGRADOS EN CHASIS PARA APLICACIONES LAN/WAN TIPO RJ45 • 1 SLOT PARA MÓDULOS DE SERVICIO • 4 SLOT PARA MÓDULO EHWIC • 2 SLOT PARA MÓDULO EHWIC DE DOBLE ANCHO • 1 SLOT PARA MÓDULO ISM • SOPORTE DE INSERCIÓN Y EXTRACCIÓN EN LÍNEA DE LOS MÓDULOS • 2 SLOTS PARA MEMORIA DSP (PVDM) • 512 MB DE MEMORIA DRAM ECC DDR2 YA INSTALADA • SOPORTE MÁXIMO DE HASTA 2 GB DE MEMORIA DRAM ECC DDR2 • MEMORIA COMPACT FLASH DE 256 MB YA INSTALADA • SOPORTE MÁXIMO DE HASTA 4 GB • 2 RANURAS USB 2.0 EXTERNAS TIPO A • UN PUERTO DE CONSOLA USB (TIPO B; HASTA 115,2 KBPS) • UN PUERTO SERIE DE CONSOLA (HASTA 115,2 KBPS) • UN PUERTO SERIE AUXILIAR (HASTA 115,2 KBPS) ESPECIFICACIONES DE ALIMENTACIÓN: • FUENTE DE ALIMENTACIÓN INTERNA DE RANGO AUTOMÁTICO DE 100 A 240 VCA • FRECUENCIA DE ENTRADA DE ENERGÍA DE 47 A 63 HZ • RANGO DE CA DE ENTRADA DE LA FUENTE DE ALIMENTACIÓN DE CA (MÁX.) DE 2.2 A 1.0 A • IMPULSO TRANSITORIO DE CORRIENTE DE ENTRADA DE CA MENOR A 50 A • CONSUMO NORMAL DE ENERGÍA (SIN MÓDULOS) 50 W • POTENCIA MÁXIMA CON FUENTE DE ALIMENTACIÓN DE CA 210 W (PLATAFORMA ÚNICAMENTE) 250 W • POTENCIA POE MÁXIMA EN TERMINALES DESDE UNA FUENTE DE ALIMENTACIÓN POE 200 W • CAPACIDAD DE POTENCIA POE MÁXIMA EN TERMINALES CON POE AUMENTADA 750 W ESPECIFICACIONES FÍSICAS.		

	• DIMENSIONES (AL X AN X PR) 44.5 X 438.2 X 304.9 MM (3.5 X 17.25 X 12 PULG.) • ALTURA DE BASTIDOR 3 UNIDADES DE BASTIDOR (2 RU) • MONTAJE EN BASTIDOR 48,3 CM (19 PULG.) EIA/58,4 CM (23 PULG.) • PESO CON FUENTE DE ALIMENTACIÓN DE CA (SIN MÓDULOS) 8.2 KG (39 LIBRAS) • PESO CON FUENTE DE ALIMENTACIÓN POE (SIN MÓDULOS) 8.6 KG (40 LIBRAS) • PESO NORMAL (CON MÓDULOS) 9.5 KG (60 LIBRAS) • FLUJO DE AIRE DESDE EL FRENTE HACIA LA PARTE POSTERIOR DESDE LA PARTE POSTERIOR HACIA EL FRENTE (CON CONJUNTO DE VENTILADORES NEBS)DESDE UNA LATERAL HACIA OTRA LATERAL ESPECIFICACIONES REGLAMENTARIAS: • SEGURIDAD: • UL 60950-1 • CAN/CSA C22.2 Nº 60950-1 • EN 60950-1 • AS/NZS 60950-1 • IEC 60950-1 • EMC • CFR TÍTULO 47, PARTE 15 • ICES-003 CLASE A • EN 55022 CLASE A • CISPR 22 CLASE A • AS/NZS 3548, CLASE A • VCCI V-3 • CNS 13438 • EN 300-386 • EN 61000 (INMUNIDAD) • EN 55024, CISPR 24 • EN 50082-1 • TELECOMUNICACIONES:		

	• TIA/EIA/IS-968 • CS-03 • ANSI T1.101 • ITU-T G.823, G.824 • IEEE 802.3 • DIRECTIVA RTTE DEBERÁ SOPORTAR LOS SIGUIENTES PROTOCOLOS: • IPV4, IPV6, RUTAS ESTÁTICAS, OSPF (ABRIR PRIMERO LA RUTA MÁS CORTA), EIGRP (IGRP MEJORADO), BGP (PROTOCOLO DE PUERTA DE ENLACE FRONTERIZA), REFLECTOR DE RUTA BGP, IS-IS (SISTEMA INTERMEDIO A SISTEMA INTERMEDIO), IGMPV3 (PROTOCOLO DE ADMINISTRACIÓN DE GRUPOS DE INTERNET DE MULTIDIFUSIÓN), PIM SM (MULTIDIFUSIÓN INDEPENDIENTE DEL PROTOCOLO EN MODO DISPERSO), PIM-SSM (MULTIDIFUSIÓN INDEPENDIENTE DEL PROTOCOLO-MULTIDIFUSIÓN ESPECÍFICA DEL ORIGEN), DVMRP (PROTOCOLO DE ROUTING MULTIDIFUSIÓN CON VECTOR DE DISTANCIA), MULTIDIFUSIÓN IPV4 A IPV6, MPLS, VPN DE CAPA 2 Y CAPA 3, IPSEC (SEGURIDAD DE PROTOCOLOS DE INTERNET), L2TPV3, ISIS, BFD (DETECCIÓN BIDIRECCIONAL DE LA EXPEDICIÓN), IEEE802.1AH, IEEE802.3AG. DEBERÁ SOPORTAR LAS SIGUIENTES ENCAPSULACIONES • GRE (ENCAPSULADO DE ROUTING GENÉRICO), ETHERNET, VLAN 802.1Q, PPP (PROTOCOLO PUNTO A PUNTO), MLPPP (PROTOCOLO DE ENLACES MÚLTIPLES PUNTO A PUNTO), FRAME RELAY, MLFR (FRAME RELAY DE ENLACES MÚLTIPLES) (FR15 Y FR16), HDLC (CONTROL DE ALTO NIVEL PARA ENLACES DE DATOS), SERIE (RS-232, RS-449, X.21, V.35 Y EIA-530), PPPOE (PROTOCOLO PUNTO A PUNTO SOBRE ETHERNET) Y ATM. DEBERÁ SOPORTAR LOS SIGUIENTES MECANISMOS DE CALIDAD DE SERVICIO: • QOS, CBWFQ (MECANISMO DE COLA DE ESPERA EQUITATIVO Y PONDERADO BASADO EN CLASES), WRED (DETECCIÓN TEMPRANA ALEATORIA Y PONDERADA), QOS JERÁRQUICA, PBR (ROUTING BASADO EN POLÍTICAS), PFR (ROUTING DE ALTO RENDIMIENTO) Y NBAR (ROUTING AVANZADO CON BASE EN LA RED). EL EQUIPO SERÁ DE LA MISMA MARCA QUE EL SISTEMA DE TELEFONÍA, GARANTIZANDO EL 100% DE COMPATIBLIDAD SIN NECESIDAD DE COMPONENTES O SOFTWARE ADICIONAL. EL EQUIPO INCLUIRÁ UN AÑO DE GARANTÍA PROPORCIONADA POR EL FABRICANTE, CON SERVICIO 8X5XNBD, INCLUYENDO RE-EMPLAZO DE EQUIPO.		

G)	**SUMINISTRO E INSTALACIÓN DE SWITCH CAPA 2:** **DESCRIPCIÓN** • EL EQUIPO DEBERÁ CONTAR CON LA VERSIÓN MÁS RECIENTE LIBERADA DEL SISTEMA OPERATIVO CON QUE CUENTE EL FABRICANTE. • TODO EL SOFTWARE DEBERÁ RESIDIR Y EJECUTARSE CON RECURSOS PROPIOS DEL EQUIPO. • EL EQUIPO DEBERÁ SER COMPATIBLE Y MANEJAR LAS FUNCIONALIDADES AL 100% DE LOS EQUIPOS SWIITCHES 05 SOLICITADOS POR EL LICITANTE. • SE DEBERÁN INCLUIR LOS CABLES NECESARIOS PARA SU INTERCONEXIÓN. • EL EQUIPO OFERTADO DEBE DE SOPORTAR SER MONTADO EN RACK DE 19 PULGADAS. • LAS CARACTERÍSTICAS ENUNCIADAS A CONTINUACIÓN SON MÍNIMAS, PUDIENDO OFERTAR UN EQUIPO QUE SUPERE LOS REQUERIMIENTOS SOLICITADOS. • SERÁ DEL MISMO FABRICANTE QUE LA SOLUCIÓN DE TELEFONÍA PARA GARANTIZAR EL 100% DE INTEROPERATIBLIIDAD **CARACTERÍSTICAS GENERALES** • SWITCH DE ACCESO CON CAPACIDAD DE AL MENOS 48 PUERTOS CONMUTADOS 10/100 CON AUTO DETECCIÓN, POE (IEEE 802.3AF) INTEGRADO , 2 PUERTOS 10/100/100 FIJOS Y 2 PUERTOS GIGABIT ETHERNET DE PROPÓSITO DUAL, PARA 1000 BASEX Y PARA 1000BASET • MANEJO DE AL MENOS 255 VLAN'S ACTIVAS A TRAVÉS DEL ESTÁNDAR 802.1Q. EL MECANISMO DE SEGMENTACIÓN DE VLAN DEBERÁ SER 100% COMPATIBLE CON LA ASIGNACIÓN DE VLANS DE VOZ Y DATOS MANEJADO POR LOS TELÉFONOS IP A ADQUIRIR POR EL LICITANTE • MANEJO DE PRIORIZACIÓN DE CLASES DE SERVICIO A TRAVÉS DEL ESTÁNDAR 802.1P. • LOS ENTRONCAMIENTOS DE VLANS DEBERÁN PODER CREARSE DESDE CUALQUIER PUERTO UTILIZANDO LOS PROTOCOLOS 802.1Q. • OPERACIÓN FULL DUPLEX DE ANCHO DE BANDA A LAS ESTACIONES FINALES Y SERVIDORES, ASÍ COMO AUTO NEGOCIACIÓN EN TODOS LOS PUERTOS 10/100 MBPS. • MANEJO DE AL MENOS 8000 DIRECCIONES MAC. • MANEJO DEL ESTÁNDAR 802.1X. • ACTUALIZACIÓN A LAS CARACTERÍSTICAS DEL SWITCH A TRAVÉS DE SOFTWARE. • MANEJO DE NTP, DHCP SNOOPING. • SOPORTE DE IGMP VERSIÓN 3 SNOOPING,. • EL ACCESO A LAS INTERFACES DE ADMINISTRACIÓN DE LOS EQUIPOS PODRÁ SER LLEVADA A CABO MEDIANTE SSL, SSH, TELNET, ETC. • MANEJO DE AGREGACIÓN DE PUERTOS PARA QUE PUEDAN SER TRATADOS COMO UNA SOLA TRONCAL, CON DISPOSITIVOS QUE MANEJEN 802.3AD. • MANEJO MÍNIMO DE 4 COLAS DE EGRESO POR PUERTO EN HARDWARE CON MANEJO DE MECANISMOS DE ENCOLAMIENTO QUE GARANTICEN UN TRATO PRIORITARIO PARA TRÁFICO DE VOZ. • BACKPLANE DE AL MENOS 16 GBPS Y MANEJO DE AL MENOS 10 MPPS. • SEGURIDAD: MANEJO DE AUTENTICACIÓN DE USUARIOS MEDIANTE 802.1X POR PUERTO Y POR VLAN, SEGURIDAD A	PIEZA	2

	NIVEL DE PUERTO BASADA EN MAC, SOPORTE DE SSHV2, MANEJO DE SNMPV3. **ADMINISTRACIÓN:** • MANEJAR EL ACCESO VÍA TELNET. • MANEJO DE CONFIGURACIÓN VÍA WEB. • MANEJO DE TFTP PARA ACTUALIZACIÓN DE VERSIONES DEL SISTEMA OPERATIVO Y DE CONFIGURACIÓN. • MANEJO DE ESPEJEO DE PUERTOS DE UN SWITCH REMOTO PARA ANÁLISIS DE TRÁFICO. • ADMINISTRACIÓN LOCAL POR MEDIO DE PUERTO DE CONSOLA (INTERFAZ DE LÍNEA DE COMANDOS). • COMPATIBILIDAD CON AL MENOS CUATRO GRUPOS RMON (HISTORIAL, ESTADÍSTICAS, ALARMAS Y EVENTOS) PARA MEJORAR LA GESTIÓN, EL CONTROL Y EL ANÁLISIS DEL TRÁFICO. • MANEJO DE JUMBO FRAMES. • MANEJO DE IPV4 Y SOPORTE DE IPV6. • MANEJO DE RADIUS • INSPECCIÓN DINÁMICA DE ARP • DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER UNIR VARIOS ENLACES FÍSICOS; EN UN ENLACE LÓGICO, Y ANTE LA CAÍDA DE UN ENLACE FÍSICO, SÓLO DISMINUYA EL PERFORMANCE DE ESE ENLACE Y NO DE TODO EL ENLACE LÓGICO. • DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER ESTABLECER POR UN LAPSO DE TIEMPO LA MAC ADDRESS DE UN EQUIPO, Y PODER BORRARLA AL FINALIZAR EL TIEMPO ESTABLECIDO; PERMITIENDO A OTRO EQUIPO CONECTARSE AL MISMO TIEMPO • CADA UNO DE LOS EQUIPOS SWITCHES LAN PROPUESTOS, DEBERÁ MANEJAR DOS VLANS ACTIVAS POR PUERTO, UNA VLAN PARA EL TRÁFICO DE VOZ GENERADO POR EL TELÉFONO IP Y OTRA VLAN PARA EL TRÁFICO GENERADO POR LA PC CONECTADA AL TELÉFONO IP. LA ASIGNACIÓN DE LA VLAN DE VOZ A UN TELÉFONO IP CONECTADO, DEBERÁ SER DE MANERA AUTOMÁTICA. • CADA EQUIPO SWITCH LAN STANDALONE DEBERÁ CONTAR CON LA FUNCIONALIDAD DE AUTO-MDIX (AUTOMATIC MEDIUM-DEPENDENT INTERFACE CROSSOVER) EN LOS PUERTOS EN COBRE (UTP). • MANEJO DE LAS SIGUIENTES CARACTERÍSTICAS GENERALES: • LIMITACIÓN DE ANCHO DE BANDA EN BASE A DIRECCIÓN IP FUENTE/DESTINO, DIRECCIÓN MAC FUENTE/DESTINO Y EN BASE A PUERTO TCP/UDP, ASÍ COMO EL SOPORTE DE 64 POLÍTICAS INDIVIDUALES. • MANEJO DE DIFERENTES NIVELES DE USUARIOS PARA LA ADMINISTRACIÓN DE LOS EQUIPOS. • CAPACIDAD DE SOPORTAR ADICIONALMENTE UNA FUENTE DE PODER REDUNDANTE EXTERNA **ESTÁNDARES** • IEEE 802.1D SPANNING TREE PROTOCOL • IEEE 802.1P COS PRIORITIZATION • IEEE 802.1Q VLAN • IEEE 802.1S • IEEE 802.1W • IEEE 802.1X • IEEE 802.1AB (LLDP) • IEEE 802.3AD • IEEE 802.3AF		

	• IEEE 802.3AH (100BASE-X SINGLE/MULTIMODE FIBER ONLY) • IEEE 802.3X FULL DUPLEX ON 10BASE-T, 100BASE-TX, AND 1000BASE-T PORTS • IEEE 802.3 10BASE-T SPECIFICATION • IEEE 802.3U 100BASE-TX SPECIFICATION • IEEE 802.3AB 1000BASE-T SPECIFICATION • IEEE 802.3Z 1000BASE-X SPECIFICATION • 100BASE-BX (SFP) • 100BASE-FX (SFP) • 100BASE-LX (SFP) • 1000BASE-BX (SFP) • 1000BASE-SX (SFP) • 1000BASE-LX/LH (SFP) • 1000BASE-ZX (SFP) • 1000BASE-CWDM SFP 1470 NM • 1000BASE-CWDM SFP 1490 NM • 1000BASE-CWDM SFP 1510 NM • 1000BASE-CWDM SFP 1530 NM • 1000BASE-CWDM SFP 1550 NM • 1000BASE-CWDM SFP 1570 NM • 1000BASE-CWDM SFP 1590 NM • 1000BASE-CWDM SFP 1610 NM • RMON I AND II STANDARDS • SNMPV1, SNMPV2C, AND SNMPV3 INCLUIRÁ GARANTÍA PROPORCIONADA POR EL FABRICANTE, DURANTE UN AÑO Y NIVEL 8X5XNBD		
H)	**SUMINISTRO E INSTALACIÓN DE EQUIPO DE RED SWITCH DE CAPA 2:** **DESCRIPCIÓN** • EL EQUIPO DEBERÁ CONTAR CON LA VERSIÓN MÁS RECIENTE LIBERADA DEL SISTEMA OPERATIVO CON QUE CUENTE EL FABRICANTE. • TODO EL SOFTWARE DEBERÁ RESIDIR Y EJECUTARSE CON RECURSOS PROPIOS DEL EQUIPO. • EL EQUIPO DEBERÁ SER COMPATIBLE Y MANEJAR LAS FUNCIONALIDADES AL 100% DE LOS EQUIPOS SWIITCHES 05 SOLICITADOS POR EL LICITANTE. • SE DEBERÁN INCLUIR LOS CABLES NECESARIOS PARA SU INTERCONEXIÓN. • EL EQUIPO OFERTADO DEBE DE SOPORTAR SER MONTADO EN RACK DE 19 PULGADAS. • LAS CARACTERÍSTICAS ENUNCIADAS A CONTINUACIÓN SON MÍNIMAS, PUDIENDO OFERTAR UN EQUIPO QUE SUPERE LOS REQUERIMIENTOS SOLICITADOS. • SERÁ DEL MISMO FABRICANTE QUE LA SOLUCIÓN DE TELEFONÍA PARA GARANTIZAR EL 100% DE INTEROPERATIBLIIDAD **CARACTERÍSTICAS GENERALES** • SWITCH DE ACCESO CON CAPACIDAD DE AL MENOS 24 PUERTOS CONMUTADOS 10/100 CON AUTO DETECCIÓN, POE (IEEE 802.3AF) INTEGRADO Y 2 PUERTOS GIGABIT ETHERNET DE PROPÓSITO DUAL, PARA 1000 BASEX Y PARA 1000BASET • MANEJO DE AL MENOS 255 VLAN'S ACTIVAS A TRAVÉS DEL ESTÁNDAR 802.1Q. EL MECANISMO DE SEGMENTACIÓN DE VLAN DEBERÁ SER 100% COMPATIBLE CON LA ASIGNACIÓN DE VLANS DE VOZ Y DATOS MANEJADO POR LOS TELÉFONOS IP A ADQUIRIR POR EL LICITANTE • MANEJO DE PRIORIZACIÓN DE CLASES DE SERVICIO A	PIEZA	4

	TRAVÉS DEL ESTÁNDAR 802.1P. • LOS ENTRONCAMIENTOS DE VLANS DEBERÁN PODER CREARSE DESDE CUALQUIER PUERTO UTILIZANDO LOS PROTOCOLOS 802.1Q. • OPERACIÓN FULL DUPLEX DE ANCHO DE BANDA A LAS ESTACIONES FINALES Y SERVIDORES, ASÍ COMO AUTO NEGOCIACIÓN EN TODOS LOS PUERTOS 10/100 MBPS. • MANEJO DE AL MENOS 8000 DIRECCIONES MAC. • MANEJO DEL ESTÁNDAR 802.1X. • ACTUALIZACIÓN A LAS CARACTERÍSTICAS DEL SWITCH A TRAVÉS DE SOFTWARE. • MANEJO DE NTP, DHCP SNOOPING. • SOPORTE DE IGMP VERSIÓN 3 SNOOPING,. • EL ACCESO A LAS INTERFACES DE ADMINISTRACIÓN DE LOS EQUIPOS PODRÁ SER LLEVADA A CABO MEDIANTE SSL, SSH, TELNET, ETC. • MANEJO DE AGREGACIÓN DE PUERTOS PARA QUE PUEDAN SER TRATADOS COMO UNA SOLA TRONCAL, CON DISPOSITIVOS QUE MANEJEN 802.3AD. • MANEJO MÍNIMO DE 4 COLAS DE EGRESO POR PUERTO EN HARDWARE CON MANEJO DE MECANISMOS DE ENCOLAMIENTO QUE GARANTICEN UN TRATO PRIORITARIO PARA TRÁFICO DE VOZ. • BACKPLANE DE AL MENOS 16 GBPS Y MANEJO DE AL MENOS 6 MPPS. • SEGURIDAD: MANEJO DE AUTENTICACIÓN DE USUARIOS MEDIANTE 802.1X POR PUERTO Y POR VLAN, SEGURIDAD A NIVEL DE PUERTO BASADA EN MAC, SOPORTE DE SSHV2, MANEJO DE SNMPV3. **ADMINISTRACIÓN:** • MANEJAR EL ACCESO VÍA TELNET. • MANEJO DE CONFIGURACIÓN VÍA WEB. • MANEJO DE TFTP PARA ACTUALIZACIÓN DE VERSIONES DEL SISTEMA OPERATIVO Y DE CONFIGURACIÓN. • MANEJO DE ESPEJEO DE PUERTOS DE UN SWITCH REMOTO PARA ANÁLISIS DE TRÁFICO. • ADMINISTRACIÓN LOCAL POR MEDIO DE PUERTO DE CONSOLA (INTERFAZ DE LÍNEA DE COMANDOS). • COMPATIBILIDAD CON AL MENOS CUATRO GRUPOS RMON (HISTORIAL, ESTADÍSTICAS, ALARMAS Y EVENTOS) PARA MEJORAR LA GESTIÓN, EL CONTROL Y EL ANÁLISIS DEL TRÁFICO. • MANEJO DE JUMBO FRAMES. • MANEJO DE IPV4 Y SOPORTE DE IPV6. • MANEJO DE RADIUS • INSPECCIÓN DINÁMICA DE ARP • DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER UNIR VARIOS ENLACES FÍSICOS; EN UN ENLACE LÓGICO, Y ANTE LA CAÍDA DE UN ENLACE FÍSICO, SÓLO DISMINUYA EL PERFORMANCE DE ESE ENLACE Y NO DE TODO EL ENLACE LÓGICO. • DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER ESTABLECER POR UN LAPSO DE TIEMPO LA MAC ADDRESS DE UN EQUIPO, Y PODER BORRARLA AL FINALIZAR EL TIEMPO ESTABLECIDO; PERMITIENDO A OTRO EQUIPO CONECTARSE AL MISMO TIEMPO • CADA UNO DE LOS EQUIPOS SWITCHES LAN PROPUESTOS, DEBERÁ MANEJAR DOS VLANS ACTIVAS POR PUERTO, UNA VLAN PARA EL TRÁFICO DE VOZ GENERADO POR EL TELÉFONO IP Y OTRA VLAN PARA EL TRÁFICO GENERADO POR LA PC CONECTADA AL TELÉFONO IP. LA ASIGNACIÓN DE LA		

	VLAN DE VOZ A UN TELÉFONO IP CONECTADO, DEBERÁ SER DE MANERA AUTOMÁTICA. • CADA EQUIPO SWITCH LAN STANDALONE DEBERÁ CONTAR CON LA FUNCIONALIDAD DE AUTO-MDIX (AUTOMATIC MEDIUM-DEPENDENT INTERFACE CROSSOVER) EN LOS PUERTOS EN COBRE (UTP). • MANEJO DE LAS SIGUIENTES CARACTERÍSTICAS GENERALES: • LIMITACIÓN DE ANCHO DE BANDA EN BASE A DIRECCIÓN IP FUENTE/DESTINO, DIRECCIÓN MAC FUENTE/DESTINO Y EN BASE A PUERTO TCP/UDP, ASÍ COMO EL SOPORTE DE 64 POLÍTICAS INDIVIDUALES. • MANEJO DE DIFERENTES NIVELES DE USUARIOS PARA LA ADMINISTRACIÓN DE LOS EQUIPOS. • CAPACIDAD DE SOPORTAR ADICIONALMENTE UNA FUENTE DE PODER REDUNDANTE EXTERNA **ESTÁNDARES** • IEEE 802.1D SPANNING TREE PROTOCOL • IEEE 802.1P COS PRIORITIZATION • IEEE 802.1Q VLAN • IEEE 802.1S • IEEE 802.1W • IEEE 802.1X • IEEE 802.1AB (LLDP) • IEEE 802.3AD • IEEE 802.3AF • IEEE 802.3AH (100BASE-X SINGLE/MULTIMODE FIBER ONLY) • IEEE 802.3X FULL DUPLEX ON 10BASE-T, 100BASE-TX, AND 1000BASE-T PORTS • IEEE 802.3 10BASE-T SPECIFICATION • IEEE 802.3U 100BASE-TX SPECIFICATION • IEEE 802.3AB 1000BASE-T SPECIFICATION • IEEE 802.3Z 1000BASE-X SPECIFICATION • 100BASE-BX (SFP) • 100BASE-FX (SFP) • 100BASE-LX (SFP) • 1000BASE-BX (SFP) • 1000BASE-SX (SFP) • 1000BASE-LX/LH (SFP) • 1000BASE-ZX (SFP) • 1000BASE-CWDM SFP 1470 NM • 1000BASE-CWDM SFP 1490 NM • 1000BASE-CWDM SFP 1510 NM • 1000BASE-CWDM SFP 1530 NM • 1000BASE-CWDM SFP 1550 NM • 1000BASE-CWDM SFP 1570 NM • 1000BASE-CWDM SFP 1590 NM • 1000BASE-CWDM SFP 1610 NM • RMON I AND II STANDARDS • SNMPV1, SNMPV2C, AND SNMPV3 INCLUIRÁ GARANTÍA PROPORCIONADA POR EL FABRICANTE, DURANTE UN AÑO Y NIVEL 8X5XNBD		
I)	**SUMINISTRO E INSTALACIÓN DE SWITCH CAPA 3:** **DESCRIPCIÓN** • EL EQUIPO DEBERÁ CONTAR CON LA VERSIÓN MÁS RECIENTE LIBERADA DEL SISTEMA OPERATIVO CON QUE CUENTE EL FABRICANTE. • TODO EL SOFTWARE DEBERÁ RESIDIR Y EJECUTARSE CON	PIEZA	1

	RECURSOS PROPIOS DEL EQUIPO. • SE DEBERÁN INCLUIR LOS CABLES NECESARIOS PARA SU INTERCONEXIÓN. • EL EQUIPO OFERTADO DEBE PODER SER MONTADO EN RACK DE 19 PULGADAS OCUPANDO 1 RU DE ESPACIO. • LAS CARACTERÍSTICAS ENUNCIADAS A CONTINUACIÓN SON MÍNIMAS, PUDIENDO OFERTAR UN EQUIPO QUE SUPERE LOS REQUERIMIENTOS SOLICITADOS. • SERÁ DEL MISMO FABRICANTE QUE LA SOLUCIÓN DE TELEFONÍA PARA GARANTIZAR EL 100% DE INTEROPERATIBLIIDAD **CARACTERÍSTICAS GENERALES** • SWITCH DE ACCESO CON CAPACIDAD DE AL MENOS 24 PUERTOS CONMUTADOS 10/100/1000. • EL EQUIPO DEBERÁ INCLUIR UN MÓDULO DE RED CON 4 SLOTS SFP PARA CONEXIÓN DE GBICS A 1 GIGABIT ETHERNET. • DEBERÁN INCLUIRSE 8 GBICS (TRANCEIVERS) PARA FIBRA COMPATIBLES CON EL MODULO INDICADO EN EL PUNTO ANTERIOR TIPO1000BASE-SX PARA FIBRA MULTIMODO DE 850NM CON CONECTOR TIPO DUAL LC/PC. • EL EQUIPO PROPUESTO DEBE SER CAPAZ DE FORMAR UN ARREGLO DE AL MENOS 8 (OCHO) SWITCHES PARA PODER SER ADMINISTRADO COMO UN SÓLO DISPOSITIVO, EL APILAMIENTO DEBERÁ SER DE LA MISMA CAPACIDAD DEL BACKPLANE (MATRIZ DE CONMUTACIÓN) MANEJADO POR ESTOS EQUIPOS Y PROVISTO MEDIANTE UN PUERTO DEDICADO A ESTAS FUNCIONES. • MANEJO DE AL MENOS 1000 VLAN'S ACTIVAS A TRAVÉS DEL ESTÁNDAR 802.1Q. • MANEJO DE PRIORIZACIÓN DE CLASES DE SERVICIO A TRAVÉS DEL ESTÁNDAR 802.1P. • LOS ENTRONCAMIENTOS DE VLANS DEBERÁN PODER CREARSE DESDE CUALQUIER PUERTO UTILIZANDO LOS PROTOCOLOS 802.1Q. • OPERACIÓN FULL DUPLEX DE ANCHO DE BANDA A LAS ESTACIONES FINALES Y SERVIDORES, ASÍ COMO AUTO NEGOCIACIÓN EN TODOS LOS PUERTOS 10/100/1000 MBPS. • MANEJO DE AL MENOS 12000 DIRECCIONES MAC. • MANEJO DEL ESTÁNDAR 802.1X. • ACTUALIZACIÓN A LAS CARACTERÍSTICAS DEL SWITCH A TRAVÉS DE SOFTWARE. • MANEJO DE NTP, DHCP SNOOPING. • SOPORTE DE IGMP VERSIÓN 3 SNOOPING, • EL ACCESO A LAS INTERFACES DE ADMINISTRACIÓN DE LOS EQUIPOS PODRÁ SER LLEVADA A CABO MEDIANTE SSL, SSH, TELNET, ETC. • SOPORTE DE PROTOCOL INDEPENDENT MULTICAST (PIM) PARA RUTEO MULTICAST, INCLUYENDO PIM SPARSE MODE (PIM-SM), PIM DENSE MODE (PIM-DM), Y PIM SPARSE-DENSE MODE. • MANEJO DE AGREGACIÓN DE PUERTOS PARA QUE PUEDAN SER TRATADOS COMO UNA SÓLA TRONCAL MEDIANTE EL MANEJO DEL PROTOCOLO 802.3AD. • MANEJO MÍNIMO DE 4 COLAS DE EGRESO POR PUERTO EN HARDWARE CON MANEJO DE MECANISMOS DE ENCOLAMIENTO QUE GARANTICEN UN TRATO PRIORITARIO PARA TRÁFICO DE VOZ. • BACKPLANE DE AL MENOS 160 GBPS Y MANEJO DE AL MENOS 65.5 MILLONES DE PAQUETES POR SEGUNDO.		

	• SEGURIDAD: MANEJO DE AUTENTICACIÓN DE USUARIOS MEDIANTE 802.1X POR PUERTO Y POR VLAN, SEGURIDAD A NIVEL DE PUERTO BASADA EN MAC, SOPORTE DE SSHV2, MANEJO DE SNMPV3. **ADMINISTRACIÓN:** • MANEJAR EL ACCESO VÍA TELNET. • MANEJO DE CONFIGURACIÓN VÍA WEB. • MANEJO DE TFTP PARA ACTUALIZACIÓN DE VERSIONES DEL SISTEMA OPERATIVO Y DE CONFIGURACIÓN. • MANEJO DE ESPEJEO DE PUERTOS DE UN SWITCH REMOTO PARA ANÁLISIS DE TRÁFICO. • ADMINISTRACIÓN LOCAL POR MEDIO DE PUERTO DE CONSOLA (INTERFAZ DE LÍNEA DE COMANDOS). • COMPATIBILIDAD CON AL MENOS CUATRO GRUPOS RMON (HISTORIAL, ESTADÍSTICAS, ALARMAS Y EVENTOS) PARA MEJORAR LA GESTIÓN, EL CONTROL Y EL ANÁLISIS DEL TRÁFICO. • MANEJO DE JUMBO FRAMES • MANEJO DE IPV4 Y SOPORTE DE IPV6. • MANEJO DE RADIUS • INSPECCIÓN DINÁMICA DE ARP • PROTECCIÓN CONTRA AMENAZAS DE IP SPOOFING Y FILTROS (LISTAS DE CONTROL DE ACCESO) POR IP Y POR MAC. • DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER UNIR VARIOS ENLACES FÍSICOS EN UN ENLACE LÓGICO Y ANTE LA CAÍDA DE UN ENLACE FÍSICO SÓLO DISMINUYA EL PERFORMANCE DE ESE ENLACE Y NO DE TODO EL ENLACE LÓGICO. • DEBERÁ MANEJAR LA FUNCIONALIDAD DE PODER ESTABLECER POR UN LAPSO DE TIEMPO LA MAC ADDRESS DE UN EQUIPO, Y PODER BORRARLA AL FINALIZAR EL TIEMPO ESTABLECIDO; PERMITIENDO A OTRO EQUIPO CONECTARSE AL MISMO TIEMPO • CADA UNO DE LOS EQUIPOS SWITCHES LAN PROPUESTOS, DEBERÁ MANEJAR DOS VLANS ACTIVAS POR PUERTO, UNA VLAN PARA EL TRÁFICO DE VOZ GENERADO POR EL TELÉFONO IP Y OTRA VLAN PARA EL TRÁFICO GENERADO POR LA PC CONECTADA AL TELÉFONO IP. LA ASIGNACIÓN DE LA VLAN DE VOZ A UN TELÉFONO IP CONECTADO, DEBERÁ SER DE MANERA AUTOMÁTICA. • CADA EQUIPO SWITCH LAN STANDALONE DEBERÁ CONTAR CON LA FUNCIONALIDAD DE AUTO-MDIX (AUTOMATIC MEDIUM-DEPENDENT INTERFACE CROSSOVER) EN LOS PUERTOS EN COBRE (UTP). • MANEJO DE RIP Y RUTAS ESTÁTICAS, Y SOPORTE DE LOS SIGUIENTES PROTOCOLOS MEDIANTE UNA ACTUALIZACIÓN EN SOFTWARE A FUTURO: • OPEN SHORTEST PATH FIRST (OSPF) VERSION 2. • SOPORTE DE BORDER GATEWAY PROTOCOL (BGP) VERSIÓN 4. • LIMITACIÓN DE ANCHO DE BANDA EN BASE A DIRECCIÓN IP FUENTE/DESTINO, DIRECCIÓN MAC FUENTE/DESTINO Y EN BASE A PUERTO TCP/UDP, ASÍ COMO EL SOPORTE DE 64 POLÍTICAS INDIVIDUALES. • MANEJO DE DIFERENTES NIVELES DE USUARIOS PARA LA ADMINISTRACIÓN DE LOS EQUIPOS. • CAPACIDAD DE SOPORTAR ADICIONALMENTE UNA FUENTE DE PODER REDUNDANTE EXTERNA **ESTÁNDARES**		

	• IEEE 802.1S • IEEE 802.1W • IEEE 802.1X • IEEE 802.1X-REV • IEEE 802.3AD • IEEE 802.1AE • 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 SPECIFICATION • IEEE 802.3U 100BASE-TX SPECIFICATION • IEEE 802.3AB 1000BASE-T SPECIFICATION • IEEE 802.3Z 1000BASE-X SPECIFICATION INCLUIRÁ GARANTÍA PROPORCIONADA POR EL FABRICANTE, DURANTE UN AÑO Y NIVEL 8X5XNBD		
J)	**SUMINISTRO E INSTALACIÓN DE EQUIPO DE SEGURIDAD DE RED QUE SEA DEL TIPO ADMINISTRACIÓN UNIFICADA DE AMENAZAS, DONDE SE DEBERÁN OFRECER LAS FUNCIONALIDADES QUE ABAJO SE DETALLAN YA INCLUIDAS Y LISTAS PARA SER UTILIZADAS:** CARACTERÍSTICAS DEL 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 DEL SISTEMA OPERATIVO INCLUIDO QUE DEBERA TENER LAS SIGUIENTES CARACTERISTICAS • 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	PIEZA	24

	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 UNA INTERFACE/PUERTO DMZ Y 2 PUERTOS PARA ENLACES WAN. • 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, PERMITIR QUE ANTE LA PRESENCIA DE DOS ENLACES A INTERNET, SE PUEDA DECIDIR CUÁL DE 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. • 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 INTERFACE (INTERFACE-MODE VPN) • EN MODO INTERFACE, LA VPN IPSEC DEBERÁ PODER		

		TENER ASIGNADA UNA DIRECCIÓN IP, TENER RUTAS ASIGNADAS PARA SER ENCAMINADAS POR ESTA INTERFACE Y DEBERÁ SER CAPAZ DE ESTAR PRESENTE COMO INTERFACE FUENTE O DESTINO EN POLÍTICAS DE FIREWALL. • 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 • 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 PODRÁ 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 4000 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. • DEBE 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 DEBE 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. • DEBE OFRECERSE 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 DEBE 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 DEBE SOPORTAR EL ANÁLISIS DE ARCHIVOS DEL TIPO: MS-WORD, PDF, TEXTO, ARCHIVOS COMPRIMIDOS. • DEBE 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 DEBEN 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 DEBE 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 DEBE 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 DEBE PERMITIR LA BÚSQUEDA DE PATRONES EN ARCHIVOS MEDIANTE LA DEFINICIÓN DE EXPRESIONES REGULARES. CONTROL DE APLICACIONES • LO SOLUCIÓN DEBE SOPORTAR LA CAPACIDAD DE IDENTIFICAR LA APLICACIÓN QUE ORIGINA CIERTO TRÁFICO A PARTIR DE LA INSPECCIÓN DEL MISMO. • LA IDENTIFICACIÓN DE LA APLICACIÓN DEBE SER INDEPENDIENTE DEL PUERTO Y PROTOCOLO HACIA EL CUAL ESTÉ DIRECCIONADO DICHO TRÁFICO. • LAS SOLUCIÓN DEBE TENER UN LISTADO DE AL MENOS 1000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE. • EL LISTADO DE APLICACIONES DEBE ACTUALIZARSE PERIÓDICAMENTE. • PARA APLICACIONES IDENTIFICADAS DEBEN PODER DEFINIRSE AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) DEBEN PODER DEFINIRSE AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES DE TIPO P2P DEBE PODER DEFINIRSE ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING. • PREFERENTEMENTE DEBEN SOPORTAR MAYOR GRANULARIDAD EN LAS ACCIONES. INSPECCIÓN DE CONTENIDO SSL • LA SOLUCIÓN DEBE 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 DEBE REQUERIR NINGÚN CAMBIO DE CONFIGURACIÓN EN LAS APLICACIONES O SISTEMA OPERATIVO DEL USUARIO. • PARA EL CASO DE URL FILTERING, DEBE SER POSIBLE CONFIGURAR EXCEPCIONES DE INSPECCIÓN DE HTTPS. DICHAS EXCEPCIONES EVITAN QUE EL TRÁFICO SEA INSPECCIONADO PARA LOS SITIOS CONFIGURADOS. LAS EXCEPCIONES DEBEN PODER DETERMINARSE AL MENOS POR CATEGORÍA DE FILTRADO. 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 DEBE CONTAR CON UN ALGORITMO (APPLICATION LAYER GATEWAY) DE SIP • DEBE PODER HACERSE INSPECCIÓN DE ENCABEZADOS DE SIP • DEBEN PODER LIMITARSE LA CANTIDAD DE REQUERIMIENTOS SIP QUE SE HACEN POR SEGUNDO. ESTO DEBE PODER DEFINIRSE POR CADA MÉTODO SIP. • LA SOLUCIÓN DEBE SOPORTAR SIP HNT (HOSTED NAT TRANSVERSAL). ALTA DISPONIBILIDAD • DEBERA 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. • DEBERA DE SOPORTAR ALTA DISPONIBILIDAD EN MODO		

	ACTIVO-PASIVO • DEBERA DE SOPORTAR ALTA DISPONIBILIDAD EN MODO ACTIVO-ACTIVO • DEBERA 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 • DEBERA DE SER POSIBLE DEFINIR INTERFACES DE GESTIÓN INDEPENDIENTES PARA CADA MIEMBRO EN UN CLUSTER. CARACTERÍSTICAS DE GERENCIA • DEBERA TENER UNA INTERFASE 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 INTERFASE DEBE SOPORTAR SSL SOBRE HTTP (HTTPS) • LA INTERFASE GRÁFICA DE USUARIO (GUÏ) VÍA WEB DEBERÁ PODER ESTAR EN ESPAÑOL Y EN INGLÉS, CONFIGURABLE POR EL USUARIO. • DEBERA TENER UNA INTERFASE BASADA EN LÍNEA DE COMANDO (CLI) PARA ADMINISTRACIÓN DE LA SOLUCIÓN. • DEBERA DE TENER UN PUERTO SERIAL DEDICADO PARA ADMINISTRACIÓN. ESTE PUERTO DEBE ESTAR ETIQUETADO E IDENTIFICADO PARA TAL EFECTO. • LA COMUNICACIÓN DEBERA DE ESTAR CIFRADA Y AUTENTICADA CON USERNAME Y PASSWORD, TANTO COMO PARA LA INTERFASE 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. • DEBERA DE DAR SOPORTE DE SNMP VERSIÓN 2 • DEBERA DE DAR SOPORTE DE SNMP VERSIÓN 3 • DEBERA DE DAR SOPORTE DE AL MENOS 3 SERVIDORES SYSLOG PARA PODER ENVIAR BITÁCORAS A SERVIDORES DE SYSLOG REMOTOS • DEBERA DE DAR SOPORTAR PARA ALMACENAMIENTO DE EVENTOS EN UN REPOSITORIO QUE PUEDA CONSULTARSE LUEGO CON SQL. • DEBERA 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. • DEBE 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 DEBE 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 • DEBE SER POSIBLE LA DEFINICIÓN Y ASIGNACIÓN DE RECURSOS DE FORMA INDEPENDIENTE PARA CADA		

	INSTANCIA VIRTUAL • DEBE SER POSIBLE DEFINIR DISTINTOS SERVIDORES DE LOG (SYSLOG) PARA CADA INSTANCIA VIRTUAL. • DEBE SER POSIBLE DEFINIR Y MODIFICAR LOS MENSAJES MOSTRADOS POR EL DISPOSITIVO DE FORMA INDEPENDIENTE PARA CADA INSTANCIA VIRTUAL. ESTÁNDARES Y CERTIFICACIONES • LA SOLUCIÓN DEBERÍA 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 ***DESEMPEÑO / CONECTIVIDAD*** EL EQUIPO DEBE POR LO MENOS OFRECER LAS SIGUIENTES CARACTERÍSTICAS DE DESEMPEÑO Y CONECTIVIDAD A) THROUGHPUT - FIREWALL: 1. 9 GBPS - VPN (3DES): 140 MBPS - ANTIVIRUS: 190 MBPS - IPS: 350 MBPS B) CONEXIONES CONCURRENTES TOTALES		

	• 1 MILLON C) NUEVAS CONEXIONES POR SEGUNDO • 12 MIL D) INTERFACES DE RED 1 INTERFACES 10/100 MBPS (DMZ) 2 INTERFACES 10/100/1000 MBPS BASADAS EN COBRE.WAN 6 PUERTOS DE SWITCH 10/100 ***LICENCIAMIENTO, ACTUALIZACIONES Y GARANTÍA*** EL LICENCIAMIENTO DE TODAS LAS FUNCIONALIDADES DEBE SER ILIMITADO EN CUANTO A USUARIOS, BUZÓN, CONEXIONES Y CLIENTES. LA VIGENCIA DE LAS ACTUALIZACIONES PARA LOS SERVICIOS DE ANTIVIRUS, ANTISPAM, IPS Y URL FILTERING DEBE PROVEERSE POR AL MENOS 1 AÑO. ASÍ MISMO INCLUIRÁ SOPORTE Y GARANTÍA DE HARDWARE POR UN AÑO.		
K)	**SUMINISTRO E INSTALACIÓN DE EQUIPO DE SEGURIDAD DE RED QUE SEA DEL TIPO ADMINISTRACIÓN UNIFICADA DE AMENAZAS, DONDE SE DEBERÁN OFRECER LAS FUNCIONALIDADES QUE ABAJO SE DETALLAN YA INCLUIDAS Y LISTAS PARA SER UTILIZADAS:** FUNCIONALIDADES Y CARACTERÍSTICAS DEL SISTEMA: CARACTERÍSTICAS DEL 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 DEL SISTEMA OPERATIVO INCLUIDO QUE DEBERA TENER LAS SIGUIENTES CARACTERISTICAS • SISTEMA OPERATIVO BLINDADO, ESPECÍFICO PARA SEGURIDAD QUE SEA COMPATIBLE CON EL APPLIANCE. POR SEGURIDAD Y FACILIDAD DE ADMINISTRACIÓN Y	PIEZA	1

		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 UNA INTERFACE/PUERTO DMZ Y 2 PUERTOS PARA ENLACES WAN. • 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, PERMITIR QUE ANTE LA PRESENCIA DE DOS ENLACES A INTERNET, SE PUEDA DECIDIR CUÁL DE 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. • 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 INTERFACE (INTERFACE-MODE VPN)		

		• EN MODO INTERFACE, LA VPN IPSEC DEBERÁ PODER TENER ASIGNADA UNA DIRECCIÓN IP, TENER RUTAS ASIGNADAS PARA SER ENCAMINADAS POR ESTA INTERFACE Y DEBERÁ SER CAPAZ DE ESTAR PRESENTE COMO INTERFACE FUENTE O DESTINO EN POLÍTICAS DE FIREWALL. • 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 • 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 PODRÁ 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 4000 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. • DEBE 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 DEBE 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. • DEBE OFRECERSE 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 DEBE 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 DEBE SOPORTAR EL ANÁLISIS DE ARCHIVOS DEL TIPO: MS-WORD, PDF, TEXTO, ARCHIVOS COMPRIMIDOS. • DEBE 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 DEBEN 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 DEBE 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 DEBE 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 DEBE PERMITIR LA BÚSQUEDA DE PATRONES EN ARCHIVOS MEDIANTE LA DEFINICIÓN DE EXPRESIONES REGULARES. CONTROL DE APLICACIONES • LO SOLUCIÓN DEBE SOPORTAR LA CAPACIDAD DE IDENTIFICAR LA APLICACIÓN QUE ORIGINA CIERTO TRÁFICO A PARTIR DE LA INSPECCIÓN DEL MISMO. • LA IDENTIFICACIÓN DE LA APLICACIÓN DEBE SER INDEPENDIENTE DEL PUERTO Y PROTOCOLO HACIA EL CUAL ESTÉ DIRECCIONADO DICHO TRÁFICO. • LAS SOLUCIÓN DEBE TENER UN LISTADO DE AL MENOS 1000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE. • EL LISTADO DE APLICACIONES DEBE ACTUALIZARSE PERIÓDICAMENTE. • PARA APLICACIONES IDENTIFICADAS DEBEN PODER DEFINIRSE AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) DEBEN PODER DEFINIRSE AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES DE TIPO P2P DEBE PODER DEFINIRSE ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING. • PREFERENTEMENTE DEBEN SOPORTAR MAYOR GRANULARIDAD EN LAS ACCIONES. INSPECCIÓN DE CONTENIDO SSL • LA SOLUCIÓN DEBE 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 DEBE REQUERIR NINGÚN CAMBIO DE CONFIGURACIÓN EN LAS APLICACIONES O SISTEMA OPERATIVO DEL USUARIO. • PARA EL CASO DE URL FILTERING, DEBE SER POSIBLE CONFIGURAR EXCEPCIONES DE INSPECCIÓN DE HTTPS. DICHAS EXCEPCIONES EVITAN QUE EL TRÁFICO SEA INSPECCIONADO PARA LOS SITIOS CONFIGURADOS. LAS EXCEPCIONES DEBEN PODER DETERMINARSE AL MENOS POR CATEGORÍA DE FILTRADO. 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 DEBE CONTAR CON UN ALG (APPLICATION LAYER GATEWAY) DE SIP • DEBE PODER HACERSE INSPECCIÓN DE ENCABEZADOS DE SIP • DEBEN PODER LIMITARSE LA CANTIDAD DE REQUERIMIENTOS SIP QUE SE HACEN POR SEGUNDO. ESTO DEBE PODER DEFINIRSE POR CADA MÉTODO SIP. • LA SOLUCIÓN DEBE SOPORTAR SIP HNT (HOSTED NAT TRANSVERSAL). ALTA DISPONIBILIDAD • DEBERA 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. • DEBERA DE SOPORTAR ALTA DISPONIBILIDAD EN MODO		

	ACTIVO-PASIVO • DEBERA DE SOPORTAR ALTA DISPONIBILIDAD EN MODO ACTIVO-ACTIVO • DEBERA 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 • DEBERA DE SER POSIBLE DEFINIR INTERFACES DE GESTIÓN INDEPENDIENTES PARA CADA MIEMBRO EN UN CLUSTER. CARACTERÍSTICAS DE GERENCIA • DEBERA TENER UNA INTERFASE 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 INTERFASE DEBE SOPORTAR SSL SOBRE HTTP (HTTPS) • LA INTERFASE GRÁFICA DE USUARIO (GUÏ) VÍA WEB DEBERÁ PODER ESTAR EN ESPAÑOL Y EN INGLÉS, CONFIGURABLE POR EL USUARIO. • DEBERA TENER UNA INTERFASE BASADA EN LÍNEA DE COMANDO (CLI) PARA ADMINISTRACIÓN DE LA SOLUCIÓN. • DEBERA DE TENER UN PUERTO SERIAL DEDICADO PARA ADMINISTRACIÓN. ESTE PUERTO DEBE ESTAR ETIQUETADO E IDENTIFICADO PARA TAL EFECTO. • LA COMUNICACIÓN DEBERA DE ESTAR CIFRADA Y AUTENTICADA CON USERNAME Y PASSWORD, TANTO COMO PARA LA INTERFASE 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. • DEBERA DE DAR SOPORTE DE SNMP VERSIÓN 2 • DEBERA DE DAR SOPORTE DE SNMP VERSIÓN 3 • DEBERA DE DAR SOPORTE DE AL MENOS 3 SERVIDORES SYSLOG PARA PODER ENVIAR BITÁCORAS A SERVIDORES DE SYSLOG REMOTOS • DEBERA DE DAR SOPORTAR PARA ALMACENAMIENTO DE EVENTOS EN UN REPOSITORIO QUE PUEDA CONSULTARSE LUEGO CON SQL. • DEBERA 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. • DEBE 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 DEBE 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 • DEBE SER POSIBLE LA DEFINICIÓN Y ASIGNACIÓN DE RECURSOS DE FORMA INDEPENDIENTE PARA CADA		

	INSTANCIA VIRTUAL • DEBE SER POSIBLE DEFINIR DISTINTOS SERVIDORES DE LOG (SYSLOG) PARA CADA INSTANCIA VIRTUAL. • DEBE SER POSIBLE DEFINIR Y MODIFICAR LOS MENSAJES MOSTRADOS POR EL DISPOSITIVO DE FORMA INDEPENDIENTE PARA CADA INSTANCIA VIRTUAL. ESTÁNDARES Y CERTIFICACIONES • LA SOLUCIÓN DEBERÍA 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 ***DESEMPEÑO / CONECTIVIDAD*** EL EQUIPO DEBE POR LO MENOS OFRECER LAS SIGUIENTES CARACTERÍSTICAS DE DESEMPEÑO Y CONECTIVIDAD A) THROUGHPUT - FIREWALL: 8 GBPS - VPN (3DES): 4.5 GBPS - ANTIVIRUS: 550 MBPS - IPS: 1.4 GBPS B) CONEXIONES CONCURRENTES TOTALES		

	• 2 MILLONES C) NUEVAS CONEXIONES POR SEGUNDO • 50 MIL D) INTERFACES DE RED 10 INTERFACES 10/100/1000 MBPS BASADAS EN COBRE.WAN LICENCIAMIENTO, ACTUALIZACIONES Y GARANTÍA EL LICENCIAMIENTO DE TODAS LAS FUNCIONALIDADES DEBE SER ILIMITADO EN CUANTO A USUARIOS, BUZÓN, CONEXIONES Y CLIENTES. LA VIGENCIA DE LAS ACTUALIZACIONES PARA LOS SERVICIOS DE ANTIVIRUS, ANTISPAM, IPS Y URL FILTERING DEBE PROVEERSE POR AL MENOS 1 AÑO. ASÍ MISMO INCLUIRÁ SOPORTE Y GARANTÍA DE HARDWARE POR UN AÑO.		
L)	**SERVICIOS DE INGENIERÍA** COMO PARTE DE LOS ENTREGABLES DE LOS SERVICIOS DE INGENIERÍA SE DEBERÁ GESTIONAR EL CICLO DE VIDA DEL PROYECTO, INCLUYENDO COMO MÍNIMO LAS FASES DE INICIO, DISEÑOS DE ALTO Y BAJO NIVEL, IMPLEMENTACIÓN, VALIDACIÓN, PUESTA EN PRODUCIÓN, CAPACITACIÓN DE USUARIO Y ADMINISTRACIÓN. EL RESULTADO DE ESTA GESTIÓN SE ENTREGARÁ FORMANDO LA MEMORIA TÉCNICA DEL PROYECTO. COMO PARTE DE LA PROPUESTA TÉCNICA DE ESTE INCISO SE DEBERÁ INCLUIR EL MÉTODO DE GESTIÓN DEL PROYECTO QUE SE SEGUIRÁ, DEBIENDO BASARSE EN MARCOS DE GESTIÓN VALIDADOS. A CONTINUACIÓN SE DETALLA EL ALCANCE DE LOS SERVICIOS DE INGENIERÍA, SUJETOS AL CUMPLIMIENTO DE LA GESTIÓN DEL PROYECTO, QUE SE DEBERÁN INCLUIR RELACIONADOS CON LOS BIENES DESCRITOS EN LA PARTIDA ÚNICA, ASÍ COMO LA INTEGRACIÓN CON LA INFRAESTRUCTURA EXISTENTE DEL TRIBUNAL SUPERIOR DE JUSTICIA. CONECTIVIDAD EQUIPOS DE SEGURIDAD PERIMETRAL, CENTRAL Y SITIOS REMOTOS LA RED DEL TRIBUNAL SUPERIOR DE JUSTICIA SE EXTIENDE A VARIOS SITIOS UBICADOS EN LOS DIFERENTES MUNICIPIOS EN EL ESTADO DE TABASCO. ALGUNOS DE LOS SITIOS SU MEDIO DE CONECTIVIDAD VARIA DESDE ENLACE INALÁMBRICO, TÚNELES VPN A TRAVÉS DE UNA RED DE DATOS PUBLICA O ENLACES DEDICADOS, PARA LO CUAL DEBERÁN HABILITARSE LOS EQUIPOS UTM (24) DESCRITOS EN LA PARTIDA ÚNICA PARA LA RECEPCIÓN DE TALES ENLACES APLICANDO LAS POLÍTICAS DE CALIDAD DE SERVICIO CORRESPONDIENTES PARA CADA TIPO DE SERVICIO DE VOZ Y DATOS QUE SE TRANSMITAN ENTRE LOS SITIOS REMOTOS Y LAS OFICINAS CENTRALES EN EL CASO QUE LA COMUNICACIÓN DEBA ESTABLECERSE VÍA VPN UTILIZANDO UN MEDIO DE RED PÚBLICO DEBERÁN CONFIGURARSE CON CIFRADO DE DATOS Y, EN ALGUNOS, PRIORIZACIÓN DE DATOS, PARA GARANTIZAR EL BUEN FUNCIONAMIENTO DE APLICACIONES COMO TELEFONÍA Y VIDEOCONFERENCIA ENTRE OTRAS. SE DEBERÁ ESTABLECER ADEMÁS UN DISEÑO LÓGICO DE DIRECCIONAMIENTO IP QUE PERMITA LA INTERCOMUNICACIÓN DE RUTEO ENTRE LOS SITIOS INVOLUCRADOS, ASÍ COMO LA PREVISIÓN DE NUEVOS		

	SITIOS QUE PUEDAN LLEGAR A INTEGRARSE A LA RED DEL TRIBUNAL. DEBERÁ CONFIGURARSE ADEMÁS LOS SIGUIENTES TEMAS DE SEGURIDAD TANTO EN EL EQUIPO DE SEGURIDAD PERIMETRAL CENTRAL COMO EL DE LOS SITIOS REMOTOS: • CONFIGURACIÓN BÁSICA DE FIREWALL • CONFIGURACIÓN DE DIRECCIONES POR SITIO Y/O GRUPOS DE USUARIOS. • CONFIGURACIÓN DE SERVICIOS PERMITIDOS ADICIONALES. • CONFIGURACIÓN DE SENSORES DE PROTECCIÓN DE INTRUSOS. • CONFIGURACIÓN DE FILTRADO DE CONTENIDO Y FILTRADO URL. • CONFIGURACIÓN DE PROTECCIÓN ANTISPAM. • CONFIGURACIÓN DE PREVENCIÓN DE FUGA DE INFORMACIÓN. • CONFIGURACIÓN DE CONTROL DE APLICACIONES POR GRUPO DE USUARIOS. • CONFIGURACIÓN DE PERFIL DE PROTECCIÓN POR GRUPO DE USUARIOS. • CREACIÓN DE POLÍTICAS GRUPO DE USUARIOS CON ASIGNACIÓN DE PERFILES DE PROTECCIÓN. • CONFIGURACIÓN DE VPN'S DE TIPO SSL PARA USUARIOS MÓVILES. • CONFIGURACIÓN DE EQUIPO FIREWALL PARA INTERACCIÓN CON EQUIPO DE CON SISTEMA DE ANÁLISIS Y CORRELACIÓN DE EVENTOS. SWITCHING OFICINAS CENTRALES PARA EL SITIO CENTRAL DEBERÁN CONFIGURARSE LO SIGUIENTE: CONFIGURACIÓN DE EQUIPOS DE SWITCHEO • CONFIGURACIÓN BASE DE SWITCH CORE DESCRITO EN LA PARTIDA ÚNICA • GENERACIÓN Y ASIGNACIÓN DE VLAN ASÍ COMO SEGMENTOS DE RED A UTILIZAR • CONFIGURACIÓN Y APLICACIÓN DE CALIDAD DE SERVICIO VOZ/DATOS • SELECCIÓN Y CONFIGURACIÓN DE PROTOCOLOS DE RUTEO HACIA EL LOS SITIOS REMOTOS • CONFIGURACIÓN DE PUERTOS UPLINKS ENTRE MDF E IDF • ASIGNACIÓN DE VLAN EN PUERTOS SEGÚN APLICACIÓN O USO		

	SOLUCIÓN DE TELEFONÍA SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE SERVIDORES DE GESTIÓN DE TELEFONÍA IP • INSTALACIÓN DE 2 SISTEMAS DE GESTIÓN TELEFÓNICA • CONFIGURACIÓN DE LA SOLUCIÓN EN CLÚSTER DE 2 SERVIDORES • CREACIÓN DE GRUPOS LÓGICOS DE DIRECTORIO CON UNA CANTIDAD MÁXIMA DE 30, ACORDE AL PLAN DE MARCACIÓN A IMPLEMENTAR. • CREACIÓN DE ZONAS MARCACIÓN, CON UNA CANTIDAD MÁXIMA DE 30, CON UNA CANTIDAD MÍNIMA DE 10 PARA EL PLAN DE MARCACIÓN A IMPLEMENTAR. • CREACIÓN DE GRUPOS DE DISPOSITIVOS PERMITIENDO LA UTILIZACIÓN DE AL MENOS 2 CÓDEC DE COMUNICACIÓN. • HABILITACIÓN DE DID. • CREACIÓN Y CONFIGURACIÓN DE TRANSCODER • CREACIÓN Y CONFIGURACIÓN DE CONSOLAS DE ATENCIÓN. • CONFIGURACIÓN DE SISTEMA DE RESPALDO Y RESTAURACIÓN. • DESARROLLO DE UN PLAN DE MARCACIÓN INTERNO PARA EL SITIO CENTRAL Y LOS SITIOS REMOTOS. • CREACIÓN DE PLANTILLA DE AGREGACIÓN DE DISPOSITIVOS E IMPLEMENTACIÓN DE LA MISMA. • CREACIÓN DE PLANTILLA DE AGREGACIÓN DE USUARIOS E IMPLEMENTACIÓN DE LA MISMA. • CREACIÓN DE PLANTILLA DE AGREGACIÓN DE CÓDIGOS DE AUTORIZACIÓN PARA LOS USUARIOS CREADOS E IMPLEMENTACIÓN DE LA MISMA. • CREACIÓN DE PERMISOS DE MARCACIÓN POR USUARIOS, DISPOSITIVO, GRUPOS, ETC. • HABILITACIÓN Y PERSONALIZACIÓN DE LA TOTALIDAD DE DISPOSITIVOS DE ACUERDO A LISTADO DE USUARIOS PROPORCIONADA POR EL TRIBUNAL SUPERIOR DE JUSTICIA. • INSTALACIÓN DE LA TOTALIDAD DE LOS DISPOSITIVOS Y PRUEBA DE FUNCIONALIDAD DE LOS MISMOS. • INTEGRACIÓN CON SISTEMA DE RESPUESTA INTERACTIVA. • INTEGRACIÓN CON SISTEMA DE TARIFICACIÓN. • GENERACIÓN DE UN RESPALDO DEL SISTEMA EN FUNCIONALIDAD AL 100 %.		

	SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE GATEWAY DE VOZ (PARA REALIZAR ESTA INGENIERÍA SERÁ NECESARIA LA ACEPTACIÓN POR PARTE DEL PROVEEDOR DEL EQUIPO) • INTEGRACIÓN DE GATEWAY DE VOZ CON SISTEMA GESTOR DE TELEFONÍA IP • CREACIÓN DE PLAN DE MARCACIÓN HACIA SISTEMA DE TELEFONÍA IP DEL TRIBUNAL SUPERIOR DE JUSTICIA • HABILITACIÓN DE 1 E1 DE TRONCALES DIGITALES • INTEGRACIÓN DE TRONCALES TELEFÓNICAS • CREACIÓN DE PLAN DE MARCACIÓN HACIA RED PÚBLICA • ENRUTAMIENTO DE DID • CREACIÓN Y CONFIGURACIÓN DE TRANSCODER • GENERACIÓN DE UN RESPALDO DEL EQUIPO EN SU FUNCIONALIDAD AL 100 %. SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE SISTEMA CONTESTADOR DE VOZ (PARA REALIZAR ESTA INGENIERÍA SERÁ NECESARIA LA ACEPTACIÓN POR PARTE DEL PROVEEDOR DEL EQUIPO GATEWAY DE VOZ) • INSTALACIÓN DE MÓDULO DE RED DE SISTEMA DE RESPUESTA INTERACTIVA DE VOZ EN GATEWAY DE VOZ • INTEGRACIÓN CON SERVIDOR DE GESTIÓN DE TELEFONÍA IP • CREACIÓN DE GRUPO DE LÍNEAS DE RESPUESTA • GENERACIÓN DE AL MENOS 2 SCRIPT DE RESPUESTA INTERACTIVA DE VOZ PARA RE-ENVÍO DE LLAMADA A EXTENSIONES INTERNAS DEL COMPLEJO • VALIDACIÓN DE LA INTEGRACIÓN DE LOS SISTEMAS DE IVR Y GESTORES DE TELEFONÍA IP • GENERACIÓN DE UN RESPALDO DEL SISTEMA EN FUNCIONALIDAD AL 100 %. DE IGUAL MANERA, EL LICITANTE PARA ELABORAR SU PROPUESTA, DEBERÁ DE CONTEMPLAR EL CERTIFICADO CADA NODO DE RED, DONDE SE CONECTARÁ UN DISPOSITIVO DE TELEFONÍA IP, DE ACUERDO A LOS PARÁMETROS DE LA CATEGORÍA DEL SISTEMA DE CABLEADO ESTRUCTURADO INSTALADO EN EL(OS) EDIFICIO(S), ESTA REVISIÓN INCLUIRÁ: • REPORTE IMPRESO DEL CUMPLIMIENTO DE ACUERDO A LA NORMA VIGENTE DE CADA NODO DE RED. SE INCLUIRÁ UN INFORME IMPRESO Y ELECTRÓNICO DE VERIFICACIÓN POR CADA PUNTO DE LOS PARÁMETROS DE DESEMPEÑO SEGÚN LA TIA/EIA-568B SEGÚN LA CATEGORÍA REQUERIDA, ESTO SE REALIZARÁ CON UN EQUIPO CERTIFICADOR PARA MEDIR ESTOS PARÁMETROS DE DESEMPEÑO, LOS CUALES FORMARÁN PARTE DEL DOCUMENTO		

	"MEMORIA TÉCNICA DE LA INSTALACIÓN". ESTE DOCUMENTO SE ENTREGARÁ EN FORMA IMPRESA Y EN RESPALDO ELECTRÓNICO. • SUSTITUCIÓN DE CONECTORES, RE-CONEXIÓN MECÁNICA DE LOS MISMOS A NIVEL DE PANEL DE PARCHEO Y PLACA (EXTREMO A EXTREMO), • SUSTITUCIÓN DE CORDONES DE PARCHEO NECESARIOS PARA EL CORRECTO DESEMPEÑO DEL CANAL, • IDENTIFICACIÓN DE LOS NODOS. TODOS LOS ELEMENTOS DEL SISTEMA DE CABLEADO ESTRUCTURADO INCLUYENDO: CABLES, PLACAS, JACK DE LA PLACA, PATCH PANEL, JACK DE PATCH PANEL, SERÁN IDENTIFICADOS DE ACUERDO A LA NORMA VIGENTE.		

Los licitantes, para la presentación de sus ofertas, deberán ajustarse estrictamente a los requisitos, especificaciones técnicas y tecnología que se solicitan en estas bases y, en su caso, a lo que se derive de la junta de aclaraciones; por lo que en sus cotizaciones y cédulas de descripción técnica, deberán presentar sus ofertas estrictamente apegadas a lo requerido. (DOCUMENTO No. 4)

5.2. NORMAS DE CALIDAD.

Para participar en este proceso licitatorio, se requiere que todos los componentes de los bienes que se oferten sean nuevos, de reciente fabricación y provenir directamente del fabricante, toda vez que no se aceptarán ofertas de equipos genéricos que presenten adiciones, variación y/o sustituciones, realizadas por el comercializador u otra persona representante del fabricante.

Sólo se aceptarán ofertas de marcas registradas y originales, por lo cual, los licitantes deberán expedir carta compromiso, bajo protesta de decir verdad, en la que manifiesten que los bienes que ofertarán y entregarán, de ser adjudicados, cumplen totalmente con las características y especificaciones señaladas en estas bases, así como que al momento de la entrega, los bienes estarán en buen estado y no presentarán mala calidad en su empaque original, así como serán completamente coincidentes con las características y especificaciones establecidas en estas bases y

lo ofertado; por lo que no habrá sustituciones entre lo ofertado y lo que finalmente se entregue. **(DOCUMENTO No. 5)**

A fin de garantizar lo anterior, se solicita que los fabricantes de los equipos cuenten con las siguientes certificaciones:

Para la partida única, para el fabricante de los incisos A), B), C), D), E), F), G), H), I), J), y K):

- Certificado ISO 9001:2008 para equipos electrónicos en diseño, desarrollo, producción, comercialización, servicio y soporte para soluciones de redes y comunicaciones. (**DOCUMENTO No. 6**)
- Aquellos certificados en cumplimiento de las normas internacionales del fabricante que se juzguen necesarios para los equipos electrónicos en diseño, desarrollo, producción, comercialización, servicio y soporte para soluciones de redes y comunicaciones. (**DOCUMENTO No. 7**)

En cuanto a las certificaciones requeridas, se deberá exhibir copia simple vigente, incluyendo la dirección http:// oficial del fabricante para corroborar dicha información.

Los documentos anteriores así señalados deberán expedirse por el licitante en papel membretado, original, con sello y firma autógrafa de persona facultada, y expedidos Bajo Protesta de Decir Verdad.

5.3. GARANTÍAS Y SERVICIOS.

5.3.1. CAPACIDAD DE PRODUCCIÓN Y/O DISTRIBUCIÓN.

Los licitantes que oferten la partida única deberán exhibir tres cartas; dos cartas expedidas por el fabricante o distribuidor mayorista (**DOCUMENTOS Nos. 8 y 9**), y otra por el licitante (**DOCUMENTO No. 10**), en las que se exprese lo siguiente:

En la primera, el fabricante, **o en su caso el distribuidor mayorista de los bienes,** se obligará de manera solidaria a respaldar la oferta del participante durante todo el proceso licitatorio (**DOCUMENTO No. 8**). En la segunda carta, el fabricante manifestará que el licitante es un Distribuidor Autorizado para los bienes involucrados

en la Partida Única, así como su nivel de certificación profesional con que cuenta (**DOCUMENTO No 9**).

En la tercera, el licitante manifestará que cuenta con la capacidad suficiente para suministrar en tiempo y forma, los bienes involucrados en la Partida Única. (**DOCUMENTO No. 10**) Estos documentos deberán expedirse en papel membretado, original y firma autógrafa de persona facultada, y bajo protesta de decir verdad.

El licitante que participe en la partida única deberá presentar copia de certificados profesionales en bienes y servicios relacionados emitidas por el fabricante. Dichos certificados deberán estar emitidos a nombre del personal del licitante, o bien, a nombre del licitante, y serán las siguientes:

- CERTIFICACIÓN DE IMPLEMENTACIÓN DE REDES CONVERGENTES
- CERTIFICACIÓN DE DISEÑO DE REDES CONVERGENTES
- CERTIFICACIÓN DE DISEÑO DE ARQUITECTURA DE SOLUCIONES DE COLABORACIÓN
- CERTIFICACIÓN DE ESPECIALISTA DE SOPORTE DE SOLUCIONES DE COLABORACIÓN
- CERTIFICACIÓN DE IMPLEMENTACIÓN, OPERACIÓN, CONFIGURACIÓN Y SOPORTE (TROUBLESHOOTING) DE TELEFONÍA IP EN UNA RED CONVERGENTE
- CERTIFICACIÓN DE DISEÑO DE SOLUCIONES DE RED CON TELEFONÍA IP MULTI-SERVICIO, INCLUYENDO SOLUCIONES DE ALTA DISPONIBILIDAD, SEÑALIZACIÓN SIP, INTEGRACIÓN DE TCM PBX Y SISTEMAS DE BUZONES DE VOZ IP INTEGRADO CON EL SISTEMA DE TELEFONÍA IP
- CERTIFICACIÓN DE DISEÑO, IMPLEMENTACIÓN Y SOPORTE DE LA INTEGRACIÓN DE VOZ, VIDEO Y COLABORACIÓN WEB EN UNA RED CONVERGENTE

- CERTIFICACIÓN DE PLANIFICACIÓN, DISEÑO, IMPLEMENTACIÓN, Y OPERACIÓN DE SISTEMAS DE ATENCIÓN A USUARIOS BASADOS EN TELEFONÍA IP
- CERTIFICACIÓN DE DISEÑO DE SEGURIDAD EN REDES, INCLUYENDO FIREWALLS, SISTEMAS DE PREVENCIÓN DE INTRUSOS, CONTROL DE ADMISIÓN O ACCESO A LA RED Y SISTEMAS DE MONITORIZACIÓN Y ANÁLISIS DE VULNERABILIDADES, EN BASE A REDES CONVERGENTES
- CERTIFICACIÓN DE FUNDAMENTOS DE PROCESOS DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
- CERTIFICACIÓN EN INSTALACIÓN DE CABLEADO ESTRUCTURADO

La copia de las certificaciones deberán ser vigentes a la fecha de la presentación de las propuestas técnico económicas. (**DOCUMENTO No. 11**)

Los licitantes para comprobar que el personal certificado pertenece a su plantilla laboral, deberán presentar copia vigente del documento de liquidación del IMSS o bien, impresión del archivo SUA (Sistema Único de Autodeterminación). (**DOCUMENTO No. 12**).

NOTA IMPORTANTE: Todas las cartas que se solicitan de apoyo por parte del Fabricante y/o distribuidor hacia el licitante, deberán de venir en Papel Original y firma autógrafa de persona legalmente autorizada; referenciadas a la presente licitación, con fecha igual a la de la Presentación y Apertura de Proposiciones Técnicas.

5.3.2. REFACCIONES.

Para todos las partidas los licitantes deberán presentar carta de garantía expedida por el fabricante, o bien por el distribuidor mayorista en la que se garantice a la convocante por un tiempo mínimo de **cinco años,** la existencia en el mercado de refacciones para los equipos involucrados en los incisos A), C), D), E), F), G), H), I), J), y K). (**DOCUMENTO No. 13**)

5.3.3. ASISTENCIA Y SOPORTE TÉCNICO.

Para la partida única los licitantes garantizarán el servicio de asistencia y soporte técnico, sin costo extra para El Tribunal, mediante una carta compromiso expedida bajo protesta de decir verdad, en la que exprese lo siguiente:

- Las condiciones bajo las que proporcionará el servicio.
- El nombre, domicilio, teléfonos y personas a quienes deberá dirigirse El Tribunal, para solicitar el servicio.
- Para los incisos A), C), D), E), F), G), H), I), J), y K). el tiempo máximo de respuesta para prestar el servicio de garantía por parte del fabricante, cuyo procedimiento será el previsto por el propio fabricante, de acuerdo a la aplicación de las políticas de garantía, será de al siguiente día hábil, contadas a partir de la recepción del reporte.
- Para los incisos A), C), D), E), F), G), H); I), J), y K). el Proveedor asumen la obligación de proporcionar un equipo que sustituya, en calidad de préstamo, el equipo dañado, cuando el tiempo de reparación del mismo supere al siguiente día hábil el cual se devolverá cuando el equipo adquirido haya sido reparado y se encuentre funcionando al 100%.
- Para los incisos **C), D), E), F), G), H), y J)**, a juicio del Proveedor, aceptará mantener un número de equipos para respaldo y sustitución de los incisos en mención, **con posibilidad de ser verificado el stock mencionado**.
- Para las incisos A), C), D), E), F), G) H); J), K), la garantía del fabricante, en la que se implique la sustitución del equipo deberá ser en sitio.
- Que las obligaciones anteriores, tendrán vigencia de un año y estos será sin costo extra para El Tribunal. (**DOCUMENTO No. 14**)

De igual manera, el licitante deberá de presentar carta Bajo Protesta de Decir Verdad, que posterior a la conclusión del servicio de ingeniería, de acuerdo al alcance especificado en el inciso L), tras su liberación y aceptación por parte de El Tribunal, mantendrá por un periodo mínimo de tres meses posteriores a la liberación y aceptación, un sistema de *help-desk,* sin costo para la Convocante, en donde se

especifique el método de contacto, procedimiento de registro de incidencias, escalamiento, solución y liberación de las mismas (**DOCUMENTO No. 15**).

El licitante, preferentemente, deberá contar con un centro de servicio en esta ciudad de Villahermosa, Tabasco, o bien con un número telefónico que, sin costo para El Tribunal, funcione las 24 horas del día, los 365 días del año, para recibir reportes de fallas en los equipos involucrados en los incisos A), C), D), E), F), G), H), I), J) y K). (**DOCUMENTO No. 16**)

5.3.4. CARTA DE GARANTÍA.

Para todos los casos los licitantes deberán presentar una carta **"de garantía",** con vigencia de **un año** a partir de la fecha de entrega de los bienes, en la que indicará además:

a) Que será responsable de los vicios ocultos o defectos de fabricación que presenten los bienes suministrados, obligándose a realizar la sustitución del 100% de los bienes que le sean devueltos, en un plazo **máximo de 72 horas**, a partir de la devolución.
b) El procedimiento para efectuar cambios y/o devoluciones, así como lugar y horarios.

En el caso de que por causas imputables al proveedor, éste no efectúe la reposición en el plazo arriba señalado, **El Tribunal podrá rescindir total o parcialmente el contrato**, quedando el proveedor obligado a rembolsar la cantidad recibida, más los intereses generados, calculados a la tasa que señale la Ley de Ingresos de la Federación vigente, para el caso de prórroga de créditos fiscales, que se calcularán sobre el monto no reintegrado, computándose por días calendario, desde la fecha de devolución de los bienes, hasta aquella en que se pongan efectivamente las cantidades a disposición de El Tribunal; independientemente que **podrá hacerse efectiva la fianza que garantiza el cumplimiento del contrato**. (**DOCUMENTO No. 17**)

5.3.5 CASOS DE RECHAZO.

Si en el momento de la recepción de los bienes en el almacén se observan daños o defectos que afecten la duración y funcionalidad parcial o total de uno o más equipos, El Tribunal se abstendrá de recibirlos. En estos casos, el proveedor deberá sustituir los equipos rechazados, en un término no mayor a ***72 horas,*** con las características y especificaciones requeridas en las bases de licitación en este contrato, sujetándose a la inspección y aceptación del personal encargado de su recepción. La reposición del bien dentro del término señalado, no exime al proveedor de la sanción que proceda en el caso de que el nuevo bien, presente también defectos.

5.3.6 PATENTES Y MARCAS

El licitante garantizará a El Tribunal:

a) Que con su oferta no se infringe la normatividad relativa a patentes, marcas registradas, otros derechos reservados o protegidos por la ley a favor de terceros.
b) Que el fabricante, distribuidor, o él mismo, cuentan con todos los permisos o autorizaciones correspondientes, lo que deberá acreditarse con la documentación relativa, en original o copia certificada notarialmente.
c) En caso contrario, mediante carta responsiva en la que se comprometa a liberar a El Tribunal de cualquier responsabilidad o reclamación que resulte.
d) Reintegrar los gastos que en que se incurra por lo anterior, más los intereses generados, calculados a la tasa que señale la Ley de Ingresos de la Federación vigente, para el caso de prórroga de créditos fiscales.

Para los efectos anteriores, se emitirá carta expedida por el licitante en la que bajo protesta de decir verdad, en papel membretado original y firma autógrafa se exprese lo señalado anteriormente, (**DOCUMENTO No. 18**)

6. INFORMACIÓN ESPECÍFICA DE LA LICITACIÓN.

6.1. REQUISITOS PARA PARTICIPAR.

Los interesados deberán cubrir los siguientes requisitos:

a) Ser personas físicas o jurídicas colectivas, legalmente constituidas; con capacidad legal para ser sujetos de obligaciones y derechos; no estar impedidos civil, mercantil o administrativamente para ejercer a plenitud sus derechos y cumplir sus obligaciones.
b) Comprar las bases de la presente licitación.
c) Presentar sus propuestas debidamente requisitadas y en los tiempos establecidos en estas bases.
d) Contar con suficiencia económica, técnica, logística y, con el respaldo de los fabricantes y/o distribuidores, según sea el caso.
e) No encontrarse en ninguno de los supuestos que marca el artículo 51 de la Ley, así como en situación de atraso o incumplimiento respecto de otro u otros contratos celebrados con El Tribunal. (**DOCUMENTO No. 19**)

Para la acreditación de lo anterior, el licitante deberá expedir conforme a lo que establece el artículo 51 de la Ley, documento original en papel membretado, en el que bajo protesta de decir verdad, manifieste que no se encuentra en ninguno de los supuestos que menciona el citado artículo de Ley.

f) Para este proceso licitatorio, la convocante no solicitará ***EQUIPOS MUESTRA*****;** sin embargo, el Licitante emitirá carta Bajo Protesta de Decir la Verdad, en la cual manifieste que cuenta con experiencia para la ejecución de proyectos similares y que contengan un mínimo de 500 servicios activos de red y que involucren tecnologías de switching, routing, seguridad perimetral y Telefonía IP; anexando además lo siguiente: a) Dos constancias originales como mínimo emitidas en papel membretado del usuario final y firmados autógrafamente; dichos documentos deberán contener los datos: nombre, puesto, dirección, teléfono, etc. De la persona quien lo firma para que la Convocante pueda corroborar la información y; b) Resumen técnico del alcance de al menos un proyecto de los indicados **(DOCUMENTO No. 20).**
g) No incurrir en falsedad en la información que se proporcione.

h) Cédula de Identificación Fiscal (**DOCUMENTO No. 21**), así como encontrarse debidamente inscritos y registrados en el Padrón de Proveedores del Tribunal Superior de Justicia del estado de Tabasco, lo que acreditará mediante la solicitud y correspondiente expedición de la constancia de encontrarse registrado ante la Oficialía Mayor del Poder Judicial Estatal. Por lo que deberán indefectiblemente adjuntar copia simple del documento de registro. (**DOCUMENTO No. 22**)

6.2. CALENDARIO DE LA LICITACIÓN.

- Periodo de Venta de Bases: Del 08 al 14 de Junio de 2013, en horas hábiles.
- Junta de aclaración de bases: 17 de Junio de 2013 a las 10:00 horas.
- Acto de presentación de proposiciones y apertura de propuestas técnicas (primera etapa): 24 de Junio de 2013 a las 10:00 hrs.
- Acto de apertura de proposiciones económicas (segunda etapa): 26 de Junio de 2013 a las 10:00 horas.
- Acto de fallo: 28 de Junio de 2013 a las 10:00 horas.
- Firma de contrato: Dentro de los diez días naturales siguientes a la fecha de la notificación del fallo, en días y horas hábiles; en la Oficialía Mayor.
- Período y lugar de entrega de los bienes adquiridos: Dentro de los 45 días naturales siguientes a la fecha de suscripción del contrato, en días y horas hábiles, en el Almacén del Tribunal, ubicado en el sótano del edificio sede del Tribunal Superior de Justicia, sito en la calle Independencia Esq. Nicolas Bravo S/N, Col. Centro, Villahermosa, Tabasco, C.P. 86000.

La Junta de aclaración de las bases, así como los actos de presentación y apertura de proposiciones técnicas y económicas, y de fallo; se llevarán a cabo en la Sala anexa al auditorio Antonio Suárez Hernández, sito en el sótano del edificio sede del Tribunal; calle Independencia s/n, esq. Con Nicolás Bravo, S/N, Col. Centro. Villahermosa, Tabasco. C.P. 86000.

7. PROPUESTAS.

La entrega de proposiciones se hará por escrito, en dos sobres cerrados que contendrán: uno, la propuesta técnica; y el otro, la propuesta económica. La documentación legal y administrativa, se entregará simultáneamente con la propuesta técnica, dentro o fuera del sobre respectivo; a elección del licitante.

7.1. REQUISITOS

Las proposiciones que los licitantes presenten deberán cumplir con los siguientes requisitos:

a) Presentarse por escrito en idioma español. Los folletos y anexos técnicos podrán presentarse en el idioma del país de origen de los bienes, acompañados de una traducción simple al español.
b) Ofertar el 100% de los bienes requeridos por esta convocante.
c) Ser claros y no establecer ninguna condición, ni emplear abreviaturas o presentar raspaduras o enmendaduras.
d) Elaboradas en papel membretado y suscritas de manera autógrafa por persona legalmente facultada.
e) Expresar que la oferta tendrá vigencia a partir del inicio del proceso licitatorio, durante el periodo de suministro de los bienes objeto de esta licitación, y hasta la fecha de terminación del contrato respectivo.
f) Las cotizaciones serán en precios netos y fijos, en moneda nacional, por lo que no se aceptaran ofertas con precios escalonados, o en moneda extranjera.
g) Desglosar el impuesto al valor agregado.
h) El precio ofertado incluirá todos aquellos cargos por los servicios de asistencia y soporte técnico en sitio; la entrega será Libre a bordo destino almacén (LAB).
i) De preferencia, integrarlas en el orden indicado, en carpetas con separadores y pestañas indicativas de cada documento. La omisión de lo anterior no será motivo de desechamiento de la propuesta, pero su observancia será conveniente para la mejor conducción del proceso.
j) Presentar información verídica, toda vez que de detectarse alguna imprecisión, alteración o falsedad, será motivo de descalificación.

k) En la presentación y cotejo de la información esta deberá de ser coincidente, toda imprecisión entre lo que originalmente se presente y las copias que se exhiban para entregar a la convocante como parte de la propuesta será motivo de desechamiento de la proposición, toda vez que no se garantiza la legalidad de la documentación que no se presente de manera correcta.

7.2. ACREDITACIÓN DE PERSONALIDAD Y REGISTRO EN EL PADRON DE PROVEEDORES.

Con el objeto de acreditar su correcta inscripción en el padrón de Proveedores del Poder Judicial del estado; los licitantes deberán anexar original y copia simple de la constancia que solicitarán ante la Oficialía Mayor del Poder Judicial del estado; a fin de que esta les extienda la constancia correspondiente. En el entendido de que aquellos proveedores que aún y encontrarse registrados en el padrón de proveedores del Poder judicial se encuentren en situación de atraso o de incumplimiento respecto de otro y otros contratos con el Tribunal, no serán acreedores de la citada constancia. Por lo que estando a lo dispuesto en el artículo 51 de la Ley, no serán considerados solventes para participar del presente proceso licitatorio. (**DOCUMENTO No. 22**)

A fin de acreditar su personalidad; los licitantes deberán presentar debidamente requisitado el **Anexo No. 2 (**formato a que hace referencia el punto 8 del acuerdo publicado por la SECODAM en el Diario Oficial de la Federación el 11 de abril de 1997), o bien, escrito en el que bajo protesta de decir verdad**, (DOCUMENTO No. 23)** informe lo siguiente:

a) Del licitante:

Clave del Registro Federal de Contribuyentes; nombre y domicilio, así como, en su caso, de su apoderado o representante. Tratándose de personas morales, además, descripción del objeto social de la empresa; número y fecha de las escrituras públicas en las que conste el acta constitutiva y, en su caso, sus reformas o modificaciones, señalando nombre, número y circunscripción del notario o fedatario público que las protocolizó; así como fecha y datos de su inscripción en el Registro Público de Comercio, y relación del nombre de los socios que aparezcan en éstas.

Nota: Las personas físicas participantes, llenarán el formato o elaborarán el escrito con los datos de su acta de nacimiento.

b) Del representante del licitante:

Número y fecha de las escrituras públicas en las que les fueron otorgadas las facultades para suscribir la propuesta, señalando nombre, número y circunscripción del notario o fedatario público que las protocolizó.

No será motivo de descalificación, la falta de identificación o acreditamiento de la persona que solamente entregue las propuestas, pero únicamente podrá participar durante el desarrollo del acto, con el carácter de oyente.

7.3. PROPUESTA TECNICA.

El sobre No. 1, Propuesta Técnica, deberá contener la siguiente documentación:

Número de Documento	Nombre del Documento	Descripción, o contenido del documento
1	Pago de Bases	Expedido por la Tesorería Judicial
2	Carta de contenido nacional del producto.	Expedida por el Licitante, bajo su responsabilidad manifestará el porcentaje de contenido nacional con el que cuenta el producto que oferta. Aplica para todas las partidas.
3	Carta de Procedencia del Bien	Expedida por el **Licitante** en la que bajo protesta de decir verdad se especifique el país de origen del bien, o en su caso, la información que juzgue conveniente para que se identifique plenamente el país de origen, en los empaques de los equipos. Aplica para todos los incisos, con excepción del inciso O).

4	Relación de bienes o cédula de propuesta técnica	Elaborarla tomando como referencia el Anexo No. 1 de las presentes bases Aplica para todas las partidas.
5	Carta de normas de calidad.	Expedida por el Licitante, y debe de contener en esencia lo descrito en el rubro denominado: Normas de Calidad. Aplica para todos los incisos, a excepción del inciso O).
6	Certificado ISO 9001:2008 a nombre del fabricante para equipos electrónicos en diseño, desarrollo, producción, comercialización, servicio y soporte para soluciones de redes y comunicaciones.	No se aceptará certificado ISO 9001:2008, con características distintas a lo especificado. En copia vigente, se incluirá la dirección httpp:// oficial del fabricante para corroborar dicha información. Aplica para la partida única incisos o copia certificada. Sólo aplica para la partida única incisos A), B), C), D), E), F), G), H), I), J), y K).
7	Certificado internacionales a nombre del fabricante	En copia vigente de certificados internacionales de acuerdo a lo solicitado. Se incluirá la dirección httpp:// oficial del fabricante para corroborar dicha información. Aplica para la partida única incisos o copia certificada. Sólo aplica para la partida única incisos A), B), C), D), E), F), G), H), I), J), y K).
8	Carta de obligación solidaria.	Expedida por el fabricante del equipo **(o en su caso por el distribuidor mayorista)**, con los requisitos enunciados.
9	Carta de Distribución Autorizada	Expedida por el fabricante del equipo, con los requisitos enunciados.
10	Carta de capacidad de distribución del licitante.	Expedida por el licitante del equipo, con los requisitos enunciados.
11	Certificaciones Profesionales	Copia de los certificados con los requisitos enunciados.
12	Documento de liquidación	Copia del documento vigente de liquidación del IMSS o SUA con los

	del IMSS o SUA	requisitos enunciados.
13	Carta de garantía de existencia de refacciones.	Expedida por el fabricante o distribuidor del equipo y una vigencia de 5 años. Aplica para los incisos señalados.
14	Carta compromiso de asistencia y soporte técnico en sitio	Expedida por el licitante, en la que explica las condiciones bajo las cuales prestarán el servicio.
15	Carta compromiso de asistencia y soporte técnico de la ingeniería	Expedida por el licitante, en la que explica las condiciones bajo las cuáles prestarán el servicio de *help-desk.*
16	Carta de Centro de Servicio.	Expedida por el licitante en el que especifica la ubicación de su centro de servicio y o bien, de su call-center. Aplica para la Partida Única.
17	Carta de garantía.	Expedida por el licitante, con una vigencia de 1 año. Y que contemple, garantía, devoluciones y casos de rechazo.
18	Carta de liberación de responsabilidades	Expedida por el licitante. Aplica para la partida única.
19	Carta del artículo 51	Expedida por el licitante en la que manifestará bajo protesta de decir verdad que no se encuentra en ninguno de los supuestos que marca el Artículo 51, y muy especialmente que no se encuentra en situación de atraso respecto del cumplimiento de contratos celebrados con El Tribunal.
20	Experiencia en proyectos similares	Expedido por el Licitante de acuerdo a lo solicitado.
21	Registro Federal de Contribuyentes	Original o copia certificada para el cotejo y copia simple para el expediente.

22	Registro Vigente en el Padrón de Proveedores del Poder Judicial del estado de Tabasco	Lo que acreditará mediante la solicitud y correspondiente expedición de la constancia de encontrarse registrado ante la Oficialía Mayor del Poder Judicial Estatal. Por lo que deberán indefectiblemente adjuntar copia simple del documento de registro.
23	Formato para acreditar la personalidad.	Elaborado según el Anexo No. 2. O bien tomando el Acuerdo del D.O.F. del 11/abril/1997.
24	Catálogos técnicos de los bienes que oferten a El Tribunal	Estos deben de ser legibles, y en español, o bien con su traducción simple en el caso de venir en inglés, lo descrito en el catálogo no sustituye la información que deberá contener la cédula de propuesta técnica. Los catálogos deberán ser originales de imprenta, o bien una impresión legible directamente bajada del sitio web del fabricante. Los cuales deberán venir con sello y firma autógrafa del licitante o fabricante.
25	Carta compromiso de entrega	Expedida por el licitante, y enunciando el período de entrega que será dentro de los 45 días naturales siguientes a la fecha de suscripción del contrato. Aplica para todas la partida única.
26	Carta de conformidad y aceptación de las bases, anexos y de las condiciones para la junta de aclaraciones.	Escrito libre en el que el licitante expresa bajo protesta de decir verdad que habiendo las presentes bases, las ha leído y comprende en su totalidad el alcance y contenido de las mismas. Así como que acepta sujetarse a las disposiciones establecidas para la

		celebración de la Junta de Aclaraciones.
27	Currículo de la empresa	Se solicita para acreditar la experiencia y solvencia de la empresa licitante, firmado por persona con poder para actos de administración y/o dominio que incluya copia de los últimos contratos vigentes; en los casos de no contar con contratos que se encuentren vigentes, podrán anexar las copias de los últimos tres contratos que hayan celebrado. Al final del documento, el representante legal deberá de hacer constar bajo protesta de decir verdad, que los datos contenidos en el presente currículo, son ciertos, y autoriza El Tribunal, para que esta realice las investigaciones que considere pertinentes, a fin de verificar los datos que se proporcionan. Preferentemente se deberán de anexar contratos de hasta dos años anteriores celebrados con otras instituciones y que se relacionen con el tipo de bien que se encuentra sujeto a proceso licitatorio.
28	Cheque de Garantía para Sostenimiento de la Oferta.	Mediante cheque no negociable con la leyenda “para abono en cuenta del beneficiario”, a nombre del Tribunal Superior de Justicia, con un mínimo del cinco por ciento del total de su oferta económica; incluyendo el IVA. (Conforme a lo dispuesto por el artículo 31, fracción I, de la Ley)
29	Declaración de Integridad	El licitante expedirá una declaración bajo protesta de decir verdad, en la que se manifestará que se abstendrá por si o a través de interpósita persona de inducir conductas que pudieran alterar el correcto y legal funcionamiento del presente proceso licitatorio.

El Tribunal verificará que la documentación presentada cumpla con los requerimientos establecidos en estas bases.

De detectarse alguna imprecisión, alteración o falsedad, será motivo de descalificación.

7.4. DOCUMENTACIÓN LEGAL ADMINISTRATIVA.

Será motivo de descalificación la falta de documentos legales administrativos, distintos a la documentación técnica; estos, a elección del licitante, podrán entregarse dentro o fuera del sobre que contenga la propuesta técnica.

Número de Documento	Nombre del documento	Descripción o contenido del documento
1.	Original y copia de la declaración anual del I.S.R. de los ejercicios 2011 y 2012.	En caso de empresas de reciente creación: original y copia del alta ante el SAT.
2.	Original y copia de los estados financieros auditados, de los dos años anteriores; incluyendo el comparativo de razones financieras básicas correspondiente a los mismos periodos.	Se anexarán copias de la identificación oficial y la cédula profesional del contador público que los elabora y los firma. Cabe señalar, que el contador público que los elabore deberá insertarles la leyenda de que son expedidos bajo protesta de decir verdad y que los datos que en los mismos se reflejan son verídicos y fehacientes.
3.	Acta constitutiva de la empresa, o acta de nacimiento, si es persona física.	Original o copia certificada por notario, así como copia simple para su cotejo.
4.	Poder notarial del representante legal de la empresa.	En original y copia simple para cotejo. (En su caso)
5.	Acta de la última asamblea general ordinaria	En original y copia simple para cotejo. (En su caso)

7.5. PROPUESTA ECONÓMICA.

El sobre No. 2, deberá contener lo siguiente:

1) Cédula de propuesta económica, según **Anexo No. 3.**
2) Disco compacto con formato en excel, en el que se encuentre el archivo digital de la cedula de la propuesta económica.

El precio ofertado incluirá todos aquellos cargos por los servicios de asistencia y soporte técnico en sitio.

Se recomienda proteger con cinta adhesiva transparente, la información que proporcionen en sus cotizaciones, relativa a precios unitarios, descuentos, impuestos, subtotales, totales y porcentajes de descuentos e importes. Se hace la aclaración que si bien para efectos de aceptación de la propuesta no es exigible el cumplimiento de lo anterior, es conveniente para la mejor conducción del proceso.

8.- DESARROLLO DE LA LICITACION.

8.1. ACTOS Y PARTICIPANTES

La junta de aclaración a las bases así como los actos de presentación de proposiciones y apertura de propuestas técnicas; de apertura de propuestas económicas y de fallo, tendrán lugar en la Sala anexa al auditorio Antonio Suárez Hernández, del Tribunal, sito en el sótano del edificio Sede, en la calle Independencia S/N, esq. Nicolás Bravo Col. Centro de esta ciudad de Villahermosa, Tabasco, C.P. 86000, en las fechas y horarios señalados en la **Base** denominada: ***CALENDARIO DE LA LICITACIÓN***, y con la participación de:

- **Por El Tribunal:**
    a) Los integrantes del Comité de Compras del Poder Judicial.
    b) El Director de Estadística, Informática y Computación, Responsable de la evaluación técnica y especializada,
    c) El Director de la Contraloría del Tribunal, o su representante.

d) El Titular de la Unidad de Transparencia y Acceso a la Información, o su representante.

- **Por los licitantes:**

Su asistencia a los eventos es optativa, por lo que no se afectará la validez del acto o reunión de no asistir alguno; podrán enviar sus propuestas técnicas y económicas, utilizando el servicio postal o de mensajería bajo su estricta responsabilidad. En el entendido de que todo aquel sobre que llegue después del inicio del acto de presentación de proposiciones y del acto de apertura de propuestas técnicas no será considerado.

8.2. REGISTRO DE PARTICIPANTES.

Los licitantes que lo deseen, deberán presentarse en el lugar, el día y en punto de la hora señalada en estas bases, para la celebración de los actos: Junta de aclaraciones; de presentación y apertura de propuestas técnicas y económicas y de fallo, para su registro y participación, previa identificación.

8.3. ACLARACIÓN A LAS BASES

8.3.1. DUDAS O CUESTIONAMIENTOS PREVIOS

Los licitantes podrán plantear sus dudas o cuestionamientos técnicos, legales o administrativos, por escrito, en papel membretado, a más tardar el día **14 de junio del 2013, hasta las 12.00 horas**, presentado o enviado a la Dirección de Estadística, Informática y Computación, a los teléfonos: **358-20-00 ext. 2029**, o bien enviándolos por correo electrónico al Director de Estadística, Informática y Computación, voltairejesus@tsj-tabasco.gob.mx a efecto de que la convocante esté en posibilidad de analizarlos y hacer las correspondientes aclaraciones en la citada junta, por lo que después del día y hora mencionada no se aceptarán preguntas.

Es indispensable que al escrito de dudas o cuestionamientos, el licitante anexe copia de su recibo de pago de las bases, pues de no hacerlo no se dará respuesta a sus planteamientos.

8.3.2 JUNTA DE ACLARACIONES.

El día 17 de Junio de 2013 a las **10:00 horas**, en la sala anexa al Auditorio Antonio Suárez Hernández; se llevará a cabo la junta de aclaraciones al contenido de estas bases y sus anexos, de acuerdo a lo siguiente:

a) Presentación de los servidores públicos de la convocante.
b) Lista de asistencia de licitantes.
c) Declaración de inicio del acto.
d) Lectura en voz alta por quien presida el evento, de las preguntas y correspondientes respuestas a los cuestionamientos que previamente y por escrito hayan presentado los licitantes.
e) Se levantará el acta correspondiente, se le dará lectura y una vez firmada por los servidores públicos y los licitantes presentes, se les entregará copia a aquellos que acrediten el pago de las bases.
f) Los licitantes que hayan comprado las bases, pero no asistan a la junta, podrán consultar el acta en el la pagina de la Secretaria de la Contraloría del gobierno del estado; http://contraloria.tabasco.gob.mx/content/licitaciones-2013, o bien solicitar una copia fotostática de la misma, en la Coordinación de Control Presupuestal o en la Unidad de Transparencia y Acceso a la Información de El Tribunal, en días y horas hábiles.

Cualquier modificación a las bases de la licitación, derivada del resultado de la junta de aclaraciones, será considerada como parte integrante de las propias bases de la licitación; sin que sea necesario hacer la publicación que ordena la Ley.

La convocante en este acto podrá realizar las modificaciones y aclaraciones que considere pertinentes, en beneficio del proceso licitatorio.

Así también y conforme a lo que dispone el artículo 36, fracción IV, del Reglamento de la Ley; que textualmente dice: ***"…En la junta de aclaraciones la convocante dará respuesta únicamente a las preguntas que formulen los licitantes, siempre que***

estén directamente relacionadas con las bases de licitación y las especificaciones técnicas de los bienes o servicios que se pretendan adquirir o contratar; con las formalidades que establezca la convocante…". Esta convocante se abstendrá de recibir todo comentario u opinión que no se encuentren directamente relacionados con una duda sobre el contenido de las bases del citado proceso. Así también, el derecho a la libre manifestación de ideas que consagra el artículo 6 de la Constitución General de la república, toda opinión deberá ser plasmada por escrito y atendiendo a las formalidades que establece la constitución para estos efecto, es decir; ejercer este derecho de manera libre, pacífica y respetuosa.

La asistencia a la junta de aclaraciones será opcional para los licitantes, pero los acuerdos que se tomen en ésta serán obligatorios para todos.

Se entregará copia del acta a cada uno de los licitantes que haya asistido a la reunión, los que no hayan asistido a la junta podrán solicitarla por escrito a la convocante.

8.4. ACTO DE PRESENTACIÓN DE PROPOSICIONES Y APERTURA DE PROPUESTAS TÉCNICAS.
(PRIMERA ETAPA)

El día 24 de Junio de 2013, en punto de las **10:00 horas**, se cerrará el recinto donde se llevará a cabo el acto, y no se aceptará por ninguna circunstancia otra oferta. A continuación se iniciará la reunión conforme al siguiente orden:

a) Presentación de servidores públicos de la convocante;
b) Lista de asistencia de licitantes;
c) Declaración de inicio el acto;
d) Se solicitará a los licitantes o representantes presentes, la entrega de los dos sobres que contengan sus propuestas, y en su caso, la documentación complementaria solicitada;

e) Seguidamente se dará cuenta con las propuestas que se hayan recibido a través del servicio postal o de mensajería;
f) Los sobres recibidos serán rubricados por los servidores públicos y por los licitantes presentes, a fin de verificar que se encuentren debidamente cerrados;

A continuación, se abrirán exclusivamente los sobres que contengan las propuestas técnicas y se procederá a verificar preliminarmente, que la propuesta técnica incluya todos los documentos solicitados en la base D*ENOMINADA* ***PROPUESTA TÉCNICA***

La revisión que se efectuará a los documentos presentados como oferta técnica, en este acto será únicamente cuantitativa, sin analizar el contenido o procedencia de los documentos.

La omisión de algún documento requerido en esta propuesta, se le hará saber al licitante en el mismo acto, siempre y cuando se encuentre presente, a fin de que personalmente lo corrobore, y de confirmarse la omisión se desechará la propuesta. En el acta correspondiente se hará constar lo anterior, así como los caso de omisiones de los licitantes que no asistan, cuyas propuestas también serán desechadas.

Las proposiciones técnicas que no sean desechadas en este acto, se recibirán para su evaluación en el acto de análisis técnico, a que se refiere la base **denominada:** ***PROCEDIMIENTO DE EVALUACION QUE SE APLICARA A LAS PROPUESTAS TÉCNICAS:***

a. Por lo menos un licitante, si asistiere alguno y dos servidores públicos que hayan participado, rubricarán en todas sus fojas, cada una de las proposiciones técnicas que se hayan presentado, así como los correspondientes sobres cerrados que contengan las propuestas económicas de los licitantes, incluidos los de aquellos cuyas propuestas

hubieren sido desechadas, quedando éstos en custodia de la convocante.

b. Concluida esta etapa, se procederá a levantar el acta correspondiente, en la que se harán constar las propuestas técnicas aceptadas para su análisis, así como las que hubieren sido desechadas y las causas que lo motivaron.
c. En el acta se asentarán las observaciones, que en su caso hubiesen formulado los participantes.

d. Se dará lectura al acta y será firmada por los servidores públicos asistentes, así como por los licitantes si asistiere alguno.

e. La omisión de la firma de los licitantes, no invalidara el contenido y efectos del acta.

8.4.1. **PROCEDIMIENTO DE EVALUACION QUE SE APLICARA A LAS PROPUESTAS TÉCNICAS**

8.4.2. REVISION DOCUMENTAL:

Del día 24 al 25 de Junio de 2013, el Director de Informática y el personal del Tribunal, especializado en la materia, efectuará el análisis detallado de la documentación legal y técnica presentada por los licitantes. Dicho análisis consistirá en lo siguiente:

a) Se verificará que las propuestas incluyan la información, los documentos y los requisitos solicitados en estas bases de licitación, lo que se anotará en una tabla comparativa de evaluación bajo el esquema de **"cumple",** o **"no cumple",** por lo que en ningún caso estará sujeta a mecanismos de puntos o porcentajes.
b) 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.

c) 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 equipos; a la cual se refiere la base **denominada: *DESCRIPCIÓN Y CANTIDAD*.** La propuesta que no cumpla lo anterior será desechada.

d) Realizado el análisis correspondiente, los resultados serán asentados en una 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.

e) El resultado será dado a conocer a los licitantes en la segunda etapa, previo a la apertura de las propuestas económicas, a quienes se les pedirá que firmen de enterados. La falta de firma de los licitantes no invalidará el acto.

8.5. ACTO DE APERTURA DE PROPOSICIONES ECONÓMICAS (SEGUNDA ETAPA).

El día 26 de Junio de 2013 en punto de las **10:00 horas**, se cerrará el recinto donde se llevará a cabo el acto, de acuerdo con el siguiente programa.

a) Presentación de los servidores públicos.
b) Lista de asistencia a los licitantes.
c) Declaración de inicio del acto.
d) Se dará lectura al resultado del análisis de las propuestas técnicas, a fin de que se den por enterados del mismo los licitantes y los servidores públicos presentes.
e) Una vez conocidas las propuestas técnicas aceptadas, para continuar a la apertura de los sobre que contienen las propuestas económicas, se separarán éstos y se procederá a verificar que se encuentren cerrados. Por lo menos uno de los servidores públicos presentes y un licitante, si asistiera alguno, rubricarán dichos sobres.
f) A los licitantes cuyas propuestas técnicas hayan sido desechadas, se les proporcionará copia del acta de análisis, y se les informará que pueden solicitar

por escrito las aclaraciones que considere pertinentes. A continuación se les solicitará abandonen el recinto, a fin de proseguir a la apertura de las propuestas económicas que procedan.

g) Se procederá a abrir primero las propuestas económicas de los licitantes presentes, en el orden en que hayan registrado su asistencia al acto. En seguida, se abrirán las propuestas económicas de los licitantes ausentes, en el orden que determine el servidor público que presida el acto.
h) Al abrir cada sobre, se sustraerá la documentación y se dará lectura en voz alta al importe de las propuestas, y se asentarán en el acta correspondiente
i) Las proposiciones económicas serán rubricadas por lo menos por un licitante, si asistiere alguno y por dos servidores públicos de la convocante.
j) Las propuestas económicas serán aceptadas para su análisis.
k) Concluida esta etapa, se procederá a levantar el acta correspondiente, en la que se harán constar las propuestas aceptadas.
l) En dicha acta se asentaran las observaciones que en su caso, hubiesen formulado los participantes.
m) Se dará lectura al acta y será firmada por todos los servidores públicos asistentes, así como por los licitantes que asistan y quieran hacerlo
n) La omisión de la firma de los licitantes, no invalidará el contenido y efectos del acta.

8.6. EVALUACION DE LAS PROPUESTAS ECONOMICAS.

En el periodo comprendido del 26 al 27 de Junio de 2013; el Tribunal Superior de Justicia elabora el análisis económico a las proposiciones presentadas.

Para la evaluación de las propuestas económicas, se verificará que las mismas incluyan la información, documentos y requisitos solicitados en estas bases.

La evaluación en ningún caso estará sujeta a mecanismos de puntos o porcentajes.

Con el CD en formato en excell y su contenido, se elaborará un cuadro comparativo, que permita el análisis en igualdad de condiciones, de las propuestas aceptadas.

Si de dicho análisis resulta que dos o más proposiciones cumplen con todos los requisitos solicitados, siendo iguales en condiciones, se adjudicara al licitante cuyo precio sea el más bajo.

El Tribunal podrá declinar las propuestas cuyo costo sea de tal forma desproporcionado con respecto a los del mercado, que evidencie no poder cumplir con la entrega de los bienes requeridos.

No se considerarán las propuestas, cuando el volumen ofertado sea menor al 100% solicitado por El Tribunal en la presente licitación.

La adjudicación de la licitación se hará a la proposición solvente más baja que haya cumplido con los requisitos señalados en las presentes bases y satisfagan las mejores condiciones para el área usuaria y garantice satisfactoriamente el cumplimiento de las obligaciones respectivas.

Los licitantes que no cumplan con alguno de los requisitos exigidos en las bases, serán descalificados.

8.7. ACTO DE FALLO.

El día 28 de Junio de 2013 a las **10:00 horas**, se cerrará el recinto donde se llevará a cabo este acto, de acuerdo con el siguiente programa.

a) Presentación de los servidores públicos de la convocante.
b) Lista de asistencia de licitantes.
c) Declaración de inicio del acto.
d) Se dará lectura al resultado del análisis efectuado a las propuestas económicas.

e) Se dará lectura al fallo, mencionando al licitante ganador por ser la propuesta más baja, el montos de la adjudicación, y el cumplimiento con los requisitos establecidos en la presente bases de licitación.

f) Se levantará el acta correspondiente, en la que se asentarán en forma circunstanciada las incidencias del acto, así como el fallo y las observaciones que en su caso, hubiesen formulado los participantes.

g) Se dará lectura al acta y se firmará por los servidores públicos asistentes, así como por los licitantes presentes.

h) En el mismo acto de fallo, El Tribunal informará a los demás licitantes presentes las razones por las cuales sus propuestas no resultaron ganadoras.

Contra la resolución que contenga el fallo, no procederá recurso alguno, sin embargo, los participantes podrán inconformarse en los términos que señala el artículo 71 de la Ley.

Los licitantes que no asistan, para efecto de su notificación, tendrán a su disposición copia del acta respectiva en la Unidad de Transparencia y Acceso a la Información. Siendo de la exclusiva responsabilidad de los licitantes acudir a enterarse de su contenido y obtener copia del acta.

I) La omisión de la firma de los licitantes, no invalidará el contenido y efectos del acta.

9. FIRMA DEL CONTRATO.

El contrato será suscrito dentro del término que establece el Artículo 41 de la ley, en horas hábiles, en las oficinas de la Oficialía Mayor de El Tribunal.

Si el licitante adjudicado, por causas imputables a él, no firma el contrato dentro de un plazo de 10 días naturales siguientes al de notificación del fallo, El Tribunal podrá adjudicar el contrato al licitante que hubiese presentado la siguiente proposición solvente más baja, y así sucesivamente, en caso de que este último no acepte la

adjudicación, siempre y cuando la diferencia en precios con respecto a la postura ganadora no sea superior al 10%.

Para firmar el contrato, el proveedor deberá presentar original o copia certificada, así como copia simple para que previo cotejo, se anexe al expediente respectivo, de los siguientes documentos:

a) Acta constitutiva y, en su caso, de reformas o modificaciones, protocolizadas ante fedatarios públicos e inscritos en el Registro Público de la Propiedad y del Comercio, tratándose de persona jurídica colectiva; o acta de nacimiento si es persona física.

b) En su caso, poder notarial del representante legal, con facultades suficientes para suscribir el contrato.

c) Identificación oficial (credencial de elector, pasaporte vigente o cartilla militar) con fotografía y firma del licitante, o del representante legal que suscriba el contrato.

9.1. VIGENCIA DEL CONTRATO.

La vigencia del contrato será de: **1 años, contados a partir de la fecha de suscripción.**

9.2.- MODIFICACIONES QUE SE PODRÁN EFECTUAR AL CONTRATO.

El Tribunal con fundamento en el artículo 43 de la ley, podrá dentro del ejercicio correspondiente a su firma, incrementar las cantidades de los bienes solicitados, siempre que el monto total de las modificaciones no rebase en su conjunto el 10% de los conceptos y volúmenes originales y que el precio unitario sea igual al pactado originalmente en el contrato que se modifique.

9.3. GARANTÍA DE CUMPLIMIENTO.

El proveedor adjudicado deberá presentar garantía de cumplimiento del contrato, a más tardar dentro de los diez días naturales siguientes a la firma del mismo, de acuerdo a lo siguiente:

Mediante la exhibición de fianza expedida por compañía legalmente autorizada, por el equivalente al 20% del importe total del contrato, incluyendo el IVA, y será expedida a favor del Tribunal Superior de Justicia del estado de Tabasco.

La póliza de fianza deberá contener, además de las cláusulas que la ley establece, lo siguiente:

a) Que la fianza se otorga para garantizar el cumplimiento de todas y cada una de las obligaciones del contrato celebrado con la Tribunal Superior de Justicia del estado de Tabasco, derivado de la adjudicación de la que fue objeto en el proceso de Licitación Pública Estatal No. 560630001-003-13.

b) Que la fianza continuará vigente, aun cuando se otorguen prórrogas o esperas al proveedor, para el cumplimiento de las obligaciones que se garantizan.

c) A elección de El Tribunal podrá reclamarse el pago de la fianza por cualquiera de los procedimientos establecidos, por lo que la afianzadora incluirá expresamente en el texto de la fianza que se somete a elección del beneficiario, a cualesquiera de los procedimientos legales establecidos en los artículos 93, 93 bis, 95, 95 bis y 118, de la Ley Federal de Instituciones de Fianzas.

d) La compañía afianzadora se somete a la jurisdicción y competencia de los tribunales de la ciudad de Villahermosa, Tabasco.

e) Para la cancelación de la fianza será indispensable la autorización expresa y por escrito de El Tribunal.

9.4. ACREDITACION DEL ADJUDICADO, DE ENCONTRARSE AL CORRIENTE EN EL CUMPLIMIENTO DE SUS OBLIGACIONES FISCALES.

El licitante que resulte adjudicado deberá presentar, previo a la firma del contrato, escrito bajo protesta de decir verdad, en el cual manifieste lo siguiente:

a) Que ha presentado en tiempo y forma las declaraciones relativas a impuestos federales, distintos a las del ISAN e ISTUV, correspondientes a los tres últimos ejercicios fiscales, así como que ha presentado las declaraciones de pagos provisionales correspondientes al año 2013. Si tiene menos de tres años de inscrito en el RFC, la manifestación a que se refiere este rubro, corresponderá al periodo de inscripción.

b) Que no tiene adeudos fiscales firmes por impuestos federales, distintos a ISAN e ITSUV.

En caso de contar con autorización para el pago a plazo, manifestara que no ha incurrido durante el 2013 en las causales de revocación a que hace referencia el artículo 66 fracción III, del código fiscal de la federación.

El escrito deberá ser suscrito por el interesado o por persona legalmente autorizada para ello, indicándose el nombre, razón o denominación social del proveedor, su domicilio fiscal su RFC, el número de la presente licitación pública y monto total adjudicado sin incluir el IVA.

9.5 PLAZO Y LUGAR DE ENTREGA

La entrega de la totalidad de los bienes objeto de este concurso se efectuará dentro del plazo siguiente:

Dentro de los 45 días naturales siguientes a la fecha de la emisión del fallo.

La entrega deberá realizarse de lunes a viernes, en horario de 9:00 a 15:00 hrs., en el almacén del Tribunal.

El Tribunal no autorizará condonación de sanciones por retraso en las entregas, por causas imputables al proveedor.

Queda bajo la más estricta responsabilidad del proveedor, la transportación de los bienes hasta el lugar de entrega de conformidad con el contrato, razón por la cual no será aceptada condición alguna en cuanto a cargos adicionales por concepto de fletes, maniobras de carga y descarga, seguros u otros costos adicionales para El Tribunal.

9.6 REQUISITOS PARA LA ENTREGA DE LOS EQUIPOS.

a) Copia del pedido.

b) Original y Copia de la factura original (se hará referencia al número y fecha del contrato).

c) Él proveedor deberá suministrar a El Tribunal, los bienes con las características pactadas en el contrato.

d) Será responsabilidad del proveedor realizar por su cuenta las maniobras de carga y descarga de los bienes en el almacén donde se realice la entrega.

e) La entrega deberá realizarse por representante autorizado por el proveedor, puesto que no se aceptarán envíos por paquetería o mensajería.

f) Al momento de la entrega, El Tribunal verificará que los equipos que se entreguen, coincidan con lo ofertado, que sean completamente nuevos y provengan directamente del fabricante. No se aceptarán bienes que presenten adiciones, variación y/o sustituciones, o que no coincidan con lo ofertado en el proceso licitatorio.

g) El proveedor deberá mantener durante las distintas remesas de abasto los mismos niveles de calidad.

9.7 EMPAQUES

La forma de empaque y embalaje que utilice el proveedor, deberá garantizar la entrega de los bienes en condiciones óptimas de envase y presentación de los productos, a prueba de humedad y polvo, de tal manera que preserve la calidad y condiciones óptimas durante el transporte y el almacenaje, sin merma de su vida útil y deberán contener siempre etiquetas que por la naturaleza del producto se requieran, con la información básica siguiente:

- Tipo de producto
- Fecha de fabricación.
- Registro del producto.
- Forma de estiba y estiba máxima.
- Nombre y domicilio del fabricante o del distribuidor (en su caso)
- Condiciones de almacenamiento que deberán observarse.

En caso de que los bienes requieran condiciones de almacenamiento, temperaturas y transportes especiales, éstos deberán ser señalados claramente en los marbetes por el proveedor.

9.8.- FACTURACION Y PAGOS

Las condiciones de pago serán:

Crédito a 15 días naturales, posteriores a la presentación de la factura respectiva y a la entrega de los bienes en el almacén del Tribunal Superior de Justicia y visto bueno del Director de Informática, previa entrega de los bienes en los términos del contrato.

Los bienes serán pagados en moneda nacional por la Tesorería Judicial del Tribunal Superior de Justicia del Estado de Tabasco con recursos del IFOS a través de los mecanismos que para ello tiene implementado.

Para que la obligación de pago se haga exigible, el proveedor deberá, sin excepción alguna, presentar durante sus entregas, la documentación completa requerida y debidamente requisitada para realizar el trámite de pago, consistente en:

a) Factura correspondiente deberá describir los bienes amparados, precios unitarios, importe total, impuesto al valor agregado, ***número de licitación***, ***de partidas y de contrato.***

b) Número de cuenta bancaria y sucursal anexando el formato de **ABONO CUENTA** que emite la Tesorería Judicial del Tribunal Superior de Justicia del Estado de Tabasco. En el caso de que el licitante adjudicado no tenga cuenta bancaria registrada, deberá realizar el trámite de registro a más tardar 5 días hábiles posteriores a la notificación del fallo en caso contrario se cancelara la adjudicación correspondiente, pudiendo la convocante adjudicar el contrato al licitante que haya presentado la segunda proposición solvente más baja, y así sucesivamente en caso de que éste no acepte la adjudicación, siempre que la diferencia en precio entre la proposición ganadora y la que se pretende adjudicar no sea superior al diez por ciento de la primera.

c) La factura deberá ser a nombre del Tribunal Superior de Justicia, Registro Federal de Contribuyente: TSJ-250202-PH0 con domicilio en: Independencia Esq. Nicolás Bravo S/N Col. Centro, Villahermosa Tabasco., Código Postal 86000.

d) Dicha documentación deberá presentarse en La Unidad de Compras del Tribunal Superior de Justicia, en días hábiles y horas hábiles.

e) La factura deberá de llevar la siguiente leyenda: Recibí de los Ingresos Fiscales Ordinarios (IFOS), la cantidad de $.....(importe con letra del monto total con I.V.A.), por los conceptos de los bienes que a continuación se detallan:……. Nombre y firma del Representante Legal.

Es necesario que la factura que se presente, reúna los requisitos fiscales que establece la legislación vigente en la materia; en caso de que no sea así, El Tribunal le retendrá a el proveedor los pagos a su favor, hasta en tanto se subsanen dichas omisiones.

9.9 RESCISIÓN ADMINISTRATIVA Y TERMINACIÓN ANTICIPADA DEL CONTRATO

El Tribunal podrá rescindir administrativamente el contrato, en caso de incumplimiento de las obligaciones a cargo del proveedor, siguiendo el procedimiento a que se refiere el artículo 49 de la ley. Asimismo podrá darlo por terminado anticipadamente, cuando concurran razones de interés general, o cuando por causas justificadas se extinga la necesidad de requerir los bienes.

10. MODIFICACIONES QUE SE PODRÁN EFECTUAR DURANTE EL PROCESO LICITATORIO.

10.1. A LA CONVOCATORIA.

Hasta inclusive el quinto día natural previo a la presentación y apertura de proposiciones, se podrán modificar los plazos u otros aspectos establecidos en la convocatoria, que no impliquen sustitución o variación sustancial de los bienes solicitados o la adición de otros distintos; en este caso, las modificaciones se harán del conocimiento de los interesados a través de los medios utilizados para la publicación de la convocatoria.

10.2. A LAS BASES.

Hasta inclusive el quinto día natural previo a la presentación y apertura de proposiciones, se podrán modificar los plazos u otros aspectos establecidos en estas bases, que no impliquen sustitución o variación sustancial de los bienes solicitados o la adición de otros distintos, en este caso, se notificará mediante comunicación escrito dirigido a todos los participantes con acuse de recibo.

En el caso de que las modificaciones se deriven de la junta de aclaraciones la notificación mediante comunicación escrita no será necesaria, se entrega copia del acta respectiva a casa uno de los participantes que hayan adquirido las bases de la Licitación Pública y asistido a la citada junta.

De no comparecer los interesados dentro del plazo mencionado, se considerará que se han hecho sabedores para todos los efectos legales a que haya lugar, de las modificaciones correspondientes.

11. DESCALIFICACIÓN DE LOS LICITANTES.

Serán causas de descalificación de los licitantes:

a) No cumplir con cualquiera de los requisitos establecidos en estas bases, o los que se deriven del acto de aclaración de bases.

b) El acuerdo con otros licitantes para elevar el costo de los bienes solicitados.

c) Presentar proposiciones con precios escalonados.

d) Presentar la proposición económica en moneda extranjera.

e) Presentar la propuesta en idioma diferente al español.

f) Presentar documentos alterados, que contengan hechos o afirmaciones falsos.

g) La comprobación de que el licitante no cuenta con la capacidad de producción y/o distribución para garantizar el suministro de los bienes ofertados.

h) Encontrarse en alguno de los supuestos establecidos en el artículos 51 de la Ley

i) Omitir en alguno de los documentos solicitados, la expresión: **"bajo protesta de decir verdad",** cuando así se haya solicitado en las bases.

j) Incurrir en alguna violación a las disposiciones de la Ley, al Reglamento o a cualquier otro ordenamiento legal en la materia.

k) La comprobación de que los costos incluidos en la propuesta son sustancialmente inferiores a los del mercado, y por lo tanto se ponga en riesgo el suministro de los bienes.

l) La comprobación de que el licitante no cuenta con la capacidad económica o técnica suficiente para garantizar el suministro de los bienes y servicios ofertados.

m) Que el proveedor no se encuentre respaldado en los términos requeridos en estas bases, por sus distribuidores y/o fabricantes de los bienes.

n) La omisión de algún documento solicitado en estas bases.

ñ) Omitir la presentación del disco con formato en Excel, o poner el contenido de la información en algún formato ilegible.

o) Cuando los documentos que se soliciten presenten inconsistencias, diferencias, sean divergentes en algunas de sus partes y en tal sentido no sean susceptibles de tomarse por ciertos los hechos que en los mismos se consignen.

12. SUSPENSION Y CANCELACIÓN.

12.1. SUSPENSION TEMPORAL DE LA LICITACIÓN

El Tribunal podrá suspender el procedimiento, en los siguientes casos:

a) Cuando se presuma la existencia de acuerdos entre dos o más licitantes, para elevar los precios de los bienes objeto de la licitación.

b) Cuando se presenten casos fortuitos o de fuerza mayor que hagan necesaria la suspensión.

c) Cuando lo determine la Contraloría.

De presentarse alguna de las causales anteriores, se notificará por escrito a los interesados la suspensión, y se asentará dicha circunstancia en el acta correspondiente a la etapa en que se encuentre el procedimiento.
Si desaparecen las causas que motivaren la suspensión, o bien, cuando El Tribunal reciba la resolución que al efecto emita la Contraloría, previo aviso a los interesados, se reanudará el procedimiento, a partir del acto en que se hubiera decretado la suspensión, sin efectos retroactivos.

12.2. CANCELACIÓN DE LA LICITACIÓN

Podrá cancelarse la licitación, en los siguientes casos:

a) Por caso fortuito o fuerza mayor.
b) Si se descalifica a todos los licitantes.
c) Cuando la contraloría declare nulo el procedimiento licitatorio.

La cancelación se notificara por escrito a todos los interesados, y El Tribunal podrá convocar a una nueva licitación.

13. DECLARACIÓN DE LICITACIÓN DESIERTA

El Tribunal podrá declarar desierta la licitación, cuando:

a) No se inscriba ningún licitante.
b) Ninguna de las ofertas presentadas reúna los requisitos establecidos en estas bases.
c) Los precios cotizados en las proposiciones económicas no sean convenientes a la situación económica y presupuestal del Tribunal, o bien los bienes presentados no reúnan en conjunto la totalidad de requerimientos y especificaciones solicitadas.

En caso de declararse desierta la licitación, El Tribunal formulará una segunda convocatoria.

14. INCONFORMIDAD.

En contra de la resolución que contenga el fallo, no procederá recurso alguno; sin embargo, los participantes podrán inconformarse en los términos que señala el Articulo 71 de la Ley.

15. CONTROVERSIAS.

Las controversias que se susciten con motivo de la interpretación o cumplimiento del contrato que se derive de la presente licitación, serán resueltas por los tribunales locales de la ciudad de Villahermosa, Tabasco, por lo que las partes renuncian expresamente a cualquier otro fuero que pudiere corresponderles en razón de su domicilio presente o futuro.

16. SANCIONES.

Cuando un licitante o proveedor viole alguna disposición de la ley, no firme el contrato dentro del término establecido en la misma, no cumpla sus obligaciones contractuales, o proporcione información falsa, se hará del conocimiento de la Contraloría, a fin de que se proceda en los términos del artículo 66 de la Ley.

17. NO NEGOCIACIÓN DE CONDICIONES.

Bajo ninguna circunstancia podrán ser negociadas las condiciones establecidas en estas bases, o las propuestas presentadas por los licitantes.

El proveedor al que se adjudique el contrato, no podrá transmitir bajo ningún título, los derechos y obligaciones que se deriven del mismo, salvo los derechos de cobro.

18.- SITUACIONES NO PREVISTAS EN ESTAS BASES.

Cualquier situación que no haya sido prevista en las presentes bases, será resuelta por El Tribunal escuchando la opinión de las autoridades competentes, con base en las disposiciones aplicables.

19.- SUPLETORIEDAD

Conforme a lo dispuesto en el artículo 12 del La Ley, para todo lo no previsto en estas bases y en la legislación que rige la materia de adquisiciones, arrendamientos y servicios del estado; se estará a dispuesto en el Código Civil y el Código de Procedimientos Civiles; ambos del estado libre y soberano de Tabasco

ANEXO "1"

Formato para Cédula de Propuesta Técnica

RELACION DE BIENES OFERTADOS

LOTE	DESCRIPCION (CARACTERISTICAS DE LOS BIENES OFERTADOS A DETALLE, INLCUYENDO MARCA Y MODELO)	CANTIDAD	UNIDAD DE MEDIDA
UNICO			

A T E N T A M E N T E:

NOMBRE DEL REPRESENTANTE	CARGO EN LA EMPRESA	FIRMA

ANEXO “2”

FORMATO DE ACREDITAMIENTO DE LA PERSONALIDAD

Licitación pública Estatal No._____
Adquisición de _____

(NOMBRE) 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 pública, a nombre y representación de: (PERSONA FISICA O MORAL).

Registro Federal de Contribuyentes:
Domicilio:
Calle y Número:
Colonia: **Delegación o Municipio:**
Código Postal: **Entidad Federativa:**
Córreo 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:

Anexo No. 3

Formato de Propuesta Económica

RELACION DE BIENES OFERTADOS CON PRECIOS INCLUIDOS

LOTE	DESCRIPCION (CARACTERISTICAS DE LOS BIENES OFERTADOS A DETALLE, INLCUYENDO MARCA Y MODELO)	CANTIDAD	UNIDAD DE MEDIDA	COSTO UNITARIO
UNICO				
			SUB-TOTAL	
			IVA DESGLOSADO	
			TOTAL	

A T E N T A M E N T E:

NOMBRE DEL REPRESENTANTE	CARGO EN LA EMPRESA	FIRMA

Deberá incluir la siguiente leyenda:

- **Los precios arriba ofertados, se consideraran fijos e incondicionados.**
- **Se encuentran vigentes durante todo el proceso licitatorio, y en caso de ser adjudicados, serán respetados durante la vigencia del contrato.**
- **Condiciones de crédito: 30 días naturales contados a partir de la fecha de presentación de la factura y de toda la documentación requerida para trámites de pago en la secretaria de finanzas.**
- **Fecha compromiso de entrega.**

Nota: El presente formato podrá ser reproducido por el participante, en el modo que estime conveniente, debiendo respetar su contenido, preferentemente en el orden indicado.