Contrato de adquisición de diversas licencias informáticas e intelectuales y equipo de cómputo y tecnología de la información, que celebran por una parte el Estado de Campeche, representado en este acto por el ingeniero Gustavo Manuel Ortiz González, en su carácter de Secretario de Administración e Innovación Gubernamental, a quien en lo sucesivo se le denominará "El Estado" y por la otra parte la persona moral denominada Estrategias en Tecnología Corporativa, S.A. de C.V., representada en este acto por el ciudadano Juan Gualberto Cabrera Pérez, a quien en lo sucesivo se denominará "El Proveedor" al tenor de las siguientes declaraciones y cláusulas:

Declaraciones

1.- Declara "El Estado" a través de su representante:

1.1.- Que de acuerdo con los artículos 40, 41, 42 y 43 de la Constitución Política de los Estados Unidos Mexicanos, 1, 2, 4, 23, 24, 26, 59, 71 fracciones XV inciso a) y XXXI y 72 de la Constitución Política del Estado de Campeche, 1, 2, 12 y 16 de la Ley Orgánica de la Administración Pública del Estado de Campeche; Campeche es un Estado Libre y Soberano que forma parte integrante de la Federación, cuya Administración Pública Centralizada se encuentra conformada por las dependencias que lo integran, estando facultados sus titulares para que en representación del Estado de Campeche suscriban convenios, contratos y demás actos jurídicos con la Federación, con los otros Estados de la República, con los Ayuntamientos de los Municipios de la Entidad y con personas físicas y morales.

1.2.- Que el ingeniero Gustavo Manuel Ortiz González, comparece en su carácter de Secretario de Administración e Innovación Gubernamental, personalidad que acredita con el nombramiento expedido a su favor por el Ejecutivo Estatal el día 03 de noviembre de 2015 y está facultado para celebrar el presente instrumento según lo previsto por los artículos 4, 16 fracción III y 23 fracciones X, XI y XXIII de la Ley Orgánica de la Administración Pública del Estado de Campeche.

1.3.- Que mediante oficio número SSPCAM/RF/0687/2018 de fecha 17 de agosto de 2018, el Dr. Jorge de Jesús Argáez Uribe, Secretario de Seguridad Pública, solicitó la adquisición de licencias, equipos de cómputo y de tecnologías de la información, otros mobiliarios y equipos de administración, para destinarse a la dependencia a su cargo.

1.4.- Que según a lo establecido por los artículos 1, 3, 4, 6, 21, 22, 23 y demás aplicables de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche, en relación con los artículos 1°, 25 fracción VII, 49 segundo párrafo y demás aplicables de la Ley de Coordinación Fiscal; 1, 2 fracción IV y demás relativos aplicables de la Ley de Presupuesto de Egresos del Estado de Campeche, para el ejercicio fiscal 2018; la presente operación de compraventa se efectúa mediante la modalidad de Licitación Pública Estatal número **SAIG-EST-026-18.**

1.5.- Que la erogación de la presente compra se encuentra prevista y será cubierta con recursos provenientes del Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP), con base en el siguiente esquema programático: **Ejercicio Fiscal.-** 2018, **Programa con Prioridad Nacional de Seguridad Pública.-** Tecnologías, Infraestructura y Equipamiento de Apoyo a la Operación Policial; **Subprograma.-** Fortalecimiento de Programas Prioritarios Locales de las Instituciones de Seguridad Pública e Impartición de Justicia; **Programa con Prioridad Nacional de Seguridad Pública.-** Fortalecimiento al Sistema Penitenciario Nacional y de Ejecución de Medidas para Adolescentes; **Subprograma.-** Fortalecimiento al Sistema Penitenciario Nacional; **Subprograma.-** Fortalecimiento de la Autoridad Administrativa Especializada del Sistema de Justicia Penal para Adolescentes; **Programa con Prioridad Nacional de Seguridad Pública.-** Fortalecimiento de Capacidades para la Prevención y Combate a Delitos de Alto Impacto; **Subprograma.-** Modelo Homologado de Unidades de Policía Cibernética; **Capítulo 5000.-** Bienes muebles, inmuebles e intangibles.

OPERADO CON RECURSOS 2018

FASP

1.6.- Que tiene establecido su domicilio en la calle 8, sin número, colonia Centro, código postal 24000, de la ciudad de San Francisco de Campeche, Campeche, mismo que señala para los fines y efectos legales de este contrato.

2.- Declara "El Proveedor" a través de su representante:

2.1.- Ser una sociedad mercantil, constituida bajo escritura pública No. 1,391, libro décimo, tomo VI, de fecha 14 de julio de 2006; otorgada ante la fe del Lic. Mario Humberto Torres Verdín, notario público número 128 de Guadalajara, Jalisco, inscrita en el Registro Público de la Propiedad y del Comercio del Estado de Jalisco, mediante el folio mercantil electrónico número 32134 * 1, de fecha 11 de septiembre de 2006, con capacidad de comercializar los bienes y servicios que en este caso requiere "El Estado".

2.2.- Que su representante legal es el ciudadano Juan Gualberto Cabrera Pérez, quien acredita su personalidad con la escritura pública número 19,074 de fecha 13 de junio de 2018, pasada ante la fe del Lic. Carlos Montaño Pedraza, titular de la notaría pública número 130 con ejercicio en la Demarcación Notarial correspondiente al Primer Distrito Registral en el Estado de Nuevo León y se identifica con credencial para votar expedida a su favor por el Instituto Nacional Electoral, con folio 0127067747716.

2.3.- Que tiene capacidad jurídica para contratar y reúne las condiciones técnicas y económicas para obligarse a proveer los bienes y servicios objeto de este contrato.

2.4.- Que conoce el contenido y los requisitos que establece la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche.

2.5.- Que tiene establecido su domicilio en: Avenida Mariano Otero N1249-12 GWTC Torre Atlántico, Colonia Rinconada del Bosque, Código Postal 44530, Guadalajara, Jalisco; mismo que señala para todos los fines y efectos legales de este contrato.

2.6.- Que su número del padrón de proveedores es: 2895, renovado el día 04 de mayo de 2018.

2.7.- Que su Registro Federal de Contribuyentes es: ETC060715147.

3.- De ambas partes:

3.1.- Que en razón de lo declarado anteriormente y con fundamento en lo previsto por los artículos 39, 40, 41, 46, 47, 50, 51, 52, 53, 58, 60 y demás relativos aplicables de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche, así como por los artículos 1755, 1756, 1757, 1758, 1759, 1760, 2135, 2136, 2147, 2148, 2150, 2154, 2168, 2182, 2183, 2184, 2190 y 2192 del Código Civil del Estado de Campeche, han decidido formalizar la compraventa al tenor de las siguientes:

Cláusulas

Primera.- Objeto: "El Estado" encomienda a "El Proveedor" a entregar los bienes y servicios, acatando para ello lo establecido en el presente contrato y su anexo único, mismo que se detalla a continuación:

Partida 1.- "6 licencias informáticas"				
Cant.	**Unidad de Medida**	**Descripción**	**Precio Unitario**	**Importe**
1	Licencia	LICENCIA DE ANTIVIRUS PARA 200 USUARIOS	$131,500.00	$131,500.00

OPERADO CON RECURSOS 2018

FASP

		CON LAS SIGUIENTES CARACTERISTICAS Y FUNCIONALIDADES: KASPERSKY ENDPOINT SECURITY FOR BUSINESS NIVEL: SELECT .		
1	Licencia	**RENOVACION DE LICENCIA PARA FORTIGATE** CON EL NÚMERO DE SERIE: FGT3HD3915808215 LICENCIA: FORTICARE	65,202.00	65,202.00
1	Licencia	**LICENCIA PARA CONMUTADOR TELEFÓNICO** CON PÓLIZA DE SOPORTE POR 36 MESES MARCA: ALCATEL LICENCIA: SOLUTION PREMIER SERVICE	224,927.00	224,927.00
1	Licencia	**LICENCIA DE OFFICE 365 PARA 100 USUARIOS** LICENCIA: OFFICE O365PROPLUSOPEN	160,500.00	160,500.00
1	Licencia	**SISTEMA OPERATIVO WINDOWS PRO-10 64GB PARA 50 USUARIOS** LICENCIA: WINPRO 10 SNGL OLP NL LEGALIZATION GETGENUINE	72,050.00	72,050.00
1	Licencia	**LICENCIA DE EQUIPO DE SEGURIDAD PARA EMAIL CON 1 AÑO DE SOPORTE** MARCA: FORTINET MODELO: FML-200E	183,919.00	183,919.00
			Subtotal	**$838,098.00**
			16 % I.V.A.	**$134,095.68**
			Total	**$972,193.68**

OPERADO CON RECURSOS 2018

Partida 2.- "4 licencias informáticas"

Cant.	Unidad de Medida	Descripción	Precio Unitario	Importe
2	Licencia	**LICENCIA DE ANTIVIRUS PARA 50 USUARIOS** KASPERSKY ENDPOINT SECURITY FOR BUSINESS NIVEL: SELECT	$40,950.00	$81,900.00
2	Licencia	**RENOVACION DE LICENCIAS DE EQUIPO DE SEGURIDAD INFORMATICA PARA 2 EQUIPOS DE SEGURIDAD INFORMATICA FORTINET 90D** CON NUMEROS DE SERIE: FGT90D3Z15015304, FGT90D3Z15015298 LICENCIA: FORTICARE	37,068.97	74,137.94
			Subtotal	**$156,037.94**
			16 % I.V.A.	**$24,966.07**
			Total	**$181,004.01**

FAS

Partida 3.- "1 licencia antivirus"

Cant.	Unidad de Medida	Descripción	Precio Unitario	Importe
1	Licencia	**LICENCIA ANTIVIRUS PARA 50 USUARIOS** KASPERSKY ENDPOINT SECURITY FOR	$40,950.00	$40,950.00

		BUSINESS NIVEL: SELECT		
			Subtotal	**$40,950.00**
			16 % I.V.A.	**$6,552.00**
			Total	**$47,502.00**

Partida 4.- "1 conmutador de datos"				
Cant.	**Unidad de Medida**	**Descripción**	**Precio Unitario**	**Importe**
1	Pieza	**CONMUTADOR DE DATOS** MARCA: ALCATEL-LUCENT MODELO: OS6350-P48-US	$83,000.00	$83,000.00
			Subtotal	**$83,000.00**
			16 % I.V.A.	**$13,280.00**
			Total	**$96,280.00**

Partida 5.- "1 equipo de seguridad informática"				
Cant.	**Unidad de Medida**	**Descripción**	**Precio Unitario**	**Importe**
1	Pieza	**EQUIPO DE SEGURIDAD INFORMATICA** MARCA: FORTINET MODELO: FG-200E-BDL	$129,310.34	$129,310.34
			Subtotal	**$129,310.34**
			16 % I.V.A.	**$20,689.65**
			Total	**$149,999.99**

Mismos que "El Proveedor" se obliga a entregar en su totalidad acatando para ello lo establecido en el presente contrato, anexo único, bases de la licitación, así como los diversos ordenamientos y normas legales aplicables.

Segunda.- Monto del contrato: El monto total del contrato es de **$1,446,979.68 (son: Un millón cuatrocientos cuarenta y seis mil novecientos setenta y nueve pesos 68/100 M.N.) con I.V.A. incluido,** precio fijo con el cual se considera satisfecho "El Proveedor", mismo que se desglosa de la siguiente manera:

Concepto	**Monto Total**	
Partida 1.- "6 licencias informáticas"		**$972,193.68**
Partida 2.- "4 licencias informáticas"		**$181,004.01**
Partida 3.- "1 licencia antivirus"		**$47,502.00**
Partida 4.- "1 conmutador de datos"		**$96,280.00**
Partida 5.- "1 equipo de seguridad informática"		**$149,999.99**
	Gran Total	**$1,446,979.68**

Tercera.- Plazo y condiciones de entrega: "El Proveedor" se obliga a cumplir con la entrega de los bienes y servicios objeto de este contrato en un tiempo máximo de **49 días naturales contados a partir de la notificación del fallo de la Licitación Pública Estatal No. SAIG-EST-026-18**. Así mismo, "El Proveedor", previo a la entrega de los bienes y servicios, deberá notificar en un término de 5 días hábiles, la entrega de los mismos a la Secretaría de Seguridad Pública.

Cuarta.- Modificaciones al contrato: En el caso de que se requiera modificación en cuanto conceptos, volúmenes o plazos de cumplimiento, esta se realizará por causas debidamente justificadas y de común acuerdo entre las partes, de conformidad con lo establecido en el artículo 44 de la Ley de Adquisiciones,

OPERADO CON RECURSOS 2018 - FASP

Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche, debiendo "El Proveedor" presentar en su caso en un plazo máximo de cinco días hábiles antes de que finalice el plazo del contrato, escrito de solicitud y documentación que compruebe las razones de la solicitud, ante la Dirección de Recursos Materiales de la Secretaría de Administración e Innovación Gubernamental, para su autorización.

Quinta.- Forma de pago: Las partes convienen que los bienes y servicios del presente contrato sean pagados contra entrega-recepción de los mismos a satisfacción de "El Estado" y mediante la formulación de las facturas correspondientes, mismas que serán presentadas por "El Proveedor" para su revisión, autorización y pago en las oficinas que le indique "El Estado".

Sexta.- Requisitos de la factura: Además de los datos fiscales, la(s) factura(s) deberá(n) expedirse en términos de lo establecido por los artículos 29 y 29-A del Código Fiscal de la Federación y Anexo 20 "Guía de llenado de los CFDI emitidos por la Federación, Entidades, Entidades Federativas y los Municipios por Contribuciones, Derechos, Productos, aprovechamientos, Apoyos y Estímulos que otorguen".

Séptima.– Para garantizar el cumplimiento y vicios ocultos del contrato: "El Proveedor" otorgará garantía relativa al cumplimiento y vicios ocultos del contrato, por el 20% del monto total de este, a través de póliza de fianza que deberá contener entre otras, las siguientes declaraciones expresas de la Institución que la otorgue:

a) Que sea expedida a favor del Gobierno del Estado de Campeche, teniendo la fianza una vigencia por un periodo de doce meses posteriores a la entrega total de los bienes y servicios a satisfacción de "El Estado".

b) Que se otorgue atendiendo a las estipulaciones expresamente establecidas en este contrato.

c) Que garantice la entrega de los bienes y servicios adquiridos, de acuerdo con las estipulaciones establecidas en el mismo instrumento contractual.

d) Que en caso de que exista inconformidad por parte de "El Estado" respecto de los bienes y servicios adquiridos, "El Proveedor" se obliga a responder tanto de los defectos, sus obligaciones contractuales, sus fallas en la entrega, así como de cualquier responsabilidad que le sea imputable, obligándose a que la fianza permanezca vigente hasta que este subsane las causas que motivaron la inconformidad.

e) Para ser cancelada la fianza será requisito indispensable la conformidad expresa y por escrito de "El Estado", a través de la Secretaría de Administración e Innovación Gubernamental.

f) Que la institución afianzadora acepte expresamente e indefectiblemente lo establecido en los artículos 178, 279, 280 y 282 de la Ley de Instituciones de Seguros y de Fianzas en vigor.

g) Que la fianza continuará vigente en caso de que se otorguen prórrogas al cumplimiento del contrato, así como durante la substanciación de todos los recursos legales o juicios que se interpongan y hasta que se dicte resolución definitiva por autoridad competente.

"El Proveedor" deberá presentar la garantía de cumplimiento y vicios ocultos, en un plazo máximo de 5 días hábiles siguientes a la firma del presente instrumento contractual.

Octava.- Recepción de los bienes y servicios: La recepción de los bienes y servicios será total, conforme al plazo establecido en la cláusula tercera de este instrumento y se realizará en las instalaciones que ocupan las oficinas de la Secretaría Seguridad Pública, sita: Avenida López Portillo por avenida Lázaro

OPERADO CON RECURSOS 2018

FASP

Cárdenas, sin número, colonia Laureles, código postal 24096, San Francisco de Campeche, Campeche, o en el domicilio, que para tales efectos señale "El Estado", pudiendo este reclamar en caso de no estar satisfecho con la calidad de los bienes y servicios objeto del presente contrato conforme a lo señalado en los lineamientos, requisitos y plazos que para tal efecto se establecen en el mismo.

Novena.- Vigilancia, seguimiento, recepción de los bienes y servicios por parte de "El Estado": "El Estado" designa como responsable para la vigilancia, seguimiento y recepción de los bienes y servicios adquiridos, en este caso a la Licda. Emma Vanessa Valle Abreu, Subdirectora de Recursos Federales, en coordinación con el Ing. Juan Carlos Chávez Chan, Subdirector de Informática, ambos de la Secretaría de Seguridad Pública, o por personal que estos mismos designen, quienes deberán en todo momento exigir a "El Proveedor" la entrega total de los bienes y servicios.

Décima.- Responsabilidades de "El Proveedor": "El Proveedor" se obliga a que los bienes y servicios objeto del presente contrato, cumplan con las normas de calidad requeridas y que la adquisición se efectúe a satisfacción de "El Estado" así como a responder por su cuenta y riesgo de los defectos de dichos bienes y servicios, atendiendo para tal efecto las condiciones de garantía requeridas por "El Estado".

Décima primera.- Recursos humanos: Los recursos humanos necesarios para realizar los servicios objeto de este contrato serán entregados por "El Proveedor". "El Estado" se excluye de toda relación laboral hacia los trabajadores de "El Proveedor".

Décima segunda.- Responsabilidad laboral: Queda expresamente convenido que cada parte es responsable de las relaciones laborales que tenga con su propio personal y de las relaciones contractuales que tengan con sus propios contratistas. No existirán relaciones laborales, ni de ninguna otra índole entre "El Estado" y el personal que "El Proveedor" contrate o emplee para el desarrollo de los servicios convenidos, por lo que en el supuesto de que "El Estado" llegase a recibir cualquier reclamación por este concepto, "El Proveedor" se obliga a sacarlo en paz, a salvo, libre de responsabilidades y daños de cualquier naturaleza, y a reembolsarle en su caso, cualquier erogación que hubiere tenido que realizar por tal motivo.

Décima tercera.- El anexo único del presente contrato es parte integral de este instrumento contractual y solo podrá ser modificado o adicionado mediante un instrumento por escrito firmado por cada una de las partes y entregado a la otra parte.

Décima cuarta.- "El Proveedor" se obliga a no ceder a terceras personas físicas o morales, sus derechos y obligaciones sobre los bienes y servicios que amparan este contrato, sin previa aprobación expresa y por escrito de "El Estado", en los términos de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche.

Décima quinta.- Suspensión temporal del contrato: "El Estado" podrá suspender temporalmente en todo o en parte la adquisición contratada en cualquier momento, por causas justificadas o razones de interés general, sin que ello implique su terminación definitiva. El presente contrato podrá continuar produciendo todos sus efectos legales, una vez que hayan desaparecido las causas que motivaron dicha suspensión.

Décima sexta.- Penas convencionales: Por la demora en la entrega de los bienes y servicios objeto de este contrato, "El Estado" procederá a un descuento en la facturación por una cantidad igual a 5 al millar diario por cada día que "El Proveedor" incumpla con la entrega de los bienes y servicios, hasta por 20 días naturales, concluido este plazo y si "El Proveedor" continua con el incumplimiento, "El Estado" procederá a la rescisión del contrato, haciéndose efectiva la garantía de cumplimiento y vicios ocultos del contrato.

OPERADO CON RECURSOS FASP 2018

Décima séptima.- Rescisión administrativa del contrato: "El Estado" podrá en cualquier momento rescindir administrativamente este contrato cuando "El Proveedor" incurra en incumplimiento de cualquiera de las obligaciones estipuladas en el presente contrato, aplicando en su caso a "El Proveedor" la garantía señalada en el presente instrumento contractual.

Décima octava.- Las partes se obligan a sujetarse estrictamente para la adquisición objeto de este contrato, a todas y cada una de las cláusulas que lo integran, así como a los términos y requisitos que establece este contrato, la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles del Estado de Campeche y demás disposiciones legales que le sean aplicables.

Décima novena.- Ausencia de vicios del consentimiento: Ambas partes manifiestan que en la celebración del presente contrato no existe ningún error, dolo, violencia, mala fe, ni enriquecimiento ilícito que pudiese invalidarlo.

Vigésima.- Para la interpretación y cumplimiento del contenido del presente contrato, así como para todo aquello que no esté expresamente establecido en el mismo, las partes se someten a jurisdicción de los tribunales establecidos en la ciudad de San Francisco de Campeche, Estado de Campeche, renunciando a cualquier otro que por su domicilio presente o futuro pudiere corresponderles.

Leído lo que fue el presente contrato, ambas partes se manifiestan conformes con su contenido, procediendo a suscribirlo por cuadriplicado, en la ciudad de San Francisco de Campeche, Campeche, el día 16 de octubre de dos mil dieciocho.

Por "El Estado"

Ing. Gustavo Manuel Ortiz González
Secretario de Administración e
Innovación Gubernamental

Por "El Proveedor"

C. Juan Gualberto Cabrera Pérez
Rep. legal de Estrategias en Tecnología
Corporativa, S.A. de C.V.

Testigos

Licda. Elsy Daniela Chuc Solis
Directora de Recursos Materiales.

Licda. Denice Elizabeth Castro Córdova
Subdirectora de Licitaciones y Contratos.

OPERADO CON RECURSOS FASP 2018

Anexo Único

Partida	Cant.	Unidad de Medida	Descripción
1	6	Licencia	(1) LICENCIA DE ANTIVIRUS PARA 200 USUARIOS CON LAS SIGUIENTES CARACTERÍSTICAS Y FUNCIONALIDADES: KASPERSKY ENDPOINT SECURITY FOR BUSINESS NIVEL: SELECT • LICENCIA ANTIVIRUS POR TRES AÑOS • ANTIMALWARE • FIREWALL • PROTECCIÓN ASISTIDA EN LA NUBE • CONTROL DE APLICACIONES • LISTA BLANCA DE APLICACIONES • CONTROL WEB • CONTROL DE DISPOSITIVOS • PROTECCIÓN DEL SERVIDOR DE ARCHIVOS • MANEJO DEL DISPOSITIVO MÓVIL (MDM) • SEGURIDAD DE ENDPOINT MÓVIL (PARA TABLETS Y SMARTPHONES) • ENCRIPTACIÓN • CONFIGURACIÓN Y DESPLIEGUE DE SISTEMAS • ESCÁNER DE VULNERABILIDADES AVANZADO • CONTROL DE ADMISIÓN A LA RED • MANEJO DE PARCHES • SEGURIDAD PARA EL SERVIDOR DE CORREO • PROTECCIÓN DEL GATEWAY DE WEB/INTERNET • SEGURIDAD DEL SERVIDOR DE COLABORACIÓN (1) RENOVACIÓN DE LICENCIA PARA FORTIGATE CON EL NÚMERO DE SERIE: FGT3HD3915808215. LICENCIA: FORTICARE **FUNCIONALIDADES Y CARACTERÍSTICAS** **FIREWALL** o LAS REGLAS DE FIREWALL ANALIZAN LAS CONEXIONES QUE ATRAVIESEN EN EL EQUIPO, ENTRE INTERFACES, GRUPOS DE INTERFACES (O ZONAS) Y VLANS. o POR GRANULARIDAD Y SEGURIDAD, EL FIREWALL PUEDE ESPECIFICAR POLÍTICAS TOMANDO EN CUENTA PUERTO FÍSICO FUENTE Y DESTINO. ESTO ES, EL PUERTO FÍSICO FUENTE Y EL PUERTO FÍSICO DESTINO FORMAN PARTE DE LA ESPECIFICACIÓN DE LA REGLA DE FIREWALL. o SE PUEDEN DEFINIR POLÍTICAS DE FIREWALL QUE SEAN INDEPENDIENTES DEL PUERTO DE ORIGEN Y PUERTO DE DESTINO. o LAS REGLAS DEL FIREWALL TOMAN 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 o SOPORTA REGLAS DE FIREWALL PARA TRÁFICO DE MULTICAST, PUDIENDO ESPECIFICAR PUERTO FÍSICO FUENTE, PUERTO FÍSICO DESTINO, DIRECCIONES IP FUENTE, DIRECCIÓN IP DESTINO. o LAS REGLAS DE FIREWALL TIENEN LIMITANTES Y/O VIGENCIA EN BASE A TIEMPO. o LAS REGLAS DE FIREWALL TIENEN LIMITANTES Y/O VIGENCIA EN BASE A FECHAS (INCLUYENDO DÍA, MES Y AÑO) o SOPORTAN LA CAPACIDAD DE DEFINIR NUEVOS SERVICIOS TCP Y UDP QUE NO ESTÉN CONTEMPLADOS EN LOS PREDEFINIDOS. o SE DEFINE EL TIEMPO DE VIDA DE UNA SESIÓN INACTIVA DE FORMA INDEPENDIENTE POR PUERTO Y PROTOCOLO (TCP Y UDP) o TIENE LA CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES ESTÁTICO, UNO A UNO, NAT. o POSEE CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES DINÁMICO, MUCHOS A UNO, PAT. o SOPORTA REGLAS DE FIREWALL EN IPV6 CONFIGURABLES TANTO POR CLI (COMMAND LINE INTERFACE, INTERFACE DE LÍNEA DE COMANDO) COMO POR GUI (GRAPHICAL USER

OPERADO CON RE... 2018

FAS...

Partida	Cant.	Unidad de Medida	Descripción
			INTERFACE, INTERFACE GRAFICA DE USUARIO), o LA SOLUCIÓN TIENE 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. o EN LA SOLUCIÓN DE BALANCEO DE CARGA ENTRE SERVIDORES, SE SOPORTA PERSISTENCIA DE SESIÓN MEDIANTE HTTP COOKIE O SSL SESSION ID o EN LA SOLUCIÓN DE BALANCEO DE CARGA ENTRE SERVIDORES SE SOPORTAN MECANISMOS PARA DETECTAR LA DISPONIBILIDAD DE LOS SERVIDORES, DE FORMA TAL DE PODER EVITAR ENVIAR TRÁFICO A UN SERVIDOR NO DISPONIBLE. o EL EQUIPO PERMITE LA CREACIÓN DE POLÍTICAS DE TIPO FIREWALL CON CAPACIDAD DE SELECCIONAR CAMPOS COMO DIRECCIÓN, IDENTIFICADOR DE USUARIOS O IDENTIFICADOR DE DISPOSITIVOS PARA EL CASO DE DISPOSITIVOS MÓVILES COMO SMARTPHONES Y TABLETAS. o EL EQUIPO PERMITE LA CREACIÓN DE POLÍTICAS DE TIPO VPN CON CAPACIDAD DE SELECCIONAR CAMPOS COMO IPSEC O SSL SEGÚN SEA EL TIPO DE VPN. o LA SOLUCIÓN TIENE LA CAPACIDAD DE HACER CAPTURA DE PAQUETES POR POLÍTICA DE SEGURIDAD IMPLEMENTADA PARA LUEGO SER EXPORTADO EN FORMATO PCAP. o LA SOLUCIÓN DE SEGURIDAD TIENE LA CAPACIDAD DE PERMITIR LA CREACIÓN DE SERVICIOS DE FIREWALL PARA IMPLEMENTAR DENTRO DE LAS POLÍTICAS DE SEGURIDAD Y CATEGORIZARLOS DE MANERA PERSONALIZADA. o LA SOLUCIÓN ES CAPAZ DE INTEGRAR LOS SERVICIOS DENTRO DE LAS CATEGORÍAS DE FIREWALL PREDEFINIDAS O PERSONALIZADAS Y ORDENARLOS ALFABÉTICAMENTE. o EL DISPOSITIVO DE SEGURIDAD ES CAPAZ DE DETERMINAR ACCESOS Y DENEGACIÓN A DIFERENTES TIPOS DE TRÁFICO PREDEFINIDOS DENTRO DE UNA LISTA LOCAL DE POLÍTICAS. o LA SOLUCIÓN ES CAPAZ DE HABILITAR O DESHABILITAR EL PASO DE TRÁFICO A TRAVÉS DE PROCESADORES DE PROPÓSITO ESPECÍFICO, SI EL DISPOSITIVO CUENTA CON ESTOS PROCESADORES INTEGRADOS DENTRO DEL MISMO. o LA SOLUCIÓN PUEDE CREAR E IMPLEMENTAR POLÍTICAS DE TIPO MULTICAST Y DETERMINAR EL SENTIDO DE LA POLÍTICA, ASÍ COMO TAMBIÉN LA HABILITACIÓN DEL NAT DENTRO DE CADA INTERFACE DEL DISPOSITIVO. o EL DISPOSITIVO DE SEGURIDAD ES CAPAZ DE CREAR E INTEGRAR POLÍTICAS CONTRA ATAQUES DOS LAS CUALES SE PUEDEN APLICAR POR INTERFACES. o EL DISPOSITIVO DE GENERAR LOGS DE CADA UNA DE LAS POLÍTICAS APLICADAS PARA EVITAR LOS ATAQUES DE DOS. o LA SOLUCIÓN DE SEGURIDAD PERMITE CONFIGURAR EL MAPEO DE PROTOCOLOS A PUERTOS DE MANERA GLOBAL O ESPECIFICA. o LA SOLUCIÓN ES CAPAZ DE CONFIGURAR EL BLOQUEO DE ARCHIVOS O CORREOS ELECTRÓNICOS POR TAMAÑO, O POR CERTIFICADOS SSL INVÁLIDOS. o EL DISPOSITIVO INTEGRA LA INSPECCIÓN DE TRÁFICO TIPO SSL Y SSH BAJO PERFILES PREDEFINIDOS O PERSONALIZADOS. o EL DISPOSITIVO ES CAPAZ DE EJECUTAR INSPECCIÓN DE TRAFICO SSL EN TODOS LOS PUERTOS Y SELECCIONAR BAJO QUE CERTIFICADO ES VÁLIDO ESTE TRÁFICO. o TIENE LA CAPACIDAD DE HACER ESCANEO A PROFUNDIDAD DE TRAFICO TIPO SSH DENTRO DE TODOS O CIERTO RANGO DE PUERTOS CONFIGURADOS PARA ESTE ANÁLISIS. o LA SOLUCIÓN PERMITE BLOQUEAR O MONITOREAR TODA LA ACTIVIDAD DE TIPO EXEC, PORT-FORWARD, SSH-SHELL, Y X-11 SSH. **ANTIVIRUS** o ES CAPAZ DE ANALIZAR, ESTABLECER CONTROL DE ACCESO Y DETENER ATAQUES Y HACER ANTIVIRUS EN TIEMPO REAL EN LOS SIGUIENTES PROTOCOLOS APLICATIVOS: HTTP, SMTP, IMAP, POP3, FTP. o EL ANTIVIRUS PUEDE CONFIGURARSE EN MODO PROXY, ASÍ COMO EN MODO DE FLUJO. EN EL PRIMER CASO, LOS ARCHIVOS SERÁN TOTALMENTE RECONSTRUIDOS POR EL MOTOR ANTES DE HACER LA INSPECCIÓN. EN EL SEGUNDO CASO, LA INSPECCIÓN DE ANTIVIRUS SE HARÁ POR CADA PAQUETE DE FORMA INDEPENDIENTE. o 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. o EL ANTIVIRUS INTEGRADO SOPORTA LA CAPACIDAD DE INSPECCIONAR Y DETECTAR VIRUS EN TRÁFICO IPV6. o LA CONFIGURACIÓN DE ANTIVIRUS EN TIEMPO REAL SOBRE LOS PROTOCOLOS HTTP, SMTP, IMAP, POP3 Y FTP ESTA COMPLETAMENTE INTEGRADA A LA ADMINISTRACIÓN DEL

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			DISPOSITIVO "APPLIANCE", QUE PERMITA LA APLICACIÓN DE ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. o EL ANTIVIRUS SOPORTA 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. o EL "APPLIANCE" DE MANERA OPCIONAL PUEDE INSPECCIONAR POR TODOS LOS VIRUS CONOCIDOS (ZOO LIST). o EL ANTIVIRUS INTEGRADO TIENE LA CAPACIDAD DE PONER EN CUARENTENA ARCHIVOS ENCONTRADOS INFECTADOS QUE ESTÉN CIRCULANDO A TRAVÉS DE LOS PROTOCOLOS HTTP, FTP, IMAP, POP3, SMTP. o EL ANTIVIRUS INTEGRADO TIENE LA CAPACIDAD DE PONER EN CUARENTENA A LOS CLIENTES CUANDO SE HAYA DETECTADO QUE LOS MISMOS ENVÍAN ARCHIVOS INFECTADOS CON VIRUS. o EL ANTIVIRUS INCLUYE CAPACIDADES DE DETECCIÓN Y DETENCIÓN DE TRÁFICO SPYWARE, ADWARE Y OTROS TIPOS DE MALWARE/GRAYWARE QUE PUDIERAN CIRCULAR POR LA RED. o EL ANTIVIRUS PUEDE HACER INSPECCIÓN Y CUARENTENA DE ARCHIVOS TRANSFERIDOS POR MENSAJERÍA INSTANTÁNEA (INSTANT MESSAGING). o EL ANTIVIRUS ES CAPAZ DE FILTRAR ARCHIVOS POR EXTENSIÓN. o EL ANTIVIRUS ES CAPAZ DE FILTRAR ARCHIVOS POR TIPO DE ARCHIVO (EJECUTABLES, POR EJEMPLO) SIN IMPORTAR LA EXTENSIÓN QUE TENGA EL ARCHIVO. o 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). o LAS FIRMAS DE ANTIVIRUS SON DEL MISMO FABRICANTE QUE EL "APPLIANCE". o EL SISTEMA ES CAPAZ DE INTEGRARSE A FUTURO CON UNA SOLUCIÓN DE SANBOXING DEL MISMO FABRICANTE DE MANERA QUE SE PUEDA APROVECHAR LAS FIRMAS GENERADAS EN EL FIREWALL. **ANTISPAM** O LA CAPACIDAD ANTISPAM INCLUIDA ES 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. O LA CAPACIDAD ANTISPAM INCLUIDA PERMITE ESPECIFICAR LISTAS BLANCAS (CONFIABLES, A LOS CUALES SIEMPRE SE LES PASA) Y LISTAS NEGRAS (NO CONFIABLES, A LOS CUALES SIEMPRE LES BLOQUEA). LAS LISTAS BLANCAS Y LISTAS NEGRAS PODRÁN SER POR DIRECCIÓN IP O POR DIRECCIÓN DE CORREO ELECTRÓNICO (E-MAIL ADDRESS). O LA CAPACIDAD ANTISPAM PUEDE CONSULTAR UNA BASE DE DATOS DONDE SE REVISE DIRECCIÓN IP DEL EMISOR DEL MENSAJE, URLS CONTENIDOS DENTRO DEL MENSAJE Y "CHECKSUM" DEL MENSAJE, COMO MECANISMOS PARA DETECCIÓN DE SPAM. O EN EL CASO DE ANÁLISIS DE SMTP, LOS MENSAJES ENCONTRADOS COMO SPAM PUEDEN SER ETIQUETADOS O RECHAZADOS (DESCARTADOS). EN EL CASO DE ETIQUETAMIENTO DEL MENSAJE, TIENE LA FLEXIBILIDAD PARA ETIQUETARSE EN EL MOTIVO (SUBJECT) DEL MENSAJE O A TRAVÉS UN ENCABEZADO MIME EN EL MENSAJE. **FILTRAJE DE URLS (URL FILTERING)** O FACILIDAD PARA INCORPORAR CONTROL DE SITIOS A LOS CUALES NAVEGUEN LOS USUARIOS, MEDIANTE CATEGORÍAS. POR FLEXIBILIDAD, EL FILTRO DE URLS TIENE 75 CATEGORÍAS Y 54 MILLONES DE SITIOS WEB EN LA BASE DE DATOS. O PUEDE CATEGORIZAR CONTENIDO WEB REQUERIDO MEDIANTE IPV6. O FILTRADO DE CONTENIDO BASADO EN CATEGORÍAS EN TIEMPO REAL, INTEGRADO A LA PLATAFORMA DE SEGURIDAD "APPLIANCE". SIN NECESIDAD DE INSTALAR UN SERVIDOR O "APPLIANCE" O DISPOSITIVO EXTERNO, LICENCIAMIENTO DE UN PRODUCTO EXTERNO O SOFTWARE ADICIONAL PARA REALIZAR LA CATEGORIZACIÓN DEL CONTENIDO. O CONFIGURABLE DIRECTAMENTE DESDE LA INTERFAZ DE ADMINISTRACIÓN DEL DISPOSITIVO "APPLIANCE". CON CAPACIDAD PARA PERMITIR ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. O PERMITE 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.

RECIBIDO CON RECURSOS
2018

FAS

Partida	Cant.	Unidad de Medida	Descripción
			O 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) SON PERSONALIZABLES. O CAPACIDAD DE FILTRADO DE SCRIPTS EN PÁGINAS WEB (JAVA/ACTIVE X). O LA SOLUCIÓN DE FILTRAJE DE CONTENIDO SOPORTA 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 PARA NAVEGADORES TALES COMO GOOGLE, YAHOO! Y BING. O LA SOLUCIÓN ES CAPAZ DE PODER BLOQUEAR EL ACCESO CUENTAS DE DOMINIOS ESPECÍFICOS A SERVICIOS DE GOOGLE COMO POR EJEMPLO GMAIL, GDOCS. O ES POSIBLE DEFINIR CUOTAS DE TIEMPO PARA LA NAVEGACIÓN. DICHAS CUOTAS PUEDEN ASIGNARSE POR CADA CATEGORÍA Y POR GRUPOS. O ES POSIBLE EXCEPTUAR LA INSPECCIÓN DE HTTPS POR CATEGORÍA. O EL EQUIPO TENDRÁ LA CAPACIDAD PARA QUE AUTOMÁTICAMENTE REDIRIJA EL TRÁFICO DE WWW.YOUTUBE.COM A HTTP://WWW.YOUTUBE.COM/EDUCATION PARA QUE SE ACCEDA ÚNICAMENTE A CONTENIDO CATEGORIZADO POR EL PORTAL COMO CONTENIDO EDUCATIVO. **PROTECCIÓN CONTRA INTRUSOS (IPS)** o EL DETECTOR Y PREVENTOR DE INTRUSOS SE IMPLEMENTA TANTO EN LÍNEA COMO FUERA DE LÍNEA. EN LÍNEA, EL TRÁFICO A SER INSPECCIONADO PASA A TRAVÉS DEL EQUIPO. FUERA DE LÍNEA, EL EQUIPO RECIBE EL TRÁFICO A INSPECCIONAR DESDE UN SWITCH CON UN PUERTO CONFIGURADO EN SPAN O MIRROR. o ES POSIBLE DEFINIR POLÍTICAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES PARA TRÁFICO IPV6. A TRAVÉS DE SENSORES. o TIENE CAPACIDAD DE DETECCIÓN DE MÁS DE 4000 ATAQUES. o CUENTA CON CAPACIDAD DE ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS IPS MEDIANTE TECNOLOGÍA DE TIPO "PUSH" (PERMITE RECIBIR LAS ACTUALIZACIONES CUANDO LOS CENTROS DE ACTUALIZACIÓN ENVÍEN NOTIFICACIONES SIN PROGRAMACIÓN PREVIA), ADICIONAL A TECNOLOGÍAS TIPO "PULL" (CONSULTA LOS CENTROS DE ACTUALIZACIÓN POR VERSIONES NUEVAS) o EL DETECTOR Y PREVENTOR DE INTRUSOS SE ENCUENTRA 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 ESTA 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 PERMITE LA PROTECCIÓN DE ESTE SERVICIO POR POLÍTICA DE CONTROL DE ACCESO. o EL DETECTOR Y PREVENTOR DE INTRUSOS PUEDE SOPORTAR CAPTAR ATAQUES POR VARIACIONES DE PROTOCOLO Y ADEMÁS POR FIRMAS DE ATAQUES CONOCIDOS (SIGNATURE BASED / MISUSE DETECTION). o BASADO EN ANÁLISIS DE FIRMAS EN EL FLUJO DE DATOS EN LA RED, Y PERMITE CONFIGURAR FIRMAS NUEVAS PARA CUALQUIER PROTOCOLO. o CUENTA CON ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS PARA EL DETECTOR DE INTRUSOS o EL DETECTOR DE INTRUSOS MITIGA LOS EFECTOS DE LOS ATAQUES DE NEGACIÓN DE SERVICIOS. o MÉTODOS DE NOTIFICACIÓN: o ALARMAS MOSTRADAS EN LA CONSOLA DE ADMINISTRACIÓN DEL APPLIANCE. o ALERTAS VÍA CORREO ELECTRÓNICO. o CUENTA CON LA CAPACIDAD DE CUARENTENA, ES DECIR PROHIBIR EL TRÁFICO SUBSIGUIENTE A LA DETECCIÓN DE UN POSIBLE ATAQUE. ESTA CUARENTENA PUEDE DEFINIRSE PARA EL TRÁFICO PROVENIENTE DEL ATACANTE O PARA EL TRÁFICO DEL ATACANTE AL ATACADO. o LA CAPACIDAD DE CUARENTENA OFRECE LA POSIBILIDAD DE DEFINIR EL TIEMPO EN QUE SE BLOQUEA EL TRÁFICO. TAMBIÉN PUEDE DEFINIRSE EL BLOQUEO DE FORMA "INDEFINIDA", HASTA QUE UN ADMINISTRADOR TOME UNA ACCIÓN AL RESPECTO. o SE OFRECE LA POSIBILIDAD DE GUARDAR INFORMACIÓN SOBRE EL PAQUETE DE RED QUE DETONÓ LA DETECCIÓN DEL ATAQUE, ASÍ COMO LOS 5 PAQUETES SUCESIVOS. ESTOS PAQUETES PUEDEN SER VISUALIZADOS POR UNA HERRAMIENTA QUE SOPORTE EL FORMATO

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			PCAP. o SE INCLUYE PROTECCIÓN CONTRA AMENAZAS AVANZADAS Y PERSISTENTES (ADVANCED PERSISTENT THREATS). DENTRO DE ESTOS CONTROLES SE INCLUYEN: o 1. PROTECCIÓN CONTRA BOTNETS: SE BLOQUEAN INTENTOS DE CONEXIÓN A SERVIDORES DE BOTNETS, PARA ELLO SE CUENTA CON UNA LISTA DE LOS SERVIDORES DE BOTNET MÁS UTILIZADO. DICHA LISTA SE ACTUALIZA DE FORMA PERIÓDICA POR EL FABRICANTE. o 2. SANDBOXING: LA FUNCIONALIDAD DE SANDBOX HACE QUE EL ARCHIVO SEA EJECUTADO EN UN AMBIENTE SEGURO PARA ANALIZAR SU COMPORTAMIENTO Y, A BASE DEL MISMO, TOMAR UNA ACCIÓN SOBRE EL MISMO. **PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP)** O LA SOLUCIÓN OFRECE LA POSIBILIDAD DE DEFINIR REGLAS QUE PERMITEN ANALIZAR LOS DISTINTOS ARCHIVOS QUE CIRCULAN A TRAVÉS DE LA RED EN BÚSQUEDA DE INFORMACIÓN CONFIDENCIAL. O LA FUNCIONALIDAD SOPORTA EL ANÁLISIS DE ARCHIVOS DEL TIPO: MS-WORD, PDF, TEXTO, ARCHIVOS COMPRIMIDOS. O SE SOPORTA EL ESCANEO DE ARCHIVOS EN LOS SIGUIENTES PROTOCOLOS: HTTP, POP3, SMTP, IMAP, NNTP Y FTP. O ANTE LA DETECCIÓN DE UNA POSIBLE FUGA DE INFORMACIÓN SE PUEDEN APLICAR LAS SIGUIENTES ACCIONES: BLOQUEAR EL TRÁFICO DEL USUARIO, BLOQUEAR EL TRÁFICO DE LA DIRECCIÓN IP DE ORIGEN, REGISTRAR EL EVENTO. O EN CASO DEL BLOQUEO DE USUARIOS, LA SOLUCIÓN PERMITE DEFINIR POR CUÁNTO TIEMPO SE HARÁ EL BLOQUEO O EN SU DEFECTO BLOQUEAR POR TIEMPO INDEFINIDO HASTA QUE EL ADMINISTRADOR TOME UNA ACCIÓN. O LA SOLUCIÓN SOPORTA LA CAPACIDAD DE GUARDAR UNA COPIA DEL ARCHIVO IDENTIFICADO COMO POSIBLE FUGA DE INFORMACIÓN. ESTA COPIA PODRÍA SER ARCHIVADA LOCALMENTE O EN OTRO DISPOSITIVO. O LA SOLUCIÓN PERMITE LA BÚSQUEDA DE PATRONES EN ARCHIVOS MEDIANTE LA DEFINICIÓN DE EXPRESIONES REGULARES. o PROVEE LA FUNCIONALIDAD DE FILTRADO DE FUGA DE INFORMACIÓN. DENTRO DE LAS TÉCNICAS DE DETECCIÓN SE CONSIDERAN COMO MÍNIMO LAS SIGUIENTES: o FILTRADO POR TIPO DE ARCHIVO o FILTRADO POR NOMBRE DE ARCHIVO o FILTRADO POR EXPRESIONES REGULARES: SE DETECTAN LOS ARCHIVOS SEGÚN LAS EXPRESIONES REGULARES QUE SE ENCUENTRAN DENTRO DE LOS MISMOS. o FINGERPRINTING: TOMA UNA MUESTRA DEL ARCHIVO QUE SE CONSIDERA COMO CONFIDENCIAL. SEGÚN ESTO SE BLOQUEAN ARCHIVOS QUE SON IGUALES A ESTA MUESTRA. o WATERMARKING: SE INSERTA UN "SELLO DE AGUA" DENTRO DEL ARCHIVO CONSIDERADO COMO CONFIDENCIAL. DE ACUERDO A ESTO SE ANALIZAN LOS ARCHIVOS EN BUSCA DE ESTE SELLO DE AGUA, ESTE SE DETECTA INCLUSO SI EL ARCHIVO SUFRE CAMBIOS. **CONTROL DE APLICACIONES** O LA SOLUCIÓN SOPORTA LA CAPACIDAD DE IDENTIFICAR LA APLICACIÓN QUE ORIGINA CIERTO TRÁFICO A PARTIR DE LA INSPECCIÓN DEL MISMO. O LA IDENTIFICACIÓN DE LA APLICACIÓN ES INDEPENDIENTE DEL PUERTO Y PROTOCOLO HACIA EL CUAL ESTÉ DIRECCIONADO DICHO TRÁFICO. O LAS SOLUCIÓN TIENE UN LISTADO DE 3,000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE. O EL LISTADO DE APLICACIONES SE ACTUALIZA PERIÓDICAMENTE. O PARA APLICACIONES IDENTIFICADAS PUEDEN DEFINIRSE LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. O PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) PUEDEN DEFINIRSE LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOGS. O PARA APLICACIONES DE TIPO P2P PUEDE DEFINIRSE ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING. O PREFERENTEMENTE SOPORTA MAYOR GRANULARIDAD EN LAS ACCIONES. **INSPECCIÓN DE CONTENIDO SSL** O LA SOLUCIÓN SOPORTA LA CAPACIDAD DE INSPECCIONAR TRÁFICO QUE ESTÉ SIENDO ENCRIPTADO MEDIANTE TLS PARA LOS SIGUIENTES PROTOCOLOS: HTTPS, IMAPS, SMTPS, POP3S.

OPERADO CON RECURSOS 2018

FAS

Partida	Cant.	Unidad de Medida	Descripción
			O LA INSPECCIÓN SE REALIZA MEDIANTE LA TÉCNICA CONOCIDA COMO HOMBRE EN EL MEDIO (MITM - MAN IN THE MIDDLE). O LA INSPECCIÓN DE CONTENIDO ENCRIPTADO NO REQUIERE NINGÚN CAMBIO DE CONFIGURACIÓN EN LAS APLICACIONES O SISTEMA OPERATIVO DEL USUARIO. O PARA EL CASO DE URL FILTERING, ES POSIBLE CONFIGURAR EXCEPCIONES DE INSPECCIÓN DE HTTPS. DICHAS EXCEPCIONES EVITAN QUE EL TRÁFICO SEA INSPECCIONADO PARA LOS SITIOS CONFIGURADOS. LAS EXCEPCIONES PUEDEN DETERMINARSE POR CATEGORÍA DE FILTRADO. o EL EQUIPO TIENE LA CAPACIDAD DE ANALIZAR CONTENIDO CIFRADO (SSL O SSH) PARA LAS FUNCIONALIDADES DE FILTRADO DE URLS, CONTROL DE APLICACIONES, PREVENCIÓN DE FUGA DE INFORMACIÓN, ANTIVIRUS E IPS **SOPORTE DEL FABRICANTE.** "EL PROVEEDOR" INCLUYE EL SOPORTE DEL FABRICANTE PARA LOS BIENES MENCIONADOS, CONSIDERANDO LA VIGENCIA SOLICITADA EN ESTE ANEXO TÉCNICO. INCLUYENDO CON ELLO QUE "EL ESTADO" CUENTA CON EL RESPALDO DEL FABRICANTE PARA ESCALAR FALLAS QUE REQUIERAN DE ANÁLISIS, DIAGNÓSTICO Y SOLUCIÓN DE FALLAS, ASÍ COMO PARA EL REEMPLAZO AVANZADO DE PARTES, CON LOS SIGUIENTES ALCANCES ADICIONALES CON RESPECTO A LOS EQUIPOS: o ACCESO A ACTUALIZACIONES DE LOS SERVICIOS DE SEGURIDAD o ACCESO A LA BASE DE DATOS DE CONOCIMIENTO DEL FABRICANTE EN UN ESQUEMA 24X7 o SOPORTE TELEFÓNICO 24X7 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES o SOPORTE WEB 24X7 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES o SOPORTE VÍA CHAT 24X7 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES o SOPORTE DE SOFTWARE CON RELEASES DE MANTENIMIENTO Y UPGRADES A NUEVAS VERSIONES **RESPALDO DE FABRICANTE** LAS LICENCIAS DE SEGURIDAD INFORMÁTICA UTM CUENTAN CON EL RESPALDO POR PARTE DEL FABRICANTE Y "EL PROVEEDOR" ENTREGA, LA SIGUIENTE DOCUMENTACIÓN: o "EL PROVEEDOR" ENTREGA LA DOCUMENTACIÓN EXPEDIDA POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD INFORMÁTICA UTM EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" ES INTEGRADOR AUTORIZADO DE LOS EQUIPOS DEL MAS ALTO NIVEL Y HABILITADOS PARA DISTRIBUIR, IMPLEMENTAR Y BRINDAR SERVICIOS ADMINISTRADOS, AUTORIZADO PARA REVENDER LOS PRODUCTOS/SERVICIOS DEL FABRICANTE. o "EL PROVEEDOR" INCLUYE UN CERTIFICADO O CERTIFICADOS EXPEDIDOS POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD INFORMÁTICA UTM EN LA QUE MANIFIESTA "EL PROVEEDOR" CUENTA CON LAS CERTIFICACIONES REQUERIDAS PARA BRINDAR SERVICIOS DE INSTALACIÓN Y SOPORTE DE LOS EQUIPOS DE SEGURIDAD SOLICITADOS. o "EL PROVEEDOR" CUENTA CON DOS INGENIEROS CERTIFICADOS EN LA SOLUCIÓN PROPUESTA, PARA REALIZAR LAS ACTIVIDADES DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO Y EN MARCHA NIVEL EXPERTO AVALADO POR EL FABRICANTE. o "EL PROVEEDOR" DEMUESTRA SU EXPERIENCIA EN EL SOPORTE DE LAS LICENCIAS DE SEGURIDAD INFORMÁTICA, A TRAVÉS DE LA DOCUMENTACIÓN DE CLIENTES EXCLUSIVAMENTE DE GOBIERNO EN DONDE HAYA INSTALADO EQUIPOS DE LA MISMA MARCA CON CARACTERÍSTICAS SIMILARES A LOS REQUERIDOS POR "EL ESTADO", LA CUAL CONTIENE LA SIGUIENTE INFORMACIÓN: NOMBRE, DIRECCIÓN, TELÉFONO Y CORREO ELECTRÓNICO DE LOS CLIENTES Y UNA DESCRIPCIÓN DEL PROYECTO DE MEDIA CUARTILLA. "EL ESTADO" SE RESERVARÁ EL DERECHO DE VERIFICAR DICHA INFORMACIÓN. **SOPORTE DEL PROVEEDOR** SE INCLUYE EL SERVICIO DE SOPORTE PARA EL EQUIPO: CON LOS SIGUIENTES SERVICIOS: o DURACIÓN DE 12 MESES o ATENCIÓN DE FALLAS CON UN TIEMPO MÁXIMO DE 2 HORAS CON ESQUEMA 5X8. o SE CONSIDERA UN (1) MANTENIMIENTO PREVENTIVO AL AÑO PARA LOS EQUIPOS, PREVIO ACUERDO CON EL USUARIO FINAL. LOS INSUMOS NECESARIOS PARA EL MANTENIMIENTO CORREN POR CUENTA DE "EL PROVEEDOR". o INCLUYE SOPORTE TELEFÓNICO SIN COSTO ADICIONAL EN HORARIO DE LUNES A VIERNES EN HORARIO DE OFICINA.

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			o PARA LOS EQUIPOS O SOFTWARE DE LA SOLUCIÓN DE SEGURIDAD PARA LOS CUALES EL FABRICANTE LIBERE NUEVAS VERSIONES DENTRO DE LA VIGENCIA DE LA PÓLIZA DE SOPORTE, "EL PROVEEDOR" REALIZA LA INSTALACIÓN SIN COSTO PARA "EL ESTADO" DE DICHAS ACTUALIZACIONES. **ASISTENCIA TÉCNICA** "EL PROVEEDOR" CUENTA CON UN CENTRO DE CONSULTA O ASESORÍA TELEFÓNICA QUE PERMITE AL PERSONAL TÉCNICO DE "EL ESTADO" ACLARACIONES Y CONSULTAS SOBRE EL USO Y CONFIGURACIÓN DE LOS EQUIPOS ANTES MENCIONADOS. PARA ESTA CLASE DE SERVICIO NO SE TOTALIZAN HORAS MENSUALES EN UNO O VARIOS EVENTOS Y NO HAY RESTRICCIÓN EN LA DURACIÓN DE CADA EVENTO. LOS DATOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGRA EN EL CONTROL DE EVENTOS E INCIDENTES SON: o IDENTIFICADOR DEL REPORTE O NÚMERO DE INCIDENTE O EVENTO o IDENTIFICADOR DEL USUARIO QUE REPORTA. ESTOS SON LOS DATOS QUE IDENTIFICAN AL USUARIO QUE LEVANTÓ EL REPORTE. NOMBRE, TELÉFONO, CORREO ELECTRÓNICO Y UBICACIÓN. LA DEFINICIÓN FINAL DE ESTOS DATOS SE ACORDARÁ CON "EL PROVEEDOR" o HORA EN QUE REPORTA EL PROBLEMA POR PARTE DEL USUARIO AUTORIZADO o TIPO DE FALLO o DESCRIPCIÓN DEL FALLO o TIEMPO DE SOLUCIÓN DEL INCIDENTE Y RESTABLECIMIENTO DEL SERVICIO. **TIEMPOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN** EL TIEMPO DEL INICIO DE ATENCIÓN O RESPUESTA A UN REPORTE EFECTUADO A "EL PROVEEDOR", QUIEN PROPORCIONA UN FOLIO DE ATENCIÓN AL RECIBIRLO TIEMPO MÁXIMO DE SOLUCIÓN DE FALLAS DESPUÉS DEL INICIO DE LA ATENCIÓN: 2 HORAS COMO MÁXIMO PARA INICIO DE DIAGNÓSTICO, EN EL CASO DE FALLAS MAYORES SU ATENCIÓN SE CONTINUA AÚN FUERA DE HORARIO DE COBERTURA HASTA SU SOLUCIÓN, SIN NINGÚN COSTO, SIEMPRE QUE HAYA INICIADO SU ATENCIÓN DENTRO DEL HORARIO DE SERVICIO. EN EL CASO DE QUE EN ALGUNA REPARACIÓN DE LOS EQUIPOS SE REQUIERA CAMBIO O SUSTITUCIÓN DE ALGUNA PARTE O COMPONENTE, "EL PROVEEDOR" TIENE LA OBLIGACIÓN DE REMPLAZARLO EN SITIO, DENTRO DEL TIEMPO MÁXIMO DE ATENCIÓN DEL REPORTE. SI EL EQUIPO NO PUEDE REPARARSE DENTRO DE LOS TIEMPOS ESTABLECIDOS, "EL PROVEEDOR" SUSTITUYE EL EQUIPO O PARTE DAÑADA CON EQUIPO DE RESPALDO QUE CUENTA CON LAS MISMAS CARACTERÍSTICAS O SUPERIORES QUE EL EQUIPO ORIGINAL, ESTA SUSTITUCIÓN SE EFECTÚA DENTRO DE LOS TIEMPOS MÁXIMOS DE ATENCIÓN DEFINIDOS Y PERMANECE DURANTE EL TIEMPO QUE TARDA LA COMPOSTURA DEL EQUIPO DAÑADO. EN EL CASO DE QUE EXISTAN EQUIPOS DE RESPALDO INSTALADOS AL TÉRMINO DEL CONTRATO, ESTOS SIGUEN DANDO EL SERVICIO HASTA QUE SE REPAREN LOS EQUIPOS DAÑADOS, AÚN CUANDO HAYA TERMINADO LA VIGENCIA DEL CONTRATO, EXTENDIÉNDOSE LOS DERECHOS QUE SE OTORGAN PARA ESTOS REPORTES DE FALLA, EN LOS TÉRMINOS ORIGINALES. SI DESPUÉS DE REALIZAR EL MANTENIMIENTO CORRECTIVO A UN EQUIPO, ESTE VUELVE A PRESENTAR LA MISMA FALLA, SE CONSIDERA COMO NO REALIZADO Y SU REPARACIÓN SE REALIZARÁ SIN CARGO ALGUNO. "EL PROVEEDOR" ESTA OBLIGADO A CONTINUAR CON LA ATENCIÓN, SIN COSTO, DE FALLAS O PROBLEMAS DETECTADOS DENTRO DE LA VIGENCIA DEL CONTRATO HASTA SU SOLUCIÓN, AÚN CUANDO ÉSTA, SE EXTIENDA MÁS ALLÁ DE AQUÉLLA; PRORROGÁNDOSE LOS DERECHOS QUE OTORGA DICHO CONTRATO PARA ESTOS REPORTES DE FALLA, EN LOS TÉRMINOS ORIGINALES. **MANTENIMIENTO PREVENTIVO** EL MANTENIMIENTO PREVENTIVO SE DA A TODOS Y CADA UNO DE LOS EQUIPOS INVENTARIADOS SEÑALADOS EN EL PROGRAMA DE MANTENIMIENTO PREVENTIVO, 1 (UNA) VEZ DURANTE LA VIGENCIA DEL CONTRATO, CON EXCEPCIÓN ÚNICA EN AQUELLOS CASOS EN DONDE LOS EQUIPOS NO PUEDEN DEJAR DE OPERAR, EN CUYO CASO "EL PROVEEDOR" NOTIFICA PARA QUE DE MANERA CONJUNTA SE PROGRAMEN. EL MANTENIMIENTO SE PROPORCIONADO AL "HARDWARE" Y AL "SOFTWARE" QUE COMPONEN LOS EQUIPOS, CON LA FINALIDAD DE MANTENER LA VIGENCIA TECNOLÓGICA DEL EQUIPO, ESTE MANTENIMIENTO INCLUYE LAS ACTUALIZACIONES DEL "SOFTWARE" A LA ÚLTIMA VERSIÓN GRATUITA EMITIDA POR EL FABRICANTE Y QUE NO REQUIERAN MODIFICACIONES EN EL HARDWARE DEL EQUIPO.

PERMANECIÓN RECIBIDOS
2018

FASP

Partida	Cant.	Unidad de Medida	Descripción
			"EL PROVEEDOR" PROPORCIONA, POR ESCRITO, UN ANALISIS EXPERTO DEL ESTADO QUE GUARDA EL HARDWARE Y SOFTWARE, CON LA FINALIDAD DE GARANTIZAR UN ÓPTIMO NIVEL DEL FUNCIONAMIENTO DE LOS EQUIPOS. SE ELABORAN Y REVISAN CONJUNTAMENTE CON EL PERSONAL TÉCNICO DE "EL PROVEEDOR", EL PROGRAMA DE TRABAJO, LAS ACTIVIDADES Y FECHAS DEL MANTENIMIENTO PREVENTIVO A DETALLE; CON CANTIDADES, NOMBRES DE LOS RESPONSABLES A EJECUTAR Y SUPERVISAR LA APLICACIÓN DE DICHOS SERVICIOS, A MÁS TARDAR EN LA SEGUNDA SEMANA CONTADA A PARTIR DE LA FORMALIZACIÓN DEL CONTRATO. SE ENTREGA COPIA DE LOS PROGRAMAS, PROCEDIMIENTOS O CALENDARIOS FORMALIZADOS CONJUNTAMENTE EN LA FASE DE REVISIÓN. EN CASO DE QUE EXISTAN MODIFICACIONES AL PROGRAMA VALIDADO, ESTAS SE REGISTRAN POR ESCRITO Y DE COMÚN ACUERDO ENTRE AMBAS PARTES. PARA EL CUMPLIMIENTO DEL PROGRAMA DE MANTENIMIENTO PREVENTIVO, "EL PROVEEDOR" PRESENTA POR ESCRITO LOS RECURSOS HUMANOS Y TÉCNICOS, ASÍ COMO PROTOCOLOS DE PRUEBA, CON LOS QUE CUBRE EL SERVICIO. **MANTENIMIENTO CORRECTIVO** "EL PROVEEDOR" PROPORCIONA LOS MANTENIMIENTOS CORRECTIVOS SURGIDOS DURANTE LA VIGENCIA DEL CONTRATO, AL HARDWARE Y SOFTWARE DEL EQUIPO, EN EL CUAL INCLUYEN LAS REFACCIONES Y/O PARTES ORIGINALES Y ACTUALIZACIONES DEL "SOFTWARE" QUE SE REQUIEREN PARA REPARACIONES DEL EQUIPO, ASÍ MISMO SE SUMINISTRA LA MANO DE OBRA PARA SU INSTALACIÓN. LOS EQUIPOS QUE SE UTILICEN EN TODOS LOS CASOS, TIENEN CALIDAD Y CARACTERÍSTICAS TÉCNICAS IGUALES O SUPERIORES A LAS DEL EQUIPO ORIGINAL, DE TAL MANERA QUE SE GARANTIZA EL FUNCIONAMIENTO ADECUADO DEL HARDWARE Y SOFTWARE. SE APLICAN PRUEBAS DE DIAGNÓSTICO Y OPERACIÓN DE RESPALDO ANTES DE PROCEDER A LA REPARACIÓN DEL MISMO, SEGÚN RESULTE EL DIAGNÓSTICO APLICADO. AL FINALIZAR SE ENTREGA COPIA DEL REPORTE DE SERVICIO DE MANTENIMIENTO CORRECTIVO. EN EL CASO DE UNA CONTINGENCIA MAYOR O DE SEVERIDAD CRÍTICA, "EL PROVEEDOR" ASIGNA UN INGENIERO EN SITIO HASTA LA RESOLUCIÓN TOTAL DEL PROBLEMA. **PROCEDIMIENTO DE ESCALAMIENTO** SE INCLUYE UNA RELACIÓN CON NOMBRES DE RESPONSABLES, TELÉFONOS, CORREOS ELECTRÓNICOS Y CELULARES, ASÍ COMO LOS HORARIOS DE ATENCIÓN PARA LEVANTAR REPORTES DE MANTENIMIENTO CORRECTIVO, ASÍ COMO LOS NÚMEROS DE RADIOLOCALIZADORES PARA REPORTAR FALLAS FUERA DE LOS HORARIOS DE SERVICIO, LOS TIEMPOS DE RESPUESTA SE SUJETAN TAMBIÉN A LO ESTIPULADO EN EL PUNTO DE "TIEMPOS MÁXIMOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN" DE ESTE ANEXO. CONTIENE EL PROCEDIMIENTO DE ESCALAMIENTO DESDE EL MOMENTO EN QUE SE REPORTE UNA FALLA EN UN EQUIPO HASTA SU SOLUCIÓN Y LOS NOMBRES Y CARGOS DE LOS RESPONSABLES EN CADA PROCESO.
			(1) LICENCIA PARA CONMUTADOR TELEFÓNICO CON PÓLIZA DE SOPORTE SE INCLUYE LA RENOVACIÓN DE LA PÓLIZA DE SOPORTE CORRESPONDIENTE AL CONMUTADOR TELEFÓNICO ALCATEL OMNIPCX ENTERPRISE CPU ID F104CA99, LA CUAL ES POR UN PERIODO DE 36 MESES Y CUMPLE CON LAS SIGUIENTES ESPECIFICACIONES: MARCA: ALCATEL LICENCIA: SOLUTION PREMIER SERVICE 1. INCLUYE UNA MESA DE AYUDA 5X8 POR 36 MESES. 2. INCLUYE UN ANÁLISIS REMOTO DE ERROR Y PROPUESTA INICIAL DE SOLUCIÓN. 3. EL SOPORTE TELEFÓNICO ES ATENDIDO 5X8 CON TIEMPO DE RESPUESTA DE 2 HORAS PARA REPORTES CON PRIORIDAD 1. 4. SOPORTE TELEFÓNICO ES ATENDIDO 5X8 CON TIEMPO DE RESPUESTA DE 2 HORAS PARA REPORTES CON PRIORIDAD 2. 5. EL SOPORTE EN SITIO ES 5X8 CON TIEMPO DE RESPUESTA AL DÍA SIGUIENTE PARA REPORTES CON PRIORIDAD 1. 6. SOPORTE EN SITIO ES 5X8 CON TIEMPO DE RESPUESTA AL DÍA SIGUIENTE PARA REPORTES CON PRIORIDAD 2. 7. EL TIEMPO DE INGENIERO EN SITIO SE DETERMINA UNA VEZ CONCLUIDO EL PRIMER DIAGNÓSTICO. 8. SE INCLUYEN ACTUALIZACIONES DE LICENCIAS DE MODO REMOTO

Partida	Cant.	Unidad de Medida	Descripción
			9. INCLUYE REFACCIONES PARA EL MANTENIMIENTOS CORRECTIVOS LOS CUALES SON 100% COMPATIBLE CON EL CONMUTADOR TELEFÓNICO ALCATEL OMNIPCX ENTERPRISE 10. CON RESPECTO AL SISTEMA DE PROTECCIÓN CONTRA DESCARGAR ATMOSFÉRICAS, SE CONSIDERAN LAS ADECUACIONES NECESARIAS PARA EL CORRECTO FUNCIONAMIENTO DE LOS EQUIPOS. EL CONMUTADOR TELEFÓNICO ALCATEL OMNIPCX ENTERPRISE CUENTA CON SOPORTE DIRECTO DE FABRICANTE DURANTE EL PERIODO DE LA GARANTÍA, EL CUAL PERMITE OBTENER LAS ACTUALIZACIONES DE SOFTWARE MAYORES Y MENORES, PARCHES Y FIXES. "EL PROVEEDOR" REALIZA LA INSTALACIÓN DE DICHAS ACTUALIZACIONES DE SOFTWARE SIN COSTO PARA EL USUARIO, DURANTE EL PERIODO DE VIGENCIA. **REPORTE DE FALLAS** "EL PROVEEDOR" CUENTA CON UNA MESA DE SERVICIO BASADA EN ITIL PARA RECIBIR CUALQUIER EVENTO RELACIONADO CON LA OPERACIÓN DEL CONMUTADOR TELEFÓNICO POR PARTE DEL USUARIO. SE ANEXAN LOS CERTIFICADOS ITIL DE 3 PERSONAS DE LA MESA DE AYUDA. ESTE CENTRO DE ATENCIÓN ES PROPIO DE "EL PROVEEDOR" Y ESTA UBICADO EN SUS INSTALACIONES, MEDIANTE EL USO DE SUS PROPIAS HERRAMIENTAS Y DE MANERA DEDICADA PARA EL SOPORTE DE LA INFRAESTRUCTURA DE COMUNICACIONES. LAS TAREAS MÍNIMAS QUE "EL PROVEEDOR" REALIZA CON LA MESA DE AYUDA SON: RECIBIR, REGISTRAR, ANALIZAR, RESOLVER Y CANALIZAR LOS REPORTES DE INCIDENTES O FALTAS, DAR SEGUIMIENTO Y SOLUCIÓN A LOS REPORTES INFORMANDO A LOS USUARIOS OPORTUNAMENTE; ASÍ MISMO, GENERARÁ UN REGISTRO HISTÓRICO QUE PERMITA CONSULTAS, GENERACIÓN DE REPORTES Y SEGUIMIENTO SOBRE EL TIPO DE FALLAS PRESENTADAS Y LA FORMA COMO SE SOLUCIONARON. LA ATENCIÓN Y SOPORTE SON POSIBLES A TRAVÉS DE UN NÚMERO TELEFÓNICO ÚNICO CON SERVICIO 01-800 SIN COSTO ADICIONAL PARA EL USUARIO Y A TRAVÉS DE CORREO O UNA PÁGINA WEB LOS DATOS MÍNIMOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGREN EN EL CONTROL DE EVENTOS E INCIDENTES SERÁN: O IDENTIFICADOR DEL REPORTE O NÚMERO DE INCIDENTE O EVENTO O IDENTIFICADOR DEL USUARIO QUE REPORTA. ESTOS SON LOS DATOS QUE IDENTIFICAN AL USUARIO QUE LEVANTÓ EL REPORTE. NOMBRE, TELÉFONO, CORREO ELECTRÓNICO Y UBICACIÓN. O HORA EN QUE REPORTA EL PROBLEMA POR PARTE DEL USUARIO AUTORIZADO O TIPO DE FALLO O DESCRIPCIÓN DEL FALLO O TIEMPO DE SOLUCIÓN DEL INCIDENTE Y RESTABLECIMIENTO DEL SERVICIO. CUENTA CON 2 PERSONAS CERTIFICADAS EN EL PRODUCTO. "EL PROVEEDOR" TIENE LAS SIGUIENTES RESPONSABILIDADES: O IDENTIFICAR LA CAUSA DE LA RAÍZ DE TALES PROBLEMAS O ASEGURAR QUE LOS RECURSOS APROPIADOS SE ASIGNEN CONFORME SEA NECESARIO PARA IDENTIFICAR, SOLVENTAR LA FALLA, Y DAR SEGUIMIENTO AL INFORME SOBRE CUALQUIER CONSECUENCIA DE LA FALLA. O PROPORCIONAR AL CLIENTE UN REPORTE ESCRITO DETALLADO QUE INFORME LA CAUSA Y EL PROCEDIMIENTO PARA CORREGIRLA O MITIGARLA CUANDO SEA POSIBLE. PROPORCIONAR ACTUALIZACIONES DE MANERA MENSUAL. O VERIFICAR QUE TODAS LAS ACCIONES NECESARIAS SE HAN TOMADO PARA PREVENIR LA REPETICIÓN DE TAL FALLA. O MANTENER LOS PROCESOS DE ADMINISTRACIÓN DE CAMBIOS, INCLUYENDO LOS PROCEDIMIENTOS Y MÉTODOS VIGENTES PARA LOS CAMBIOS. O MANTENER LAS HERRAMIENTAS Y PROCESOS DE ADMINISTRACIÓN DE PROBLEMAS PARA LA GESTIÓN DE TODOS LOS PROBLEMAS Y ACCIONES PREVENTIVAS DESDE LA IDENTIFICACIÓN DE LA CAUSA RAÍZ HASTA EL CIERRE DEL PROBLEMA. O PREPARAR Y COMUNICAR LOS IMPACTOS MEDIANTE LA DOCUMENTACIÓN DE LA CAUSA RAÍZ DEL PROBLEMA, LOS ESFUERZOS PARA CORREGIR TEMPORAL O PERMANENTEMENTE EL PROBLEMA Y LOS SIGUIENTES PASOS PARA SU SEGUIMIENTO. O ESCALACIÓN DE LOS PROBLEMAS QUE HAYAN REBASADO LOS UMBRALES DE

Partida	Cant.	Unidad de Medida	Descripción
			RESPUESTA BASADOS EN LA SEVERIDAD DEL PROBLEMA. **SOPORTE POR PARTE DEL FABRICANTE** "EL PROVEEDOR" INCLUYE LA SIGUIENTE DOCUMENTACIÓN: • DOCUMENTACIÓN EXPEDIDA POR EL POR EL FABRICANTE DE LOS CONMUTADOR TELEFÓNICO EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" CUENTA CON EL NIVEL DE CERTIFICACIÓN ADECUADA PARA PROPORCIONAR SERVICIO TÉCNICO AL EQUIPO. • DOS CERTIFICADOS NIVEL EXPERTO EXPEDIDA O AVALADA POR EL POR EL FABRICANTE DEL EQUIPO, PARA REALIZAR LAS ACTIVIDADES DE INSTALACIÓN, CONFIGURACIÓN Y SOPORTE TÉCNICO.
			(1) LICENCIA DE OFFICE 365 PARA 100 USUARIOS LICENCIA: OFFICE O365PROPLUSOPEN LAS SIGUIENTES CARACTERÍSTICAS: • OFFICE COMO SUBSCRIPCIÓN • SE TENDRÁ SIEMPRE LAS ÚLTIMAS VERSIONES DE: • WORD • EXCEL • POWERPOINT • OUTLOOK • ONENOTE • REQUISITOS DEL SISTEMA: WINDOWS, MAC OS
			(1) SISTEMA OPERATIVO WINDOWS PRO 10 64B PARA 50 USUARIOS LICENCIA: WINPRO 10 SNGL OLP NL LEGALIZATION GETGENUINE • SOFTWARE: KIT DE LEGALIZACIÓN • IDIOMA: ESPAÑOL • SISTEMA MÍNIMO REQUERIDO • CPU: 1 GHZ • MEMORIA: 1 GB • ESPACIO EN DISCO: 20 GB • SOPORTE DE ARQUITECTURA • SOPORTA SISTEMAS X86 Y 64-BIT
			(1) LICENCIA DE EQUIPO DE SEGURIDAD PARA EMAIL CON 1 AÑO DE SOPORTE MARCA: FORTINET MODELO: FML-200E SE INCLUYE EL SUMINISTRO E INSTALACIÓN DE LICENCIA Y EQUIPO PARA EL ANÁLISIS Y CONTROL DE ACCESO DE LOS CORREOS ELECTRÓNICOS EL CUAL CUMPLE CON LAS SIGUIENTES CARACTERÍSTICAS Y FUNCIONALIDADES: **PROTECCIÓN.** • SOLUCIÓN COMPLETA INCLUYE LA CAPACIDAD DE PODER REALIZAR ANTISPAM, ANTIVIRUS, ANTISPYWARE Y CONTROL DE GUSANOS. • ES CAPAZ DE PROTEGER CORREO ELECTRÓNICO ENTRANTE (DESDE INTERNET) Y CORREO SALIENTE (HACIA INTERNET). • LA SOLUCIÓN ES CAPAZ DE PROTEGER DE 60,000 VIRUS DIFERENTES Y 300,000 ATAQUES POR VIRUS CONOCIDOS EN TOTAL. • TIENE LA CAPACIDAD DE CONECTARSE EN TIEMPO REAL A UNA BASE DE DATOS CENTRALIZADA DEL FABRICANTE PARA DESCARGAR ACTUALIZACIONES ANTISPAM. • INCLUYE LA PROTECCIÓN CONTRA ATAQUES DE NEGACIÓN DE SERVICIO POR MAIL BOMBING. • INCLUYE VERIFICACIONES DE DNS EN REVERSA PARA PROVEER PROTECCIÓN TIPO ANTI-

OPERADO CON RECURSO
2018
FASP

Partida	Cant.	Unidad de Medida	Descripción
			SPOOFING. • PERMITE LA OPCIÓN DE ESTABLECER LÍMITES EN LA TASA DE CORREOS ENVIADOS (E-MAIL RATE LIMIT). • TIENE LA CAPACIDAD DE SOPORTAR MÚLTIPLES DOMINIOS DE CORREO ELECTRÓNICO. • PERMITE LA POSIBILIDAD DE ESTABLECER POLÍTICAS POR DESTINATARIO/RECEPTOR DE CORREO ELECTRÓNICO POR DOMINIO, PARA CORREO ENTRANTE O CORREO SALIENTE. • TIENE LA CAPACIDAD DE ESTABLECER PERFILES (POLÍTICAS) GRANULARES DE DETECCIÓN DE SPAM Y VIRUS. ES DECIR, PODER DEFINIR CONFIGURACIONES ESPECÍFICAS DE MECANISMOS ANTISPAM/ANTIVIRUS. • PERMITE LA OPCIÓN DE FUNCIONAR COMO SMTP MAIL GATEWAY PARA SERVIDORES DE CORREO ELECTRÓNICO EXISTENTES. • PERMITE RUTEO DE CORREO BASADO EN LDAP. • TIENE LA CAPACIDAD DE PODER HACER CUARENTENA DE CORREO, Y ACCEDER ESA CUARENTENA MEDIANTE WEBMAIL Y POP3. • PERMITE REALIZAR RESÚMENES DIARIOS DE CUARENTENA. • PERMITE EL ALMACENAMIENTO BASADO EN POLÍTICAS PARA DECIDIR EL ALMACENAMIENTO DE CORREO ELECTRÓNICO PARA MENSAJES ENTRANTES Y SALIENTES, INCLUYENDO SOPORTE DE RESPALDO PARA ALMACENAMIENTO REMOTO. • SOPORTA COLAS DE CORREO PARA MENSAJES FALLIDOS, RETARDADOS Y NO ENTREGABLES. • TIENE LA CAPACIDAD DE PODER HACER AUTENTICACIÓN PARA SMTP A TRAVÉS DE LDAP, RADIUS, POP3 O IMAP. • MANTIENE UNA LISTA DE REPUTACIÓN DE REMITENTES LOCALES BASADO EN: NÚMERO DE VIRUS ENVIADOS, CANTIDAD DE SPAM ENVIADO, NÚMERO DE RECEPTORES EQUIVOCADOS. • PERMITE EL FILTRAJE DE ARCHIVOS ANEXOS (ATTACHMENTS) Y CONTENIDO DE MENSAJE DE CORREO. • PERMITE LA INSPECCIÓN PROFUNDA DE CABECERAS DE CORREO. • PERMITE FILTRAJE ESTADÍSTICO BAYESIANO. • TIENE LA CAPACIDAD DE BLOQUEAR USANDO LISTAS EN TIEMPO REAL DE URIS Y/O URLS DE SPAM. • PERMITE EL FILTRAJE POR PALABRA PROHIBIDA (BANNED WORD). • PERMITE LA ADMINISTRACIÓN DE SPAM CON CAPACIDADES DE ACEPTAR, REENVIAR (RELAY) RECHAZAR (REJECT) O DESCARTAR (DISCARD). • PERMITE EL RASTREO POR ANÁLISIS DE IMÁGENES PARA DETECTAR SPAM. • PERMITE EL SOPORTE A LISTAS NEGRAS (BLACKLIST) DE TERCEROS. • PERMITE REVISIÓN TIPO LISTA GRIS (GRAYLIST). • PERMITE LA REVISIÓN DE IPS FALSIFICADAS (FORGED IP). • PERMITE LISTAS NEGRAS Y BLANCAS (USUARIOS/IPS PERMITIDOS O NEGADOS) A NIVEL GLOBAL POR EQUIPO Y PERSONALIZADO POR USUARIO. • SOPORTA EL RASTREO DE ANTIVIRUS/ANTISPYWARE DE ARCHIVOS COMPRIMIDOS Y ANIDADOS. • TIENE LA POSIBILIDAD DE REEMPLAZO/EDICIÓN DE MENSAJES DE NOTIFICACIÓN EN ANTIVIRUS/ANTISPYWARE. • INCLUYE EL BLOQUEO POR TIPO DE ARCHIVO EN ANTIVIRUS/ANTISPYWARE. • SOPORTA LA PERSISTENCIA DE BASE DE DATOS DE GRAYLIST. • SOPORTA MODOS DE OPERACIÓN DONDE EL DISPOSITIVO DE PROTECCIÓN ANTISPAM SE ENCUENTRA EN MODO TRANSPARENTE (BRIDGE), EN MODO GATEWAY (RELAY) O EN MODO SERVIDOR (DONDE SOPORTE CUENTAS LOCALES DE CORREO ELECTRÓNICO CON ACCESO SMTP, POP3, IMAP) • SOPORTA ALMACENAMIENTO LOCAL O REMOTO DE LOS CORREOS ELECTRÓNICOS QUE HAN PASADO A TRAVÉS DEL DISPOSITIVO. • PERMITE LA UTILIZACIÓN DE UN AGENTE DE TRANSFERENCIA DE CORREO (MTA) BASADO EN ESTÁNDARES. • POR SEGURIDAD Y EFICIENCIA, EL SISTEMA TIENE PROPÓSITO ESPECÍFICO BASADO EN UN SISTEMA OPERATIVO PRE-ENDURECIDO/ASEGURADO. NO SE ACEPTARÁN DISPOSITIVOS BASADOS EN HARDWARE GENÉRICO Y/O CON SISTEMAS OPERATIVOS GENÉRICOS. **ADMINISTRACIÓN.** • INCLUYE INTERFACE DE CONFIGURACIÓN VÍA WEB (HTTP, HTTPS). • LOS ADMINISTRADORES SON POR DOMINIO Y PUEDE ASIGNARSE DE QUÉ EQUIPOS (POR DIRECCIÓN IP Y MÁSCARA) PUEDE EL ADMINISTRADOR CONECTARSE.

OPERADO CON RECURSO FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			• SOPORTA DOS NIVELES DE ADMINISTRACIÓN: LECTURA/ESCRITURA (READ/WRITE) Y SÓLO LECTURA (READ-ONLY). • SOPORTA UN SNMP VERSIÓN 1 / VERSIÓN 2 USANDO MIBS ESTÁNDARES Y MIBS PRIVADOS CON TRAPS BASADAS EN UMBRALES. • SOPORTA UN REGISTRO (LOGGING) DE INCIDENTES ANTIVIRUS. • SOPORTA REGISTRO (LOGGING) DE ACTIVIDAD ANTISPAM. • SOPORTA A UN SYSLOG LOCAL O EXTERNO. **REPORTES.** • PERMITE LA GENERACIÓN DE REPORTES DE ACTIVIDAD ANALIZANDO LOS ARCHIVOS DE BITÁCORAS (LOGS) Y PRESENTAR LA INFORMACIÓN EN TABLAS (FORMA TABULAR) Y EN FORMA GRÁFICA. • PERMITE LA GENERACIÓN DE REPORTES BAJO DEMANDA O UN REPORTE CALENDARIZADO EN INTERVALOS ESPECÍFICOS. • INCLUYE 100 DIFERENTES TIPOS DE REPORTES EN CINCO CATEGORÍAS DISTINTAS, PARA EL DIFERENTE TIPO DE ACTIVIDAD REGISTRADO. • PERMITE QUE LOS REPORTES PUEDEN SER GENERADOS Y ENVIADOS COMO PDF **ALTA DISPONIBILIDAD** • SOPORTA EL MONITOREO DE ENLACES. • SOPORTA EL FAILOVER DE ENLACES. • SOPORTA CAPACIDADES DE CONFIGURACIÓN DE EQUIPOS EN ACTIVO-PASIVO. • SOPORTA SINCRONIZACIÓN DE DATOS DE CORREO. • SOPORTA PASO A EQUIPO SECUNDARIO CON CONSERVACIÓN DE ESTADO (STATEFUL FAILOVER). • PERMITE LA DETECCIÓN Y NOTIFICACIÓN DE FALLA DE DISPOSITIVOS. **ESTÁNDARES Y CERTIFICACIONES** EL EQUIPO CUMPLE CON LOS SIGUIENTES ESTÁNDARES DE INTERNET RFC • RFC 1869 - SMTP SERVICE EXTENTIONS • RFC 1891 - SMTP DELIVERY STATUS NOTIFICATIONS • RFC 1892 - MULTIPART / REPORT • RFC 1893 - MAIL SYSTEM STATUS CODES • RFC 1894 - DELIVERY STATUS NOTIFICATIONS • RFC 1985 - SMTP SERVICE EXTENTION FOR REMOTE MESSAGE QUEUE STARTING • RFC 2034 - SMTP SERVICE EXTENTIONS FOR RETURNING ENHANCED ERROR CODES • RFC 2045 - MIME • RFC 2505 - ANTISPAM RECOMMENDATIONS FOR SMTP MTAS • RFC 2554 - SMTP SERVICE EXTENSION FOR AUTHENTICATION • RFC 2821 - SMTP (SIMPLE MAIL TRANSFER PROTOCOL) • RFC 2822 - INTERNET MAIL HEADER FORMAT **LICENCIAMIENTO Y ACTUALIZACIONES** • TAMAÑO DE LICENCIA. NO TIENE RESTRICCIÓN POR LICENCIA EN CUANTO A USUARIOS O BUZONES DE CORREO (MAILBOXES) A SER PROTEGIDOS. • VIGENCIA DE LICENCIA DE ACTUALIZACIÓN. INCLUYE LA CAPACIDAD DE PODER HACER ACTUALIZACIONES DE FIRMAS ANTISPAM, ANTIVIRUS Y CUALQUIER OTRA ACTUALIZACIÓN NECESARIA PARA LA CORRECTA OPERACIÓN DEL EQUIPO CON LAS CARACTERÍSTICAS ARRIBA DESCRITAS, POR ESPACIO MÍNIMO DE 1 AÑO. **DESEMPEÑO / ALMACENAMIENTO/ CONECTIVIDAD / ALIMENTACIÓN** EL EQUIPO OFRECE LAS SIGUIENTES CARACTERÍSTICAS DE DESEMPEÑO Y CONECTIVIDAD. CONECTIVIDAD: • INTERFACES GIGABIT ETHERNET: 4, RJ45. • DISCO DURO DE 1TB. • PERFILES ANTIVIRUS/ANTISPAM PARA EL FILTRAJE DE CORREOS DEFINIBLES POR EQUIPO 50 PARA DOMINIOS Y 60 POR SISTEMA • NÚMERO DE POLÍTICAS BASADAS EN DESTINATARIO/RECEPTOR DE CORREO PARA CORREO ENTRANTE/SALIENTE POR DOMINIO DE CORREO 60. • NÚMERO DE POLÍTICAS BASADAS EN DESTINATARIO/RECEPTOR DE CORREO PARA CORREO ENTRANTE/SALIENTE POR SISTEMA DE CORREO 300.

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			• DESEMPEÑO EN MENSAJES PARA CORREO POR HORA DEFINIBLES A UN TAMAÑO PROMEDIO DE MENSAJE DE 100 KB EN MODO REENVÍO DE CORREO SOLAMENTE (SIN ANTISPAM NI ANTIVIRUS) 80 MIL. • DESEMPEÑO EN MENSAJES PARA CORREO POR HORA DEFINIBLES A UN TAMAÑO PROMEDIO DE MENSAJE DE 100 KB EN MODO DE FILTRAJE ANTISPAM • 71 MIL. • DESEMPEÑO EN MENSAJES PARA CORREO POR HORA DEFINIBLES A UN TAMAÑO PROMEDIO DE MENSAJE DE 100 KB EN MODO DE FILTRAJE ANTISPAM MAS ANTIVIRUS 61K • CAPACIDAD DEL EQUIPO PARA SOPORTAR 150 MAILBOXES EN MODO SERVIDOR. **SOPORTE DEL FABRICANTE.** "EL PROVEEDOR" INCLUYE EL SOPORTE DEL FABRICANTE PARA LOS BIENES MENCIONADOS, CONSIDERANDO LA VIGENCIA SOLICITADA EN ESTE ANEXO TÉCNICO. INCLUYENDO. CON ELLO QUE "EL ESTADO" CUENTA CON EL RESPALDO DEL FABRICANTE PARA ESCALAR FALLAS QUE REQUIERAN DE ANÁLISIS, DIAGNÓSTICO Y SOLUCIÓN DE FALLAS, ASÍ COMO PARA EL REEMPLAZO AVANZADO DE PARTES, CON LOS SIGUIENTES ALCANCES ADICIONALES CON RESPECTO A LOS EQUIPOS: • DURACIÓN DE 12 MESES • ACCESO A LA BASE DE DATOS DE CONOCIMIENTO DEL FABRICANTE EN UN ESQUEMA 8X5 • SOPORTE TELEFÓNICO 8X5 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE WEB 8X5 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE VÍA CHAT 8X5 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE DE SOFTWARE CON RELEASES DE MANTENIMIENTO Y UPGRADES A NUEVAS VERSIONES • SOPORTE DE HARDWARE **RESPALDO DE FABRICANTE** LAS LICENCIAS DE SEGURIDAD INFORMÁTICA SOLICITADA EN ESTE CONCEPTO CUENTAN CON EL RESPALDO POR PARTE DEL FABRICANTE Y "EL PROVEEDOR" ENTREGA LA SIGUIENTE DOCUMENTACIÓN: • DOCUMENTACIÓN EXPEDIDA POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD DE CORREO ELECTRÓNICO EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" ES INTEGRADOR AUTORIZADO DE LOS EQUIPOS DEL MAS ALTO NIVEL Y HABILITADOS PARA DISTRIBUIR, IMPLEMENTAR Y BRINDAR SERVICIOS ADMINISTRADOS, AUTORIZADO PARA REVENDER LOS PRODUCTOS/SERVICIOS DEL FABRICANTE. • CARTA CERTIFICADO O CERTIFICADOS EXPEDIDOS POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS SEGURIDAD DE CORREO ELECTRÓNICO EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" CUENTA CON LAS CERTIFICACIONES REQUERIDAS PARA BRINDAR SERVICIOS DE INSTALACIÓN Y SOPORTE DE LOS EQUIPOS DE SEGURIDAD SOLICITADOS. • DOS INGENIEROS CERTIFICADOS EN LA SOLUCIÓN PROPUESTA, PARA REALIZAR LAS ACTIVIDADES DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO Y EN MARCHA. NIVEL EXPERTO AVALADO POR EL FABRICANTE. • "EL PROVEEDOR" DEMUESTRA SU EXPERIENCIA EN EL SOPORTE DE LAS LICENCIAS DE SEGURIDAD INFORMÁTICA SOLICITADO, A TRAVÉS DE LA DOCUMENTACIÓN DE CLIENTES EXCLUSIVAMENTE DE GOBIERNO EN DONDE HAYA INSTALADO EQUIPOS DE LA MISMA MARCA CON CARACTERÍSTICAS SIMILARES A LOS REQUERIDOS POR "EL ESTADO", LA CUAL CONTIENE LA SIGUIENTE INFORMACIÓN: NOMBRE, DIRECCIÓN, TELÉFONO Y CORREO ELECTRÓNICO DE LOS CLIENTES Y UNA DESCRIPCIÓN DEL PROYECTO DE MEDIA CUARTILLA. "EL ESTADO" SE RESERVARÁ EL DERECHO DE VERIFICAR DICHA INFORMACIÓN. **SOPORTE DEL PROVEEDOR** SE INCLUYE EL SERVICIO DE SOPORTE PARA EL EQUIPO/LICENCIA: CON LOS SIGUIENTES SERVICIOS: • DURACIÓN DE 12 MESES • ATENCIÓN DE FALLAS CON UN TIEMPO MÁXIMO DE 2 HORAS CON ESQUEMA 5X8. • SE CONSIDERA UN (1) MANTENIMIENTO PREVENTIVO AL AÑO PARA LOS EQUIPOS, PREVIO ACUERDO CON "EL ESTADO". LOS INSUMOS NECESARIOS PARA EL MANTENIMIENTO CORREN POR CUENTA DE "EL PROVEEDOR". • INCLUYE SOPORTE TELEFÓNICO SIN COSTO ADICIONAL EN HORARIO DE LUNES A

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			VIERNES EN HORARIO DE OFICINA. • PARA LOS EQUIPOS O SOFTWARE DE LA SOLUCIÓN DE SEGURIDAD PARA LOS CUALES EL FABRICANTE LIBERE NUEVAS VERSIONES DENTRO DE LA VIGENCIA DE LA PÓLIZA DE SOPORTE, "EL PROVEEDOR" REALIZA LA INSTALACIÓN SIN COSTO PARA "EL ESTADO" DICHAS ACTUALIZACIONES. **ASISTENCIA TÉCNICA** "EL PROVEEDOR" CUENTA CON UN CENTRO DE CONSULTA O ASESORÍA TELEFÓNICA QUE PERMITE AL PERSONAL TÉCNICO DE "EL ESTADO" REALIZAR ACLARACIONES Y CONSULTAS SOBRE EL USO Y CONFIGURACIÓN DE LOS EQUIPOS ANTES MENCIONADOS. PARA ESTA CLASE DE SERVICIO NO SE TOTALIZAN HORAS MENSUALES EN UNO O VARIOS EVENTOS Y NO HAY RESTRICCIÓN EN LA DURACIÓN DE CADA EVENTO. LOS DATOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGRA EN EL CONTROL DE EVENTOS E INCIDENTES SON: • IDENTIFICADOR DEL REPORTE O NÚMERO DE INCIDENTE O EVENTO • IDENTIFICADOR DEL USUARIO QUE REPORTA. ESTOS SON LOS DATOS QUE IDENTIFICAN AL USUARIO QUE LEVANTÓ EL REPORTE. NOMBRE, TELÉFONO, CORREO ELECTRÓNICO Y UBICACIÓN. LA DEFINICIÓN FINAL DE ESTOS DATOS SE ACORDARÁ CON EL "EL PROVEEDOR" • HORA EN QUE REPORTA EL PROBLEMA POR PARTE DEL USUARIO AUTORIZADO • TIPO DE FALLO • DESCRIPCIÓN DEL FALLO • TIEMPO DE SOLUCIÓN DEL INCIDENTE Y RESTABLECIMIENTO DEL SERVICIO. **TIEMPOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN** EL TIEMPO DEL INICIO DE ATENCIÓN O RESPUESTA A UN REPORTE EFECTUADO "EL PROVEEDOR" PROPORCIONA UN FOLIO DE ATENCIÓN AL RECIBIRLO. TIEMPO MÁXIMO DE SOLUCIÓN DE FALLAS DESPUÉS DEL INICIO DE LA ATENCIÓN ES: 2 HORAS COMO MÁXIMO PARA INICIO DE DIAGNÓSTICO, EN EL CASO DE FALLAS MAYORES SU ATENCIÓN SE CONTINUA AÚN FUERA DE HORARIO DE COBERTURA HASTA SU SOLUCIÓN, SIN NINGÚN COSTO, SIEMPRE QUE HAYA INICIADO SU ATENCIÓN DENTRO DEL HORARIO DE SERVICIO. "EL PROVEEDOR" ESTA OBLIGADO A CONTINUAR CON LA ATENCIÓN, SIN COSTO, DE FALLAS O PROBLEMAS DETECTADOS DENTRO DE LA VIGENCIA DEL CONTRATO HASTA SU SOLUCIÓN, AÚN CUANDO ÉSTA, SE EXTIENDA MÁS ALLÁ DE AQUÉLLA; PRORROGÁNDOSE LOS DERECHOS QUE OTORGA DICHO CONTRATO PARA ESTOS REPORTES DE FALLA, EN LOS TÉRMINOS ORIGINALES. **MANTENIMIENTO PREVENTIVO** EL MANTENIMIENTO PREVENTIVO SE DA A TODOS Y CADA UNO DE LOS EQUIPOS INVENTARIADOS SEÑALADOS EN EL PROGRAMA DE MANTENIMIENTO PREVENTIVO, 1 (UNA) VEZ DURANTE LA VIGENCIA DEL CONTRATO, CON EXCEPCIÓN ÚNICA EN AQUELLOS CASOS EN DONDE LOS EQUIPOS NO PUEDEN DEJAR DE OPERAR, EN CUYO CASO "EL PROVEEDOR" NOTIFICA PARA QUE DE MANERA CONJUNTA SE PROGRAMEN. EL MANTENIMIENTO SE PROPORCIONADO AL "HARDWARE" Y AL "SOFTWARE" QUE COMPONEN LOS EQUIPOS, CON LA FINALIDAD DE MANTENER LA VIGENCIA TECNOLÓGICA DEL EQUIPO, ESTE MANTENIMIENTO INCLUYE LAS ACTUALIZACIONES DEL "SOFTWARE" A LA ÚLTIMA VERSIÓN GRATUITA EMITIDA POR EL FABRICANTE Y QUE NO REQUIERAN MODIFICACIONES EN EL HARDWARE DEL EQUIPO. "EL PROVEEDOR" PROPORCIONA, POR ESCRITO, UN ANÁLISIS EXPERTO DEL ESTADO QUE GUARDA EL HARDWARE Y SOFTWARE, CON LA FINALIDAD DE GARANTIZAR UN ÓPTIMO NIVEL DEL FUNCIONAMIENTO DE LOS EQUIPOS. SE ELABORA Y REVISA CONJUNTAMENTE CON EL PERSONAL TÉCNICO "EL PROVEEDOR", EL PROGRAMA DE TRABAJO, LAS ACTIVIDADES Y FECHAS DEL MANTENIMIENTO PREVENTIVO A DETALLE; CON CANTIDADES, NOMBRES DE LOS RESPONSABLES A EJECUTAR Y SUPERVISAR LA APLICACIÓN DE DICHOS SERVICIOS, A MÁS TARDAR EN LA SEGUNDA SEMANA CONTADA A PARTIR DE LA FORMALIZACIÓN DEL CONTRATO. SE ENTREGA COPIA DE LOS PROGRAMAS, PROCEDIMIENTOS O CALENDARIOS FORMALIZADOS CONJUNTAMENTE EN LA FASE DE REVISIÓN. EN CASO DE QUE EXISTAN MODIFICACIONES AL PROGRAMA VALIDADO, ESTAS SE REGISTRAN POR ESCRITO Y DE COMÚN ACUERDO ENTRE AMBAS PARTES. PARA EL CUMPLIMIENTO DEL PROGRAMA DE MANTENIMIENTO PREVENTIVO, "EL PROVEEDOR" PRESENTA POR ESCRITO LOS RECURSOS HUMANOS Y TÉCNICOS, ASÍ COMO PROTOCOLOS DE PRUEBA, CON LOS QUE CUBRE EL SERVICIO.

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			MANTENIMIENTO CORRECTIVO "EL PROVEEDOR" PROPORCIONA LOS MANTENIMIENTOS CORRECTIVOS SURGIDOS DURANTE LA VIGENCIA DEL CONTRATO, AL HARDWARE Y SOFTWARE DEL EQUIPO, EN EL CUAL INCLUYEN LAS REFACCIONES Y/O PARTES ORIGINALES Y ACTUALIZACIONES DEL "SOFTWARE" QUE SE REQUIEREN PARA REPARACIONES DEL EQUIPO, ASÍ MISMO SE SUMINISTRA LA MANO DE OBRA PARA SU INSTALACIÓN. LOS EQUIPOS QUE SE UTILICEN EN TODOS LOS CASOS, TIENEN CALIDAD Y CARACTERÍSTICAS TÉCNICAS IGUALES O SUPERIORES A LAS DEL EQUIPO ORIGINAL, DE TAL MANERA QUE SE GARANTIZA EL FUNCIONAMIENTO ADECUADO DEL HARDWARE Y SOFTWARE. SE APLICAN PRUEBAS DE DIAGNÓSTICO Y OPERACIÓN DE RESPALDO ANTES DE PROCEDER A LA REPARACIÓN DEL MISMO, SEGÚN RESULTE EL DIAGNÓSTICO APLICADO. AL FINALIZAR SE ENTREGA COPIA DEL REPORTE DE SERVICIO DE MANTENIMIENTO CORRECTIVO. EN EL CASO DE UNA CONTINGENCIA MAYOR O DE SEVERIDAD CRÍTICA, "EL PROVEEDOR" ASIGNA UN INGENIERO EN SITIO HASTA LA RESOLUCIÓN TOTAL DEL PROBLEMA. **PROCEDIMIENTO DE ESCALAMIENTO** SE INCLUYE UNA RELACIÓN CON NOMBRES DE RESPONSABLES, TELÉFONOS, CORREOS ELECTRÓNICOS Y CELULARES, ASÍ COMO LOS HORARIOS DE ATENCIÓN PARA LEVANTAR REPORTES DE MANTENIMIENTO CORRECTIVO, ASÍ COMO LOS NÚMEROS DE RADIOLOCALIZADORES PARA REPORTAR FALLAS FUERA DE LOS HORARIOS DE SERVICIO, LOS TIEMPOS DE RESPUESTA SE SUJETAN TAMBIÉN A LO ESTIPULADO EN EL PUNTO DE "TIEMPOS MÁXIMOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN" DE ESTE ANEXO. CONTIENE EL PROCEDIMIENTO DE ESCALAMIENTO DESDE EL MOMENTO EN QUE SE REPORTE UNA FALLA EN UN EQUIPO HASTA SU SOLUCIÓN Y LOS NOMBRES Y CARGOS DE LOS RESPONSABLES EN CADA PROCESO. **SERVICIO DE INSTALACIÓN** • INSTALACIÓN Y CONFIGURACIÓN DEL EQUIPO • REGISTRO DE LOS APPLIANCE EN EL PORTAL WEB DEL FABRICANTE • ACTUALIZACIÓN DE FIRMWARE • PRUEBA DE FUNCIONALIDAD • TRANSFERENCIA DE CONOCIMIENTOS Y MEMORIA TÉCNICA • SE CONSIDERAN LAS CONEXIONES NECESARIAS DE FIBRA ÓPTICA CON EL EQUIPO DE SEGURIDAD PRIMARIO • SE CONSIDERAN LAS ADECUACIONES ELÉCTRICAS NECESARIAS PARA EL CORRECTO FUNCIONAMIENTO DE LOS EQUIPOS
2	4	Licencia	**(2) LICENCIA ANTIVIRUS PARA 50 USUARIOS** CON LAS SIGUIENTES CARACTERÍSTICAS Y FUNCIONALIDADES: KASPERSKY ENDPOINT SECURITY FOR BUSINESS NIVEL: SELECT • LICENCIA ANTIVIRUS POR TRES AÑOS • ANTIMALWARE • FIREWALL • PROTECCIÓN ASISTIDA EN LA NUBE • CONTROL DE APLICACIONES • LISTA BLANCA DE APLICACIONES • CONTROL WEB • CONTROL DE DISPOSITIVOS • PROTECCIÓN DEL SERVIDOR DE ARCHIVOS • MANEJO DEL DISPOSITIVO MÓVIL (MDM) • SEGURIDAD DE ENDPOINT MÓVIL (PARA TABLETS Y SMARTPHONES) • ENCRIPTACIÓN • CONFIGURACIÓN Y DESPLIEGUE DE SISTEMAS • ESCÁNER DE VULNERABILIDADES AVANZADO • CONTROL DE ADMISIÓN A LA RED • MANEJO DE PARCHES • SEGURIDAD PARA EL SERVIDOR DE CORREO

Partida	Cant.	Unidad de Medida	Descripción
			• PROTECCIÓN DEL GATEWAY DE WEB/INTERNET • SEGURIDAD DEL SERVIDOR DE COLABORACIÓN
		Licencia	**(2) RENOVACIÓN DE LICENCIAS DE EQUIPO DE SEGURIDAD INFORMÁTICA** SE CONSIDERA LA RENOVACIÓN DE LA LICENCIA PARA 2 EQUIPOS DE SEGURIDAD INFORMÁTICA FORTINET 90D CON NÚMEROS DE SERIE: FGT90D3Z15015304, FGT90D3Z15015298 LAS CUALES CUMPLEN CON: LICENCIA: FORTICARE **FIREWALL** • LAS REGLAS DE FIREWALL ANALIZAN LAS CONEXIONES QUE ATRAVIESEN EN EL EQUIPO, ENTRE INTERFACES, GRUPOS DE INTERFACES (O ZONAS) Y VLANS. • POR GRANULARIDAD Y SEGURIDAD, EL FIREWALL PUEDE ESPECIFICAR POLÍTICAS TOMANDO EN CUENTA PUERTO FÍSICO FUENTE Y DESTINO. ESTO ES, EL PUERTO FÍSICO FUENTE Y EL PUERTO FÍSICO DESTINO FORMAN PARTE DE LA ESPECIFICACIÓN DE LA REGLA DE FIREWALL. • ES POSIBLE DEFINIR POLÍTICAS DE FIREWALL QUE SEAN INDEPENDIENTES DEL PUERTO DE ORIGEN Y PUERTO DE DESTINO. • LAS REGLAS DEL FIREWALL TOMAN 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. • 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 PUEDEN TENER LIMITANTES Y/O VIGENCIA EN BASE A TIEMPO. • LAS REGLAS DE FIREWALL PUEDEN TENER LIMITANTES Y/O VIGENCIA EN BASE A FECHAS (INCLUYENDO DÍA, MES Y AÑO) • SOPORTA LA CAPACIDAD DE DEFINIR NUEVOS SERVICIOS TCP Y UDP QUE NO ESTÉN CONTEMPLADOS EN LOS PREDEFINIDOS. • PUEDE DEFINIRSE EL TIEMPO DE VIDA DE UNA SESIÓN INACTIVA DE FORMA INDEPENDIENTE POR PUERTO Y PROTOCOLO (TCP Y UDP) • CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES ESTÁTICO, UNO A UNO, NAT. • CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES DINÁMICO, MUCHOS A UNO, PAT. • SOPORTA REGLAS DE FIREWALL EN IPV6 CONFIGURABLES TANTO POR CLI (COMMAND LINE INTERFACE, INTERFACE DE LINEA DE COMANDO) COMO POR GUI (GRAPHICAL USER INTERFACE, INTERFACE GRÁFICA DE USUARIO), • LA SOLUCIÓN TIENE 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, SOPORTA PERSISTENCIA DE SESIÓN MEDIANTE HTTP COOKIE O SSL SESSION ID • EN LA SOLUCIÓN DE BALANCEO DE CARGA DE ENTRE SERVIDORES SOPORTA MECANISMOS PARA DETECTAR LA DISPONIBILIDAD DE LOS SERVIDORES, DE FORMA TAL DE PODER EVITAR ENVIAR TRÁFICO A UN SERVIDOR NO DISPONIBLE. • EL EQUIPO PERMITE LA CREACIÓN DE POLÍTICAS DE TIPO FIREWALL CON CAPACIDAD DE SELECCIONAR CAMPOS COMO DIRECCIÓN, IDENTIFICADOR DE USUARIOS O IDENTIFICADOR DE DISPOSITIVOS PARA EL CASO DE DISPOSITIVOS MÓVILES COMO SMARTPHONES Y TABLETAS. • EL EQUIPO PERMITE LA CREACIÓN DE POLÍTICAS DE TIPO VPN CON CAPACIDAD DE SELECCIONAR CAMPOS COMO IPSEC O SSL SEGÚN SEA EL TIPO DE VPN • LA SOLUCIÓN TIENE LA CAPACIDAD DE HACER CAPTURA DE PAQUETES POR POLÍTICA DE SEGURIDAD IMPLEMENTADA PARA LUEGO SER EXPORTADO EN FORMATO PCAP. • LA SOLUCIÓN DE SEGURIDAD PERMITE LA CREACIÓN DE SERVICIOS DE FIREWALL PARA IMPLEMENTAR DENTRO DE LAS POLÍTICAS DE SEGURIDAD Y CATEGORIZARLOS DE MANERA PERSONALIZADA • LA SOLUCIÓN ES CAPAZ DE INTEGRAR LOS SERVICIOS DENTRO DE LAS CATEGORÍAS DE FIREWALL PREDEFINIDAS O PERSONALIZADAS Y ORDENARLOS ALFABÉTICAMENTE • EL DISPOSITIVO DE SEGURIDAD DETERMINA ACCESOS Y DENEGACIÓN A DIFERENTES TIPOS DE TRÁFICO PREDEFINIDOS DENTRO DE UNA LISTA LOCAL DE POLÍTICAS. • LA SOLUCIÓN ES CAPAZ DE HABILITAR O DESHABILITAR EL PASO DE TRAFICO A TRAVÉS

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			DE PROCESADORES DE PROPOSITO ESPECIFICO, SI EL DISPOSITIVO CUENTA CON ESTOS PROCESADORES INTEGRADOS DENTRO DEL MISMO • LA SOLUCIÓN CREA E IMPLEMENTA POLÍTICAS DE TIPO MULTICAST Y DETERMINAR EL SENTIDO DE LA POLÍTICA, ASÍ COMO TAMBIÉN LA HABILITACIÓN DEL NAT DENTRO DE CADA INTERFACE DEL DISPOSITIVO. • EL DISPOSITIVO DE SEGURIDAD ES CAPAZ DE CREAR E INTEGRAR POLÍTICAS CONTRA ATAQUES DOS LAS CUALES SE PUEDEN APLICAR POR INTERFACES. • EL DISPOSITIVO DE GENERAR LOGS DE CADA UNA DE LAS POLÍTICAS APLICADAS PARA EVITAR LOS ATAQUES DE DOS. • LA SOLUCIÓN DE SEGURIDAD PERMITE CONFIGURAR EL MAPEO DE PROTOCOLOS A PUERTOS DE MANERA GLOBAL O ESPECIFICA. • LA SOLUCIÓN CAPAZ DE CONFIGURAR EL BLOQUEO DE ARCHIVOS O CORREOS ELECTRÓNICOS POR TAMAÑO, O POR CERTIFICADOS SSL INVÁLIDOS. • EL DISPOSITIVO INTEGRARA LA INSPECCIÓN DE TRÁFICO TIPO SSL Y SSH BAJO PERFILES PREDEFINIDOS O PERSONALIZADOS. • EL DISPOSITIVO ES CAPAZ DE EJECUTAR INSPECCIÓN DE TRAFICO SSL EN TODOS LOS PUERTOS Y SELECCIONAR BAJO QUE CERTIFICADO SERÁ VÁLIDO ESTE TRÁFICO. • TIENE LA CAPACIDAD DE HACER ESCANEO A PROFUNDIDAD DE TRAFICO TIPO SSH DENTRO DE TODOS O CIERTO RANGO DE PUERTOS CONFIGURADOS PARA ESTE ANÁLISIS. • LA SOLUCIÓN PERMITE BLOQUEAR O MONITOREAR TODA LA ACTIVIDAD DE TIPO EXEC, PORT-FORWARD, SSH-SHELL, Y X-11 SSH. **ANTIVIRUS** • ES CAPAZ DE ANALIZAR, ESTABLECER CONTROL DE ACCESO Y DETENER ATAQUES Y HACER ANTIVIRUS EN TIEMPO REAL EN LOS SIGUIENTES PROTOCOLOS APLICATIVOS: HTTP, SMTP, IMAP, POP3, FTP. • EL ANTIVIRUS PUEDE CONFIGURARSE EN MODO PROXY COMO EN MODO DE FLUJO. EN EL PRIMER CASO, LOS ARCHIVOS SERÁN TOTALMENTE RECONSTRUIDOS POR EL MOTOR ANTES DE HACER LA INSPECCIÓN. EN EL SEGUNDO CASO, LA INSPECCIÓN DE ANTIVIRUS SE HARÁ POR CADA PAQUETE DE FORMA INDEPENDIENTE. • 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 SOPORTA LA CAPACIDAD DE INSPECCIONAR Y DETECTAR VIRUS EN TRÁFICO IPV6. • LA CONFIGURACIÓN DE ANTIVIRUS EN TIEMPO REAL SOBRE LOS PROTOCOLOS HTTP, SMTP, IMAP, POP3 Y FTP ESTA COMPLETAMENTE INTEGRADA A LA ADMINISTRACIÓN DEL DISPOSITIVO APPLIANCE, QUE PERMITE LA APLICACIÓN DE ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. • EL ANTIVIRUS SOPORTA 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 DE MANERA OPCIONAL PUEDE INSPECCIONAR POR TODOS LOS VIRUS CONOCIDOS. • EL ANTIVIRUS INTEGRADO TIENE 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 TIENE LA CAPACIDAD DE PONER EN CUARENTENA A LOS CLIENTES CUANDO SE HAYA DETECTADO QUE LOS MISMOS ENVÍAN ARCHIVOS INFECTADOS CON VIRUS. • EL ANTIVIRUS INCLUYE CAPACIDADES DE DETECCIÓN Y DETENCIÓN DE TRÁFICO SPYWARE, ADWARE Y OTROS TIPOS DE MALWARE/GRAYWARE QUE PUDIERAN CIRCULAR POR LA RED. • EL ANTIVIRUS PUEDE HACER INSPECCIÓN Y CUARENTENA DE ARCHIVOS TRANSFERIDOS POR MENSAJERÍA INSTANTÁNEA (INSTANT MESSAGING) PARA MSN MESSENGER. • EL ANTIVIRUS ES CAPAZ DE FILTRAR ARCHIVOS POR EXTENSIÓN • EL ANTIVIRUS ES CAPAZ DE FILTRAR ARCHIVOS POR TIPO DE ARCHIVO (EJECUTABLES, POR EJEMPLO) SIN IMPORTAR LA EXTENSIÓN QUE TENGA EL ARCHIVO • 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

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			TECNOLOGÍAS TIPO "PULL" (CONSULTAR LOS CENTROS DE ACTUALIZACIÓN POR VERSIONES NUEVAS) **ANTISPAM** • LA CAPACIDAD ANTISPAM INCLUIDA ES 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. • LA CAPACIDAD ANTISPAM INCLUIDA PERMITE ESPECIFICAR LISTAS BLANCAS (CONFIABLES, A LOS CUALES SIEMPRE SE LES TIENE QUE PASAR) Y LISTAS NEGRAS (NO CONFIABLES, A LOS CUALES SIEMPRE LES TIENE QUE BLOQUEAR). LAS LISTAS BLANCAS Y LISTAS NEGRAS SON POR DIRECCIÓN IP O POR DIRECCIÓN DE CORREO ELECTRÓNICO (E-MAIL ADDRESS). • LA CAPACIDAD ANTISPAM PUEDE CONSULTAR UNA BASE DE DATOS DONDE SE REVISE 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, TIENE LA FLEXIBILIDAD PARA ETIQUETARSE EN EL MOTIVO (SUBJECT) DEL MENSAJE O A TRAVÉS UN ENCABEZADO MIME EN EL MENSAJE. **FILTRAJE DE URLS (URL FILTERING)** • FACILIDAD PARA INCORPORAR CONTROL DE SITIOS A LOS CUALES NAVEGUEN LOS USUARIOS, MEDIANTE CATEGORÍAS. POR FLEXIBILIDAD, EL FILTRO DE URLS TIENE 75 CATEGORÍAS Y 54 MILLONES DE SITIOS WEB EN LA BASE DE DATOS. • PUEDE CATEGORIZAR CONTENIDO WEB REQUERIDO MEDIANTE IPV6. • 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. • CONFIGURABLE DIRECTAMENTE DESDE LA INTERFAZ DE ADMINISTRACIÓN DEL DISPOSITIVO APPLIANCE. CON CAPACIDAD PARA PERMITIR ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. • PERMITE 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 • LA SOLUCIÓN PERMITE REALIZAR EL FILTRADO DE CONTENIDO, TANTO REALIZANDO RECONSTRUCCIÓN DE TODA LA SESIÓN (MODO PROXY) COMO REALIZANDO INSPECCIÓN PAQUETE A PAQUETE SIN REALIZAR RECONSTRUCCIÓN DE LA COMUNICACIÓN (MODO FLUJO). • 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) SON PERSONALIZABLES. ESTOS MENSAJES DE REMPLAZO PUEDE APLICARSE PARA CONEXIONES HTTP Y HTTPS, TANTO EN MODO PROXY COMO EN MODO FLUJO. • LOS MENSAJES DE REMPLAZO PUEDEN SER PERSONALIZADOS POR CATEGORÍA DE FILTRADO DE CONTENIDO. • CAPACIDAD DE FILTRADO DE SCRIPTS EN PÁGINAS WEB (JAVA/ACTIVE X). • LA SOLUCIÓN DE FILTRAJE DE CONTENIDO SOPORTA EL FORZAMIENTO DE "SAFE SEARCH" O "BÚSQUEDA SEGURA" INDEPENDIENTEMENTE DE LA CONFIGURACIÓN EN EL BROWSER DEL USUARIO. ESTA FUNCIONALIDAD NO PERMITE QUE LOS BUSCADORES RETORNEN RESULTADOS CONSIDERADOS COMO CONTROVERSIALES. ESTA FUNCIONALIDAD SE SOPORTARÁ PARA GOOGLE, YAHOO! Y BING. • ES POSIBLE DEFINIR CUOTAS DE TIEMPO PARA LA NAVEGACIÓN. DICHAS CUOTAS PUEDE ASIGNARSE POR CADA CATEGORÍA Y POR GRUPOS. • SERÁ POSIBLE EXCEPTUAR LA INSPECCIÓN DE HTTPS POR CATEGORÍA. • CUENTA CON LA CAPACIDAD DE IMPLEMENTAR EL FILTRO DE EDUCACIÓN DE YOUTUBE POR PERFIL DE FILTRO DE CONTENIDO PARA TRAFICO HTTP, GARANTIZANDO DE MANERA CENTRALIZADA, QUE TODAS LAS SESIONES ACEPTADAS POR UNA POLÍTICA DE SEGURIDAD CON ESTE PERFIL, VAN A PODER ACCEDER SOLAMENTE A CONTENIDO DE TIPO EDUCATIVO EN YOUTUBE, BLOQUEANDO CUALQUIER TIPO DE CONTENIDO NO EDUCATIVO. • EL SISTEMA DE FILTRADO DE URLS TIENE 3 MÉTODOS DE INSPECCIÓN: 1. MODO DE FLUJO: LA PAGINA ES INSPECCIONADA PAQUETE A PAQUETE SIN RECONSTRUIR LA PÁGINA COMPLETA.

Partida	Cant.	Unidad de Medida	Descripción
			2. MODO PROXY: LA PAGINA ES RECONSTRUIDA COMPLETAMENTE PARA SER ANALIZADA A PROFUNDIDAD. 3. MODO DNS: LA INSPECCIÓN SE BASA ÚNICAMENTE EN LA CATEGORIZACIÓN DEL DOMINIO ACCESADO. • SE INCLUYE LA FUNCIONALIDAD DE REPUTACIÓN BASADA EN FILTRADO DE URLS. • LA FUNCIONALIDAD DE REPUTACIÓN BUSCA QUE, AL ACCEDER A PAGINAS DE CONTENIDO NO DESEADO (TALES COMO MALWARE, PORNOGRAFÍA, CONSUMO DE ANCHO DE BANDA EXCESIVO, ETC) SE ASIGNE UN PUNTAJE A CADA USUARIO O IP CADA VEZ VISITA UNA PÁGINA DE ESTA ÍNDOLE. DE ACUERDO A ESTO SE EXTRAE LOS USUARIOS QUE INFRINGEN LAS POLÍTICAS DE FILTRADO CON MÁS FRECUENCIA CON EL FIN DE DETECTAR ZOMBIES DENTRO DE LA RED. • EL SISTEMA DE FILTRADO DE URLS INCLUYE LA CAPACIDAD DE DEFINIR CUOTAS DE NAVEGACIÓN BASADAS EN VOLUMEN DE TRÁFICO CONSUMIDO. • SE INCORPORA LA FUNCIONALIDAD DE FILTRADO EDUCATIVO DE YOUTUBE (YOUTUBE EDUCATION FILTER) • EN DICHO SISTEMA CADA ORGANISMO OBTIENE UN ID DE YOUTUBE PARA HABILITAR EL CONTENIDO EDUCATIVO DEL MISMO. SE INSERTA DICHO CÓDIGO EN LA CONFIGURACIÓN DE FILTRADO DE URLS DEL EQUIPO PARA PODER HABILITAR ÚNICAMENTE EL CONTENIDO EDUCATIVO DE YOUTUBE. **PROTECCIÓN CONTRA INTRUSOS (IPS)** • EL DETECTOR Y PREVENTOR DE INTRUSOS PUEDE IMPLEMENTARSE TANTO EN LÍNEA COMO FUERA DE LÍNEA. EN LÍNEA, EL TRÁFICO A SER INSPECCIONADO PASARÁ A TRAVÉS DEL EQUIPO. FUERA DE LÍNEA, EL EQUIPO RECIBE EL TRÁFICO A INSPECCIONAR DESDE UN SWITCH CON UN PUERTO CONFIGURADO EN SPAN O MIRROR. • ES POSIBLE DEFINIR POLÍTICAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES PARA TRÁFICO IPV6. A TRAVÉS DE SENSORES. • CAPACIDAD DE DETECCIÓN DE MÁS DE 4000 ATAQUES. • 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 ESTA 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 ESTA 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 PERMITE LA PROTECCIÓN DE ESTE SERVICIO POR POLÍTICA DE CONTROL DE ACCESO. • EL DETECTOR Y PREVENTOR DE INTRUSOS SOPORTA CAPTAR ATAQUES POR VARIACIONES DE PROTOCOLO Y ADEMÁS POR FIRMAS DE ATAQUES CONOCIDOS (SIGNATURE BASED / MISUSE DETECTION). • BASADO EN ANÁLISIS DE FIRMAS EN EL FLUJO DE DATOS EN LA RED, Y PERMITIR CONFIGURAR FIRMAS NUEVAS PARA CUALQUIER PROTOCOLO. • ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS PARA EL DETECTOR DE INTRUSOS • EL DETECTOR DE INTRUSOS MITIGA LOS EFECTOS DE LOS ATAQUES DE NEGACIÓN DE SERVICIOS. • MÉTODOS DE NOTIFICACIÓN: o ALARMAS MOSTRADAS EN LA CONSOLA DE ADMINISTRACIÓN DEL APPLIANCE. o ALERTAS VÍA CORREO ELECTRÓNICO. o TIENE LA CAPACIDAD DE CUARENTENA, ES DECIR PROHIBIR EL TRÁFICO SUBSIGUIENTE A LA DETECCIÓN DE UN POSIBLE ATAQUE. ESTA CUARENTENA PUEDE DEFINIRSE PARA EL TRÁFICO PROVENIENTE DEL ATACANTE O PARA EL TRÁFICO DEL ATACANTE AL ATACADO. o LA CAPACIDAD DE CUARENTENA OFRECE 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. o OFRECE LA POSIBILIDAD DE GUARDAR INFORMACIÓN SOBRE EL PAQUETE DE RED QUE DETONÓ LA DETECCIÓN DEL ATAQUE, ASÍ COMO LOS 5 PAQUETES SUCESIVOS. ESTOS PAQUETES PUEDEN SER VISUALIZADOS POR UNA HERRAMIENTA QUE SOPORTE EL FORMATO PCAP. • SE INCLUYE PROTECCIÓN CONTRA AMENAZAS AVANZADAS Y PERSISTENTES

FASP ¡PERAÚO CON RECURSOS 2018

Partida	Cant.	Unidad de Medida	Descripción
			(ADVANCED PERSISTENT THREATS). DENTRO DE ESTOS CONTROLES SE INCLUYE: • 1. PROTECCIÓN CONTRA BOTNETS: SE BLOQUEAN INTENTOS DE CONEXIÓN A SERVIDORES DE BOTNETS, PARA ELLO SE CUENTA CON UNA LISTA DE LOS SERVIDORES DE BOTNET MÁS UTILIZADO. DICHA LISTA SE ACTUALIZA DE FORMA PERIÓDICA POR EL FABRICANTE. • 2. SANDBOXING: LA FUNCIONALIDAD DE SANDBOX HACE QUE EL ARCHIVO SEA EJECUTADO EN UN AMBIENTE SEGURO PARA ANALIZAR SU COMPORTAMIENTO Y, A BASE DEL MISMO, TOMAR UNA ACCIÓN SOBRE EL MISMO. **PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP)** • LA SOLUCIÓN OFRECE 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 SOPORTA EL ANÁLISIS DE ARCHIVOS DEL TIPO: MS-WORD, PDF, TEXTO, ARCHIVOS COMPRIMIDOS. • SOPORTA EL ESCANEO DE ARCHIVOS EN LOS SIGUIENTES PROTOCOLOS: HTTP, POP3, SMTP, IMAP, NNTP Y FTP. • ANTE LA DETECCIÓN DE UNA POSIBLE FUGA DE INFORMACIÓN PUEDEN 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 PERMITE 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 SOPORTA LA CAPACIDAD DE GUARDAR UNA COPIA DEL ARCHIVO IDENTIFICADO COMO POSIBLE FUGA DE INFORMACIÓN. ESTA COPIA ES ARCHIVADA LOCALMENTE O EN OTRO DISPOSITIVO. • LA SOLUCIÓN PERMITE LA BÚSQUEDA DE PATRONES EN ARCHIVOS MEDIANTE LA DEFINICIÓN DE EXPRESIONES REGULARES. • SE PROVEE LA FUNCIONALIDAD DE FILTRADO DE FUGA DE INFORMACIÓN. DENTRO DE LAS TÉCNICAS DE DETECCIÓN SE CONSIDERA COMO MÍNIMO LAS SIGUIENTES: 1. FILTRADO POR TIPO DE ARCHIVO 2. FILTRADO POR NOMBRE DE ARCHIVO 3. FILTRADO POR EXPRESIONES REGULARES: SE DETECTARÁN LOS ARCHIVOS SEGÚN LAS EXPRESIONES REGULARES QUE SE ENCUENTREN DENTRO DE LOS MISMOS. 4. FINGERPRINTING: SE TOMARÁ UNA MUESTRA DEL ARCHIVO QUE SE CONSIDERE COMO CONFIDENCIAL. SEGÚN ESTO SE BLOQUEARÁN ARCHIVOS QUE SEAN IGUALES A ESTA MUESTRA. 5. WATERMARKING: SE INSERTARÁ UN "SELLO DE AGUA" DENTRO DEL ARCHIVO CONSIDERADO COMO CONFIDENCIAL. DE ACUERDO A ESTO SE ANALIZARÁN LOS ARCHIVOS EN BUSCA DE ESTE SELLO DE AGUA, ESTE SE DETECTARÁ INCLUSO SI EL ARCHIVO SUFRIÓ CAMBIOS. **CONTROL DE APLICACIONES** • LO SOLUCIÓN SOPORTA LA CAPACIDAD DE IDENTIFICAR LA APLICACIÓN QUE ORIGINA CIERTO TRÁFICO A PARTIR DE LA INSPECCIÓN DEL MISMO. • LA IDENTIFICACIÓN DE LA APLICACIÓN ES INDEPENDIENTE DEL PUERTO Y PROTOCOLO HACIA EL CUAL ESTÉ DIRECCIONADO DICHO TRÁFICO. • LA SOLUCIÓN TIENE UN LISTADO DE 1000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE. • EL LISTADO DE APLICACIONES SE ACTUALIZA PERIÓDICAMENTE. • PARA APLICACIONES IDENTIFICADAS SE PUEDEN DEFINIR LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) PUEDEN DEFINIRSE LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES DE TIPO P2P PUEDE DEFINIRSE ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING. • PREFERENTEMENTE SOPORTA MAYOR GRANULARIDAD EN LAS ACCIONES. **INSPECCIÓN DE CONTENIDO SSL** • LA SOLUCIÓN SOPORTA LA CAPACIDAD DE INSPECCIONAR TRÁFICO QUE ESTÉ SIENDO ENCRIPTADO MEDIANTE TLS PARA LOS SIGUIENTES PROTOCOLOS: HTTPS, IMAPS, SMTPS, POP3S. • LA INSPECCIÓN SE REALIZA MEDIANTE LA TÉCNICA CONOCIDA COMO HOMBRE EN EL MEDIO (MITM - MAN IN THE MIDDLE).

Partida	Cant.	Unidad de Medida	Descripción
			• LA INSPECCIÓN DE CONTENIDO ENCRIPTADO NO REQUIERE NINGUN CAMBIO DE CONFIGURACIÓN EN LAS APLICACIONES O SISTEMA OPERATIVO DEL USUARIO. • PARA EL CASO DE URL FILTERING, ES POSIBLE CONFIGURAR EXCEPCIONES DE INSPECCIÓN DE HTTPS. DICHAS EXCEPCIONES EVITAN QUE EL TRÁFICO SEA INSPECCIONADO PARA LOS SITIOS CONFIGURADOS. LAS EXCEPCIONES PUEDEN DETERMINARSE POR CATEGORÍA DE FILTRADO. • EL EQUIPO ES CAPAZ DE ANALIZAR CONTENIDO CIFRADO (SSL O SSH) PARA LAS FUNCIONALIDADES DE FILTRADO DE URLS, CONTROL DE APLICACIONES, PREVENCIÓN DE FUGA DE INFORMACIÓN, ANTIVIRUS E IPS **SOPORTE DEL FABRICANTE.** "EL PROVEEDOR" INCLUYE EL SOPORTE DEL FABRICANTE PARA LOS BIENES MENCIONADOS, CONSIDERANDO LA VIGENCIA SOLICITADA EN ESTE ANEXO TÉCNICO. INCLUYENDO, CON ELLO QUE "EL ESTADO" CUENTA CON EL RESPALDO DEL FABRICANTE PARA ESCALAR FALLAS QUE REQUIERAN DE ANÁLISIS, DIAGNÓSTICO Y SOLUCIÓN DE FALLAS, ASÍ COMO PARA EL REEMPLAZO AVANZADO DE PARTES, CON LOS SIGUIENTES ALCANCES ADICIONALES CON RESPECTO A LOS EQUIPOS: • ACCESO A LA BASE DE DATOS DE CONOCIMIENTO DEL FABRICANTE EN UN ESQUEMA 8X5 • SOPORTE TELEFÓNICO 24X7 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE WEB 24X7 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE VÍA CHAT 24X7 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE DE SOFTWARE CON RELEASES DE MANTENIMIENTO Y UPGRADES A NUEVAS VERSIONES • SOPORTE DE HARDWARE TIPO REEMPLAZO AVANZADO **RESPALDO DE FABRICANTE** LAS LICENCIAS DE SEGURIDAD INFORMÁTICA UTM SOLICITADAS EN ESTE CONCEPTO CUENTAN CON EL RESPALDO POR PARTE DEL FABRICANTE Y "EL PROVEEDOR" ENTREGA LA SIGUIENTE DOCUMENTACIÓN: o DOCUMENTACIÓN EXPEDIDA POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD INFORMÁTICA UTM EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" ES INTEGRADOR AUTORIZADO DE LOS EQUIPOS DEL MAS ALTO NIVEL Y HABILITADOS PARA DISTRIBUIR, IMPLEMENTAR Y BRINDAR SERVICIOS ADMINISTRADOS, AUTORIZADO PARA REVENDER LOS PRODUCTOS/SERVICIOS DEL FABRICANTE. o CERTIFICADO O CERTIFICADOS EXPEDIDA POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD INFORMÁTICA UTM EN LA QUE MANIFIESTE "EL PROVEEDOR" CUENTA CON LAS CERTIFICACIONES REQUERIDAS PARA BRINDAR SERVICIOS DE INSTALACIÓN Y SOPORTE DE LOS EQUIPOS DE SEGURIDAD SOLICITADOS. o DOS INGENIEROS CERTIFICADOS EN LA SOLUCIÓN PROPUESTA, PARA REALIZAR LAS ACTIVIDADES DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO Y EN MARCHA. NIVEL EXPERTO AVALADO POR EL FABRICANTE. o "EL PROVEEDOR" DEMUESTRA SU EXPERIENCIA EN EL SOPORTE DE LAS LICENCIAS DE SEGURIDAD INFORMÁTICA SOLICITADO, A TRAVÉS DE LA DOCUMENTACIÓN DE CLIENTES EXCLUSIVAMENTE DE GOBIERNO EN DONDE HAYA INSTALADO EQUIPOS DE LA MISMA MARCA CON CARACTERÍSTICAS SIMILARES A LOS REQUERIDOS POR "EL ESTADO", LA CUAL CONTIENE LA SIGUIENTE INFORMACIÓN: NOMBRE, DIRECCIÓN, TELÉFONO Y CORREO ELECTRÓNICO DE LOS CLIENTES Y UNA DESCRIPCIÓN DEL PROYECTO DE MEDIA CUARTILLA. "EL ESTADO" SE RESERVARÁ EL DERECHO DE VERIFICAR DICHA INFORMACIÓN. **SOPORTE DEL PROVEEDOR** SE INCLUYE COMO PARTE DE LA PROPUESTA EL SERVICIO DE SOPORTE PARA EL EQUIPO: CON LOS SIGUIENTES SERVICIOS: o DURACIÓN DE 12 MESES o ATENCIÓN DE FALLAS CON UN TIEMPO MÁXIMO DE 2 HORAS CON ESQUEMA 5X8. o SE CONSIDERA UN (1) MANTENIMIENTO PREVENTIVO AL AÑO PARA LOS EQUIPOS, PREVIO ACUERDO CON "EL ESTADO". LOS INSUMOS NECESARIOS PARA EL MANTENIMIENTO CORREN POR CUENTA DE "EL PROVEEDOR". o INCLUYE SOPORTE TELEFÓNICO SIN COSTO ADICIONAL EN HORARIO DE LUNES A VIERNES EN HORARIO DE OFICINA. o PARA LOS EQUIPOS O SOFTWARE DE LA SOLUCIÓN DE SEGURIDAD PARA LOS CUALES EL FABRICANTE LIBERE NUEVAS VERSIONES DENTRO DE LA VIGENCIA DE LA PÓLIZA DE SOPORTE,

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			"EL PROVEEDOR" REALIZA LA INSTALACIÓN SIN COSTO PARA "EL ESTADO" DE DICHAS ACTUALIZACIONES. **ASISTENCIA TÉCNICA** "EL PROVEEDOR" CUENTA CON UN CENTRO DE CONSULTA O ASESORÍA TELEFÓNICA QUE PERMITE AL PERSONAL TÉCNICO DE "EL ESTADO" REALIZAR ACLARACIONES Y CONSULTAS SOBRE EL USO Y CONFIGURACIÓN DE LOS EQUIPOS ANTES MENCIONADOS. PARA ESTA CLASE DE SERVICIO NO SE TOTALIZAN HORAS MENSUALES EN UNO O VARIOS EVENTOS Y NO HAY RESTRICCIÓN EN LA DURACIÓN DE CADA EVENTO. LOS DATOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGRA EN EL CONTROL DE EVENTOS E INCIDENTES SON: o IDENTIFICADOR DEL REPORTE O NÚMERO DE INCIDENTE O EVENTO o IDENTIFICADOR DEL USUARIO QUE REPORTA. ESTOS SON LOS DATOS QUE IDENTIFICAN AL USUARIO QUE LEVANTÓ EL REPORTE. NOMBRE, TELÉFONO, CORREO ELECTRÓNICO Y UBICACIÓN. LA DEFINICIÓN FINAL DE ESTOS DATOS SE ACORDARÁ CON "EL PROVEEDOR" o HORA EN QUE REPORTA EL PROBLEMA POR PARTE DEL USUARIO AUTORIZADO o TIPO DE FALLO o DESCRIPCIÓN DEL FALLO o TIEMPO DE SOLUCIÓN DEL INCIDENTE Y RESTABLECIMIENTO DEL SERVICIO. **TIEMPOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN** EL TIEMPO DEL INICIO DE ATENCIÓN O RESPUESTA A UN REPORTE EFECTUADO A "EL PROVEEDOR" QUIEN PROPORCIONA UN FOLIO DE ATENCIÓN AL RECIBIRLO TIEMPO MÁXIMO DE SOLUCIÓN DE FALLAS DESPUÉS DEL INICIO DE LA ATENCIÓN ES: 2 HORAS COMO MÁXIMO PARA INICIO DE DIAGNÓSTICO, EN EL CASO DE FALLAS MAYORES SU ATENCIÓN SE CONTINUA AÚN FUERA DE HORARIO DE COBERTURA HASTA SU SOLUCIÓN, SIN NINGÚN COSTO, SIEMPRE QUE HAYA INICIADO SU ATENCIÓN DENTRO DEL HORARIO DE SERVICIO. EN EL CASO DE QUE EN ALGUNA REPARACIÓN DE LOS EQUIPOS SE REQUIERA CAMBIO O SUSTITUCIÓN DE ALGUNA PARTE O COMPONENTE, "EL PROVEEDOR" TIENE LA OBLIGACIÓN DE REMPLAZARLO EN SITIO, DENTRO DEL TIEMPO MÁXIMO DE ATENCIÓN DEL REPORTE. SI EL EQUIPO NO PUEDE REPARARSE DENTRO DE LOS TIEMPOS ESTABLECIDOS, "EL PROVEEDOR" TIENE QUE SUSTITUIR EL EQUIPO O PARTE DAÑADA CON EQUIPO DE RESPALDO QUE CUENTE CON LAS MISMAS CARACTERÍSTICAS O SUPERIORES QUE EL EQUIPO ORIGINAL, ESTA SUSTITUCIÓN SE EFECTÚA DENTRO DE LOS TIEMPOS MÁXIMOS DE ATENCIÓN DEFINIDOS Y PERMANECE DURANTE EL TIEMPO QUE TARDA LA COMPOSTURA DEL EQUIPO DAÑADO. EN EL CASO DE QUE EXISTAN EQUIPOS DE RESPALDO INSTALADOS AL TÉRMINO DEL CONTRATO, ESTOS SIGUEN DANDO EL SERVICIO HASTA QUE SE REPAREN LOS EQUIPOS DAÑADOS, AÚN CUANDO HAYA TERMINADO LA VIGENCIA DEL CONTRATO, EXTENDIÉNDOSE LOS DERECHOS QUE SE OTORGAN PARA ESTOS REPORTES DE FALLA, EN LOS TÉRMINOS ORIGINALES. SI DESPUÉS DE REALIZAR EL MANTENIMIENTO CORRECTIVO A UN EQUIPO, ESTE VUELVE A PRESENTAR LA MISMA FALLA, SE CONSIDERA COMO NO REALIZADO Y SU REPARACIÓN SE REALIZARÁ SIN CARGO ALGUNO. "EL PROVEEDOR" ESTA OBLIGADO A CONTINUAR CON LA ATENCIÓN, SIN COSTO, DE FALLAS O PROBLEMAS DETECTADOS DENTRO DE LA VIGENCIA DEL CONTRATO HASTA SU SOLUCIÓN, AÚN CUANDO ÉSTA, SE EXTIENDA MÁS ALLÁ DE AQUÉLLA; PRORROGÁNDOSE LOS DERECHOS QUE OTORGA DICHO CONTRATO PARA ESTOS REPORTES DE FALLA, EN LOS TÉRMINOS ORIGINALES. **MANTENIMIENTO PREVENTIVO** EL MANTENIMIENTO PREVENTIVO SE DA A TODOS Y CADA UNO DE LOS EQUIPOS INVENTARIADOS SEÑALADOS EN EL PROGRAMA DE MANTENIMIENTO PREVENTIVO, 1 (UNA) VEZ DURANTE LA VIGENCIA DEL CONTRATO, CON EXCEPCIÓN ÚNICA EN AQUELLOS CASOS EN DONDE LOS EQUIPOS NO PUEDEN DEJAR DE OPERAR, EN CUYO CASO "EL PROVEEDOR" DEL SERVICIO NOTIFICA PARA QUE DE MANERA CONJUNTA SE PROGRAMEN. EL MANTENIMIENTO SE PROPORCIONADO AL "HARDWARE" Y AL "SOFTWARE" QUE COMPONEN LOS EQUIPOS, CON LA FINALIDAD DE MANTENER LA VIGENCIA TECNOLÓGICA DEL EQUIPO, ESTE MANTENIMIENTO INCLUYE LAS ACTUALIZACIONES DEL "SOFTWARE" A LA ÚLTIMA VERSIÓN GRATUITA EMITIDA POR EL FABRICANTE Y QUE NO REQUIERAN MODIFICACIONES EN EL HARDWARE DEL EQUIPO. "EL PROVEEDOR" PROPORCIONA POR ESCRITO, UN ANÁLISIS EXPERTO DEL ESTADO QUE GUARDA EL HARDWARE Y SOFTWARE, CON LA FINALIDAD DE GARANTIZAR UN ÓPTIMO NIVEL DEL FUNCIONAMIENTO DE LOS EQUIPOS. SE ELABORA Y REVISA CONJUNTAMENTE CON EL PERSONAL TÉCNICO DE "EL PROVEEDOR", EL

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			PROGRAMA DE TRABAJO, LAS ACTIVIDADES Y FECHAS DEL MANTENIMIENTO PREVENTIVO A DETALLE; CON CANTIDADES, NOMBRES DE LOS RESPONSABLES A EJECUTAR Y SUPERVISAR LA APLICACIÓN DE DICHOS SERVICIOS, A MÁS TARDAR EN LA SEGUNDA SEMANA CONTADA A PARTIR DE LA FORMALIZACIÓN DEL CONTRATO. SE ENTREGA COPIA DE LOS PROGRAMAS, PROCEDIMIENTOS O CALENDARIOS FORMALIZADOS CONJUNTAMENTE EN LA FASE DE REVISIÓN. EN CASO DE QUE EXISTAN MODIFICACIONES AL PROGRAMA VALIDADO, ESTAS SE REGISTRAN POR ESCRITO Y DE COMÚN ACUERDO ENTRE AMBAS PARTES. PARA EL CUMPLIMIENTO DEL PROGRAMA DE MANTENIMIENTO PREVENTIVO, "EL PROVEEDOR" PRESENTA POR ESCRITO LOS RECURSOS HUMANOS Y TÉCNICOS, ASÍ COMO PROTOCOLOS DE PRUEBA, CON LOS QUE CUBRE EL SERVICIO. **MANTENIMIENTO CORRECTIVO** "EL PROVEEDOR" PROPORCIONA LOS MANTENIMIENTOS CORRECTIVOS SURGIDOS DURANTE LA VIGENCIA DEL CONTRATO, AL HARDWARE Y SOFTWARE DEL EQUIPO, EN EL CUAL INCLUYEN LAS REFACCIONES Y/O PARTES ORIGINALES Y ACTUALIZACIONES DEL "SOFTWARE" QUE SE REQUIEREN PARA REPARACIONES DEL EQUIPO, ASÍ MISMO SE SUMINISTRA LA MANO DE OBRA PARA SU INSTALACIÓN. LOS EQUIPOS QUE SE UTILICEN EN TODOS LOS CASOS, TIENEN CALIDAD Y CARACTERÍSTICAS TÉCNICAS IGUALES O SUPERIORES A LAS DEL EQUIPO ORIGINAL, DE TAL MANERA QUE SE GARANTIZA EL FUNCIONAMIENTO ADECUADO DEL HARDWARE Y SOFTWARE. SE APLICAN PRUEBAS DE DIAGNÓSTICO Y OPERACIÓN DE RESPALDO ANTES DE PROCEDER A LA REPARACIÓN DEL MISMO, SEGÚN RESULTE EL DIAGNÓSTICO APLICADO. AL FINALIZAR SE ENTREGA COPIA DEL REPORTE DE SERVICIO DE MANTENIMIENTO CORRECTIVO. EN EL CASO DE UNA CONTINGENCIA MAYOR O DE SEVERIDAD CRÍTICA, "EL PROVEEDOR" ASIGNA UN INGENIERO EN SITIO HASTA LA RESOLUCIÓN TOTAL DEL PROBLEMA. **PROCEDIMIENTO DE ESCALAMIENTO** SE INCLUYE UNA RELACIÓN CON NOMBRES DE RESPONSABLES, TELÉFONOS, CORREOS ELECTRÓNICOS Y CELULARES, ASÍ COMO LOS HORARIOS DE ATENCIÓN PARA LEVANTAR REPORTES DE MANTENIMIENTO CORRECTIVO, ASÍ COMO LOS NÚMEROS DE RADIOLOCALIZADORES PARA REPORTAR FALLAS FUERA DE LOS HORARIOS DE SERVICIO, LOS TIEMPOS DE RESPUESTA SE SUJETAN TAMBIÉN A LO ESTIPULADO EN EL PUNTO DE "TIEMPOS MÁXIMOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN" DE ESTE ANEXO. CONTIENE EL PROCEDIMIENTO DE ESCALAMIENTO DESDE EL MOMENTO EN QUE SE REPORTE UNA FALLA EN UN EQUIPO HASTA SU SOLUCIÓN Y LOS NOMBRES Y CARGOS DE LOS RESPONSABLES EN CADA PROCESO.
3	1	Licencia	**LICENCIA ANTIVIRUS PARA 50 USUARIOS PARA EL SISTEMA DE JUSTICIA PENAL PARA ADOLESCENTES** CON LAS SIGUIENTES ESPECIFICACIONES TÉCNICAS: KASPERSKY ENDPOINT SECURITY FOR BUSINESS NIVEL: SELECT • ANTIMALWARE • FIREWALL • PROTECCIÓN ASISTIDA EN LA NUBE • CONTROL DE APLICACIONES • LISTA BLANCA DE APLICACIONES • CONTROL WEB • CONTROL DE DISPOSITIVOS • PROTECCIÓN DEL SERVIDOR DE ARCHIVOS • MANEJO DEL DISPOSITIVO MÓVIL (MDM) • SEGURIDAD DE ENDPOINT MÓVIL (PARA TABLETS Y SMARTPHONES) • ENCRIPTACIÓN • CONFIGURACIÓN Y DESPLIEGUE DE SISTEMAS • ESCÁNER DE VULNERABILIDADES AVANZADO • CONTROL DE ADMISIÓN A LA RED • MANEJO DE PARCHES • SEGURIDAD PARA EL SERVIDOR DE CORREO

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			• PROTECCIÓN DEL GATEWAY DE WEB/INTERNET • SEGURIDAD DEL SERVIDOR DE COLABORACIÓN
4	1	Pieza	**CONMUTADOR DE DATOS** SE CONSIDERA EL SUMINISTROS E INSTALACIÓN DE UN CONMUTADOR DE DATOS PARA LA POLICÍA CIBERNÉTICA. CON LAS SIGUIENTES ESPECIFICACIONES: MARCA: ALCATEL-LUCENT MODERLO: OS6350-P48-US **FUNCIONALIDADES** • SWITCH CAPA 2 CON FUNCIONES BÁSICAS DE CAPA 3, DE CONFIGURACIÓN FIJA Y 1RU 48 PUERTOS RJ45 10/100/1000 BASE POE Y 2 PUERTOS FIXED SFP 1GB • EL EQUIPO PERMITE A FUTURO ACTIVAR UNA LICENCIA PARA QUE LOS PUERTOS SFP FUNCIONEN A 10GB. • EL EQUIPO SOPORTA A FUTURO LA FUNCIONALIDAD DE STACK CON 2 PUERTOS DE 10GB CON UNA CAPACIDAD DE STACKING DE 40 GBPS. PUEDE SOPORTAR PUERTOS INTERNOS DE STACK O MODULO DE STACK EXTERNO. • EL EQUIPO SOPORTA 8 SWITCHES EN UN SOLO STACK Y ADMINISTRA TODOS LOS EQUIPOS BAJO SOLO UNA DIRECCIÓN IP. • EL SWITCH TIENE UNA ARQUITECTURA NON-BLOCKING • CAPACIDAD MÍNIMA DE CONMUTACIÓN DE 176 GBPS • TASA DE REENVÍO DE 131 MPPS • CAPACIDAD MÍNIMA DE 16000 DIRECCIONES MAC • CAPACIDAD MÍNIMA DE 4000 VLANS • CAPACIDAD DE ADMINISTRACIÓN VÍA A TRAVÉS DE INTERFAZ WEB. • CAPACIDAD DE ADMINISTRACIÓN VÍA CONSOLA A TRAVÉS DE LÍNEA DE COMANDOS. • CAPACIDAD DE ADMINISTRACIÓN A TRAVÉS DE HERRAMIENTA DE ADMINISTRACIÓN CENTRALIZADA DE LA MISMA MARCA DEL FABRICANTE. • IEEE 802.1W RAPID SPANNING TREE PROTOCOL (RSTP) • CAPACIDAD DE CALIDAD DE SERVICIO (QOS), SOPORTA NOTIFICACIÓN DE EVENTOS DE RED MEDIANTE ALARMAS AUTOMÁTICAS A TRAVÉS DE HERRAMIENTA DE SOFTWARE DE ASISTENTE DE RED DEL MISMO FABRICANTE. • IEEE 802.1D SPANNING TREE PROTOCOL. • IEEE 802.1X, SEGURIDAD POR PUERTOS, AUTENTIFICACIÓN DE USUARIOS. • EL EQUIPO SOPORTA 1000 GRUPOS/STACKS DE IP MULTICAST • EL EQUIPO SOPORTA RUTEO ESTÁTICO, RIP V1 Y V2, RIPNG. • CUENTA CON REDUNDANCIA EN IMAGEN DEL RELEASE Y ARCHIVO DE CONFIGURACIÓN (ARCHIVOS DUALES) CON AUTO RECUPERACIÓN EN CASO DE CORRUPCIÓN DE UNO DE LOS DIRECTORIOS A FIN DE CONTAR CON RESPALDO INTERNO INCREMENTANDO LA SEGURIDAD Y CONTINUIDAD DEL SERVICIO. • EL SWITCH CUENTA CON UNA FUENTE DE PODER AC CON CONECTOR AMERICANO, CUENTA CON 780 WATSS DISPONIBLE PARA POE. • EL SWITCH SOPORTA LA INSTALACIÓN DE UNA FUENTE DE PODER REDUNDANTE INTERNA DE LAS MISMAS ESPECIFICACIONES DE LA FUENTE PRINCIPAL, WATTAJE Y CONECTOR AMERICANO. SOPORTA CONFIGURACIÓN UNO A UNO. **ADMINISTRACIÓN** • INTERFASE DE ADMINISTRACIÓN. • SOPORTA SSH PARA SESIONES SEGURAS DE CLI, ADMINISTRACIÓN, INTERFACE DE ADMINISTRACIÓN. • INTERFACE VIA LÍNEA DE COMANDO. • SOPORTE DE SOFTWARE ASISTENTE DE RED VÍA WEB BROWSER QUE PERMITE LA ADMINISTRACIÓN DE USUARIOS. • ADMINISTRACIÓN VÍA SNMPV1, V2C Y V3. **ESTÁNDARES O NORMAS QUE CUMPLE** • CONTROL BASADO EN PUERTO PARA EL CONTROL DE TORMENTAS DE UNICAST,

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			MULTICAST Y BROADCAST. • IEEE 802.1D • IEEE 802.1P • IEEE 802.1Q • IEEE 802.1W • IEEE 802.3AD • IEEE 802.1S • IEEE 802.3X • IEEE 802.3 • IEEE 802.3U • IEEE 802.3AB • IEEE 802.3Z • IGMP (V1, V2, AND V3) SNOOPING • VRRP • RADIUS, • SNMP V3 • NTP **REQUISITOS GENERALES** • SE CONSIDERA LA ULTIMA ACTUALIZACIÓN DEL SISTEMA OPERATIVO AL MOMENTO DE LA ENTREGA • EL SOFTWARE DEL EQUIPO RESIDE Y SE EJECUTA CON RECURSOS DEL MISMO • SE CONSIDERA EL SOPORTE VÍA ELECTRÓNICA PARA LA ACTUALIZACIÓN DE VERSIONES DEL SISTEMA OPERATIVO Y DE CONFIGURACIÓN • LOS EQUIPOS INCLUYEN HERRAJES PARA MONTAR EN RACK DE 19", CABLE DE ALIMENTACIÓN POLARIZADO CON CLAVIJA TIPO AMERICANO • LOS EQUIPOS INCLUYEN CABLE ADAPTADOR USB SERIAL COMPLETAMENTE COMPATIBLE, QUE PERMITE ESTABLECER LA CONEXIÓN DESDE EL PUERTO USB DE LA COMPUTADORA DE ADMINISTRACIÓN AL PUERTO DE CONSOLA DE ADMINISTRACIÓN DEL EQUIPO. **GARANTÍA Y SERVICIOS DE LOS CONMUTADORES DE DATOS.** • SE CONSIDERA LA INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE TODOS LOS EQUIPOS SOLICITADOS, DE ACUERDO CON LAS POLÍTICAS Y LINEAMIENTOS DEL ÁREA USUARIA. EN LA CIUDAD DE SAN FRANCISCO CAMPECHE, CAMPECHE. • SE CONSIDERAN TODOS LOS GASTOS DERIVADOS DE LA INSTALACIÓN. • SE CONSIDERA UNA ATENCIÓN DE FALLAS CON UN TIEMPO MÁXIMO DE 4 HORAS DE LUNES A VIERNES DE 8 AM A 8 PM. FUERA DE ESTE HORARIO EL TIEMPO MÁXIMO DE ATENCIÓN A FALLAS ES DE 6 HORAS. POR ESPACIO DE TRES AÑOS. • SE CONSIDERA UN MANTENIMIENTO PREVENTIVO EN EL LAPSO DE UNA AÑO. • SE INCLUYE UN SOPORTE TELEFÓNICO SIN COSTO ADICIONAL EN HORARIO DE LUNES A VIERNES DE 8 AM A 8 PM. • SE INCLUYE GARANTÍA EN EQUIPOS Y ACCESORIOS POR UN (1) AÑO SE CONSIDERA SUMINISTRO DE PARTES Y/O COMPONENTES EN CASO DE QUE SE REQUIERA, EN UN TIEMPO MÁXIMO DEL SIGUIENTE DÍA HÁBIL A PARTIR DEL REPORTE DEL FALLO. LOS DAÑOS CUBIERTOS POR LA GARANTÍA INCLUYEN DEFECTOS DE FABRICACIÓN Y VICIOS OCULTOS. • LOS EQUIPOS Y REFACCIONES QUE SE UTILICEN COMO REEMPLAZO PARA EL MANTENIMIENTO CORRECTIVO SON DE LA MISMA MARCA, YA QUE SE REQUIERE QUE SEAN 100% COMPATIBLES CON LAS FUNCIONALIDADES Y CARACTERÍSTICAS DEL EQUIPO. EL COSTO DE LOS EQUIPOS O REFACCIONES, ASÍ COMO LA INSTALACIÓN, GASTOS DE ENVÍO Y CONFIGURACIÓN CORRERÁN A CUENTA DE "EL PROVEEDOR". **REPORTE DE FALLAS** • "EL PROVEEDOR" CUENTA UNA MESA DE AYUDA PARA RECIBIR CUALQUIER EVENTO RELACIONADO CON LA OPERACIÓN DE LA INFRAESTRUCTURA SOLICITADA POR PARTE DE LA SECRETARIA DE SEGURIDAD PUBLICA DEL ESTADO DE CAMPECHE. ESTE CENTRO DE ATENCIÓN ES PROPIO Y ESTA EN SUS INSTALACIONES, MEDIANTE EL USO DE SUS PROPIAS HERRAMIENTAS Y DE MANERA DEDICADA PARA EL SOPORTE DE LA

Partida	Cant.	Unidad de Medida	Descripción
			INFRAESTRUCTURA DE COMUNICACIONES. • LAS TAREAS MÍNIMAS SE REALIZAN CON LA MESA DE AYUDA SON: RECIBIR, REGISTRAR, ANALIZAR, RESOLVER Y CANALIZAR LOS REPORTES DE INCIDENTES O FALTAS, DAR SEGUIMIENTO Y SOLUCIÓN A LOS REPORTES INFORMANDO A LOS USUARIOS OPORTUNAMENTE; ASÍ MISMO, GENERARÁ UN REGISTRO HISTÓRICO QUE PERMITA CONSULTAS, GENERACIÓN DE REPORTES Y SEGUIMIENTO SOBRE EL TIPO DE FALLAS PRESENTADAS Y LA FORMA COMO SE SOLUCIONARON. • LA ATENCIÓN Y SOPORTE SE REALIZAN A TRAVÉS DE UN NÚMERO TELEFÓNICO ÚNICO CON SERVICIO 01-800 SIN COSTO ADICIONAL PARA "EL ESTADO" Y A TRAVÉS DE CORREO O UNA PÁGINA WEB • LOS DATOS MÍNIMOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGRA EN EL CONTROL DE EVENTOS E INCIDENTES SERÁN: o IDENTIFICADOR DEL REPORTE O NÚMERO DE INCIDENTE O EVENTO. o IDENTIFICADOR DEL USUARIO QUE REPORTA. ESTOS SON LOS DATOS QUE IDENTIFICAN AL USUARIO QUE LEVANTÓ EL REPORTE. NOMBRE, TELÉFONO, CORREO ELECTRÓNICO Y UBICACIÓN. LA DEFINICIÓN FINAL DE ESTOS DATOS SE ACORDARÁN CON EL USUARIO FINAL. o HORA EN QUE REPORTA EL PROBLEMA POR PARTE DEL USUARIO AUTORIZADO. o TIPO DE FALLO. o DESCRIPCIÓN DEL FALLO. o TIEMPO DE SOLUCIÓN DEL INCIDENTE Y RESTABLECIMIENTO DEL SERVICIO. • ATENCIÓN DE REPORTES: 24X7 **ADMINISTRACIÓN DE SERVICIOS** SE ALINEAN TODOS LOS PROCESOS RELACIONADOS CON LA ADMINISTRACIÓN DEL SERVICIO, A LA BIBLIOTECA DE MEJORES PRÁCTICAS DE ITIL (IT INFRASTRUCTURE LIBRARY). ESTO ENGLOBA A TODOS LOS PROCESOS DE ENTREGA Y SOPORTE DE SERVICIO: 1) ADMINISTRACIÓN DE CONFIGURACIONES 2) ADMINISTRACIÓN DE CAMBIOS 3) ADMINISTRACIÓN DE INCIDENCIAS 4) ADMINISTRACIÓN DE PROBLEMAS 5) ADMINISTRACIÓN DE LIBERACIONES 6) ADMINISTRACIÓN DE LA CAPACIDAD 7) ADMINISTRACIÓN DE LOS NIVELES DE SERVICIO 8) ADMINISTRACIÓN DE LA DISPONIBILIDAD 9) ADMINISTRACIÓN DE COSTO 10) MESA DE SERVICIO (FUNCIÓN) SE ADJUNTAN LOS DOCUMENTOS QUE CERTIFICAN AL PERSONAL PROPIO DE "EL PROVEEDOR" PARA LA IMPLEMENTACIÓN EN LAS MEJORES PRÁCTICAS DE ITIL (IT INFRASTRUCTURE LIBRARY), 3 PERSONAS, 2 PERSONAS CERTIFICADAS EN ITIL OSA. "EL PROVEEDOR" CUMPLE CON LAS SIGUIENTES ACTIVIDADES: o IDENTIFICAR LA CAUSA DE LA RAÍZ DE TALES PROBLEMAS o ASEGURAR QUE LOS RECURSOS APROPIADOS SE ASIGNEN CONFORME SEA NECESARIO PARA IDENTIFICAR, SOLVENTAR LA FALLA, Y DAR SEGUIMIENTO AL INFORME SOBRE CUALQUIER CONSECUENCIA DE LA FALLA. o PROPORCIONAR AL CLIENTE UN REPORTE ESCRITO DETALLADO QUE INFORME LA CAUSA Y EL PROCEDIMIENTO PARA CORREGIRLA O MITIGARLA CUANDO SEA POSIBLE. PROPORCIONAR ACTUALIZACIONES DE MANERA MENSUAL. o VERIFICAR QUE TODAS LAS ACCIONES NECESARIAS SE HAN TOMADO PARA PREVENIR LA REPETICIÓN DE TAL FALLA. o MANTENER LOS PROCESOS DE ADMINISTRACIÓN DE CAMBIOS, INCLUYENDO LOS PROCEDIMIENTOS Y MÉTODOS VIGENTES PARA LOS CAMBIOS. o MANTENER LAS HERRAMIENTAS Y PROCESOS DE ADMINISTRACIÓN DE PROBLEMAS PARA LA GESTIÓN DE TODOS LOS PROBLEMAS Y ACCIONES PREVENTIVAS DESDE LA IDENTIFICACIÓN DE LA CAUSA RAÍZ HASTA EL CIERRE DEL PROBLEMA. o PREPARAR Y COMUNICAR LOS IMPACTOS MEDIANTE LA DOCUMENTACIÓN DE LA CAUSA RAÍZ DEL PROBLEMA, LOS ESFUERZOS PARA CORREGIR TEMPORAL O PERMANENTEMENTE EL PROBLEMA Y LOS SIGUIENTES PASOS PARA SU SEGUIMIENTO. o ESCALACIÓN DE LOS PROBLEMAS QUE HAYAN REBASADO LOS UMBRALES DE RESPUESTA BASADOS EN LA SEVERIDAD DEL PROBLEMA

OPERADO CON RECURSOS 2018 - FASP

Partida	Cant.	Unidad de Medida	Descripción
			SOPORTE POR PARTE DEL FABRICANTE EL CONMUTADOR DE DATOS OFERTADO TIENE EL RESPALDO POR PARTE DEL FABRICANTE Y "EL PROVEEDOR" ENTREGA LA SIGUIENTE DOCUMENTACIÓN: • DOCUMENTACIÓN EXPEDIDA POR EL POR EL FABRICANTE DEL CONMUTADOR DE DATOS EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" ES DISTRIBUIDOR AUTORIZADO DE LOS EQUIPOS EN MÉXICO E INDICAR EL NIVEL DE DISTRIBUCIÓN CON EL QUE CUENTA. • DOS INGENIEROS CERTIFICADOS POR EL FABRICANTE A NIVEL EXPERTO, PARA REALIZAR LA ACTIVIDADES DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO Y EN MARCHA. **CAPACITACIÓN** SE INCLUYE LO SIGUIENTE: • TRANSFERENCIA DE CONOCIMIENTOS PARA LA ADMINISTRACIÓN, CONFIGURACIÓN E INSTALACIÓN DE LOS EQUIPOS CONMUTADORES DE DATOS PARA 3 PERSONAS. • LA CAPACITACIÓN SE REALIZARÁ EN LAS INSTALACIONES DEL ÁREA USUARIA. TODOS LOS COSTOS QUE ESTO IMPLIQUE CORRERÁN A CUENTA DE "EL PROVEEDOR". **MEMORIAS TÉCNICAS** SE ENTREGARÁ LA MEMORIA TÉCNICA DE LAS CONFIGURACIONES REALIZADAS EN CADA UNO DE LOS CONMUTADORES DE DATOS
5	1	Pieza	**EQUIPO DE SEGURIDAD INFORMÁTICA** SE CONSIDERA EL SUMINISTRO E INSTALACIÓN DE UN EQUIPO DE SEGURIDAD PERIMETRAL UTM CON LAS SIGUIENTES CARACTERÍSTICAS MÍNIMAS: MARCA: FORTINET MODELO: FG-200E-BDL • SE CONTEMPLA EL SUMINISTRO, INSTALACIÓN, PUESTA EN PUNTO Y EN MARCHA DE UN EQUIPO DE SEGURIDAD INFORMÁTICA DEL TIPO ADMINISTRACIÓN UNIFICADA DE AMENAZAS (UTM POR SUS SIGLAS EN INGLÉS). CADA EQUIPO CUENTA CON: • EL DISPOSITIVO ES UNA APPLIANCE DE PROPÓSITO ESPECÍFICO • BASADO EN TECNOLOGÍA DE CIRCUITO INTEGRADO PARA APLICACIONES ESPECÍFICAS Y QUE ES 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, ENTRE OTROS. • CAPACIDAD DE INCREMENTAR EL RENDIMIENTO DE VPN A TRAVÉS DE SOLUCIONES EN HARDWARE DENTRO DEL MISMO DISPOSITIVO. • CAPACIDAD DE REENSAMBLADO DE PAQUETES EN CONTENIDO PARA BUSCAR ATAQUES O CONTENIDO PROHIBIDO, BASADO EN HARDWARE. • EL EQUIPO PUEDE SER CONFIGURADO EN MODO GATEWAY O EN MODO TRANSPARENTE EN LA RED. • EN MODO TRANSPARENTE, EL EQUIPO NO REQUIERE HACER MODIFICACIONES EN LA RED EN CUANTO A RUTEO O DIRECCIONAMIENTO IP. • A EXCEPCIÓN DE LA FUNCIONALIDAD DE VPN'S, TODAS LAS DEMÁS FUNCIONALIDADES EN MODO GATEWAY ESTÁN PRESENTES EN MODO TRANSPARENTE. • LA HERRAMIENTA FUNCIONA DESDE UN INICIO COMO MODO GATEWAY, MODO TRANSPARENTE Y MODO PROXY EXPLÍCITO. **CARACTERÍSTICAS DEL SISTEMA OPERATIVO INCLUIDO** • SISTEMA OPERATIVO PRE-ENDURECIDO ESPECÍFICO PARA SEGURIDAD QUE SEA COMPATIBLE CON EL APPLIANCE. POR SEGURIDAD Y FACILIDAD DE ADMINISTRACIÓN Y OPERACIÓN, NO SE ACEPTAN SOLUCIONES SOBRE SISTEMAS OPERATIVOS GENÉRICOS TALES COMO GNU/LINUX, FREEBSD, SUN SOLARIS, HP-UX DE HP, AIX DE IBM O MICROSOFT WINDOWS, ENTRE OTROS. • EL SISTEMA OPERATIVO INCLUYE UN SERVIDOR DE DNS QUE PERMITE RESOLVER DE

FASP OPERADO CON RECURSOS 2018

Partida	Cant.	Unidad de Medida	Descripción
			FORMA LOCAL CIERTAS CONSULTAS DE ACUERDO A LA CONFIGURACIÓN DEL ADMINISTRADOR. **FIREWALL** • LAS REGLAS DE FIREWALL ANALIZAN LAS CONEXIONES QUE ATRAVIESEN EN EL EQUIPO, ENTRE INTERFACES, GRUPOS DE INTERFACES (O ZONAS) Y VLANS. • POR GRANULARIDAD Y SEGURIDAD, EL FIREWALL PUEDE ESPECIFICAR POLÍTICAS TOMANDO EN CUENTA PUERTO FÍSICO FUENTE Y DESTINO. ESTO ES, EL PUERTO FÍSICO FUENTE Y EL PUERTO FÍSICO DESTINO FORMAN PARTE DE LA ESPECIFICACIÓN DE LA REGLA DE FIREWALL. • ES POSIBLE DEFINIR POLÍTICAS DE FIREWALL QUE SON INDEPENDIENTES DEL PUERTO DE ORIGEN Y PUERTO DE DESTINO. • LAS REGLAS DEL FIREWALL TOMAN 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 • 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 PUEDEN TENER LIMITANTES Y/O VIGENCIA EN BASE A TIEMPO. • LAS REGLAS DE FIREWALL PUEDEN TENER LIMITANTES Y/O VIGENCIA EN BASE A FECHAS (INCLUYENDO DÍA, MES Y AÑO) • SOPORTA LA CAPACIDAD DE DEFINIR NUEVOS SERVICIOS TCP Y UDP QUE NO ESTÉN CONTEMPLADOS EN LOS PREDEFINIDOS. • PUEDE DEFINIR EL TIEMPO DE VIDA DE UNA SESIÓN INACTIVA DE FORMA INDEPENDIENTE POR PUERTO Y PROTOCOLO (TCP Y UDP) • CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES ESTÁTICO, UNO A UNO, NAT. • CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES DINÁMICO, MUCHOS A UNO, PAT. • SOPORTA 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 TIENE 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, SOPORTA PERSISTENCIA DE SESIÓN MEDIANTE HTTP COOKIE O SSL SESSION ID • EN LA SOLUCIÓN DE BALANCEO DE CARGA DE ENTRE SERVIDORES SOPORTA MECANISMOS PARA DETECTAR LA DISPONIBILIDAD DE LOS SERVIDORES, DE FORMA TAL DE PODER EVITAR ENVIAR TRÁFICO A UN SERVIDOR NO DISPONIBLE. • EL EQUIPO PERMITE LA CREACIÓN DE POLÍTICAS DE TIPO FIREWALL CON CAPACIDAD DE SELECCIONAR CAMPOS COMO DIRECCIÓN, IDENTIFICADOR DE USUARIOS O IDENTIFICADOR DE DISPOSITIVOS PARA EL CASO DE DISPOSITIVOS MÓVILES COMO SMARTPHONES Y TABLETAS. • EL EQUIPO PERMITE LA CREACIÓN DE POLÍTICAS DE TIPO VPN CON CAPACIDAD DE SELECCIONAR CAMPOS COMO IPSEC O SSL SEGÚN SEA EL TIPO DE VPN • LA SOLUCIÓN TIENE LA CAPACIDAD DE HACER CAPTURA DE PAQUETES POR POLÍTICA DE SEGURIDAD IMPLEMENTADA PARA LUEGO SER EXPORTADO EN FORMATO PCAP. • LA SOLUCIÓN DE SEGURIDAD PERMITE LA CREACIÓN DE SERVICIOS DE FIREWALL PARA IMPLEMENTAR DENTRO DE LAS POLÍTICAS DE SEGURIDAD Y CATEGORIZARLOS DE MANERA PERSONALIZADA • LA SOLUCIÓN ES CAPAZ DE INTEGRAR LOS SERVICIOS DENTRO DE LAS CATEGORÍAS DE FIREWALL PREDEFINIDAS O PERSONALIZADAS Y ORDENARLOS ALFABÉTICAMENTE • EL DISPOSITIVO DE SEGURIDAD PUEDE DETERMINAR ACCESOS Y DENEGACIÓN A DIFERENTES TIPOS DE TRÁFICO PREDEFINIDOS DENTRO DE UNA LISTA LOCAL DE POLÍTICAS • LA SOLUCIÓN ES CAPAZ DE HABILITAR O DESHABILITAR EL PASO DE TRAFICO A TRAVÉS DE PROCESADORES DE PROPÓSITO ESPECIFICO, SI EL DISPOSITIVO CUENTA CON ESTOS PROCESADORES INTEGRADOS DENTRO DEL MISMO • LA SOLUCIÓN PUEDE CREAR E IMPLEMENTAR POLÍTICAS DE TIPO MULTICAST Y DETERMINAR EL SENTIDO DE LA POLÍTICA, ASÍ COMO TAMBIÉN LA HABILITACIÓN DEL NAT DENTRO DE CADA INTERFACE DEL DISPOSITIVO • EL DISPOSITIVO DE SEGURIDAD ES CAPAZ DE CREAR E INTEGRAR POLÍTICAS CONTRA ATAQUES DOS LAS CUALES SE PUEDE APLICAR POR INTERFACES. • EL DISPOSITIVO DE GENERAR LOGS DE CADA UNA DE LAS POLÍTICAS APLICADAS PARA

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			EVITAR LOS ATAQUES DE DOS • LA SOLUCIÓN DE SEGURIDAD PERMITE CONFIGURAR EL MAPEO DE PROTOCOLOS A PUERTOS DE MANERA GLOBAL O ESPECIFICA • LA SOLUCIÓN ES CAPAZ DE CONFIGURAR EL BLOQUEO DE ARCHIVOS O CORREOS ELECTRÓNICOS POR TAMAÑO, O POR CERTIFICADOS SSL INVÁLIDOS. • EL DISPOSITIVO INTEGRA LA INSPECCIÓN DE TRÁFICO TIPO SSL Y SSH BAJO PERFILES PREDEFINIDOS O PERSONALIZADOS • EL DISPOSITIVO ES CAPAZ DE EJECUTAR INSPECCIÓN DE TRAFICO SSL EN TODOS LOS PUERTOS Y SELECCIONAR BAJO QUE CERTIFICADO SERÁ VÁLIDO ESTE TRÁFICO • TIENE LA CAPACIDAD DE HACER ESCANEO A PROFUNDIDAD DE TRAFICO TIPO SSH DENTRO DE TODOS O CIERTO RANGO DE PUERTOS CONFIGURADOS PARA ESTE ANÁLISIS • LA SOLUCIÓN PERMITE BLOQUEAR O MONITOREAR TODA LA ACTIVIDAD DE TIPO EXEC, PORT-FORWARD, SSH-SHELL, Y X-11 SSH **ANTIVIRUS** • ES CAPAZ DE ANALIZAR, ESTABLECER CONTROL DE ACCESO Y DETENER ATAQUES Y HACER ANTIVIRUS EN TIEMPO REAL EN LOS SIGUIENTES PROTOCOLOS APLICATIVOS: HTTP, SMTP, IMAP, POP3, FTP. • EL ANTIVIRUS PUEDE CONFIGURARSE EN MODO PROXY COMO EN MODO DE FLUJO. EN EL PRIMER CASO, LOS ARCHIVOS SON TOTALMENTE RECONSTRUIDOS POR EL MOTOR ANTES DE HACER LA INSPECCIÓN. EN EL SEGUNDO CASO, LA INSPECCIÓN DE ANTIVIRUS SE HARÁ POR CADA PAQUETE DE FORMA INDEPENDIENTE. • 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 SOPORTA LA CAPACIDAD DE INSPECCIONAR Y DETECTAR VIRUS EN TRÁFICO IPV6. • LA CONFIGURACIÓN DE ANTIVIRUS EN TIEMPO REAL SOBRE LOS PROTOCOLOS HTTP, SMTP, IMAP, POP3 Y FTP ESTA COMPLETAMENTE INTEGRADA A LA ADMINISTRACIÓN DEL DISPOSITIVO APPLIANCE, QUE PERMITA LA APLICACIÓN DE ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. • EL ANTIVIRUS SOPORTA 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 DE MANERA OPCIONAL PUEDE INSPECCIONAR POR TODOS LOS VIRUS CONOCIDOS. • EL ANTIVIRUS INTEGRADO TIENE 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 TIENE LA CAPACIDAD DE PONER EN CUARENTENA A LOS CLIENTES CUANDO SE HAYA DETECTADO QUE LOS MISMOS ENVÍAN ARCHIVOS INFECTADOS CON VIRUS. • EL ANTIVIRUS INCLUYE CAPACIDADES DE DETECCIÓN Y DETENCIÓN DE TRÁFICO SPYWARE, ADWARE Y OTROS TIPOS DE MALWARE/GRAYWARE QUE PUDIERAN CIRCULAR POR LA RED. • EL ANTIVIRUS PUEDE HACER INSPECCIÓN Y CUARENTENA DE ARCHIVOS TRANSFERIDOS POR MENSAJERÍA INSTANTÁNEA (INSTANT MESSAGING) PARA MSN MESSENGER. • EL ANTIVIRUS SER CAPAZ DE FILTRAR ARCHIVOS POR EXTENSIÓN • EL ANTIVIRUS ES CAPAZ DE FILTRAR ARCHIVOS POR TIPO DE ARCHIVO (EJECUTABLES, POR EJEMPLO) SIN IMPORTAR LA EXTENSIÓN QUE TENGA EL ARCHIVO • 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** • LA CAPACIDAD ANTISPAM INCLUIDA ES 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. • LA CAPACIDAD ANTISPAM INCLUIDA PERMITE ESPECIFICAR LISTAS BLANCAS

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			(CONFIABLES, A LOS CUALES SIEMPRE SE LES PASA) Y LISTAS NEGRAS (NO CONFIABLES, A LOS CUALES SIEMPRE LES BLOQUEA). LAS LISTAS BLANCAS Y LISTAS NEGRAS SON POR DIRECCIÓN IP O POR DIRECCIÓN DE CORREO ELECTRÓNICO (E-MAIL ADDRESS). • LA CAPACIDAD ANTISPAM PUEDE CONSULTAR UNA BASE DE DATOS DONDE SE REVISE 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, TIENE LA FLEXIBILIDAD PARA ETIQUETARSE EN EL MOTIVO (SUBJECT) DEL MENSAJE O A TRAVÉS UN ENCABEZADO MIME EN EL MENSAJE. **FILTRAJE DE URLS (URL FILTERING)** • FACILIDAD PARA INCORPORAR CONTROL DE SITIOS A LOS CUALES NAVEGUEN LOS USUARIOS, MEDIANTE CATEGORÍAS. POR FLEXIBILIDAD, EL FILTRO DE URLS TIENE 75 CATEGORÍAS Y 54 MILLONES DE SITIOS WEB EN LA BASE DE DATOS. • PUEDE CATEGORIZAR CONTENIDO WEB REQUERIDO MEDIANTE IPV6. • 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. • CONFIGURABLE DIRECTAMENTE DESDE LA INTERFAZ DE ADMINISTRACIÓN DEL DISPOSITIVO APPLIANCE. CON CAPACIDAD PARA PERMITIR ESTA PROTECCIÓN POR POLÍTICA DE CONTROL DE ACCESO. • PERMITE 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 • LA SOLUCIÓN PERMITE REALIZAR EL FILTRADO DE CONTENIDO, TANTO REALIZANDO RECONSTRUCCIÓN DE TODA LA SESIÓN (MODO PROXY) COMO REALIZANDO INSPECCIÓN PAQUETE A PAQUETE SIN REALIZAR RECONSTRUCCIÓN DE LA COMUNICACIÓN (MODO FLUJO). • 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) SON PERSONALIZABLES. ESTOS MENSAJES DE REMPLAZO PUEDEN APLICARSE PARA CONEXIONES HTTP Y HTTPS, TANTO EN MODO PROXY COMO EN MODO FLUJO. • LOS MENSAJES DE REMPLAZO PUEDEN SER PERSONALIZADOS POR CATEGORÍA DE FILTRADO DE CONTENIDO. • CAPACIDAD DE FILTRADO DE SCRIPTS EN PÁGINAS WEB (JAVA/ACTIVE X). • LA SOLUCIÓN DE FILTRAJE DE CONTENIDO SOPORTA 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 PARA GOOGLE, YAHOO! Y BING. • ES POSIBLE DEFINIR CUOTAS DE TIEMPO PARA LA NAVEGACIÓN. DICHAS CUOTAS PUEDEN ASIGNARSE POR CADA CATEGORÍA Y POR GRUPOS. • ES POSIBLE EXCEPTUAR LA INSPECCIÓN DE HTTPS POR CATEGORÍA. • CUENTA CON LA CAPACIDAD DE IMPLEMENTAR EL FILTRO DE EDUCACIÓN DE YOUTUBE POR PERFIL DE FILTRO DE CONTENIDO PARA TRAFICO HTTP, GARANTIZANDO DE MANERA CENTRALIZADA, QUE TODAS LAS SESIONES ACEPTADAS POR UNA POLÍTICA DE SEGURIDAD CON ESTE PERFIL, VAN A PODER ACCEDER SOLAMENTE A CONTENIDO DE TIPO EDUCATIVO EN YOUTBUBE, BLOQUEANDO CUALQUIER TIPO DE CONTENIDO NO EDUCATIVO. • EL SISTEMA DE FILTRADO DE URLS TIENE 3 MÉTODOS DE INSPECCIÓN: 1. MODO DE FLUJO: LA PAGINA ES INSPECCIONADA PAQUETE A PAQUETE SIN RECONSTRUIR LA PÁGINA COMPLETA. 2. MODO PROXY: LA PAGINA ES RECONSTRUIDA COMPLETAMENTE PARA SER ANALIZADA A PROFUNDIDAD. 3. MODO DNS: LA INSPECCIÓN SE BASA ÚNICAMENTE EN LA CATEGORIZACIÓN DEL DOMINIO ACCESADO. • SE INCLUYE LA FUNCIONALIDAD DE REPUTACIÓN BASADA EN FILTRADO DE URLS. • LA FUNCIONALIDAD DE REPUTACIÓN BUSCA QUE, AL ACCEDER A PAGINAS DE CONTENIDO NO DESEADO (TALES COMO MALWARE, PORNOGRAFÍA, CONSUMO DE ANCHO DE BANDA EXCESIVO, ETC) SE ASIGNE UN PUNTAJE A CADA USUARIO O IP CADA VEZ VISITA UNA PÁGINA DE ESTA ÍNDOLE. DE ACUERDO CON ESTO SE EXTRAE LOS USUARIOS QUE INFRINGEN

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			LAS POLÍTICAS DE FILTRADO CON MÁS FRECUENCIA CON EL FIN DE DETECTAR ZOMBIES DENTRO DE LA RED. • EL SISTEMA DE FILTRADO DE URLS INCLUYE LA CAPACIDAD DE DEFINIR CUOTAS DE NAVEGACIÓN BASADAS EN VOLUMEN DE TRÁFICO CONSUMIDO. • SE INCORPORA LA FUNCIONALIDAD DE FILTRADO EDUCATIVO DE YOUTUBE (YOUTUBE EDUCATION FILTER) • EN DICHO SISTEMA CADA ORGANISMO OBTIENE UN ID DE YOUTUBE PARA HABILITAR EL CONTENIDO EDUCATIVO DEL MISMO. SE INSERTA DICHO CÓDIGO EN LA CONFIGURACIÓN DE FILTRADO DE URLS DEL EQUIPO PARA PODER HABILITAR ÚNICAMENTE EL CONTENIDO EDUCATIVO DE YOUTUBE. **PROTECCIÓN CONTRA INTRUSOS (IPS)** • EL DETECTOR Y PREVENTOR DE INTRUSOS PUEDE IMPLEMENTARSE TANTO EN LÍNEA COMO FUERA DE LÍNEA. EN LÍNEA, EL TRÁFICO A SER INSPECCIONADO PASARÁ A TRAVÉS DEL EQUIPO. FUERA DE LÍNEA, EL EQUIPO RECIBIRÁ EL TRÁFICO A INSPECCIONAR DESDE UN SWITCH CON UN PUERTO CONFIGURADO EN SPAN O MIRROR. • ES POSIBLE DEFINIR POLÍTICAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES PARA TRÁFICO IPV6. A TRAVÉS DE SENSORES. • CAPACIDAD DE DETECCIÓN DE MÁS DE 4000 ATAQUES. • CAPACIDAD DE ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS IPS MEDIANTE TECNOLOGÍA DE TIPO "PUSH" (PERMITE 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 ESTA 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 ESTA 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 PERMITE LA PROTECCIÓN DE ESTE SERVICIO POR POLÍTICA DE CONTROL DE ACCESO. • EL DETECTOR Y PREVENTOR DE INTRUSOS SOPORTA CAPTAR ATAQUES POR VARIACIONES DE PROTOCOLO Y ADEMÁS POR FIRMAS DE ATAQUES CONOCIDOS (SIGNATURE BASED / MISUSE DETECTION). • BASADO EN ANÁLISIS DE FIRMAS EN EL FLUJO DE DATOS EN LA RED, Y PERMITE CONFIGURAR FIRMAS NUEVAS PARA CUALQUIER PROTOCOLO. • ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS PARA EL DETECTOR DE INTRUSOS • EL DETECTOR DE INTRUSOS MITIGA LOS EFECTOS DE LOS ATAQUES DE NEGACIÓN DE SERVICIOS. • MÉTODOS DE NOTIFICACIÓN: • ALARMAS MOSTRADAS EN LA CONSOLA DE ADMINISTRACIÓN DEL APPLIANCE. • ALERTAS VÍA CORREO ELECTRÓNICO. • TIENE LA CAPACIDAD DE CUARENTENA, ES DECIR PROHIBIR EL TRÁFICO SUBSIGUIENTE A LA DETECCIÓN DE UN POSIBLE ATAQUE. ESTA CUARENTENA PUEDE DEFINIRSE PARA EL TRÁFICO PROVENIENTE DEL ATACANTE O PARA EL TRÁFICO DEL ATACANTE AL ATACADO. • LA CAPACIDAD DE CUARENTENA OFRECE LA POSIBILIDAD DE DEFINIR EL TIEMPO EN QUE SE BLOQUEARÁ EL TRÁFICO. TAMBIÉN SE DEFINE EL BLOQUEO DE FORMA "INDEFINIDA", HASTA QUE UN ADMINISTRADOR TOME UNA ACCIÓN AL RESPECTO. • OFRECE LA POSIBILIDAD DE GUARDAR INFORMACIÓN SOBRE EL PAQUETE DE RED QUE DETONÓ LA DETECCIÓN DEL ATAQUE, ASÍ COMO LOS 5 PAQUETES SUCESIVOS. ESTOS PAQUETES PUEDEN SER VISUALIZADOS POR UNA HERRAMIENTA QUE SOPORTE EL FORMATO PCAP. • SE INCLUYE PROTECCIÓN CONTRA AMENAZAS AVANZADAS Y PERSISTENTES (ADVANCED PERSISTENT THREATS). DENTRO DE ESTOS CONTROLES SE INCLUYEN: 1. PROTECCIÓN CONTRA BOTNETS: SE BLOQUEAN INTENTOS DE CONEXIÓN A SERVIDORES DE BOTNETS, PARA ELLO SE CUENTA CON UNA LISTA DE LOS SERVIDORES DE BOTNET MÁS UTILIZADO. DICHA LISTA SE ACTUALIZA DE FORMA PERIÓDICA POR EL FABRICANTE. 2. SANDBOXING: LA FUNCIONALIDAD DE SANDBOX HACE QUE EL ARCHIVO SEA EJECUTADO EN UN AMBIENTE SEGURO PARA ANALIZAR SU COMPORTAMIENTO Y, A BASE DE ESTE, TOMAR UNA

Partida	Cant.	Unidad de Medida	Descripción
			ACCIÓN SOBRE EL MISMO. **PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP)** • LA SOLUCIÓN OFRECE 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 SOPORTA EL ANÁLISIS DE ARCHIVOS DEL TIPO: MS-WORD, PDF, TEXTO, ARCHIVOS COMPRIMIDOS. • SOPORTA EL ESCANEO DE ARCHIVOS EN LOS SIGUIENTES PROTOCOLOS: HTTP, POP3, SMTP, IMAP, NNTP Y FTP. • ANTE LA DETECCIÓN DE UNA POSIBLE FUGA DE INFORMACIÓN PUEDEN 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 PERMITE 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 SOPORTA 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 PERMITE LA BÚSQUEDA DE PATRONES EN ARCHIVOS MEDIANTE LA DEFINICIÓN DE EXPRESIONES REGULARES. • SE PROVEE LA FUNCIONALIDAD DE FILTRADO DE FUGA DE INFORMACIÓN. DENTRO DE LAS TÉCNICAS DE DETECCIÓN SE CONSIDERA COMO MÍNIMO LAS SIGUIENTES: 1. FILTRADO POR TIPO DE ARCHIVO 2. FILTRADO POR NOMBRE DE ARCHIVO 3. FILTRADO POR EXPRESIONES REGULARES: SE DETECTARÁN LOS ARCHIVOS SEGÚN LAS EXPRESIONES REGULARES QUE SE ENCUENTREN DENTRO DE LOS MISMOS. 4. FINGERPRINTING: SE TOMA UNA MUESTRA DEL ARCHIVO QUE SE CONSIDERE COMO CONFIDENCIAL. SEGÚN ESTO SE BLOQUEA ARCHIVOS QUE SEAN IGUALES A ESTA MUESTRA. 5. WATERMARKING: SE INSERTARÁ UN "SELLO DE AGUA" DENTRO DEL ARCHIVO CONSIDERADO COMO CONFIDENCIAL. DE ACUERDO CON ESTO SE ANALIZAN LOS ARCHIVOS EN BUSCA DE ESTE SELLO DE AGUA, ESTE SE DETECTARÁ INCLUSO SI EL ARCHIVO SUFRIÓ CAMBIOS. **CONTROL DE APLICACIONES** • LA SOLUCIÓN SOPORTA LA CAPACIDAD DE IDENTIFICAR LA APLICACIÓN QUE ORIGINA CIERTO TRÁFICO A PARTIR DE LA INSPECCIÓN DE ESTE. • LA IDENTIFICACIÓN DE LA APLICACIÓN ES INDEPENDIENTE DEL PUERTO Y PROTOCOLO HACIA EL CUAL ESTÉ DIRECCIONADO DICHO TRÁFICO. • LA SOLUCIÓN TIENE UN LISTADO DE 1000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE. • EL LISTADO DE APLICACIONES SE ACTUALIZA PERIÓDICAMENTE. • PARA APLICACIONES IDENTIFICADAS PUEDEN DEFINIRSE LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) PUEDEN DEFINIRSE LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG. • PARA APLICACIONES DE TIPO P2P PUEDE DEFINIRSE ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING. • PREFERENTEMENTE SOPORTA MAYOR GRANULARIDAD EN LAS ACCIONES. **INSPECCIÓN DE CONTENIDO SSL** • LA SOLUCIÓN SOPORTA LA CAPACIDAD DE INSPECCIONAR TRÁFICO QUE ESTÉ SIENDO ENCRIPTADO MEDIANTE TLS PARA LOS SIGUIENTES PROTOCOLOS: HTTPS, IMAPS, SMTPS, POP3S. • LA INSPECCIÓN SE REALIZA MEDIANTE LA TÉCNICA CONOCIDA COMO HOMBRE EN EL MEDIO (MITM - MAN IN THE MIDDLE). • LA INSPECCIÓN DE CONTENIDO ENCRIPTADO NO REQUIERE NINGÚN CAMBIO DE CONFIGURACIÓN EN LAS APLICACIONES O SISTEMA OPERATIVO DEL USUARIO. • PARA EL CASO DE URL FILTERING, ES POSIBLE CONFIGURAR EXCEPCIONES DE INSPECCIÓN DE HTTPS. DICHAS EXCEPCIONES EVITAN QUE EL TRÁFICO SEA INSPECCIONADO PARA LOS SITIOS CONFIGURADOS. LAS EXCEPCIONES PUEDE DETERMINARSE POR CATEGORÍA DE FILTRADO. • EL EQUIPO ES CAPAZ DE ANALIZAR CONTENIDO CIFRADO (SSL O SSH) PARA LAS

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			FUNCIONALIDADES DE FILTRADO DE URLS, CONTROL DE APLICACIONES, PREVENCION DE FUGA DE INFORMACIÓN, ANTIVIRUS E IPS **ALTA DISPONIBILIDAD** • EL DISPOSITIVO SOPORTA ALTA DISPONIBILIDAD TRANSPARENTE, ES DECIR, SIN PÉRDIDA DE CONEXIONES EN CASO DE QUE UN NODO FALLE TANTO PARA IPV4 COMO PARA IPV6 • ALTA DISPONIBILIDAD EN MODO ACTIVO-PASIVO • ALTA DISPONIBILIDAD EN MODO ACTIVO-ACTIVO • POSIBILIDAD DE DEFINIR DOS INTERFACES PARA SINCRONÍA • EL ALTA DISPONIBILIDAD PODRÁ HACERSE DE FORMA QUE EL USO DE MULTICAST NO SEA NECESARIO EN LA RED • ES POSIBLE DEFINIR INTERFACES DE GESTIÓN INDEPENDIENTES PARA CADA MIEMBRO EN UN CLÚSTER. **CARACTERÍSTICAS DE ADMINISTRACIÓN** • INTERFACE 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 SOPORTA SSL SOBRE HTTP (HTTPS) • LA INTERFACE GRÁFICA DE USUARIO (GUI) VÍA WEB PUEDE ESTAR EN ESPAÑOL Y EN INGLÉS, CONFIGURABLE POR EL USUARIO. • INTERFACE BASADA EN LÍNEA DE COMANDO (CLI) PARA ADMINISTRACIÓN DE LA SOLUCIÓN. • PUERTO SERIAL DEDICADO PARA ADMINISTRACIÓN. ESTE PUERTO ESTA ETIQUETADO E IDENTIFICADO PARA TAL EFECTO. • COMUNICACIÓN CIFRADA Y AUTENTICADA CON USERNAME Y PASSWORD, TANTO COMO PARA LA INTERFACE GRÁFICA DE USUARIO COMO LA CONSOLA DE ADMINISTRACIÓN DE LÍNEA DE COMANDOS (SSH O TELNET) • EL ADMINISTRADOR DEL SISTEMA TIENE LAS OPCIONES INCLUIDAS 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 PUEDEN ESTAR RESTRINGIDOS A CONECTARSE DESDE CIERTAS DIRECCIONES IP CUANDO SE UTILICE SSH, TELNET,HTTP O HTTPS. • EL EQUIPO PUEDE 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. • SOPORTE DE SNMP VERSIÓN 2 • SOPORTE DE 3 SERVIDORES SYSLOG PARA ENVIAR BITÁCORAS A SERVIDORES DE SYSLOG REMOTOS • SOPORTE DE CONTROL DE ACCESO BASADO EN ROLES, CON CAPACIDAD DE CREAR 6 PERFILES PARA ADMINISTRACIÓN Y MONITOREO DEL FIREWALL. • MONITOREO DE COMPORTAMIENTO DEL APPLIANCE MEDIANTE SNMP, EL DISPOSITIVO ES CAPAZ DE ENVIAR TRAPS DE SNMP CUANDO OCURRA UN EVENTO RELEVANTE PARA LA CORRECTA OPERACIÓN DE LA RED. • ES POSIBLE DEFINIR LA DIRECCIÓN IP QUE SE UTILIZARÁ COMO ORIGEN PARA EL TRÁFICO INICIADO DESDE EL MISMO DISPOSITIVO. ESTO PUEDE HACERSE PARA EL TRÁFICO DE ALERTAS, SNMP, LOG Y GESTIÓN. **VIRTUALIZACIÓN** • EL DISPOSITIVO PUEDE VIRTUALIZAR LOS SERVICIOS DE SEGURIDAD MEDIANTE "VIRTUAL SYSTEMS", "VIRTUAL FIREWALLS" O "VIRTUAL DOMAINS". • LA INSTANCIA VIRTUAL SOPORTA FUNCIONALIDADES DE FIREWALL, VPN, URL FILTERING, IPS Y ANTIVIRUS. • SE INCLUYE LA LICENCIA PARA 10 (DIEZ) INSTANCIAS VIRTUALES DENTRO DE LA SOLUCIÓN A PROVEER. • CADA INSTANCIA VIRTUAL PUEDE TENER UN ADMINISTRADOR INDEPENDIENTE • LA CONFIGURACIÓN DE CADA INSTANCIA VIRTUAL PUEDE ESTAR AISLADA DE MANERA LÓGICA DEL RESTO DE LAS INSTANCIAS VIRTUALES.

Partida	Cant.	Unidad de Medida	Descripción
			• CADA INSTANCIA VIRTUAL PUEDE ESTAR EN MODO GATEWAY O EN MODO TRANSPARENTE A LA RED. • ES POSIBLE LA DEFINICIÓN Y ASIGNACIÓN DE RECURSOS DE FORMA INDEPENDIENTE PARA CADA INSTANCIA VIRTUAL. • ES POSIBLE DEFINIR DISTINTOS SERVIDORES DE LOG (SYSLOG) PARA CADA INSTANCIA VIRTUAL. • ES POSIBLE DEFINIR Y MODIFICAR LOS MENSAJES MOSTRADOS POR EL DISPOSITIVO DE FORMA INDEPENDIENTE PARA CADA INSTANCIA VIRTUAL. **LICENCIAMIENTO, SOPORTE Y ACTUALIZACIONES** • EL LICENCIAMIENTO DE TODAS LAS FUNCIONALIDADES ES ILIMITADO EN CUANTO A USUARIOS Y CONEXIONES LIMITÁNDOLA SOLAMENTE POR EL DESEMPEÑO DEL EQUIPO. • LA VIGENCIA DE LICENCIA DE ACTUALIZACIÓN INCLUYE LA CAPACIDAD DE HACER ACTUALIZACIONES DE FIRMAS IPS, URL FILTERING, ANTISPAM, ANTIVIRUS Y CUALQUIER OTRA ACTUALIZACIÓN NECESARIA PARA LA CORRECTA OPERACIÓN DEL EQUIPO CON LAS CARACTERÍSTICAS ARRIBA DESCRITAS, POR ESPACIO MÍNIMO DE 1 AÑO. • LA SOLUCIÓN CUENTA CON UN CENTRO DE INVESTIGACIÓN PROPIO DEL MISMO FABRICANTE PARA LA ACTUALIZACIÓN DE POLÍTICAS • EL EQUIPO INCLLUYE SOPORTE TELEFÓNICA, REEMPLAZO DE FÁBRICA, ACTUALIZACIONES DE FIRMWARE POR 1 AÑO. • EL FABRICANTE CUENTA CON UN CENTRO DE ATENCIÓN AL CLIENTE (TAC) BASADO EN LA CIUDAD DE MÉXICO CON ATENCIÓN Y SOPORTE EN LENGUAJE PORTUGUÉS, INGLÉS Y ESPAÑOL. ADEMÁS DE UN SOPORTE MUNDIAL TIPO "FOLLOW-THE-SUN". **CARACTERÍSTICAS TÉCNICAS** • EL EQUIPO CUENTA CON UN THROUGHPUT FIREWALL DE 20 GBPS, EL DESEMPEÑO DE FIREWALL APLICA TANTO PARA TRÁFICO IPV4 COMO IPV6. • EL EQUIPO CUENTA CON UN THROUGHPUT VPN IPSEC DE 9 GBPS. • EL EQUIPO CUENTA CON UN THROUGHPUT VPN SSL DE 900 MBPS. • EL EQUIPO CUENTA CON UN THROUGHPUT IPS DE 6 GBPS. • EL EQUIPO CUENTA CON UN THROUGHPUT DE PROTECCIÓN CONTRA MALWARE DE 1.2 GBPS. • EL EQUIPO CUENTA CON 2 MILLONES DE SESIONES CONCURRENTES • EL EQUIPO SOPORTA 135,000 NUEVAS SESIONES POR SEGUNDO. • EL EQUIPO PUEDE GENERAR 10,000 VPN'S IPSEC CLIENT TO GATEWAY Y 2,000 VPN'S IPSEC GATEWAY TO GATEWAY. • EL EQUIPO CUENTA DESDE UN INICIO CON LA FUNCIONALIDAD Y LICENCIAMIENTO DE 10 VIRTUAL FIREWALLS. **CARACTERÍSTICAS DE HARDWARE** • EL EQUIPO CUENTA CON 14 INTERFACES GIGAETHERNET RJ45. • EL EQUIPO CUENTA 4 SLOTS PARA INTERFACES GIGAETHERNET SFP • EL EQUIPO SOPORTA Y ADMINISTRAR 64 ACCESS POINTS FÍSICOS DE LA MISMA MARCA. • FUENTE DE PODER AC **SOPORTE DE FABRICANTE** EL DISPOSITIVO CONTEMPLA UNA SUSCRIPCIÓN DE SOPORTE Y PÓLIZA DE REEMPLAZO EN CASO DE FALLA DEL EQUIPO CON EL FABRICANTE, DE 1 AÑO, CON SOPORTE DEL FABRICANTE DE 8 HORAS X 5 DÍAS A LA SEMANA. "EL PROVEEDOR" INCLUYE EL SOPORTE DEL FABRICANTE PARA LOS BIENES MENCIONADOS, CONSIDERANDO LA VIGENCIA SOLICITADA EN ESTE ANEXO TÉCNICO. INCLUYENDO CON ELLO QUE EL ÁREA USUARIA CUENTA CON EL RESPALDO DEL FABRICANTE PARA ESCALAR FALLAS QUE REQUIERAN DE ANÁLISIS, DIAGNÓSTICO Y SOLUCIÓN DE FALLAS, ASÍ COMO PARA EL REEMPLAZO AVANZADO DE PARTES, CON LOS SIGUIENTES ALCANCES ADICIONALES CON RESPECTO A LOS EQUIPOS: • 12 MESES • ACCESO A LA BASE DE DATOS DE CONOCIMIENTO DEL FABRICANTE EN UN ESQUEMA 8X5 • SOPORTE TELEFÓNICO 8X5 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE WEB 8X5 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES • SOPORTE VÍA CHAT 8X5 PARA ATENCIÓN DE REPORTE DE FALLAS O INCIDENTES

OPERADO CON RECURSOS FASP 2018

Partida	Cant.	Unidad de Medida	Descripción
			• SOPORTE DE SOFTWARE CON RELEASES DE MANTENIMIENTO Y UPGRADES A NUEVAS VERSIONES • SOPORTE DE HARDWARE TIPO REEMPLAZO AVANZADO **RESPALDO DE FABRICANTE** EL EQUIPO DE SEGURIDAD INFORMÁTICA UTM SOLICITADA EN ESTE CONCEPTO CUENTA CON EL RESPALDO POR PARTE DEL FABRICANTE Y "EL PROVEEDOR" ENTREGA LA SIGUIENTE DOCUMENTACIÓN: o DOCUMENTACIÓN EXPEDIDA POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD INFORMÁTICA UTM EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" ES INTEGRADOR AUTORIZADO DE LOS EQUIPOS DEL MAS ALTO NIVEL Y HABILITADOS PARA DISTRIBUIR, IMPLEMENTAR Y BRINDAR SERVICIOS ADMINISTRADOS, AUTORIZADO PARA REVENDER LOS PRODUCTOS/SERVICIOS DEL FABRICANTE. o CERTIFICADO O CERTIFICADOS EXPEDIDA POR EL POR EL FABRICANTE DEL EQUIPO/LICENCIAS DE SEGURIDAD INFORMÁTICA UTM EN LA QUE MANIFIESTE QUE "EL PROVEEDOR" CUENTA CON LAS CERTIFICACIONES REQUERIDAS PARA BRINDAR SERVICIOS DE INSTALACIÓN Y SOPORTE DE LOS EQUIPOS DE SEGURIDAD SOLICITADOS. o DOS INGENIEROS CERTIFICADOS EN LA SOLUCIÓN PROPUESTA, PARA REALIZAR LAS ACTIVIDADES DE INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO Y EN MARCHA NIVEL EXPERTO AVALADO POR EL FABRICANTE. o "EL PROVEEDOR" DEMUESTRA SU EXPERIENCIA EN EL SOPORTE DE LAS LICENCIAS DE SEGURIDAD INFORMÁTICA SOLICITADO, A TRAVÉS DE LA DOCUMENTACIÓN DE CLIENTES EXCLUSIVAMENTE DE GOBIERNO EN DONDE HA INSTALADO EQUIPOS DE LA MISMA MARCA CON CARACTERÍSTICAS SIMILARES A LOS REQUERIDOS POR "EL ESTADO", LA CUAL TIENE LA SIGUIENTE INFORMACIÓN: NOMBRE, DIRECCIÓN, TELÉFONO Y CORREO ELECTRÓNICO DE LOS CLIENTES Y UNA DESCRIPCIÓN DEL PROYECTO DE MEDIA CUARTILLA. "EL ESTADO" SE RESERVARÁ EL DERECHO DE VERIFICAR DICHA INFORMACIÓN. **SOPORTE DEL PROVEEDOR** SE INCLUYE EL SERVICIO DE SOPORTE PARA EL EQUIPO CON LOS SIGUIENTES SERVICIOS: o DURACIÓN DE 12 MESES o ATENCIÓN DE FALLAS CON UN TIEMPO MÁXIMO DE 2 HORAS CON ESQUEMA 5X8. o SE CONSIDERA UN (1) MANTENIMIENTO PREVENTIVO AL AÑO PARA LOS EQUIPOS, PREVIO ACUERDO CON "EL ESTADO". LOS INSUMOS NECESARIOS PARA EL MANTENIMIENTO CORREN POR CUENTA DE "EL PROVEEDOR". o INCLUYE SOPORTE TELEFÓNICO SIN COSTO ADICIONAL EN HORARIO DE LUNES A VIERNES EN HORARIO DE OFICINA. o PARA LOS EQUIPOS O SOFTWARE DE LA SOLUCIÓN DE SEGURIDAD PARA LOS CUALES EL FABRICANTE LIBERE NUEVAS VERSIONES DENTRO DE LA VIGENCIA DE LA PÓLIZA DE SOPORTE, "EL PROVEEDOR" REALIZA LA INSTALACIÓN SIN COSTO PARA "EL ESTADO" DICHAS ACTUALIZACIONES. **ASISTENCIA TÉCNICA** "EL PROVEEDOR" CUENTA CON UN CENTRO DE CONSULTA O ASESORÍA TELEFÓNICA QUE PERMITA AL PERSONAL TÉCNICO DE "EL ESTADO" REALIZAR ACLARACIONES Y CONSULTAS SOBRE EL USO Y CONFIGURACIÓN DE LOS EQUIPOS ANTES MENCIONADOS. PARA ESTA CLASE DE SERVICIO NO SE TOTALIZAN HORAS MENSUALES EN UNO O VARIOS EVENTOS Y NO HAY RESTRICCIÓN EN LA DURACIÓN DE CADA EVENTO. LOS DATOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGRA EN EL CONTROL DE EVENTOS E INCIDENTES SON: o IDENTIFICADOR DEL REPORTE O NÚMERO DE INCIDENTE O EVENTO o IDENTIFICADOR DEL USUARIO QUE REPORTA. ESTOS SON LOS DATOS QUE IDENTIFICAN AL USUARIO QUE LEVANTÓ EL REPORTE. NOMBRE, TELÉFONO, CORREO ELECTRÓNICO Y UBICACIÓN. LA DEFINICIÓN FINAL DE ESTOS DATOS SE ACORDARÁ CON "EL PROVEEDOR" o HORA EN QUE REPORTA EL PROBLEMA POR PARTE DEL USUARIO AUTORIZADO o TIPO DE FALLO o DESCRIPCIÓN DEL FALLO o TIEMPO DE SOLUCIÓN DEL INCIDENTE Y RESTABLECIMIENTO DEL SERVICIO. **TIEMPOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN** EL TIEMPO DEL INICIO DE ATENCIÓN O RESPUESTA A UN REPORTE EFECTUADO A "EL PROVEEDOR" PROPORCIONA UN FOLIO DE ATENCIÓN AL RECIBIRLO

Partida	Cant.	Unidad de Medida	Descripción
			TIEMPO MÁXIMO DE SOLUCIÓN DE FALLAS DESPUÉS DEL INICIO DE LA ATENCIÓN ES: 2 HORAS COMO MÁXIMO PARA INICIO DE DIAGNÓSTICO, EN EL CASO DE FALLAS MAYORES SU ATENCIÓN SE CONTINUA AÚN FUERA DE HORARIO DE COBERTURA HASTA SU SOLUCIÓN, SIN NINGÚN COSTO, SIEMPRE QUE HAYA INICIADO SU ATENCIÓN DENTRO DEL HORARIO DE SERVICIO. "EL PROVEEDOR" ESTA OBLIGADO A CONTINUAR CON LA ATENCIÓN, SIN COSTO, DE FALLAS O PROBLEMAS DETECTADOS DENTRO DE LA VIGENCIA DEL CONTRATO HASTA SU SOLUCIÓN, AÚN CUANDO ÉSTA, SE EXTIENDA MÁS ALLÁ DE AQUÉLLA; PRORROGÁNDOSE LOS DERECHOS QUE OTORGA DICHO CONTRATO PARA ESTOS REPORTES DE FALLA, EN LOS TÉRMINOS ORIGINALES. **MANTENIMIENTO PREVENTIVO** EL MANTENIMIENTO PREVENTIVO SE DA A TODOS Y CADA UNO DE LOS EQUIPOS INVENTARIADOS SEÑALADOS EN EL PROGRAMA DE MANTENIMIENTO PREVENTIVO, 1 (UNA) VEZ DURANTE LA VIGENCIA DEL CONTRATO, CON EXCEPCIÓN ÚNICA EN AQUELLOS CASOS EN DONDE LOS EQUIPOS NO PUEDEN DEJAR DE OPERAR, EN CUYO CASO EL PRESTADOR DEL SERVICIO NOTIFICA PARA QUE DE MANERA CONJUNTA SE PROGRAMEN. EL MANTENIMIENTO SE PROPORCIONADO AL "HARDWARE" Y AL "SOFTWARE" QUE COMPONEN LOS EQUIPOS, CON LA FINALIDAD DE MANTENER LA VIGENCIA TECNOLÓGICA DEL EQUIPO, ESTE MANTENIMIENTO INCLUYE LAS ACTUALIZACIONES DEL "SOFTWARE" A LA ÚLTIMA VERSIÓN GRATUITA EMITIDA POR EL FABRICANTE Y QUE NO REQUIERAN MODIFICACIONES EN EL HARDWARE DEL EQUIPO. "EL PROVEEDOR" PROPORCIONA, POR ESCRITO, UN ANÁLISIS EXPERTO DEL ESTADO QUE GUARDA EL HARDWARE Y SOFTWARE, CON LA FINALIDAD DE GARANTIZAR UN ÓPTIMO NIVEL DEL FUNCIONAMIENTO DE LOS EQUIPOS. SE ELABORA Y REVISA CONJUNTAMENTE CON EL PERSONAL TÉCNICO DE "EL PROVEEDOR", EL PROGRAMA DE TRABAJO, LAS ACTIVIDADES Y FECHAS DEL MANTENIMIENTO PREVENTIVO A DETALLE; CON CANTIDADES, NOMBRES DE LOS RESPONSABLES A EJECUTAR Y SUPERVISAR LA APLICACIÓN DE DICHOS SERVICIOS, A MÁS TARDAR EN LA SEGUNDA SEMANA CONTADA A PARTIR DE LA FORMALIZACIÓN DEL CONTRATO. SE ENTREGA COPIA DE LOS PROGRAMAS, PROCEDIMIENTOS O CALENDARIOS FORMALIZADOS CONJUNTAMENTE EN LA FASE DE REVISIÓN. EN CASO DE QUE EXISTAN MODIFICACIONES AL PROGRAMA VALIDADO, ESTAS SE REGISTRAN POR ESCRITO Y DE COMÚN ACUERDO ENTRE AMBAS PARTES. PARA EL CUMPLIMIENTO DEL PROGRAMA DE MANTENIMIENTO PREVENTIVO, "EL PROVEEDOR" PRESENTA POR ESCRITO LOS RECURSOS HUMANOS Y TÉCNICOS, ASÍ COMO PROTOCOLOS DE PRUEBA, CON LOS QUE CUBRE EL SERVICIO. **MANTENIMIENTO CORRECTIVO** SE PROPORCIONAN LOS MANTENIMIENTOS CORRECTIVOS SURGIDOS DURANTE LA VIGENCIA DEL CONTRATO, AL HARDWARE Y SOFTWARE DEL EQUIPO, EN EL CUAL INCLUYEN LAS REFACCIONES Y/O PARTES ORIGINALES Y ACTUALIZACIONES DEL "SOFTWARE" QUE SE REQUIEREN PARA REPARACIONES DEL EQUIPO, ASÍ MISMO SE SUMINISTRA LA MANO DE OBRA PARA SU INSTALACIÓN. LOS EQUIPOS QUE SE UTILICEN EN TODOS LOS CASOS, TIENEN CALIDAD Y CARACTERÍSTICAS TÉCNICAS IGUALES O SUPERIORES A LAS DEL EQUIPO ORIGINAL, DE TAL MANERA QUE SE GARANTIZA EL FUNCIONAMIENTO ADECUADO DEL HARDWARE Y SOFTWARE. SE APLICAN PRUEBAS DE DIAGNÓSTICO Y OPERACIÓN DE RESPALDO ANTES DE PROCEDER A LA REPARACIÓN DE ESTE, SEGÚN RESULTE EL DIAGNÓSTICO APLICADO. AL FINALIZAR SE ENTREGA COPIA DEL REPORTE DE SERVICIO DE MANTENIMIENTO CORRECTIVO. EN EL CASO DE UNA CONTINGENCIA MAYOR O DE SEVERIDAD CRÍTICA, "EL PROVEEDOR" ASIGNA UN INGENIERO EN SITIO HASTA LA RESOLUCIÓN TOTAL DEL PROBLEMA. **PROCEDIMIENTO DE ESCALAMIENTO** SE INCLUYE UNA RELACIÓN CON NOMBRES DE RESPONSABLES, TELÉFONOS, CORREOS ELECTRÓNICOS Y CELULARES, ASÍ COMO LOS HORARIOS DE ATENCIÓN PARA LEVANTAR REPORTES DE MANTENIMIENTO CORRECTIVO, ASÍ COMO LOS NÚMEROS DE RADIOLOCALIZADORES PARA REPORTAR FALLAS FUERA DE LOS HORARIOS DE SERVICIO, LOS TIEMPOS DE RESPUESTA SE SUJETAN TAMBIÉN A LO ESTIPULADO EN EL PUNTO DE "TIEMPOS MÁXIMOS DE RESPUESTA DE ATENCIÓN/SOLUCIÓN" DE ESTE ANEXO. CONTIENE EL PROCEDIMIENTO DE ESCALAMIENTO DESDE EL MOMENTO EN QUE SE REPORTE UNA FALLA EN UN EQUIPO HASTA SU SOLUCIÓN Y LOS NOMBRES Y CARGOS DE LOS RESPONSABLES DE LA EMPRESA EN CADA PROCESO

FASP OPERADO CON RECURSOS 2018