GOBIERNO DEL ESTADO DE CAMPECHE
FONDO DE APORTACIONES PARA LA SEGURIDAD PÚBLICA
(FASP 2015)

CRECER EN GRANDE CAMPECHE 2015 - 2021

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

ESTADO: **CAMPECHE**
MUNICIPIO: **CAMPECHE**
LOCALIDAD: **SAN FRANCISCO DE CAMPECHE**

PROGRAMA: **FORTALECIMIENTO DE PROGRAMAS PRIORITARIOS DE LAS INSTITUCIONES ESTATALES DE SEGURIDAD PÚBLICA E IMPARTICIÓN DE JUSTICIA**

CONCEPTO: **"ADQUISICION DE UNA LICENCIA FIREWALL"**

CONTRATO NÚM: 086/2017 FECHA: 17 DE JULIO DE 2017

EN LA CIUDAD DE SAN FRANCISCO DE CAMPECHE, ESTADO DE CAMPECHE, A LOS 02 DÍAS DEL MES DE AGOSTO DEL AÑO DOS MIL DIECISIETE; SE HACE CONSTAR QUE SE RECIBIO DE CONFORMIDAD LA LICENCIA FIREWALL, CON LOS REQUISITOS Y PLAZOS ESTABLECIDOS, EN PRESENCIA DE LOS REPRESENTANTES QUE INTERVINIERON EN LA ENTREGA-RECEPCIÓN EL PROYECTO.

ENTREGA EL PROVEEDOR:

ESTRATEGIAS EN TECNOLOGÍA CORPORATIVA, S.A. DE C.V.

RECIBE (QUIEN OPERA EL PROYECTO)

GOB. DEL ESTADO: X NOMBRE: **DR. JORGE DE JESÚS ARGÁEZ URIBE**
GOB. MUNICIPAL: _____ CARGO: **SECRETARIO DE SEGURIDAD PÚBLICA**
GOB. FEDERAL: _____ DEPENDENCIA: **SECRETARIA DE SEGURIDAD PUBLICA**

DESCRIPCIÓN DEL PROYECTO

CANT.	CONCEPTO	UNIDAD DE MEDIDA	PRECIO UNITARIO	IMPORTE
1	**RENOVACIÓN DE LICENCIAS FORTINET** TIPO: UTM BUNDLE (24X7 FORTICARE PLUS NGFW, AV, WEB FILTERING AND ANTISPAM SERVICES). FECHA DE TÉRMINO: 30/JUNIO/2018 PARA EQUIPOS CON NÚMERO DE SERIE: *FGT60D4613054250 *FGT60D4613057081 *FGT90D3Z14017471 *FGT90D3Z14017487 ALCANCES: 1. MESA DE AYUDA 5X8 POR 12 MESES.	LICENCIA	$154,653.00	$154,653.00

OPERADO CON RECURSOS FASP 2015.

GOBIERNO DEL ESTADO CAMPECHE 2015-2021

GOBIERNO DEL ESTADO DE CAMPECHE
FONDO DE APORTACIONES PARA LA SEGURIDAD PÚBLICA
(FASP 2015)

CRECER EN GRANDE CAMPECHE 2015 - 2021

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

	2. SOPORTE TELEFÓNICO Y EN SITIO TIPO PLATA 5X8 POR 12 MESES. 3. TIEMPO DE RESPUESTA TELEFÓNICO DE 2 HORAS PARA PRIORIDAD UNO Y 4 HORAS PARA PRIORIDAD DOS, DENTRO DEL TIEMPO 5X8. 4. TIEMPO DE RESPUESTA INGENIERO EN SITIO AL DÍA SIGUIENTE HÁBIL, CON ATENCIÓN DENTRO DEL TIEMPO 5X8. 5. EL TIEMPO DE RESPUESTA PARA INGENIERO EN SITIO INICIA A CONTEO A PARTIR DE QUE SE DETERMINE LA NECESIDAD. 6. APERTURA DE CASOS CON EL FABRICANTE CON CONTRATO VIGENTE. 7. SEGUIMIENTO PUNTUAL DE CASO ABIERTO AL FABRICANTE Y EJECUCIÓN DE ACCIONES A TRAVÉS DEL ACCESO REMOTO DISPUESTO POR EL CLIENTE. 8. ANÁLISIS REMOTO DE ERROR Y PROPUESTA INICIAL DE SOLUCIÓN. 9. NOTIFICACIÓN DE EXISTENCIA DE ACTUALIZACIONES Y PARCHES VÍA EMAIL. 10. SOPORTE PARA INSTALACIÓN DE PARCHES VÍA REMOTA MEDIANTE ACCESO DISPUESTO POR EL CLIENTE. 11. SOPORTE SOBRE RESOLUCIÓN DE DUDAS SOBRE LA ADMINISTRACIÓN DE LA HERRAMIENTA VÍA EMAIL.			
			SUBTOTAL	**$154,653.00**
			16%I.V.A.	**$ 21,744.48**
			TOTAL	**$179,397.48**

	AÑO	**TOTAL**
INVERSIÓN EJERCIDA PARA LA REALIZACIÓN DEL PROYECTO	**2015**	**$ 179,397.48 M.N.**

UNA VEZ VERIFICADA LA LICENCIA POR PARTE DE LOS QUE INTERVIENEN EN ESTE ACTO, SE CONCLUYE QUE, SE ENCUENTRAN EN CONDICIONES DE SER RECIBIDOS POR LA UNIDAD RESPONSABLE.

LA PRESENTE ACTA NO EXIME AL PROVEEDOR DE LOS DEFECTOS O VICIOS OCULTOS QUE RESULTAREN EN LOS MISMOS Y SE OBLIGA A CORREGIR LAS DEFICIENCIAS DETECTADAS SIN COSTO ALGUNO PARA EL GOBIERNO DEL ESTADO DE CAMPECHE.

FASP OPERADO CON RECURSOS 2015.

GOBIERNO DEL ESTADO CAMPECHE 2015-2021

GOBIERNO DEL ESTADO DE CAMPECHE
FONDO DE APORTACIONES PARA LA SEGURIDAD PÚBLICA
(FASP 2015)

CRECER EN GRANDE
CAMPECHE
2015 - 2021

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

EL GOBIERNO DEL ESTADO DE CAMPECHE, A TRAVÉS DEL **TITULAR DE LA SECRETARÍA DE SEGURIDAD PÚBLICA,** RECIBE LOS BIENES A SU ENTERA SATISFACCIÓN.

NO HABIENDO OTRO ASUNTO QUE TRATAR, SE DA POR CONCLUÍDA LA PRESENTE ACTA, FIRMANDO AL CALCE LOS QUE EN ELLA INTERVINIERON.

ENTREGA POR "EL PROVEEDOR"

ING. JUAN GUALBERTO CABRERA PEREZ
REPRESENTANTE LEGAL

RECIBE

DR. JORGE DE JESÚS ARGAEZ URIBE
SECRETARIO DE SEGURIDAD PÚBLICA

LIC. EMMA VANESSA VALLE ABREU
SUBDIRECTORA DE RECURSOS FEDERALES DE LA SECRETARÍA DE SEGURDIAD PÚBLICA

FASP 2015. OPERADO CON RECURSOS

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

Anexo único

CANT.	DESCRIPCIÓN	UNIDAD DE MEDIDA
1	**LICENCIA PARA EQUIPO DE SEGURIDAD UTM** 1. OBJETO: ADQUISICIÓN DE LICENCIAS PARA UN SISTEMA DE SEGURIDAD INFORMÁTICA PERIMETRAL DEL TIPO ADMINISTRACIÓN UNIFICADA DE AMENAZAS (UTM POR SUS SIGLAS EN INGLÉS), DONDE SE OFRECEN LAS FUNCIONALIDADES QUE SE DETALLAN EN EL PRESENTE DOCUMENTO. 2. EQUIPOS SE CONSIDERA LA LICENCIA Y LOS SERVICIOS PARA LOS SIGUIENTES NÚMEROS DE SERIE: • FGT60D4613054250 • FGT60D4613057081 • FGT90D3Z14017471 • FGT90D3Z14017487 FIREWALL • LAS REGLAS DE FIREWALL ANALIZAN LAS CONEXIONES QUE ATRAVIESAN 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 DEBERÁN FORMAR 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 SE 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, ESPECIFICANDO 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 TIENEN 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 ESTAN CONTEMPLADOS EN LOS PREDEFINIDOS. • PUEDE DEFINIRSE EL TIEMPO DE VIDA DE UNA SESIÓN INACTIVA DE FORMA INDEPENDIENTE POR PUERTO Y PROTOCOLO (TCP Y UDP) • TIENE CAPACIDAD DE HACER TRASLACIÓN DE DIRECCIONES ESTÁTICO, UNO A UNO, NAT. • TIENE 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	**LICENCIA**

FASP OPERADO CON RECURSOS .2015.

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

	(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, SE SOPORTA PERSISTENCIA DE SESIÓN AL MENOS MEDIANTE HTTP COOKIE O SSL SESSION ID • EN LA SOLUCIÓN DE BALANCEO DE CARGA DE 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. • 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 TRÁFICO A TRAVÉS DE PROCESADORES DE PROPÓSITO ESPECÍFICO, 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 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 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 TRÁFICO SSL EN TODOS LOS PUERTOS Y SELECCIONAR BAJO QUE CERTIFICADO SERÁ VÁLIDO ESTE TRÁFICO • TIENE LA CAPACIDAD DE HACER ESCANEO A PROFUNDIDAD DE TRÁFICO TIPO SSH DENTRO DE TODOS O CIERTO RANGO DE PUERTOS CONFIGURADOS PARA ESTE ANÁLISIS • LA SOLUCIÓN PERMITIE BLOQUEAR O MONITOREAR TODA LA ACTIVIDAD DE TIPO EXEC, PORT-FORWARD, SSH-SHELL, Y X-11 SSH	

OPERADO CON RECURSOS FASP 2015.

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

ANTIVIRUS

- TIENE LA CAPACIDAD DE ANALIZAR, ESTABLECER CONTROL DE ACCESO Y DETENER ATAQUES Y HACER ANTIVIRUS EN TIEMPO REAL EN AL MENOS LOS SIGUIENTES PROTOCOLOS APLICATIVOS: HTTP, SMTP, IMAP, POP3, FTP.
- EL ANTIVIRUS SE PUEDE CONFIGURAR 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 HACE 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 ESTÁ 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 DEFINE CUÁL ES CONVENIENTE UTILIZAR PARA SU IMPLEMENTACIÓN EVALUANDO DESEMPEÑO Y SEGURIDAD.
- EL APPLIANCE PUEDE DE MANERA OPCIONAL INSPECCIONAR POR TODOS LOS VIRUS CONOCIDOS.
- EL ANTIVIRUS INTEGRADO TIENE LA CAPACIDAD DE PONER EN CUARENTENA ARCHIVOS ENCONTRADOS INFECTADOS QUE ESTAN 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 AL MENOS 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 TIENE EL ARCHIVO
- TIENE CAPACIDAD DE ACTUALIZAR AUTOMÁTICAMENTE LA FIRMA DE ANTIVIRUS 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)

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 RECHAZA EL MENSAJE.
- 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 SE LES BLOQUEA). LAS LISTAS BLANCAS Y

OPERADO CON RECURSOS FASP 2015.

LISTAS NEGRAS PUEDEN SER POR DIRECCIÓN IP O POR DIRECCIÓN DE CORREO ELECTRÓNICO (E-MAIL ADDRESS).

- LA CAPACIDAD ANTISPAM PUEDE CONSULTAR UNA BASE DE DATOS DONDE SE REVISA POR LO MENOS DIRECCIÓN IP DEL EMISOR DEL MENSAJE, URLS CONTENIDOS DENTRO DEL MENSAJE Y CHECKSUM DEL MENSAJE, COMO MECANISMOS PARA DETECCIÓN DE SPAM
- EN EL CASO DE ANÁLISIS DE SMTP, LOS MENSAJES ENCONTRADOS COMO SPAM PUEDEN SER ETIQUETADOS O RECHAZADOS (DESCARTADOS). EN EL CASO DE ETIQUETAMIENTO DEL MENSAJE, SE 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)

- TIENE FACILIDAD PARA INCORPORAR CONTROL DE SITIOS A LOS CUALES NAVEGAN LOS USUARIOS, MEDIANTE CATEGORÍAS. POR FLEXIBILIDAD, EL FILTRO DE URLS TIENE POR LO MENOS 75 CATEGORÍAS Y POR LO MENOS 54 MILLONES DE SITIOS WEB EN LA BASE DE DATOS.
- PUEDE CATEGORIZAR CONTENIDO WEB REQUERIDO MEDIANTE IPV6.
- TIENE 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.
- ES 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 PERTENECE 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.
- TIENE 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 SOPORTA AL MENOS 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

OPERADO CON RECURSOS FASP 2015.

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

ACEPTADAS POR UNA POLITICA DE SEGURIDAD CON ESTE PERFIL, PUEDEN ACCEDER SOLAMENTE A CONTENIDO DE TIPO EDUCATIVO EN YOUTUBE, BLOQUEANDO CUALQUIER TIPO DE CONTENIDO NO EDUCATIVO.

- EL SISTEMA DE FILTRADO DE URLS TIENE AL MENOS 3 MÉTODOS DE INSPECCIÓN:
  1. MODO DE FLUJO: LA PÁGINA ES INSPECCIONADA PAQUETE A PAQUETE SIN RECONSTRUIR LA PÁGINA COMPLETA.
  2. MODO PROXY: LA PÁGINA 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 PÁGINAS 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 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 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.
- ES POSIBLE DEFINIR POLÍTICAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES PARA TRÁFICO IPV6. A TRAVÉS DE SENSORES.
- TIENE CAPACIDAD DE DETECCIÓN DE MÁS DE 4000 ATAQUES.
- TIENE CAPACIDAD DE ACTUALIZACIÓN AUTOMÁTICA DE FIRMAS IPS MEDIANTE TECNOLOGÍA DE TIPO "PUSH" (PERMITIE RECIBIR LAS ACTUALIZACIONES CUANDO LOS CENTROS DE ACTUALIZACIÓN ENVÍAN NOTIFICACIONES SIN PROGRAMACIÓN PREVIA), ADICIONAL A TECNOLOGÍAS TIPO "PULL" (CONSULTA LOS CENTROS DE ACTUALIZACIÓN POR VERSIONES NUEVAS)
- EL DETECTOR Y PREVENTOR DE INTRUSOS ESTÁ 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 ESTÁ PERFECTAMENTE INTEGRADA A LA INTERFAZ DE ADMINISTRACIÓN DEL DISPOSITIVO DE SEGURIDAD APPLIANCE, SIN NECESIDAD DE INTEGRAR OTRO TIPO DE CONSOLA PARA 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).

OPERADO CON RECURSOS FASP 2015.

- BASADO EN ANÁLISIS DE FIRMAS EN EL FLUJO DE DATOS EN LA RED, 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 AL MENOS 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 BLOQUEA EL TRÁFICO. TAMBIÉN SE PUEDE DEFINIR EL BLOQUEO DE FORMA "INDEFINIDA", HASTA QUE UN ADMINISTRADOR TOME UNA ACCIÓN AL RESPECTO.
  - SE OFRECE LA POSIBILIDAD DE GUARDAR INFORMACIÓN SOBRE EL PAQUETE DE RED QUE DETONÓ LA DETECCIÓN DEL ATAQUE, ASÍ COMO AL MENOS LOS 5 PAQUETES SUCESIVOS. ESTOS PAQUETES 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 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 PERMITEN 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.
- PUEDE SOPORTAR EL ESCANEO DE ARCHIVOS EN AL MENOS LOS SIGUIENTES PROTOCOLOS: HTTP, POP3, SMTP, IMAP, NNTP Y FTP.
- ANTE LA DETECCIÓN DE UNA POSIBLE FUGA DE INFORMACIÓN PUEDE APLICARSE 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 PUEDE 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 CONSIDERAN COMO MÍNIMO LAS SIGUIENTES:
  1. FILTRADO POR TIPO DE ARCHIVO

OPERADO CON RECURSOS FASP 2015.

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

2. FILTRADO POR NOMBRE DE ARCHIVO
3. FILTRADO POR EXPRESIONES REGULARES: SE DETECTAN LOS ARCHIVOS SEGÚN LAS EXPRESIONES REGULARES QUE SE ENCUENTRAN DENTRO DE LOS MISMOS.
4. FINGERPRINTING: SE TOMA UNA MUESTRA DEL ARCHIVO QUE SE CONSIDERE COMO CONFIDENCIAL. SEGÚN ESTO SE BLOQUEAN ARCHIVOS QUE SEAN IGUALES A ESTA MUESTRA.
5. 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 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 ESTA DIRECCIONADO DICHO TRÁFICO.
- LA SOLUCIÓN TIENE UN LISTADO DE AL MENOS 1000 APLICACIONES YA DEFINIDAS POR EL FABRICANTE.
- EL LISTADO DE APLICACIONES PUEDE ACTUALIZARSE PERIÓDICAMENTE.
- PARA APLICACIONES IDENTIFICADAS SE PUEDEN DEFINIR AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG.
- PARA APLICACIONES NO IDENTIFICADAS (DESCONOCIDAS) SE PUEDEN DEFINIR AL MENOS LAS SIGUIENTES OPCIONES: PERMITIR, BLOQUEAR, REGISTRAR EN LOG.
- PARA APLICACIONES DE TIPO P2P SE PUEDEN DEFINIR ADICIONALMENTE POLÍTICAS DE TRAFFIC SHAPING.
- PUEDE SOPORTAR MAYOR GRANULARIDAD EN LAS ACCIONES.

INSPECCIÓN DE CONTENIDO SSL

- LA SOLUCIÓN PUEDE SOPORTAR LA CAPACIDAD DE INSPECCIONAR TRÁFICO QUE ESTA SIENDO ENCRIPTADO MEDIANTE TLS AL MENOS PARA LOS SIGUIENTES PROTOCOLOS: HTTPS, IMAPS, SMTPS, POP3S.
- LA INSPECCIÓN SE REALIZAR 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 PUEDEN DETERMINARSE AL MENOS 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 DE FABRICANTE
LA SOLUCIÓN CUENTA CON SOPORTE DIRECTO DEL FABRICANTE POR 12 MESES CON LOS SIGUIENTES ALCANCES:

- ACCESO A LA BASE DE DATOS DE CONOCIMIENTO DEL FABRICANTE EN UN ESQUEMA 5X8
- 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 2015.

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

- SOPORTE DE SOFTWARE CON RELEASES DE MANTENIMIENTO Y UPGRADES A NUEVAS VERSIONES
- SOPORTE DE HARDWARE TIPO REEMPLAZO AVANZADO

SOPORTE POR PARTE DE "EL PROVEEDOR"
"EL PROVEEDOR" INCLUYE UN SERVICIO DE SOPORTE PARA EL SOPORTE DE LOS EQUIPOS CON LOS SIGUIENTES ALCANCES:

- DURACIÓN DE 12 MESES
- ATENCIÓN DE FALLAS CON UN TIEMPO MÁXIMO DE 2 HORAS CON ESQUEMA 5X8.
- CONSIDERA UN (1) MANTENIMIENTO PREVENTIVO AL AÑO PARA LOS EQUIPOS, PREVIO ACUERDO CON LA CONVOCANTE. LOS INSUMOS NECESARIOS PARA EL MANTENIMIENTO CORREN POR CUENTA DE "EL PROVEEDOR".
- INCLUYE SOPORTE TELEFÓNICO SIN COSTO ADICIONAL EN HORARIO DE LUNES A VIERNES EN HORARIO DE OFICINA.
- PARA LOS EQUIPOS O SOFTWARE DE LA SOLUCIÓN DE SEGURIDAD PARA LOS CUALES EL FABRICANTE LIBERA NUEVAS VERSIONES DENTRO DE LA VIGENCIA DE LA PÓLIZA DE SOPORTE, "EL PROVEEDOR" INSTALA SIN COSTO DICHAS ACTUALIZACIONES.

REPORTE DE FALLAS

- "EL PROVEEDOR" CUENTA CON UNA MESA DE AYUDA PARA RECIBIR CUALQUIER EVENTO RELACIONADO CON LA OPERACIÓN DE LA INFRAESTRUCTURA REQUERIDA POR PARTE DE LA SECRETARÍA DE SEGURIDAD PÚBLICA. ESTE CENTRO DE ATENCIÓN ES PROPIO DE "EL PROVEEDOR". Y ESTÁ 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 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, GENERA UN REGISTRO HISTÓRICO QUE PERMITE CONSULTAS, GENERACIÓN DE REPORTES Y SEGUIMIENTO SOBRE EL TIPO DE FALLAS PRESENTADAS Y LA FORMA COMO SE SOLUCIONARON.
- LA ATENCIÓN Y SOPORTE ES POSIBLE A TRAVÉS DE UN NÚMERO TELEFÓNICO ÚNICO CON SERVICIO 01-800 SIN COSTO ADICIONAL PARA LA SECRETARIA DE SEGURIDAD PÚBLICA DE CAMPECHE Y A TRAVÉS DE CORREO O UNA PÁGINA WEB.
- LOS DATOS QUE CONTIENE UN REPORTE DE FALLA, MISMO QUE SE INTEGRAN 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 ACUERDA CON "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.
- ATENCIÓN DE FALLAS: DE LUNES A DOMINGO 24 HORAS, EL TIEMPO MÁXIMO ES DE 2 HORAS A PARTIR DEL REPORTE DE LA FALLA PARA INICIAR CON EL DIAGNÓSTICO.

OPERADO CON RECURSOS FASP 2015.

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UNA LICENCIA FIREWALL"

ACTA No. SAIG-756/2017

ADMINISTRACIÓN DE SERVICIOS

- "EL PROVEEDOR" ALINEA TODOS SUS 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:
  - ADMINISTRACIÓN DE CONFIGURACIONES
  - ADMINISTRACIÓN DE CAMBIOS
  - ADMINISTRACIÓN DE INCIDENCIAS
  - ADMINISTRACIÓN DE PROBLEMAS
  - ADMINISTRACIÓN DE LIBERACIONES
  - ADMINISTRACIÓN DE LA CAPACIDAD
  - ADMINISTRACIÓN DE LOS NIVELES DE SERVICIO
  - ADMINISTRACIÓN DE LA DISPONIBILIDAD
  - ADMINISTRACIÓN DE COSTO
  - MESA DE SERVICIO (FUNCIÓN)
- SE ADJUNTA EN LOS DOCUMENTOS COPIAS QUE CERTIFICAN AL PERSONAL PROPIO DE "EL PROVEEDOR" PARA LA IMPLEMENTACIÓN EN LAS MEJORES PRÁCTICAS DE ITIL (IT INFRASTRUCTURE LIBRARY), POR CUANDO MENOS 3 PERSONAS.

"EL PROVEEDOR" TIENE LAS SIGUIENTES RESPONSABILIDADES:

- IDENTIFICAR LA CAUSA DE LA RAÍZ DE TALES PROBLEMAS.
- 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.
- 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.
- VERIFICAR QUE TODAS LAS ACCIONES NECESARIAS SE HAN TOMADO PARA PREVENIR LA REPETICIÓN DE TAL FALLA.
- MANTENER LOS PROCESOS DE ADMINISTRACIÓN DE CAMBIOS, INCLUYENDO LOS PROCEDIMIENTOS Y MÉTODOS VIGENTES PARA LOS CAMBIOS.
- 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.
- 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.
- ESCALACIÓN DE LOS PROBLEMAS QUE HAYAN REBASADO LOS UMBRALES DE RESPUESTA BASADOS EN LA SEVERIDAD DEL PROBLEMA.