251-2025

REQUISICIÓN DE COMPRA
RECURSO ORDINARIO

SOLICITA:	José Villarreal Rodriguez	**REQ. No.**	
ÁREA o DEPARTAMENTO	Departamento de tecnologías	**FECHA:**	**12/11/2025**

PARTIDA	CLASIFICADOR	UNIDAD	CANTIDAD	DESCRIPCIÓN	P. UNITARIO	COSTO TOTAL
3271	3000	Licencia(s)	50	Kaspersky Next EDR Foundations Mexican Edition - 1 año	$ 485.99	$ 24,299.50

SUBTOTAL:	$ 24,299.50
I.V.A 16%:	$ 3,887.92
TOTAL:	**$ 28,187.42**

FORMA DE PAGO:	CHEQUE ( )	TRANSFERENCIA ( )
PARCIAL ( ) TOTAL (X)	BANCO:	NO. CUENTA:
	clabe:	

OBSERVACIONES:

José Villarreal Rodriguez	MIGUEL ANGEL TRIANA ESTRADA	LIC. IRMA GUADALUPE ACOSTA ROBLES	SALVADOR RODRÍGUEZ VELÁZQUEZ	MTRO. HASSEM RUBÉN MACÍAS BRAMBILA
SOLICITA Nombre y Firma	JEFE DE RECURSOS MATERIALES Y SERVICIOS GENERALES Nombre y Firma	VALIDACIÓN PRESUPUESTABLE, REC. FINANCIEROS Nombre y Firma	DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS Nombre y Firma	AUTORIZA - RECTOR Nombre y Firma
1	2	3	4	5
CLAVE: F-RM-01-01		REVISIÓN:04 12.11.2025		FECHA: 20 de julio de 2025

(FF-25) 8,383.36

(FF-14) 19,804.06

A2Vg6L3L9pV8mHOWtnxzl8SjuJS3w 8nVHaw vaMxeg==|0000100000070269365 4||

Sello digital del SAT:

jyvQq+INB/ySBhTEIV+fC6VO1j+7YV2lQGOtskHNbTL+/3a4KEpGVH06LlaWtQYFxBVyDR+kfx9pK+70VRncP8is7MWXjjcAWg SNxyMAHWQibEk2qmr0nMVj8pkgJvct1JBnabZGeSUMVmoF3/xOlytgYpyw +ARVjq8hxtEI+7ntG6oLHHA1b1vC0uKVM0ju/WNnV

Esta factura fiscal generara intereses moratorios del 3% mensual a partir del dia siguiente de la fecha de vencimiento. Con fundamento en los artículos 380 del Código de Comercio y 2312 del Código Civil Federal, la entrega del producto que se detalla en la presente factura; se hace bajo reserva de dominio, quedando condicionada la obtención de la propiedad del producto, hasta que sea cubierto el monto total de esta factura.

CUENTAS PARA PAGO

BANAMEX - AEVITAS SA DE CV
CLABE PESOS: 002180032163042406
CUENTA DOLARES: 0321 9307240
CLABE DOLARES: 002180032193072404

BANCOMER - AEVITAS SA DE CV
CUENTA PESOS: 165401267
CLABE PESOS: 012180001654012678
CUENTA DOLARES: 0165402271
CLABE DOLARES: 012180001654022710

HACIENDA SAT

Verificación de comprobantes fiscales digitales por internet

RFC del emisor	Nombre o razón social del emisor	RFC del receptor	Nombre o razón social del receptor
N2-ELIMINADO 7	AEVITAS	UPZ040210R31	UNIVERSIDAD POLITECNICA DE LA ZONA METROPOLITANA DE GUADALAJARA
Folio fiscal	**Fecha de expedición**	**Fecha certificación SAT**	**PAC que certificó**
E23CEC23-A251-45F9-A4B0-5A2660A12E22	2025-11-20T12:43:30	2025-11-20T12:44:15	TSP080724QW6
Total del CFDI	**Efecto del comprobante**	**Estado CFDI**	**Estatus de cancelación**
$28,187.42	Ingreso	Vigente	Cancelable con aceptación

Imprimir

UNIVERSIDAD POLITÉCNICA
DE LA ZONA METROPOLITANA DE GUADALAJARA

DEPARTAMENTO DE TECNOLOGÍAS
Oficio DPyE/SI/35/2025
Asunto: Software
Tlajomulco de Zúñiga, Jal. a 12 de noviembre del 2025

DEPARTAMENTO DE RECURSOS MATERIALES Y SERVICIOS GENERALES DE LA UNIVERSIDAD POLITÉCNICA DE LA ZONA METROPOLITANA DE GUADALAJARA

Por medio del presente solicito su apoyo para llevar acabo la compra de licenciamiento para equipo e computo. El requerimiento señalado se encuentra dentro del programa anual de adquisiciones 2025, será cubierto con recursos de la fuente de financiamiento de recursos propios (14) con la partida 3271, señalando que esta Dependencia cuenta con suficiencia presupuestal; mismas que serán utilizadas para el desarrollo de actividades académicas y administrativas.

DESCRIPCIÓN	CANTIDAD
Kaspersky Next EDR Foundations Mexican Edition	**50**

De igual forma, manifiesto que no existen productos alternativos que puedan satisfacer las necesidades detectadas a un precio más bajo, o en su caso, la inexistencia de estudios o consultorías similares a las que se soliciten; así como que esta Dependencia no cuenta con ningún contrato vigente que ampare la prestación de dichos productos/servicios y que la presente solicitud atiende a la **correcta programación de adquisiciones** de esta Área Requirente, en atención a sus necesidades reales y con sujeción al Presupuesto de Egresos aprobado.

La adquisición de software antivirus es fundamental para garantizar la seguridad informática y la protección de la información institucional. En la actualidad, las amenazas cibernéticas, como virus, malware, ransomware y accesos no autorizados, representan un riesgo constante para los equipos de cómputo y los datos sensibles que manejan las dependencias universitarias.

El uso de un antivirus actualizado permite prevenir, detectar y eliminar amenazas digitales, asegurando la continuidad operativa de los sistemas, la protección de documentos confidenciales, y el correcto funcionamiento de los equipos de cómputo utilizados por personal administrativo, docente y estudiantes.

UNIVERSIDAD POLITÉCNICA
DE LA ZONA METROPOLITANA DE GUADALAJARA

La presente solicitud se sujeta al programa anual de adquisiciones de la dependencia, previsto en el artículo 73 fracción I de la Ley de Compras Gubernamentales, Enajenaciones y Contrataciones de Servicios del Estado de Jalisco y sus Municipios.

Adjunto al presente, la siguiente documentación:

1. Original de la Investigación de mercado firmada, acompañada de 1 cotizaciones con vigencia menor a 30 días, con las características que marca el artículo 57 del Reglamento de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

Sin otro particular, agradezco la atención y quedo a sus órdenes.

ATENTAMENTE
"2025, Año de la Eliminación de la Transmisión Materno Infantil del VIH y la Sífilis en Jalisco."

Ing. José Villarreal Rodríguez
Jefe de dpto. de Tecnologías

C.c.p. Archivo

JALISCO
GOBIERNO DEL ESTADO

UNIVERSIDAD POLITECNICA
DE LA ZONA METROPOLITANA DE GUADALAJARA

ANTIVIRUS

Administración FOLIO INTERNO
Nº 1524
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

PROYECTO TIC (Política TIC)

N° o Clave de proyecto: UPZMG/2025/16

1. GLOSARIO:

Siglas o palabra	Significado
UPZMG	UNIVERSIDAD POLITÉCNICA DE LA ZONA METROPOLITANA DE GUADALAJARA

2. ANTECEDENTES

La Universidad cuenta con diversos equipos de cómputo utilizados por personal administrativo, docente y alumnos para el desarrollo de actividades académicas y de gestión. Estos equipos se encuentran conectados a la red institucional y acceden a información sensible, documentos oficiales y plataformas digitales. En los últimos meses se ha identificado la necesidad de fortalecer la seguridad informática ante el incremento de amenazas cibernéticas, como virus, malware, ransomware y accesos no autorizados.

3. JUSTIFICACIÓN

La adquisición de un software antivirus actualizado es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información institucional. Este tipo de herramienta permite prevenir, detectar y eliminar amenazas que puedan comprometer el funcionamiento de los equipos o la red universitaria. Además, reduce el riesgo de pérdida de datos, interrupciones en los servicios informáticos y daños al hardware causados por software malicioso.
Contar con una solución antivirus centralizada y con licencias vigentes también asegura el cumplimiento de las políticas de seguridad de la información establecidas por la institución.

4. OBJETIVOS

Implementar una solución antivirus institucional que brinde protección en tiempo real a todos los equipos de cómputo de la Universidad, garantizando un entorno informático seguro, confiable y eficiente para el desarrollo de las actividades académicas y administrativas.

5. REQUERIMIENTO

Partida N°: 1
Cantidad solicitada de clientes o licencias para estaciones de trabajo: 50
Descripción: **Antivirus Administrable por Consola renovación**
Partida N°: 2
Cantidad solicitada de consolas de administración o licencias para servidor: 1
Descripción: **Antivirus Administrable por Consola renovación**

Administración Dirección General de Innovación Tecnológica Gubernamental
07 NOV. 2025
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

INSTALACIÓN DE SOLUCIÓN DE ANTIVIRUS.

1. **Características de protección en puntos finales**

La solución deberá:

- Brindar protección para servidores, equipos móviles, y estaciones de trabajo sobre Windows 7, Windows 10 y 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Mac OS (Versión 10.12 y superiores) y Linux. Deberá ser capaz de proveer funcionalidad de protección con las siguientes tecnologías:

  a) Antivirus
  b) Antispyware
  c) Firewall
  d) Motor de prevención contra intrusos
  e) Motor de detección de intrusos
  f) Control de aplicaciones
  g) Control de dispositivos
  h) Control Web
  i) Terminal Server

- Permitir que el uso e integración de las tecnologías de protección sea a través de políticas configurables y flexibles en un esquema jerárquico (dominios, sitios, grupos, subgrupo, cliente, usuario, localidades, etc.) para aplicar a perfiles de usuario o equipos en base a los criterios definidos por UPZMG y deberán asignarse desde la consola de administración de la solución.
- Ser configurable para definir de forma flexible diferentes niveles de interacción con el usuario final, es decir permitir al usuario realizar algunas o varias funciones o restringirlas por completo.
- Permitir que las actualizaciones llámese versiones, parches, adecuaciones o modificaciones propias de la solución de protección puedan realizarse de forma automatizada con escasa o nula interacción administrativa, lo anterior deberá realizarse desde la consola central.
- Ser capaz de prevenir la desinstalación sin autorización de la herramienta e incluso poder utilizar una contraseña.
- Ser capaz de evitar que los procesos correspondientes que proveen la protección sean manipulados o comprometidos en forma mal intencionada o sin autorización.
- Ser capaz de enviar en forma automática a la consola y al fabricante los riesgos de seguridad detectados para su revisión y valoración.
- En caso de ser necesario, la solución deberá poder desinstalar cualquier antivirus existente antes de hacer la instalación del nuevo, mediante las mejores prácticas asegurando el buen funcionamiento del equipo de cómputo.
- Permitir la configuración flexible de acciones a tomar ante la detección de riesgos de seguridad.
- Ser capaz de configurar notificaciones sobre la detección de riesgos en base a roles o perfiles de responsabilidad definidos por la UPZMG
- Ser capaz de soportar esquemas de replicación, balanceo de cargas en las consolas de administración centralizadas para estar abiertos a la implementación de planes de recuperación de desastres y disponibilidad de servicio.

ANTIVIRUS

- Ser capaz de integrarse al directorio activo para importar y configurar estructuras organizacionales (usuarios y equipos) para ser cubiertos con la protección de seguridad.
- Ser capaz de manejar diferentes formas de instalación en los equipos de los usuarios finales (por ejemplo interactiva, silenciosa, reiniciar equipo o no).
- Contar con el respaldo de una base de datos de conocimientos, descargas, actualizaciones, documentación, soporte, seguimientos de casos de escalación, despliegue de información provista y mantenida directamente por el fabricante.
- Ser capaz de manejar un esquema que incluya cuarentena centralizada de los riesgos de seguridad detectados.
- Ser capaz de proveer protección de seguridad tanto a usuarios finales administrados centralmente como a usuarios finales descentralizados.
- La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales como a servidores de propósitos específicos o aplicativos.
- Ser capaz de poder remover antivirus de diversos fabricantes antes de poderse instalar el cliente.
- Ser capaz de soportar la administración centralizada de un ambiente de mínimo 50 usuarios finales.
- Ser capaz de soportar el uso de BDs externas (no propietarias de la solución) por ejemplo SQL server.

La tecnología de protección provista por la solución deberá ser altamente efectiva para la detección y remoción de riesgos de seguridad en la categoría de rootkits, amenazas de virus, spyware, ransomware, gusanos, troyano, software malicioso, entre otros.

La instalación del agente de protección deberá poder realizarse de al menos los siguientes métodos: local utilizando la media de instalación, remotamente desde la consola, por medio de un servidor de Intranet o utilizando herramientas de distribución de terceros.

La comunicación del agente con la consola de administración deberá poder realizarse por medio de los protocolos http y https para no provocar modificaciones en la configuración de los switches.

La solución deberá actualizar su contenido (firmas de detección de virus, firmas de detección de intrusos, listado de aplicaciones) desde la consola de administración, desde Internet, desde un equipo definido para la actualización local, inclusive en forma manual.

La solución de protección deberá incluir tecnología de antivirus y antispyware que detecte intentos de infección desde unidades de disco, unidades removibles, unidades compartidas, así como memoria.

La solución de protección podrá ser configurada para que al intentar abrir la interface del usuario solicite una contraseña, en caso de no conocer la contraseña, el usuario no podrá abrir la interface.

Las políticas para la solución de protección deberán poderse aplicar por computadora o por usuario, deberán poderse aplicar por grupo, subgrupo o a todo el universo de equipos.

La solución de protección deberá tener capacidad para identificar el tipo de red al cual se está conectando para adecuar las políticas de protección de antivirus y antispyware, spyware, ransomware, Firewall, IPS, control de Dispositivos, así como de políticas de actualización. La detección de la ubicación deberá poder realizarse por al menos las siguientes variables: rango de dirección IP, dirección IP/nombre del servidor de nombres DNS, dirección IP/nombre del servidor de WINS, default Gateway.

2. Administración

ANTIVIRUS

Deberá contar con una consola de administración centralizada, desde la cual se pueda monitorear el estado de la seguridad en los equipos de cómputo de UPZMG

La consola deberá tener la capacidad de ser accedida desde cualquier punto de la red utilizando a través de un navegador (Internet Explorer, Mozilla Firefox, Chrome).

La consola deberá indicar por medio de una representación gráfica el estado actual de la seguridad, los niveles de seguridad deberán poder ser definidos por el personal que indique la convocante.

La consola de administración deberá:

- Mostrar en una gráfica el estado de la actualización de los patrones de detección en los agentes. En una tabla de mayor detalle deberá indicar el nombre del equipo, su dirección IP, el usuario que se firmó en el equipo y el sistema operativo.
- Mostrar en una gráfica los intentos de infección más recientes, así como los equipos que presentaron dichos intentos de infección indicando además la acción tomada por el agente de protección.
- Mostrar un indicativo del estado de la seguridad en Internet, este estado deberá permitir al administrador de la solución identificar los niveles de riesgo del exterior para poder realizar ajustes en las políticas de protección.
- Funcionar como un repositorio central de políticas para las tecnologías de Antivirus, firewall personal, detección y prevención de intrusos, así como de protección al sistema operativo y control de dispositivos.
- Contar con un esquema de autenticación local, con enlace al directorio activo o con un enlace por medio de RSA para autenticación fuerte.
- Permitir la creación de administración por roles, para permitir una segregación de funciones.
- Permitir la generación de reportes gráficos que permitan identificar los intentos de infección más repetidos en el ambiente de la convocante, los equipos con mayor número intentos de infección, versión del agente de protección instalado en los equipos y un reporte de los equipos con las firmas de contenido.
- Integrar una función que permita reconocer equipos que no tengan el agente de protección instalado. Para posteriormente enviárselo a través de la consola.
- Permitir la instalación remota del agente de protección en los equipos que no cuenten con él. La instalación deberá poderse realizar dando el nombre del equipo, su dirección IP o una lista combinando ambas opciones.
- Permitir la creación de roles para definir diferentes niveles de administración.

La tecnología de antivirus deberá:

- Contar con certificación ICSA Labs en los siguientes rubros: Antivirus cleaning criteria y Desktop/Server antivirus detection.
- Ser capaz de detectar y eliminar spyware.
- Deberá ser capaz de analizar los mensajes de correo electrónico recibidos en los protocolos SMTP (Simple Mail Transfer Protocolo) y POP3 (Post Office Protocol).
- Deberá poder actualizar sus definiciones de virus desde Internet, el servidor central y desde un repositorio local, la actualización de definiciones deberá poderse programar para realizarse en un horario que no provoque afectación a la red.
- Deberá ser capaz de realizar las actualizaciones de forma óptima, firmas de virus así como el motor de búsqueda (por ejemplo utilizando actualizaciones diferenciales y métodos de distribución).
- Deberá ser capaz de analizar archivos comprimidos en al menos los siguientes formatos: ZIP, RAR, y TAR deberá ser capaz de analizar hasta 10 niveles de compresión.

- Deberá ser capaz de definir exclusiones por tipo de archivo, directorios y tipo de amenaza.
- Deberá realizar escaneos de los equipos de manera eficiente, excluyendo todos aquellos archivos que, basados en reputación por parte del fabricante, no representen un riesgo, al contar con una buena reputación.

Las políticas de antivirus de la solución deberán poderse adaptar de acuerdo al reconocimiento de la red a la cual se está conectando.

El fabricante de la solución deberá tener su propio centro de investigación y respuesta de virus, además debe poder generar actualización a contenidos para las tecnologías de antivirus, el firewall personal y detección y prevención de intrusos.

- La tecnología de antivirus deberá contar con tecnología de reputación, es decir que valide si un archivo goza de mala reputación para que este sea bloqueado, o si goza de buena reputación para que este sea excluido.

El agente deberá ofrecer protección al descargar archivos desde internet, al validar que el archivo descargado tenga una reputación aceptable, o en términos de distribución y antigüedad del mismo a nivel mundial.

La solución deberá contar con herramientas con permitan escanear máquinas virtuales off-line.

La solución deberá contar con la capacidad de excluir en las máquinas virtuales, todos aquellos archivos que ya hayan sido escaneados de una imagen base, con la finalidad de reducir el consumo de recursos.

3. Características de la tecnología de firewall personal y prevención de intrusos

La tecnología de firewall personal de la solución deberá:

- Ser de tipo stateful inspection capaz de analizar el tráfico en paquetes de tipo TCP, UDP, IP y en flujo de datos.
- Permitir la definición de reglas por aplicación, por protocolo.
- Integrar un módulo de detección y prevención de intrusos, deberá contener firmas de ataques, estas firmas deberán ser actualizadas desde Internet o desde el servidor central.
- Ser capaz de detectar y deshabilitar controladores de programas como WinPcap y VMware por considerarse riesgosos.
- Contener un módulo que permita el reconocimiento de explotación de vulnerabilidades no importando el método de explotación que se esté utilizando.
- Tener un módulo de inspección profunda para los protocolos DHCP, DNS y WINS.
- Ser capaz de configurar el navegador en modo seguro de tal manera que no publique la versión del navegador ni la dirección IP con la que sale a Internet.
- Ser capaz de detectar y bloquear ataques de OS fingerprint y de generación de secuencias de TCP.

La tecnología de detección de intrusos de la solución deberá incluir ataques en diferentes categorías, las categorías incluidas deberán ser: ataques de buffer overflow, puertas traseras, ataques de negación de servicios, puertas traseras, programas de P2P, mensajeros y propagación de amenazas.

La tecnología de detección de intrusos también se deberá integrar al navegador de internet, para brindar protección a los usuarios finales.

4. Características de control de aplicaciones para protección de sistema Operativo

La tecnología de protección de la solución al sistema operativo debe incluir:

- Mecanismos que eviten la ejecución de procesos maliciosos, estos procesos deberán poder ser definidos a través de políticas.
- Mecanismos que eviten la escritura, lectura o modificación de archivos o directorios. Estos deberán poderse definir a través de políticas.
- Mecanismos que eviten la escritura, modificación o eliminación de llaves de registro. Las llaves de registro a proteger deberán definirse por medio de políticas.

5. Características de bloqueo de dispositivos

La tecnología de bloqueo de dispositivos de la solución deberá:

- Permitir el bloqueo de los siguientes dispositivos: USB, bluetooth, PCMCIA, SCSI, Tarjetas inalámbricas, además deberá permitir la definición de nuevos dispositivos por medio del Class ID y Device ID.
- Permitir la creación de exclusiones para permitir el bloqueo de USB pero no del teclado y el Mouse por ejemplo.
- Permitir el bloqueo de ejecución de programas desde dispositivos removibles.
- Permitir utilizar los dispositivos removibles como solo lectura.

6. Condiciones generales del servicio de instalación y puesta a punto

- La vigencia del licenciamiento será durante el periodo de un año y comenzará a partir del día: 30/11/2025
- El alcance de la solución será 1 en servidores y 50 en estaciones.
- El alcance de los servicios ofrecidos deberá cubrir la instalación y puesta a punto de la solución ofertada. Se deberá brindar apoyo remoto y presencial.
- Deberá incluir soporte técnico durante la vigencia conforme a lo descrito en ANEXO A.- MATRIZ SLA's.
- El proveedor participante deberá hacer la instalación y puesta a punto del servidor antivirus en la Dependencia, en coordinación con la misma.
- El proveedor participante deberá de entregar memoria técnica a detalle de la instalación de cada uno de los componentes que integran la presente solicitud y de la operación del conjunto de la misma.
- Deberá incluir 50 certificaciones y capacitaciones presenciales orientadas al personal operativo de las dependencias del poder ejecutivo, 2 capacitaciones, acerca de la implementación y la correcta funcionalidad.
- La capacitación deberá ser impartida por personal certificado por el fabricante en las versiones que se instalarán en UPZMG

6. GARANTIAS

Garantía de mínimo un año de soporte, actualizaciones y nuevas definiciones de seguridad.

7. OBLIGACIONES DE LOS PARTICIPANTES

Toda la documentación listada en este apartado, forma parte de la documentación que deberán presentar los participantes en su propuesta técnica.

1. Deberá presentar un plan de trabajo apegado a las mejores prácticas, el cual será validado por personal de la convocante, en el cual se muestren las principales actividades, tiempos y responsables para la implementación, capacitación, incluyendo la desinstalación del producto a sustituir (en su caso).

2. Deberá presentar carta de distribuidor autorizado emitida por el fabricante, vigente en original y mencionando el número de concurso al cual participa.
3. Deberá presentar al menos 02 ingenieros certificados en la configuración e implementación de la solución propuesta, emitidos por el fabricante, vigentes y las personas presentadas serán las responsables de realizar las actividades solicitadas.
4. La propuesta deberá incluir un documento de los niveles de SLA's (de acuerdo al anexo A), así como un esquema de escalamiento de acuerdo a severidad.
5. En el documento SLA, deberá incluir números locales de la zona metropolitana de Guadalajara de su área de soporte técnico y número de celulares de los ingenieros que brindarán el soporte técnico.
6. Deberá considerar en su propuesta, cualquier tipo de componente hardware, software, mano de obra, viáticos, traslados, maniobras, herramientas, materiales, insumos, etc. que se requieran para la correcta instalación, configuración y puesta a punto de la solución y capacitación, estos puntos deberán de estar incluidos en el precio de su propuesta.
7. En la propuesta se deberá incluir de manera detallada la cantidad, número de parte, modelo y descripción de los productos y servicios ofertados, en los supuestos de descritos en párrafos anteriores.

Administración FOLIO INTERNO
No. 1524
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

ANEXO A: MATRIZ SLA (Acuerdos de calidad de servicio)

Entrega de solución incluida en el presente anexo

Entregable	Observaciones
Entrega de Licencias	• El bien o servicio, será entregado al día **siguiente de la firma del contrato**. • La entrega del mismo será en: Av. Adolf Bernard Horn Junior 8941, 45670 Cajititlán, Jal.
Instalación	• El plan de trabajo de instalación será validado por el informático de la dependencia. • Una vez realizada la instalación, se deberán entregar las memorias técnicas detalladas al encargado Informático.

Atención de llamadas de incidentes o fallas

Horario de servicio de la Mesa de Servicios	10 horas continúas de 8:00 a 18:00 hrs, (días hábiles) vía telefónica o por correo electrónico o vía Chat.

Atención para brindar soporte técnico al producto

Resolución de los reportes sobre incidentes y problemas levantados en la Mesa de Servicios de la Dependencia	Prioridad crítica: Máximo 2 Horas después de haberse detectado el incidente o problema. (cuando aplique la atención remota) o bien escalarlo para atención en sitio dentro del área metropolitana. Prioridad alta: Máximo 4 Horas después de haberse detectado el incidente o problema. (cuando aplique la atención remota) o bien escalarlo para atención en sitio dentro del área metropolitana. Prioridad baja: Máximo 8 Horas después de haberse detectado el incidente o problema. (cuando aplique la atención remota) o bien escalarlo para atención en sitio dentro del área metropolitana.

Atención a reincidencias en fallas

Administración Dirección General de Innovación Gubernamental
07 NOV 2025
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

Atención de reportes con el fabricante	Solo procederán cuando haya un dictamen conjunto que confirme el apoyo del mismo derivado de reincidencias de servicios o mal funcionamiento. Se atenderán de lunes a Domingo en cualquier horario, 7x24 días.

Administración FOLIO INTERNO
No. 1524
DIRECCIÓN DE PLANEACIÓN TECNOLÓGICA

8. ENTREGABLES

Toda la documentación listada en este apartado, forma parte de la evidencia una vez entregado el servicio o equipo al área requirente.

- Garantía por escrito de mínimo un año de soporte, actualizaciones y nuevas definiciones de seguridad.
- Certificado de licenciamiento o carta en donde se indique la cantidad, ID de licencia o número de serie, nombre del producto, titularidad y vigencia de la misma.
- MATRIZ SLA (Acuerdos de calidad de servicio) así como un esquema de escalamiento de acuerdo a severidad.
- Memoria técnica a detalle de la instalación de cada uno de los componentes que integran la presente solicitud y de la operación del conjunto de la misma.
- Carta bajo protesta de decir verdad, que se otorgarán las certificaciones para el personal de la Dependencia a quienes les sea impartida la capacitación.

9. RESPONSABLES DEL REQUERIMIENTO

Responsable de elaborar el requerimiento	
Nombre: José Villarreal Rodríguez	
Puesto: Jefe de departamento de tecnología	
e-mail: dinformatica@upzmg.edu.mx	
Fecha: 04/11/2025	Tel. /ext. 3318038800
Firma:	

Responsable de autorizar el requerimiento	
Nombre: José Villarreal Rodríguez	
Puesto: Jefe de departamento de tecnología	
e-mail: dinformatica@upzmg.edu.mx	
Fecha: 04/11/2025	Tel. /ext. 3318038800
Firma:	

Administración Dirección General de Innovación Tecnológica Gubernamental
07 NOV. 2025
VALIDACIÓN TÉCNICA
Dirección de Planeación Tecnológica

Vigencia del documento: 120 días a partir del sello de validación

GOBIERNO DEL ESTADO DE JALISCO

FECHA: 12/11/2025

NUMERO DE SOLICITUD:

ÁREA REQUIRENTE: Departamento de Tecnologías

METODOLOGÍA QUE SE UTILIZÓ: Estudio de mercado

INVESTIGACION DE MERCADO

DATOS GENERAL DEL PROVEEDOR	NOMBRE DEL PROVEEDOR:	Gama sistemas	AEVITAS, S.A. DE C.V.	INFORAMA EMPRESARIAL SA DE CV	FUENTE UTILIZADA PARA LA INVESTIGACIÓN
	CONTACTO DE VENTAS:	[redacted]	[redacted]	[redacted]	
	DOMICILIO		José María de Teresa # 65 A	Av. Faro No 2425	
	TELEFONO	3336169222	5533925601	3336231610	
	R.F.C.	GSI8110281W5	AEVITAS, S.A. DE C.V	IEM000824956	
	CORREO ELECTRONICO	mgarcia@gamasistemas.com.mx	sandy.sandoval@aevitas.com.mx	RGARCIA@INFORAMAEMPRESARIAL.C	Investigación de mercado realizada con proveedores
	ORIGEN (LOCAL, NACIONAL O INTERNACIONAL)	Local	N3-ELIMINADO 1 Nacional	Local	N4-ELIMINADO 1 N5-ELIMINAD
CONDICIONES DE VENTA	TIEMPO DE ENTREGA	10 Dias naturales	3 días	15 Dias Naturales	
	CONDICIONES DE PAGO	30 Dias Naturales	Pago de Contado	30 Días Naturales	
	NUMERO DE REGISTRO UNICO DE PROVEEDORES Y CONTRATISTAS	P00655	-	P10646	

DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	PRECIO UNITARIO	IMPORTE TOTAL (IMPUESTOS INCLUIDOS)	PRECIO UNITARIO	IMPORTE TOTAL (IMPUESTOS INCLUIDOS)	PRECIO UNITARIO	IMPORTE TOTAL (IMPUESTOS INCLUIDOS)	PRECIO PROMEDIO O MEDIA (IMPUESTOS INCLUIDOS)
Kaspersky Next EDR Foundations Mexican Edition	50	licencia	$ 734.28	$ 36,714.00	$ 563.75	$ 28,187.42	$ 917.56	$ 45,878.00	$ 36,926.47
								GRAN TOTAL	$36,926.47

MANIFIESTO:

I	DE CONFORMIDAD A LOS ARTICULOS 13, 57 Y DEMAS APLICABLES DE LA LEY DE COMPRAS GUBERNAMENTALES, ENAJENACIONES Y CONTRATACIÓN DE SERVICIOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS, ASI COMO EL ARTICULO 57 DE SU REGLAMENTO Y DEMAS CONCURRENTES, SE LLEVO A CABO LA INVESTIGACION DE MERCADO COMO LO MARCA LA MENCIONADA LEY, POR LO QUE NOS HACEMOS RESPONSABLES DE LA VERACIDAD DE LAS MANIFESTACIONES AQUI PLASMADAS, CON EL CONOCIMIENTO DE LAS CONSECUENCIAS PENALES Y ADMINISTRATIVAS QUE IMPLICARIA LA FALSEDAD DE LA INFORMACION EN LAS MISMAS.
II	SE BUSCARON BIENES Y/O SERVICIOS QUE PUDIERAN SUSTITUIR LO REQUERIDO, ASÍ COMO PROCESOS ALTERNATIVOS DE COMPRA TALES COMO RENTA, NO ENCONTRANDO MEJORES CONDICIONES PARA LO SOLICITADO.
III	SE VERIFICÓ QUE EXISTE LA OFERTA DE LOS BIENES, ARRENDAMIENTOS O SERVICIOS(DEJAR LA QUE VAYA DE ACUERDO A LO REQUERIDO), EN CALIDAD, CANTIDAD Y OPORTUNIDAD REQUERIDAS EN LA SOLICITUD DE APROVISIONAMIENTO MENCIONADA.
IV	QUE EN ÉSTA INVESTIGACIÓN SE MUESTRA EL PRECIO MAXIMO Y MINIMO DE REFERNCIA, ASI COMO LA MEDIA DE LAS TRES COTIZACIONES OBTENIDAS, SIN QUE HUBIERAN CAMBIADO LAS CONDICIONES DEL MERCADO A LA FECHA DE ENTREGA DE LA MISMA.
V	HAGO CONSTAR QUE EN NUESTROS ARCHIVOS SE RESGUARDA LA INFORMACIÓN DE LA METODOLOGÍA QUE DIO ORIGEN AL PRESENTE ESTUDIO.
VI	POR ÚLTIMO, EN RAZÓN DE LOS IMPUESTOS; EJEMPLO: LAS PARTIDAS 1, 2, 3 INCLUYEN I.V.A, LAS PARTIDAS 4 y 5 INCLUYEN IEPS Y LAS PARTIDAS 6, 7 Y 8 GRAVAN TASA 0% (ADECUAR, SEGÚN CORRESPONDA)

ANEXOS:

3 COTIZACIONES DE LOS PROVEEDORES ENUNCIADOS ANTERIORMENTE, CON VIGENCIA DE NO MAS DE 60 DIAS SIN EXCEDER EL PRESENTE EJERCICIO PRESUPUESTAL

EN EL CASO DE CONSULTORIAS, PROYECTOS O ESTUDIOS ANEXAR MANIFIESTO DE QUE NO EXISTEN TRABAJOS SIMILARES EN EL REGISTRO DE SERVICIOS DE CONSULTORIA, ESTUDIOS E INVESTIGACIONES DEL SECG.

ELABORÓ	REVISÓ	AUTORIZÓ
JOSÉ VILLARREAL RODRÍGUEZ JEFE DE DEPARTAMENTO DE TECNOLOGÍAS	SALVADOR RODRÍGUEZ VELÁZQUEZ DIRECCIÓN ADMINISTRACIÓN Y FINANZAS	MTRO. HASSEM RUBÉN MACÍAS BRAMBILA RECTOR

gama sistemas

www.gamasistemas.com.mx

Comprometidos con sus Soluciones de TI

Guadalajara, Jal. A
4 de septiembre de 2025

COTIZACION

MG 1

Para: **UNIVERSIDAD POLITECNICA DE LA ZONA METROPOLITANA DE GUADALAJARA**
ADOLF B. HORN 8941, COL. ARVENT, CP 45670
TALJOMULCO DE ZUÑIGA, JALISCO

RFC GAMA SISTEMAS;GSI8110281W5

Atención: JOSE VILLAREAL RODRÍGUEZ
Jefe de Departamento de Informatica

RENGLON	DESCRIPCIÓN	MARCA	SKU	UNIDAD DE MEDIDA	CANT	PRECIO UNITARIO	IMPORTE
1	Power BI Pro - ANUAL	Microsoft	CFQ7TTC0LHSF:0001	Licencia(s)	2	$ 3,197.00	$ 6,394.00
2	Kaspersky Next EDR Foundations Mexican Edition	Kaspersky	KL4065ZAQFS	Licencia(s)	50	$ 633.00	$ 31,650.00
3	Office LTSC Standard 2024 - PERPETUA	Microsoft	DG7GMGF0PN5D	Licencia(s)	100	$ 1,750.00	$ 175,000.00
						SUBTOTAL	$ 213,044.00
						IVA 16%	$ 34,087.04
						TOTAL	**$ 247,131.04**

CONDICIONES COMERCIALES

MONEDA
La presente propuesta se presenta en Moneda Nacional y deberá ser pagada en Moneda Nacional
VIGENCIA DE LA PROPUESTA
60 Dias Naturales
TIEMPO DE ENTREGA
15 Días naturales
CONDICIONES DE PAGO
Credito 60 días
GARANTÍAS
Garantía de acuerdo con las políticas del fabricante que incluye actualizaciones durante la vigencia
NOTA LEGAL
La información presentada como anexo a esta cotización proviene de la documentación que el fabricante tiene para este fin, por lo que Gama Sistemas no se hace responsable por errores u omisiones en dicha información.
Imágenes solo ilustrativas, podrian variar con referencia al producto cotizado.

PROVEEDOR DE JALISCO
PROVEEDOR P00655

mgarcia@gamasistemas.com.mx
(33) 3616-9222 ext. 124
3310256692

Mario Alonso Garcia Anguiano
Consultor TI

aevitas

jueves, 6 de noviembre de 2025

AEVITAS, S.A. DE C.V.
Calle: José María de Teresa # 65 A
Colonia San Ángel, Alcaldía Alvaro Obregón
CMDX C.P. 01000

Pago de Contado
MXN - Peso Mexicano
Tiempo de entrega de 2 a 3 días hábiles
Vigente al 20 de Noviembre de 2025

UNIVERSIDAD POLITECNICA DE LA ZONA METROPOLITANA DE GUADALAJARA
Jose Villareal
Sistemas
Teléfono: 3330409900 ext.930
Correo: DINFORMATICA@UPZMG.EDU.MX

Atención Comercial
Sandy sandoval
Celular 5533925601
Número Teams: 5568468225
sandy.sandoval@aevitas.com.mx

CONTRATO ANUAL

Cantidad	Descripción	Precio Unitario	Subtotal
50	Kaspersky Next EDR Foundations Mexican Edition. 50-99 User 1 year Renewal License	$ 485.99	$ 24,299.52
50	Kaspersky Next EDR Foundations Mexican Edition. 50-99 User 2 year Renewal License	$ 777.44	$ 38,872.00
50	Kaspersky Next EDR Foundations Mexican Edition. 50-99 User 3 year Renewal License	$ 1,217.87	$ 60,893.44
		Subtotal	**$ 124,064.96**
		IVA	**$ 19,850.39**
		Total MXN	**$ 143,915.35**

Terminos y Condiciones Comerciales
Sujeto a cambios sin previo aviso.
Los servicios de instalación y configuración no están incluidos y se cotizan por separado.
Los pedidos tienen la característica de no cancelación y no devolución.
Pago en Dólares o alternativamente al tipo de cambio de Banamex a la venta el día del deposito
Antes de procesar su compra es necesario confirmar que el producto y el precio sigan vigentes

Para procesar el pedido se requiere de lo siguiente.	
Cotización firmada	X
Orden de compra donde se confirmen las condiciones comerciales pactadas	X
Comprobante de pago.	X

El Cliente
UNIVERSIDAD POLITECNICA DE LA ZONA
Jose Villareal
Sistemas

El Proveedor
AEVITAS, S.A. DE C.V.

UPZMG

ADOLF B. HORN 8941, COL. ARVENT, CP 45670, TALJOMULCO DE ZUÑIGA, JALISCO

José Villareal

PRESENTE:

GUADALAJARA, JALISCO A 04 DE SEPTIEMBRE DE 2025

PARTIDA	CANT	DESCRIPCION	MARCA	PRECIO UNITARIO	IMPORTE
1	2	*Power BI Pro - ANUAL*	*Microsoft*	$ 3,500.00	$ 7,000.00
2	50	*Kaspersky Next EDR Foundations Mexican Edition - 1 año*	*Kaspersky*	$ 791.00	$ 39,550.00
3	100	*Office LTSC Standard 2024 - PERPETUA*	*Microsoft*	$ 2,250.00	$ 225,000.00
				SUBTOTAL	$ 271,550.00
				IVA	$ 43,448.00
				TOTAL	$ 314,998.00

Garantía de acuerdo con las políticas del fabricante que incluye actualizaciones durante la vigencia

ORIGEN DE LOS BIENES: Internacional
MONEDA: Pesos Mexicanos
VIGENCIA DE LA PROPUESTA; 90 DIAS NATURALES
TIEMPO DE ENTREGA: 15 dias naturales
CONDICIONES DE PAGO: 30 DÍAS NATURALES

Entregables: De acuerdo a la ofertado en el anexo tecnico.

Declaro bajo protesta de decir verdad que los precios cotizados son bajo la condición de precios fijos hasta la total prestación de los servicios o entrega de los bienes.

N7-ELIMINADO 6

RAZON SOCIAL: INFORAMA EMPRESARIAL SA DE CV
RFC: IEM000824956
PROVEEDOR P10646

GIRO: COMERCIO AL POR MAYOR DE MOBILIARIO, EQUIPO, Y ACCESORIOS DE COMPUTO

N8-ELIMINADO 1

RGARCIA@INFORAMAEMPRESARIAL.COM.MX
REPRESENTANTE LEGAL

HSBC

Pagos SPEI enviados

Fecha: 25/11/2025
Hora: 09:40:38
Página: 1

Fecha valor	25/11/2025	Clave de Rastreo:	HSBC541411
Fecha de liquidación:	25/11/2025	Hora de liquidación:	15:39:40 MX

DETALLES DEL CARGO

Cuenta Ordenante:	4032209025
Nombre del Ordenante:	PAGO A PROVEEDORES
Referencia del ordenante:	26277BB00LW9
Comisión cobrada:	8.00
Moneda:	MXN
Monto:	28,187.42

DETALLES DEL ABONO

Cuenta del Beneficiario: N1-ELIMINADO 1

Referencia Numérica: 1

Nombre del Beneficiario:	AEVITAS S.A. C.V.
Banco Receptor:	BANAMEX
Concepto de Pago:	F-A44619 LICENCIAS KASPERSKIS

*****Emitido por: HSBC México, S.A., Institución de Banca Múltiple, Grupo Financiero HSBC*****

FUNDAMENTO LEGAL

1.- ELIMINADO el nombre de un particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

2.- ELIMINADA la Clave de Registro Federal de Contribuyentes (RFC), 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

3.- ELIMINADO el nombre de un particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

4.- ELIMINADO el nombre de un particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

5.- ELIMINADO el nombre de un particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

6.- ELIMINADO el nombre de un particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

7.- ELIMINADA la firma de particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracciónes IX y X de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

8.- ELIMINADO el nombre de un particular, 1 párrafo de 1 renglón por ser un dato identificativo de conformidad con los artículos 3.2 fracción II inciso "a" y 21.1 fracción I de la LTAIPEJM, artículo 3.1 fracción IX de la LPDPPSOEJM y Lineamiento Quincuagésimo Octavo fracción I de los LGPPICR.

* "LTAIPEJM: Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
LPDPPSOEJM: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios.
LGPPICR: Lineamientos Genenerales para la Protección de la Información Confidencial y Reservada que deberán observar los sujetos obligados previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios."