**Contrato 211/2017**

**Contrato de adquisición de licencias informáticas, 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 Estrategias en Tecnología Corporativa, S.A. de C.V., representada en este acto por el Ingeniero 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 oficios número SSPCAM/RF/1179/2017, de fecha 13 de octubre, el Dr. Jorge de Jesús Argáez Uribe, Secretario de Seguridad Pública, solicitó la adquisición de diversos bienes para destinarse a la dependencia a su cargo.

**1.4.-** Que según a lo establecido por los artículos 1, 3, 6, 21, 22, 33, 35 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 y 2 fracción IV, 8 y demás concordantes de la Ley de Presupuesto de Egresos del Estado de Campeche para el Ejercicio Fiscal 2017; la presente operación de adquisición se efectúa mediante la modalidad de Licitación Pública Estatal **N°. SAIG-EST-026-17**.

**1.5.-** Que la erogación de la presente compra se encuentra prevista y será cubierta con cargo al Fondo de Aportaciones para la Seguridad Pública de los Estados y del Distrito Federal (FASP), con base en el siguiente esquema programático: **Ejercicio Fiscal:** 2017; **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; **Capítulo 5000:** Bines muebles, inmuebles e intangibles.

**1.6.-** Que tiene establecido su domicilio en la calle 8 sin número, entre calle 61 y Circuito Baluartes, colonia Centro, C.P. 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 anónima de capital variable con capacidad de comercializar los bienes y servicios que en este acto requiere "El Estado", constituida bajo Escritura Pública número 1,391 de fecha 14 de julio 2006, otorgada ante la fe del Licenciado Mario Humberto Torres Verdín, notario público número 128 de Guadalajara, Jalisco, inscrita en el Registro Público de la Propiedad y de Comercio del Estado de Jalisco, mediante el folio mercantil electrónico número 32134 * 1, de fecha 11 de septiembre de 2006.

**2.2.-** Que su representante legal es el ingeniero Juan Gualberto Cabrera Pérez, quien se identifica con su credencial para votar con folio 0106067747716, expedida por el Instituto Nacional Electoral, y acredita su personalidad con el testimonio de la Escritura Pública número 3,616 de fecha 14 de junio de 2013, pasada ante la fe del Licenciado Mario Humberto Torres Verdín, notario público número 128 de la ciudad de Guadalajara, Jalisco, inscrita en el Registro

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - -

Público de la Propiedad y de Comercio del Estado de Jalisco, mediante el folio mercantil electrónico número 32134 * 1, de fecha 20 de junio de 2013.

**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, C.P. 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: 02895, expedido el 04 de mayo de 2017.

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

**3.- De ambas partes:**

**3.1.-** Que en virtud 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, que a continuación se describen, acatando para ello lo establecido en el presente contrato y anexo único:

| Cantidad | Descripción | Unidad de medida | Precio unitario | Importe |
|---|---|---|---|---|
| 9 | (2) Renovación de licencia Fortigate 90-D, (2) renovación de licencia 60-D, (1) licencia antivirus para 200 equipos por 3 años, (1) Microsoft SQL Server 2016, (1) Microsoft Office 365 para 100 usuarios, (1) licencia WinRar para 200 usuarios y (1) licencia veeam back up & replication.<br><br>Descripción Cantidad<br>Renovación de licencias Fortigate 90-D 2<br>Renovación de licencias Fortigate 60-D 2<br>Antivirus para 200 equipos por 3 años 1<br>Microsoft SQL server 2016 1<br>Microsoft Office 365 para 100 usurios 1<br>Licencia WinRar para 200 usuarios 1<br>Licencia Veeam back up & replication 1<br><br>Licencia veeam back up & replication<br>Se integra una solución de respaldo que incluye los siguientes elementos: software de respaldo para máquinas virtuales, almacenamiento y servicios de implementación. A continuación, se describen las especificaciones de la solución solicitada por la Secretaría de Seguridad Pública.<br><br>Software de respaldo para máquinas virtuales.<br>Se incluyen 4 licencias basado en procesador con las siguientes especificaciones:<br><br>• Soporta la nueva versión de vSphere 6. | Servicio | $77,747.11 | $699,723.99 |

OPERADO CON RECURSOS - - 15 - 16 - 17 - - -

FASP

| | | | | |
|---|---|---|---|---|
| | • Cuenta con la capacidad de realizar respaldo y replicación de servidores virtuales en VMware al menos.<br>• No es un appliance pre-configurado OVF y/o OVA.<br>• Puede utilizar cualquier almacenamiento mientras esté basado en disco (NAS, SAN, DAS).<br>• Cuenta con la capacidad de procesar trabajos directamente desde datastores en la SAN.<br>• Cuenta con la capacidad de procesar trabajos directamente desde datastores NFS.<br>• No requiere de instalar ningún agente en los servidores virtuales para poder respaldarlo, replicarlo o restaurarlo.<br>• Permite comprimir y deduplicar en línea y que los respaldos sean basados en imagen.<br>• Permite restaurar archivos u objetos de las aplicaciones desde la réplica.<br>• Permite presentar el repositorio de almacenamiento a los hosts como un datastore NFS, para realizar tareas de recuperación rápidas.<br>• Cuenta con la capacidad de restaurar granular mente desde el respaldo de un servidor virtual objetos de aplicaciones, siempre y cuando éstas se ejecuten sobre un Sistema Operativo huésped soportado por el hypervisor.<br>• Permite recuperación desde el respaldo de archivos del File System del servidor virtual que haya sido respaldado, siempre y cuando el Sistema Operativo del mismo sea soportado por el hypervisor.<br>• No depende del equipo de almacenamiento utilizado para replicar los servidores virtuales, es decir, que sea replicación basada en software.<br>• Permite utilizar el/los punto(s) de restauración de los respaldos de los servidores virtuales dentro de un laboratorio aislado dentro de la misma infraestructura virtual para realizar tareas de verificación, así como pruebas o recuperación de información desde los mismos.<br>• Permite ejecutar de forma aislada un escenario de replicación para verificar las réplicas de servidores virtuales.<br>• Que la solución cuenta con la capacidad de obtener información de los trabajos realizados en las últimas 24 horas, últimos 7 días, de todos los trabajos realizados y de todos los servidores virtuales relacionados con un trabajo.<br>• Que la solución permite enviar respaldos a cinta.<br>• Puede realizar el truncado de las bitácoras transaccionales (Transaction logs) para máquinas virtuales con Microsoft Exchange y SQL Server.<br>• Puede realizar notificaciones por correo, SNMP o a través de los atributos de la máquina virtual del resultado de la ejecución de sus trabajos.<br>• Se pueden recuperar a nivel de objetos de cualquier aplicación virtualizada, en cualquier sistema operativo soportado por el Hypervisor, utilizando las herramientas de gestión de aplicaciones existentes.<br>• Incluye herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Microsoft SQL Server, con la capacidad de recuperar una base de datos a nivel de transacción. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.<br>• Incluye herramientas de fácil recuperación guiada mediante el cual los administradores de | | | |

OPERADO CON RECURSOS FASP

- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | servidores de bases de datos Oracle, con la capacidad de recuperar una base de datos, sobre Windows o Linux. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.<br>• Ofrece visibilidad instantánea, capacidades avanzadas de búsqueda y recuperación rápida de elementos individuales para Sharepoint 2010 sin la utilización de agentes.<br>• Incluye herramientas de fácil recuperación de elementos granulares de Microsoft Exchange 2010 en adelante, que no requiera inicializar la máquina virtual desde el respaldo y que pueda ser extraído en frio. (Ej. Correo, Citas de calendario, contactos, etc) y sin requerir infraestructura intermedia ("Staging")<br>• Ofrece confiabilidad en un 100% en el inicio correcto de todas sus máquinas virtuales respaldadas y en el funcionamiento del rol que cumple dichas máquinas virtuales (DNS Server, Domain Controller, Mail Server, SQL Server, etc) al momento de la recuperación.<br>• Es capaz de crear una copia de trabajo del entorno de producción de cualquier estado anterior para la resolución de problemas, pruebas de procedimientos, capacitación, etc. ejecutando una o varias máquinas virtuales desde el archivo de respaldo (backup) en un entorno aislado, sin necesidad de más espacio de almacenamiento y sin modificar el respaldo (backup).<br>• Ofrece el archivado en cinta, soportando VTL (Virtual Tape Libraries), biblioteca de cintas y drives independientes.<br>• Ofrece Trabajos de Copia de Backup con implementación de políticas de retención.<br>• Ofrece Aceleración de red "WAN", sin el uso de agentes ni configuraciones de red especiales.<br>• Incluye soporte para VMware vCloud Director con visibilidad integrada de la infraestructura vCD en la consola de backup.<br>• Incluye un Plug-in VMware para vSphere Web Client y poder monitorear la infraestructura de backup directamente desde el vSphere Web Client, con vistas detalladas y generales del estado de los trabajos y recursos de backup.<br>• No requiere hardware especifico para alcanzar la de-duplicación y compresión de la información fuera de los requerimientos estándar de cualquier software, y específicos para el caso.<br>• No requiere licencias independientes para las actividades de respaldo, recuperación y replicación.<br>• Ofrece aceleración de enlaces WAN para la réplica.<br>• Es capaz de realizar replicas en otros sitios o infraestructuras desde los respaldos realizados.<br>• Presenta un método fácil de recuperación hacia ambientes de contingencia, con las acciones pre-configuradas para evitar acciones manuales en caso de desastre.<br>• Ofrece la posibilidad de almacenar los respaldos de forma encriptada, así como asegurar el tránsito de la información bajo este esquema.<br>• Permite la delegación de tareas de recuperación, a nivel de elementos de aplicación, hacia otros usuarios, de forma tal a poder descargar la cantidad de maniobras a ejecutar por el administrador de la plataforma.<br>• Permite la verificación automatizada de los archivos de respaldo, misma que se ejecuta en un ambiente virtual aislado, configurable desde la consola | | | |

OPERADO CON RECURSOS FASP
- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | de administración de la herramienta de respaldos, y que la verificación sea ejecutando las Máquinas Virtuales directamente desde el archivo de respaldo sin la necesidad de restaurarlas a un datastore productivo.<br>• Durante la verificación automatizada, el respaldo de la Máquina Virtual permanece en estado de solo lectura, para que al finalizar la verificación, todos los cambios realizados durante el proceso no afecten el estado del archivo de respaldo utilizado para la verificación.<br>• Permite una verificación automatizada de las réplicas, permitiendo evaluar cada punto de restauración de las réplicas dentro de un ambiente virtual aislado, configurable desde la consola de administración de la herramienta de replicación, sin impactar el ambiente productivo, lo cual permitirá al administrador asegurarse que las Máquinas Virtuales réplica están trabajando como se espera.<br>• Durante las pruebas de verificación automatizadas de los respaldos y las réplicas, se realicen de forma automática dentro de cada uno de sus respectivos trabajos de verificación configurados desde la consola de administración, pruebas de heartbeat, ping y de aplicación.<br>• Permite respaldar las Máquinas Virtuales directamente desde la SAN sin requerir licenciamiento especial.<br>• Permite almacenar los archivos de respaldo sin que se requiera un licenciamiento por unidad de espacio de almacenamiento específico.<br>• Cuenta de manera integrada con la posibilidad de enviar respaldos, copias de respaldos y copia de archivos a la nube, una vez que el administrador dé de alta al proveedor de servicios desde su consola de administración.<br>• Permite restaurar desde su repositorio en la nube Máquina Virtual completa, archivos de Máquina Virtual, discos de Máquina Virtual, archivos del File System de Windows.<br>• La característica de aceleración de WAN integrada utiliza el mecanismo de duplicación global de data para reducir el envío de la información a través de la red.<br>• Permite una retención de GFS en copias de respaldos.<br>• Tiene la capacidad de monitorear la latencia en el datastore y de manera inteligente reducir o continuar con la carga de trabajo asignada para ejecutar los respaldos.<br>• Realiza la replicación en formato nativo del hypervisor, permitiendo que en caso de que no exista ninguna consola de administración durante una contingencia, el administrador pueda iniciar de forma manual la Máquina Virtual réplica e incluso seleccionar el punto de restauración en el cual desea iniciar.<br>• Permite realizar replicación desde el archivo de respaldos que se encuentra en el sitio principal o en el sitio de DR.<br>• Permite ejecutar un healthcheck de tipo CRC en los puntos de restauración dentro de los trabajos de copias de respaldos sobre el repositorio destino.<br>• Ofrece la posibilidad de almacenar los respaldos de forma encriptada, así como asegurar el tránsito de la información bajo este esquema.<br>• La encriptación de los archivos de respaldo puede aplicarse a los trabajos de respaldo, así como para | | | |

OPERADO CON RECURSOS FASP
- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | los trabajos de copia de respaldo y cintas en los pools de media.<br>• La encriptación utiliza el estándar AES a 256-bit.<br>• Conserva las propiedades de perfil de la Máquina Virtual (vSphere Tags) y permite restaurar el mismo cuando se realizan las operaciones de restauración completa de Máquina Virtual y Failback.<br>• Cuenta con la capacidad de detectar y remover los snapshots huérfanos que pueden permanecer después de las operaciones de respaldo y/o replicación de Máquinas Virtuales, asegurando al 100% su eliminación del datastore.<br>• Cuenta con una consola de tipo stand-alone que permite la conexión a la aplicación sin la necesidad de entrar directamente al servidor de respaldos o por medio de escritorio remoto.<br>• Permite utilizar un servidor de montaje (mount server) para optimizar las restauraciones en ambientes de oficinas remotas.<br>• Cuenta con la posibilidad de realizar health checks y compactación de los respaldos incrementales.<br>• La solución excluye archivos eliminados del procesamiento de los trabajos de respaldo.<br>• Permite conectividad a servicios de respaldo (Backup as a Service) y recuperación de desastres (Disaster Recovery as a Service) por medio de proveedores de servicio.<br>• Incluye una licencia de Windows Server 2012 R2 Standard Edition Open Gobierno.<br><br>Soporte por parte del fabricante<br>Se incluyen 3 años de soporte básico por parte del fabricante que incluye:<br>• Actualizaciones y parches durante la vigencia del contrato.<br>• Soporte técnico vía Web/Telefónico.<br>• Horario: Lunes a Viernes de 8:00 a 20:00 hrs.<br>• Incluye 4 niveles de severidad, para indicación del nivel de urgencia para proporcionar una rápida y efectiva respuesta.<br>Servicios de Implementación<br>• Se incluyen los servicios de implementación de toda la solución de respaldo como una solución llave en mano. Este cubre la integración tanto de las licencias del software de respaldo para máquinas virtuales y el sistema de almacenamiento SAN que actualmente tiene la Secretaría de Seguridad Púbica.<br>• Se consideran los siguientes servicios:<br>• Planeación y diseño.<br>• Instalación de consola de respaldo.<br>• Creación de 1 LUNs en el almacenamiento SAN que actualmente tiene la Secretaría de Seguridad Pública para el repositorio que utilizará la solución.<br>• Creación de 10 políticas de respaldo, se considera la integración con el Hypervisor VMware que actualmente utiliza "El Estado" para la operación de sus servidores virtuales.<br>• Pruebas de respaldo e integración.<br>• Actualización a la última versión disponible del firmware del sistema de almacenamiento SAN.<br>• Transferencia de conocimiento para la operación del software de respaldo.<br>• Entrega de Memoria Técnica. | | | |

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | • Se incluye un soporte para consultas técnicas durante un año, donde la Secretaría de Seguridad Pública puede solicitar el apoyo para los siguientes casos:<br>o Administración de las políticas de respaldo (alta, baja, cambios).<br>o Modificación en la configuración del sistema de almacenamiento tipo SAN.<br>o Asesoría para indicarle las mejores prácticas en configuración para el hypervisor, de acuerdo al entorno de operación de "El Estado".<br>• Con el fin de asegurar la calidad en la prestación de los servicios solicitados por la Secretaría de Seguridad Pública, en la propuesta técnica incluye copia simple de los siguientes certificados:<br>o Certificado de capacitación de la suite de administración de respaldo.<br>o Certificado de instalación, configuración y administración VMware vSphere versión 6.<br>o Al menos tres certificados de Profesional Data Center Virtualization de VMware.<br><br>Servicios de Mesa de Ayuda<br>Como parte de su propuesta técnica, "El Proveedor" incluye una mesa de ayuda con duración de un año, para recibir cualquier evento relacionado con la operación de la infraestructura solicitada por parte de la Secretaría de Seguridad Pública. Este centro de atención es propio y está ubicado en nuestras instalaciones, mediante el uso de sus propias herramientas y de manera dedicada para el soporte de la infraestructura de comunicaciones.<br>Los alcances de la mesa de ayuda son:<br>• 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.<br>• La atención y soporte serán posibles 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.<br>• Los datos mínimos que contendrá un reporte de falla, mismo que se integren en el control de eventos e incidentes serán:<br>• Identificador del reporte o número de incidente o evento<br>• Identificador del usuario que reporta. Estos son los datos que identifican al usuario que levantó el reporte; al menos nombre, teléfono, correo electrónico y ubicación. Las definiciones finales de estos datos se acordarán con "El Estado".<br>• Hora en que reporta el problema por parte del usuario autorizado tipo de fallo<br>o Descripción Del Fallo<br>o Tiempo De Solución Del Incidente Y Restablecimiento Del Servicio.<br>o Atención de reportes: 24x7<br><br>Administración de servicios<br>"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:<br>1. Administración de configuraciones | | | |

| | | | | |
|---|---|---|---|---|
| | 2. Administración de cambios<br>3. Administración de incidencias<br>4. Administración de problemas<br>5. Administración de liberaciones<br>6. Administración de la capacidad<br>7. Administración de los niveles de servicio<br>8. Administración de la disponibilidad<br>9. Administración de costo<br>10. Mesa de servicio (Función)<br>Se adjuntan los documentos que certifican al personal propio de "El Proveedor" de servicios para la implementación en las mejores prácticas de itil (it infrastructure library), 3 personas, al menos. Contamos con 2 personas certificadas en ITIL OSA.<br><br>"El Proveedor" adquiere las siguientes responsabilidades.<br>• Identificar la causa de la raíz de tales problemas<br>• 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.<br>• 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.<br>• Verificar que todas las acciones necesarias se han tomado para prevenir la repetición de tal falla.<br>• Mantener los procesos de administración de cambios, incluyendo los procedimientos y métodos vigentes para los cambios.<br>• 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.<br>• 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.<br>Escalación de los problemas que hayan rebasado los umbrales de respuesta basados en la severidad del problema.<br><br>Licencias WinRAR para 200 usuarios<br>Licencia perpetua de WinRAR, programa para comprimir, codificar, empaquetar y hacer copias de seguridad con una sola utilidad. Soporta todos los formatos de compresión populares (RAR, ZIP, CAB, ARJ, LZH, ACE, TAR, GZip, UUE, ISO, BZIP2, Z y 7-Zip).<br>Licencia Microsoft office 365 para 100 usuarios<br>Se incluye licencia de Microsoft Office 365 Business Essentials - Licencia de suscripción por 1 año.<br>Que incluye las siguientes aplicaciones de Office:<br>• Outlook<br>• Word<br>• Excel<br>• PowerPoint<br>• OneNote<br>• Access (solo PC)<br>• Publisher (solo PC)<br><br>Licencia Microsoft SQL server 2016 | | | |

OPERADO CON RECURSOS FASP

- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | Se incluye una licencia de Microsoft SQL Server 2016 Standard Edition Open Gobierno con las siguientes características:<br>Rendimiento<br>• OLTP-in memory<br>• Almacen de columnas in-memory<br>• Extensión de grupo de búferes a SSD<br>• Regulador de recursos<br>Disponibilidad<br>• AlwaysOn<br>• Migración dinámica y soporte para la virtualización mejorados<br>Seguridad<br>• Cifrado de datos transparente<br>• Compatibilidad con el cifrado de copias de seguridad<br>• Auditorias específicas<br>• Separación de tareas<br>Preparación para la nube<br>• Copias de seguridad en Azure<br>• Recuperación ante desastres en Microsoft<br>• Imágenes de máquinas virtuales optimizadas en la galería de Azure<br>Administración y programación<br>• Distributed Replay<br>• Administración basada en políticas<br>• Programación mejorada<br>Bi y análisis<br>• PowerPivot para Excel<br>• Servicios de integración administradors como un servidor<br>• Conector de Hadoop a través de Apache Sqoop<br>• Modelo de semántica de Bi tabular<br>• Master Data Services<br>• Data Quality Services<br><br>Antivirus para 200 equipos por 3 años<br>Licenciamiento de antivirus para 200 usuarios por tres años, que cumple con las siguientes características técnicas:<br><br>• AntiMalware<br>• Firewall<br>• Protección asistida en la nube<br>• Control de aplicaciones<br>• Lista blanca de aplicaciones<br>• Control Web<br>• Control de Dispositivos<br>• Protección del Servidor de Archivos<br>• Manejo del Dispositivo Móvil (MDM)<br>• Seguridad de Endpoint Móvil (para tablets y smartphones )<br>• Encriptación<br>• Configuración y Despliegue de Sistemas<br>• Escáner de vulnerabilidades avanzado<br>• Control de admisión a la red<br>• Manejo de parches<br>• Seguridad para el servidor de correo<br>• Protección del gateway de web/internet<br>• Seguridad del servidor de colaboración<br>2 renovación de licencia Fortigate 60-D<br><br>Adquisición de licencias para un sistema de seguridad informática perimetral del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se | | | |

OPERADO CON RECURSOS
- - 15-16-17 - - -
FASP

| | | | | |
|---|---|---|---|---|
| | ofrecen las funcionalidades que se detallan en el presente documento.<br><br>Se consideran las licencias y los servicios para los siguientes números de serie con la vigencia del servicio hasta el 19 de Julio del 2019<br><br>• FGT60D4613054250<br>• FGT60D4613057081<br><br>Funcionalidades y Características:<br><br>Firewall<br>• Las reglas de firewall analizan las conexiones que atraviesan en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.<br>• 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.<br>• Es posible definir políticas de firewall que son independientes del puerto de origen y puerto de destino.<br>• Las reglas del firewall toman en cuenta dirección IP origen, dirección IP destino y servicio (o grupo de servicios) de la comunicación que se está analizando<br>• Soporte a reglas de firewall para tráfico de multicast, especificando puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.<br>• Las reglas de firewall tienen limitantes y/o vigencia en base a tiempo.<br>• Las reglas de firewall tienen limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)<br>• Soporta la capacidad de definir nuevos servicios TCP y UDP que no estan contemplados en los predefinidos.<br>• Se puede definir el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)<br>• Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.<br>• Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.<br>• 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),<br>• 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 distribuye el tráfico entre ellas.<br>• En la solución de balanceo de carga entre servidores, se soporta persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID<br>• 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.<br>• 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.<br>• 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<br>• La solución tiene la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.<br>• La solución de seguridad deberá permitela creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada<br>• La solución es capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente<br>• El dispositivo de seguridad puede determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas<br>• 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<br>• 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<br>• El dispositivo de seguridad es capaz de crear e integrar políticas contra ataques DoS las cuales se pueden aplicar por interfaces.<br>• El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS<br>• La solución de seguridad permite configurar el mapeo de protocolos a puertos de manera global o especifica<br>• La solución es capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.<br>• El dispositivo integra la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados<br>• El dispositivo es capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado es válido este tráfico<br>• Tiene la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis<br>• La solución permite bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH<br><br>• 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.<br>• 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.<br>• 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. | | | |

OPERADO CON RECURSOS FASP
--15-16-17--

| | | | | |
|---|---|---|---|---|
| | • El Antivirus integrado soporta la capacidad de inspeccionar y detectar virus en tráfico IPv6.<br>• 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.<br>• 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.<br>• El appliance puede de manera opcional inspeccionar por todos los virus conocidos.<br>• 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<br>• 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.<br>• El Antivirus inclucye capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.<br>• El antivirus puede hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.<br>• El antivirus es capaz de filtrar archivos por extensión<br>• El antivirus es capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tiene el archivo<br>• 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)<br><br>AntiSpam<br>• 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.<br>• 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 listas negras pueden ser por dirección IP o por dirección de correo electrónico (e-mail address).<br>• 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<br>• 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.<br><br>Filtraje de URLs (URL Filtering) | | | |

OPERADO CON RECURSOS FASP
- - 15 - 16 - 17 - -

| | | | | |
|---|---|---|---|---|
| | • Tiene facilidad para incorporar control de sitios a los cuales naveguan 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.<br>• Puede categorizar contenido Web requerido mediante IPv6.<br>• 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.<br>• Es configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.<br>• 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<br>• 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).<br>• 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.<br>• Los mensajes de remplazo pueden ser personalizados por categoría de filtrado de contenido.<br>• Tiene capacidad de filtrado de scripts en páginas web (JAVA/Active X).<br>• 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.<br>• Es posible definir cuotas de tiempo para la navegación. Dichas cuotas pueden asignarse por cada categoría y por grupos.<br>• Es posible exceptuar la inspección de HTTPS por categoría.<br>• 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 politica de seguridad con este perfil, pueden acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo.<br>• El sistema de filtrado de URLs tiene al menos 3 métodos de inspección:<br>1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.<br>2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.<br>3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.<br>• Se incluye la funcionalidad de reputación basada en filtrado de URLs. | | | |

OPERADO CON RECURSOS FASP
- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | • 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.<br>• El sistema de filtrado de URLs incluye la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.<br>• Se incorpora la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)<br>• 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.<br><br>Protección contra intrusos (IPS)<br>• 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.<br>• Es posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.<br>• Tiene capacidad de detección de más de 4000 ataques.<br>• 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)<br>• 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 administrar este servicio. Esta permite la protección de este servicio por política de control de acceso.<br>• El detector y preventor de intrusos soporta captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).<br>• Basado en análisis de firmas en el flujo de datos en la red, permite configurar firmas nuevas para cualquier protocolo.<br>• Actualización automática de firmas para el detector de intrusos<br>• El Detector de Intrusos mitiga los efectos de los ataques de negación de servicios.<br>• Métodos de notificación:<br>o Alarmas mostradas en la consola de administración del appliance.<br>o Alertas vía correo electrónico.<br>o Tiene la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena puede definirse al | | | |

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.<br>o 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.<br>o 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.<br>• Se incluye protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se incluye:<br>• 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 periodica por el fabricante.<br>• 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 accion sobre el mismo.<br><br>Prevención de Fuga de Información (DLP)<br>• 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.<br>• La funcionalidad soporta el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.<br>• Puede soportar el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.<br>• 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.<br>• 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.<br>• 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.<br>• La solución permite la búsqueda de patrones en archivos mediante la definición de expresiones regulares.<br>• Se provee la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se consideran como mínimo las siguientes:<br>1. Filtrado por tipo de archivo<br>2. Filtrado por nombre de archivo<br>3. Filtrado por expresiones regulares: Se detectan los archivos según las expresiones regulares que se encuentran dentro de los mismos.<br>4. Fingerprinting: Se toma una muestra del archivo que se considere como confidencial. Según esto se bloquean archivos que sean iguales a esta muestra.<br>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. | | | |

OPERADO CON RECURSOS FASP
- - 15 - 16 - 17 - -

| | | | | |
|---|---|---|---|---|
| | Control de Aplicaciones<br>• Lo solución soporta la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.<br>• La identificación de la aplicación es independiente del puerto y protocolo hacia el cual esta direccionado dicho tráfico.<br>• La solución tiene un listado de al menos 1000 aplicaciones ya definidas por el fabricante.<br>• El listado de aplicaciones puede actualizarse periódicamente.<br>• Para aplicaciones identificadas se pueden definir al menos las siguientes opciones: permitir, bloquear, registrar en log.<br>• Para aplicaciones no identificadas (desconocidas) se pueden definir al menos las siguientes opciones: permitir, bloquear, registrar en log.<br>• Para aplicaciones de tipo P2P se pueden definir adicionalmente políticas de traffic shaping.<br>• Puede soportar mayor granularidad en las acciones.<br><br>Inspección de Contenido SSL<br>• 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.<br>• La inspección se realizar mediante la técnica conocida como Hombre en el Medio (MITM - Man In The Middle).<br>• La inspección de contenido encriptado no requiere ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.<br>• 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.<br>• 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<br><br>Soporte de Fabricante<br>La solución cuenta con soporte directo del fabricante por los meses correspondientes para cada equipo, con los siguientes alcances con respecto a los equipos:<br><br>• FGT60D4613054250<br>• FGT60D4613057081<br><br>• Acceso a actualizaciones de los servicios de seguridad<br>• Acceso a la base de datos de conocimiento del fabricante en un esquema 24x7<br>• Soporte telefónico 24x7 para atención de reporte de fallas o incidentes<br>• Soporte Web 24x7 para atención de reporte de fallas o incidentes<br>• Soporte vía Chat 24x7 para atención de reporte de fallas o incidentes<br>• Soporte de software con releases de mantenimiento y upgrades a nuevas versiones<br>• Soporte de hardware tipo reemplazo avanzado | | | |

| | | | | |
|---|---|---|---|---|
| | Respaldo de fabricante<br>Las licencias de seguridad informática UTM solicitadas en este concepto cuentan con el respaldo por parte del fabricante y "El Proveedor" entrega como parte de su propuesta la siguiente documentación:<br><br>• Se incluye como parte de la propuesta, una carta expedida por el por el fabricante del equipo/licencias de seguridad informática UTM en la que manifiesta que somos integrador autorizado de los equipos nivel Platinum y que estamos autorizados para revender los productos/servicios del fabricante.<br>• Se incluye dentro de la su propuesta técnica, una carta expedida por el por el fabricante del equipo/licencias de seguridad informática UTM en la que manifiesta contamos con las certificaciones requeridas para brindar servicios de instalación y soporte de los equipos de seguridad solicitados.<br>• Contamos con cuatro ingenieros certificados en la solución propuesta, para realizar las actividades de instalación, configuración y puesta a punto y en marcha. al menos nivel de certificación nivel 4.<br>• Se demuestra nuestra experiencia en el soporte de las licencias de seguridad informática solicitado, a través de una relación de clientes exclusivamente de gobierno en donde hemos instalado equipos de la misma marca con características similares a los requeridos por "El Estado", contiene la siguiente información: nombre, dirección, teléfono y correo electrónico de los clientes y una descripción del proyecto de al menos media cuartilla. la Secretaría se Seguridad Publica se reservará el derecho de verificar dicha información.<br><br>Soporte por parte del "El Proveedor"<br>En el caso de resultar ganadores, incluimos como parte de nuestra propuesta un servicio de soporte para los equipos con los siguientes alcances:<br><br>• Duración de 12 meses<br>• Atención de fallas con un tiempo máximo de 2 horas con esquema 5x8.<br>• Se considera (1) mantenimiento preventivo al año para los equipos, previo acuerdo con "El Estado". Los insumos necesarios para el mantenimiento corren por cuenta del "El Proveedor" ganador.<br>• Incluye soporte telefónico sin costo adicional en horario de lunes a viernes en horario de oficina.<br>• 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" se encarga de instalar sin costo dichas actualizaciones.<br><br>Reporte de fallas<br><br>• Contamos Mesa de Ayuda para recibir cualquier evento relacionado con la operación de la infraestructura requerida por parte de la Secretaria de Seguridad Pública del Estado de Campeche. Este centro de atención es propio de "El Proveedor", y se encuentra ubicado en nuestras instalaciones, mediante el uso nuestras propias herramientas y de manera dedicada para el soporte de la infraestructura de comunicaciones.<br>• Los alcances de la Mesa de Ayuda son: recibir, registrar, analizar, resolver y canalizar los reportes de | | | |

OPERADO CON RECURSOS FASP
- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | 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.<br>• La atención y soporte es posibles a través de un número telefónico único con servicio 01-800 sin costo adicional para la Secretaría de Seguridad Pública del estado de Campeche y a través de correo o una página Web.<br>• Los datos que contiene un reporte de falla, mismo que se integran en el control de eventos e incidentes son:<br>o Identificador del reporte o número de incidente o evento<br>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" ganador.<br>o Hora en que reporta el problema por parte del usuario autorizado<br>o Tipo de fallo<br>o Descripción del fallo<br>o Tiempo de solución del incidente y restablecimiento del servicio.<br>• 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.<br><br>Administración de servicios<br><br>• 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:<br>o Administración de configuraciones<br>o Administración de cambios<br>o Administración de incidencias<br>o Administración de problemas<br>o Administración de liberaciones<br>o Administración de la capacidad<br>o Administración de los niveles de servicio<br>o Administración de la disponibilidad<br>o Administración de Costo<br>o Mesa de Servicio (Función)<br><br>• 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.<br><br>En caso de resultar ganador "El Proveedor" adquiere las siguientes responsabilidades:<br>• Identificar la causa de la raíz de tales problemas.<br>• 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.<br>• 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. | | | |

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | • Verificar que todas las acciones necesarias se han tomado para prevenir la repetición de tal falla.<br>• Mantener los procesos de administración de cambios, incluyendo los procedimientos y métodos vigentes para los cambios.<br>• 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.<br>• 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.<br>• Escalación de los problemas que hayan rebasado los umbrales de respuesta basados en la severidad del problema.<br><br>2 renovación de licencia Fortigate 90-D<br>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.<br><br>Se consideran las licencias y los servicios para los siguientes números de serie con la vigencia del servicio hasta el 19 de Julio del 2019<br><br>• FGT90D3Z14017471<br>• FGT90D3Z14017487<br><br>Firewall<br>• Las reglas de firewall analizan las conexiones que atraviesan en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.<br>• 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.<br>• Es posible definir políticas de firewall que son independientes del puerto de origen y puerto de destino.<br>• Las reglas del firewall toman en cuenta dirección IP origen, dirección IP destino y servicio (o grupo de servicios) de la comunicación que se está analizando<br>• Soporte a reglas de firewall para tráfico de multicast, especificando puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.<br>• Las reglas de firewall tienen limitantes y/o vigencia en base a tiempo.<br>• Las reglas de firewall tienen limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)<br>• Soporta la capacidad de definir nuevos servicios TCP y UDP que no estan contemplados en los predefinidos.<br>• Se puede definir el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)<br>• Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.<br>• Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT. | | | |

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | • 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),<br>• 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 distribuye el tráfico entre ellas.<br>• En la solución de balanceo de carga entre servidores, se soporta persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID<br>• 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.<br>• 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.<br>• 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<br>• La solución tiene la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.<br>• La solución de seguridad deberá permitela creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada<br>• La solución es capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente<br>• El dispositivo de seguridad puede determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas<br>• 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<br>• 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<br>• El dispositivo de seguridad es capaz de crear e integrar políticas contra ataques DoS las cuales se pueden aplicar por interfaces.<br>• El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS<br>• La solución de seguridad permite configurar el mapeo de protocolos a puertos de manera global o especifica<br>• La solución es capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.<br>• El dispositivo integra la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados<br>• El dispositivo es capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado es válido este tráfico<br>• Tiene la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis | | | |

OPERADO CON RECURSOS
FASP
- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | • La solución permite bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH<br><br>• 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.<br>• 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.<br>• 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.<br>• El Antivirus integrado soporta la capacidad de inspeccionar y detectar virus en tráfico IPv6.<br>• 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.<br>• 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.<br>• El appliance puede de manera opcional inspeccionar por todos los virus conocidos.<br>• 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<br>• 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.<br>• El Antivirus inclucye capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.<br>• El antivirus puede hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.<br>• El antivirus es capaz de filtrar archivos por extensión<br>• El antivirus es capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tiene el archivo<br>• 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)<br><br>AntiSpam<br>• 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. | | | |

OPERADO CON RECURSOS FASP

- - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | • 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 listas negras pueden ser por dirección IP o por dirección de correo electrónico (e-mail address).<br>• 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<br>• 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.<br><br>Filtraje de URLs (URL Filtering)<br>• Tiene facilidad para incorporar control de sitios a los cuales naveguan 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.<br>• Puede categorizar contenido Web requerido mediante IPv6.<br>• 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.<br>• Es configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.<br>• 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<br>• 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).<br>• 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.<br>• Los mensajes de remplazo pueden ser personalizados por categoría de filtrado de contenido.<br>• Tiene capacidad de filtrado de scripts en páginas web (JAVA/Active X).<br>• 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.<br>• Es posible definir cuotas de tiempo para la navegación. Dichas cuotas pueden asignarse por cada categoría y por grupos. | | | |

OPERADO CON RECURSOS
FASP
--15-16-17---

| | | | | |
|---|---|---|---|---|
| | • Es posible exceptuar la inspección de HTTPS por categoría.<br>• 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, pueden acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo.<br>• El sistema de filtrado de URLs tiene al menos 3 métodos de inspección:<br>4. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.<br>5. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.<br>6. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.<br>• Se incluye la funcionalidad de reputación basada en filtrado de URLs.<br>• 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.<br>• El sistema de filtrado de URLs incluye la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.<br>• Se incorpora la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)<br>• 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.<br><br>Protección contra intrusos (IPS)<br>• 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.<br>• Es posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.<br>• Tiene capacidad de detección de más de 4000 ataques.<br>• 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)<br>• 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 | | | |

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | administrar este servicio. Esta permite la protección de este servicio por política de control de acceso.<br>• El detector y preventor de intrusos soporta captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).<br>• Basado en análisis de firmas en el flujo de datos en la red, permite configurar firmas nuevas para cualquier protocolo.<br>• Actualización automática de firmas para el detector de intrusos<br>• El Detector de Intrusos mitiga los efectos de los ataques de negación de servicios.<br>• Métodos de notificación:<br>o Alarmas mostradas en la consola de administración del appliance.<br>o Alertas vía correo electrónico.<br>o 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.<br>o 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.<br>o 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.<br>• Se incluye protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se incluye:<br>• 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 periodica por el fabricante.<br>• 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 accion sobre el mismo.<br><br>Prevención de Fuga de Información (DLP)<br>• 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.<br>• La funcionalidad soporta el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.<br>• Puede soportar el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.<br>• 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.<br>• 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.<br>• La solución soporta la capacidad de guardar una copia del archivo identificado como posible fuga de | | | |

FASP
OPERADO CON RECURSOS
--15-16-17---

| | | | | |
|---|---|---|---|---|
| | información. Esta copia puede ser archivada localmente o en otro dispositivo.<br>• La solución permite la búsqueda de patrones en archivos mediante la definición de expresiones regulares.<br>• Se provee la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se consideran como mínimo las siguientes:<br>1. Filtrado por tipo de archivo<br>2. Filtrado por nombre de archivo<br>3. Filtrado por expresiones regulares: Se detectan los archivos según las expresiones regulares que se encuentran dentro de los mismos.<br>4. Fingerprinting: Se toma una muestra del archivo que se considere como confidencial. Según esto se bloquean archivos que sean iguales a esta muestra.<br>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.<br><br>Control de Aplicaciones<br>• Lo solución soporta la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.<br>• La identificación de la aplicación es independiente del puerto y protocolo hacia el cual esta direccionado dicho tráfico.<br>• La solución tiene un listado de al menos 1000 aplicaciones ya definidas por el fabricante.<br>• El listado de aplicaciones puede actualizarse periódicamente.<br>• Para aplicaciones identificadas se pueden definir al menos las siguientes opciones: permitir, bloquear, registrar en log.<br>• Para aplicaciones no identificadas (desconocidas) se pueden definir al menos las siguientes opciones: permitir, bloquear, registrar en log.<br>• Para aplicaciones de tipo P2P se pueden definir adicionalmente políticas de traffic shaping.<br>• Puede soportar mayor granularidad en las acciones.<br><br>Inspección de Contenido SSL<br>• 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.<br>• La inspección se realizar mediante la técnica conocida como Hombre en el Medio (MITM - Man In The Middle).<br>• La inspección de contenido encriptado no requiere ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.<br>• 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.<br>• 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<br><br>Soporte de Fabricante | | | |

| | | | | |
|---|---|---|---|---|
| | La solución cuenta con soporte directo del fabricante por los meses correspondientes para cada equipo, con los siguientes alcances con respecto a los equipos:<br><br>• FGT90D3Z14017471<br>• FGT90D3Z14017487<br><br>• Acceso a actualizaciones de los servicios de seguridad<br>• Acceso a la base de datos de conocimiento del fabricante en un esquema 24x7<br>• Soporte telefónico 24x7 para atención de reporte de fallas o incidentes<br>• Soporte Web 24x7 para atención de reporte de fallas o incidentes<br>• Soporte vía Chat 24x7 para atención de reporte de fallas o incidentes<br>• Soporte de software con releases de mantenimiento y upgrades a nuevas versiones<br>• Soporte de hardware tipo reemplazo avanzado<br><br>Respaldo de fabricante<br>Las licencias de seguridad informática UTM solicitadas en este concepto cuentan con el respaldo por parte del fabricante y "El Proveedor" entrega como parte de su propuesta la siguiente documentación:<br><br>• Se incluye como parte de la propuesta, una carta expedida por el por el fabricante del equipo/licencias de seguridad informática UTM en la que manifiesta que somos integrador autorizado de los equipos nivel Platinum y que estamos autorizados para revender los productos/servicios del fabricante.<br>• Se incluye dentro de la su propuesta técnica, una carta expedida por el por el fabricante del equipo/licencias de seguridad informática UTM en la que manifiesta contamos con las certificaciones requeridas para brindar servicios de instalación y soporte de los equipos de seguridad solicitados.<br>• Contamos con cuatro ingenieros certificados en la solución propuesta, para realizar las actividades de instalación, configuración y puesta a punto y en marcha. al menos nivel de certificación nivel 4.<br>• Se demuestra nuestra experiencia en el soporte de las licencias de seguridad informática solicitado, a través de una relación de clientes exclusivamente de gobierno en donde hemos instalado equipos de la misma marca con características similares a los requeridos por "El Estado", contiene la siguiente información: nombre, dirección, teléfono y correo electrónico de los clientes y una descripción del proyecto de al menos media cuartilla. la Secretaría se Seguridad Publica se reservará el derecho de verificar dicha información.<br><br>Soporte por parte del "El Proveedor"<br>En el caso de resultar ganadores, incluimos como parte de nuestra propuesta un servicio de soporte para los equipos con los siguientes alcances: | | | |

| | | | | |
|---|---|---|---|---|
| | • Duración de 12 meses<br>• Atención de fallas con un tiempo máximo de 2 horas con esquema 5x8.<br>• Se considera (1) mantenimiento preventivo al año para los equipos, previo acuerdo con "El Estado". Los insumos necesarios para el mantenimiento corren por cuenta del "El Proveedor" ganador.<br>• Incluye soporte telefónico sin costo adicional en horario de lunes a viernes en horario de oficina.<br>• 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" se encarga de instalar sin costo dichas actualizaciones.<br><br>Reporte de fallas<br><br>• Contamos Mesa de Ayuda para recibir cualquier evento relacionado con la operación de la infraestructura requerida por parte de la Secretaría de Seguridad Pública del Estado de Campeche. Este centro de atención es propio de "El Proveedor", y se encuentra ubicado en nuestras instalaciones, mediante el uso nuestras propias herramientas y de manera dedicada para el soporte de la infraestructura de comunicaciones.<br>• Los alcances de 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.<br>• La atención y soporte es posibles a través de un número telefónico único con servicio 01-800 sin costo adicional para la Secretaría de Seguridad Pública del estado de Campeche y a través de correo o una página Web.<br>• Los datos que contiene un reporte de falla, mismo que se integran en el control de eventos e incidentes son:<br>o Identificador del reporte o número de incidente o evento<br>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" ganador.<br>o Hora en que reporta el problema por parte del usuario autorizado<br>o Tipo de fallo<br>o Descripción del fallo<br>o Tiempo de solución del incidente y restablecimiento del servicio.<br>• 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.<br><br>Administración de servicios<br><br>• 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: | | | |

OPERADO CON RECURSOS FASP - - 15 - 16 - 17 - - -

| | | | | |
|---|---|---|---|---|
| | o Administración de configuraciones<br>o Administración de cambios<br>o Administración de incidencias<br>o Administración de problemas<br>o Administración de liberaciones<br>o Administración de la capacidad<br>o Administración de los niveles de servicio<br>o Administración de la disponibilidad<br>o Administración de Costo<br>o Mesa de Servicio (Función)<br><br>• 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.<br><br>En caso de resultar ganador "El Proveedor" adquiere las siguientes responsabilidades:<br>• Identificar la causa de la raíz de tales problemas.<br>• 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.<br>• 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.<br>• Verificar que todas las acciones necesarias se han tomado para prevenir la repetición de tal falla.<br>• Mantener los procesos de administración de cambios, incluyendo los procedimientos y métodos vigentes para los cambios.<br>• 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.<br>• 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.<br>• Escalación de los problemas que hayan rebasado los umbrales de respuesta basados en la severidad del problema. | | | |
| | | | **Subtotal** | **$699,723.99** |
| | | | **16% I.V.A** | **$111,955.84** |
| | | | **Total** | **$811,679.83** |

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

**Segunda.- Monto del contrato:** El monto total del contrato es de **$811,679.83 (Son: Ochocientos once mil seiscientos setenta y nueve pesos 83/100 M.N.) I.V.A. incluido**, precio fijo con el cual se considera satisfecho "El Proveedor".

**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 14 días naturales; todos contados a partir de la notificación del fallo, debiendo "El Proveedor" previo a la entrega de los bienes, notificar en un término de cinco días hábiles la entrega de los mismos.

**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, 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 diez 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**: Los bienes y servicios objeto del presente contrato se pagarán 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 factura deberá contener la descripción completa de los bienes, señalando marcas, modelos y números de series. Las series podrán ser desglosadas en un anexo diferente a la factura, tratándose de la adquisición de bienes que para su funcionamiento requieran de otros bienes para su correcto desempeño, se deberán de adjuntar en el anexo de la factura, el desglose de cada uno de ellos con sus series correspondientes. En los casos en que se requiera un anexo de factura, este deberá ser emitido en hoja membretada, haciendo referencia a la fecha y número de factura, nombre y firma de "El Proveedor" o representante legal incluyendo Registro Federal de Contribuyente (R.F.C.), para la identificación plena en caso de futuros reclamos por garantías, para el caso de la adquisición de software o licencias, deberá indicar la vigencia del software y el número de licencia u OEM.

**Séptima.- Para garantizar el cumplimiento y vicios ocultos del contrato:** "El Proveedor" otorgará garantía por el 20% del monto total del presente instrumento contractual a través de póliza de fianza que deberá contener entre otras, las siguientes declaraciones expresas de la institución que las otorgue:

A).- Que sea expedida a favor del Gobierno del Estado de Campeche, teniendo la fianza de cumplimiento y vicios ocultos una vigencia de doce meses posteriores a la entrega total de los bienes y servicios a satisfacción de "El Estado".
B).- Que garantice la entrega de los bienes y servicios, de acuerdo con las estipulaciones establecidas en el mismo instrumento contractual.
C).- Que en caso de que exista inconformidad por parte de "El Estado" respecto de los bienes contratados, "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.
D).- 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.
E).- 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.
F).- 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.

**Octava.- Recepción de los bienes y servicios:** La recepción será total, conforme al plazo establecido en la cláusula tercera de este instrumento y se realizará en la ciudad de San Francisco de Campeche, Campeche, en las instalaciones que ocupa la Secretaría de Seguridad Publica, sita: Avenida López Portillo, por Avenida Lázaro Cárdenas, sin número, colonia Laureles, código postal 24096, 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 establece en el mismo.

**Novena.- Vigilancia, seguimiento, recepción de los bienes por parte de "El Estado":** "El Estado" designa como responsable para la vigilancia, seguimiento y recepción de los bienes contratados, en este caso a la licenciada Emma Vanessa Valle Abreu, Subdirectora de Recursos Federales, de la Secretaría de Seguridad Publica, o por personal que esta misma designe, quien deberá 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, atendiendo para tal efecto las condiciones de garantía requeridas por "El Estado".

**Décima primera.-** "El Proveedor" se obliga a no ceder a terceras personas físicas o morales, sus derechos y obligaciones sobre los bienes 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 segunda.- 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 Tercera.- 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, 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 del contrato.

**Décima Cuarta.- 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 Quinta.-** 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 Sexta.- 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.

**Décima Séptima.-** 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 que fue el presente contrato, ambas partes se manifiestan conformes con su contenido, procediendo a suscribirlo por triplicado, en la ciudad de San Francisco de Campeche, Campeche, el día 05 de diciembre de 2017.

**Por "El Estado"**

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

**Por "El Proveedor"**

Ing. Juan Gualberto Cabrera Pérez
Representante 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