## Anexo 1

“ROBUSTECIMIENTO DE SEGURIDAD INFORMÁTICA, ETAPA 1”

## **Introducción**

Objeto: Adquisición de soluciones y/o equipos de seguridad informática e informática forense de última generación y su licenciamiento destinado al “Robustecimiento de Seguridad Informática, Etapa 1”.

## En la propuesta se deberán incluir las garantías y servicios que más adelante se indican.

## El presente documento se divide en **doce apartados**:

|  |  |
| --- | --- |
| ***APARTADO*** | ***NOMBRE*** |
| ***A*** | **Partidas.** |
| ***B*** | **Lineamientos generales.** |
| ***C*** | **Estructura de la propuesta.** |
| ***D*** | **Características** **técnicas.** |
| ***E*** | **Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante.** |
| ***F*** | **Características de las garantías y servicios.** |
| ***G*** | **Cuadro de distribución.** |
| ***H*** | **Evaluación técnica de prototipos** |
| ***I*** | **Modelos de cartas.** |
| ***J*** | **Formatos.** |
| ***K*** | **Penas y deductivas.** |
| ***L*** | **Supervisión, control y seguimiento.** |

### A. Partidas

#### Las partidas solicitadas son las siguientes:

|  |
| --- |
| ***Soluciones de seguridad informática e informática forense de última generación y su licenciamiento destinado al “Robustecimiento de Seguridad Informática, Etapa 1”*** |
| ***PARTIDA*** | ***SUBPARTIDA*** | ***NOMBRE*** |
| **Partida 1*****Secure Web Gateways, Reporteador y Administración Centralizada BlueCoat*** | **1.1** | * Solución Secure Web Gateways con antivirus de marca BlueCoat
 |
| **1.2** | * Solución de Software de Reporteo de navegación web de marca BlueCoat
 |
| **1.3** | * Administración centralizada de Secure Web Gateway de marca BlueCoat
 |
| **Partida 2****Kits móviles de informática forense y servidores de análisis y borrado de discos duros** | **2.1** | * Kits móviles de informática forense.
 |
| **2.2** | * Servidor en formato torre para solución centralizada y análisis de evidencia de informática forense
 |
| **2.3** | * Servidor en formato torre para borrado seguro de discos duros
 |
| **Partida 3** |  | * Solución integral de protección horizontal contra amenazas de malware
 |
| **Partida 4** |  | * Solución de administración de eventos y seguridad de la información (SIEM)
 |
| **Partida 5** **Solución integral de protección contra amenazas avanzadas para el vector web, puntos finales y correo electrónico** | **5.1** | * Solución integral de protección contra amenazas avanzadas para el vector web
 |
| **5.2** | * Solución integral de protección contra amenazas avanzadas para el vector correo electrónico
 |
| **5.3** | * Solución integral de protección contra amenazas avanzadas para puntos finales
 |
| **Partida 6** |  | * Servidores de datos para servicios críticos
 |
| **Partida 7** |  | * Monitor LCD de 70 pulgadas
 |

### B. Lineamientos generales

## Los participantes deberán sujetarse a los siguientes lineamientos de carácter general:

**B.1** La propuesta deberá presentarse por partida completa, la cual, según su caso podrá estar integrada por subpartidas, debiendo ofertar la totalidad de los bienes, servicios y características mínimas que se solicitan; la propuesta que no cumpla con lo descrito en este párrafo será desechada, entendiéndose que cada partida (completa) es independiente, y el participante podrá presentar oferta de las partidas en las que desee participar.

**B.2** El participante deberá integrar su propuesta técnica separando la documentación de acuerdo a la estructura mencionada en el **apartado C. *Estructura de la propuesta***.

**B.3** Todas las cartas y formatos solicitados **deberán presentarse en original y con firma autógrafa** por la(s) persona(s) legalmente facultada(s) para ello, acorde a lo establecido en cada modelo de carta. **La omisión de lo anterior, será motivo para desechar su propuesta**.

**Todos los certificados solicitados, deberán estar vigentes a la fecha de presentación de la(s) propuesta(s), la omisión de lo anterior, será motivo para desechar su propuesta.**

**B.4** El participante deberá subrayar o marcar en la documentación técnica, folletos, páginas de Internet o cualquier documento comprobatorio que presenten, las características solicitadas con su numeral correspondiente.

En caso de que alguna especificación técnica solicitada en el presente **Anexo Técnico**, no sea descrita en los catálogos, la folletería o en los manuales, se puede presentar carta del fabricante, firmada por el representante legal de la misma, donde manifieste bajo protesta de decir verdad, que el equipo ofertado cumple con las características técnicas requeridas, siempre y cuando no contradiga algún dato ya publicado.

**B.5** Los participantes presentarán sus propuestas con las **cantidades solicitadas, y unidades de medida** (v. g.; longitud de cables, dimensiones de componentes, etc.) expresamente señaladas en cada partida del presente **Anexo Técnico**. En caso de presentarse en unidades de medida diferentes, tendrán que anexar un documento de referencia, con la conversión correspondiente.

**B.6** Los manuales de usuario podrán entregarse en formato electrónico (v.g. CD, DVD, memoria USB), con la finalidad de disminuir el uso de papel.

**B.7** La evaluación de las propuestas técnicas se realizará de manera cualitativa, conforme a la integración de las mismas, debiendo acreditar el cumplimiento de los requisitos establecidos en el presente documento.

**C. Estructura de la propuesta**

## La oferta técnica presentada contendrá las siguientes secciones:

|  |  |
| --- | --- |
| ***SECCIÓN*** | ***NOMBRE*** |
| ***Sección I*** | Descripción de los bienes y servicios objeto de su oferta. |
| ***Sección II*** | Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante. |
| ***Sección III*** | Garantías y servicios de los bienes solicitados. |

A continuación, se describe el contenido de cada una de las secciones.

|  |
| --- |
| **SECCIÓN I****DESCRIPCIÓN DE LOS BIENES Y SERVICIOS OBJETO DE SU OFERTA** |
| Se deberá llenar la(s) tabla(s) correspondiente(s) con la descripción detallada de las características de los bienes y servicios ofertados, acorde a lo solicitado como mínimo en las partidas definidas. |
| **NÚMERO DE ÍNDICE** |  | **D E S C R I P C I Ó N** | **REFERENCIA** | **PARTIDAS EN LAS QUE APLICA** |  | **MODELO O FORMATO** |
| **I.1** |  | **Descripción de los bienes y servicios objeto de su oferta.** | Apartado **D** *(“Características técnicas”), subíndice D.1* |  Todas las partidas |  | *Formato No.* ***1****, apartado* **J** *(“Formatos”)* |

|  |
| --- |
| **SECCIÓN II****CARTAS COMPROMISO, DOCUMENTOS COMPROBATORIOS Y DOCUMENTACIÓN TÉCNICA DEL FABRICANTE** |
| Cartas compromiso y documentos comprobatorios de acuerdo al orden y en los términos indicados.Las cartas compromiso deberán ser presentadas en los mismos términos que los modelos mostrados en el **apartado I** (“***Modelos de Cartas***”). No será motivo de desechamiento de la propuesta, la no observancia de los modelos de cartas sugeridos, siempre y cuando el licitante proporcione de manera clara la información requerida y ésta no cambie el sentido de lo solicitado. |
| **NÚMERO DE ÍNDICE** |  | **D E S C R I P C I Ó N** | **REFERENCIA** | **PARTIDA EN LA QUE APLICA** |  | **MODELO O FORMATO** |
| **II.1** |  | **Carta de entrega de bienes idénticos.** | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | Todas |  | *Carta No.* ***1*** *apartado* **I**  *(“Modelos de cartas”)* |
| **II.2** |  | **Carta de componentes y partes originales.** | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | Todas |  | *Carta No.****2*** *apartado* **I***(“Modelos de cartas”)* |
| **II.3** |  | **Carta de certificación de calidad.** | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | Todas |  | *Carta No.****3*** *apartado* **I***(“Modelos de cartas”)* |
| **II.4** |  | **Carta de distribuidor autorizado.** | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | Todas |  | *Carta No.****4*** *apartado* **I** *(“Modelos de cartas”)* |
| **II.5** |  | **Carta de instalación.** | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | 1,2,3,4,5 y 6 |  | *Carta No.* ***5*** *apartado* **I** *(“Modelos de cartas”)* |
| **II.6** |  | **Documentación técnica del fabricante** Nota: Podrá presentarse documentación en idioma del país de origen, pero deberá ir acompañada de una traducción simple al español, subrayando o marcando las características técnicas solicitadas con su numeral correspondiente a la partida en la que participe. | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.2*** | Todas |  | **No aplica modelo o formato de carta** |
| **II.7** |  | **Copia simple del certificado vigente correspondiente al fabricante (NOM-001-SCFI-1993) conforme lo establece(n) la(s) dependencia(s) gubernamental(es) responsable(s) de su emisión y vigilancia.** Nota: El certificado debe especificar el producto, marca y modelo ofertado. Si el certificado indica una clave genérica del modelo, se deberá incluir una carta del fabricante, explicando claramente la relación existente entre la clave y el modelo comercial del equipo. | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | Todas |  | **No aplica modelo o formato de carta** |
| **II.8** |  | **Copia simple del certificado vigente correspondiente al fabricante (NOM-019-SCFI-1998)** conforme lo establece(n) la(s) dependencia(s) gubernamental(es) responsable(s) de su emisión y vigilancia.No aplica para productos que sean operados por tensiones eléctricas inferiores o iguales a 24 volts. Nota: El certificado debe especificar el producto, marca y modelo ofertado. Si el certificado indica una clave genérica del modelo, se deberá incluir una carta del fabricante, explicando claramente la relación existente entre la clave y el modelo comercial del equipo. | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | Todas |  | **No aplica modelo o formato de carta** |
| **II.9** |  | **Carta de personal capacitado y especializado** | Apartado **E** *(“Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante”), subíndice* ***E.1*** | 1,2,3,4,5 y 6 |  | *Carta No.****9*** *apartado* **I** *(“Modelos de cartas”)* |

|  |
| --- |
| **SECCIÓN III****Garantías y servicios de los bienes solicitados** |
| De conformidad a lo solicitado en el **apartado “F”** |
| **NÚMERO DE ÍNDICE** |  | **D E S C R I P C I Ó N** | **REFERENCIA** | **PARTIDA EN LA QUE APLICA** |  | **MODELO O FORMATO** |
| **III.1** |  | **Carta de cumplimiento de términos y condiciones de las garantías y servicios.** | *A*partado **F** *(“Características de las garantías y servicios”), subíndice* ***F.1*** | Todas |  | *Carta No.* ***6*** *apartado* **I** *(“Modelos de cartas”)* |
| **III.2** |  | **Carta de cumplimiento de términos y condiciones de entrega de bienes.** | Apartado **F** *(“Características de las garantías y servicios”)subíndice* ***F.2.1*** | Todas |  | *Carta No.* ***7*** *apartado* **I** *(“Modelos de cartas”)* |
| **III.3** |  | **Número telefónico del tipo larga distancia automática nacional (lada 01-800 o equivalente).** | Apartado **F** *(“Características de las garantías y servicios”), subíndice* ***F.5.2*** | Todas |  | **No aplica modelo o formato de carta** |
| **III.4** |  | **Relación de centros de servicio.**  | Apartado **F** *(“Características de las garantías y servicios”), subíndice* ***F.5.3*** | Todas |  | *Formato No.* ***2****, apartado* ***J*** *(“Formatos”)*  |
| **III.5** |  | **Cartas de los Centros de Servicio que apoyarán para brindar los servicios de garantía.** | Apartado **F** *(“Características de las garantías y servicios”), subíndice* ***F.5.3*** | Todas |  |  *Carta No.* ***8****apartado* **I** *(“Modelos de cartas”)* |
| **III.6** |  | **Relación de centros de servicio para las ciudades restantes.** | Apartado **F** *(“Características de las garantías y servicios”), subíndice* ***F.5.3*** | Partida 6 |  | *Formato No. 3, apartado* ***J*** *(“Formatos”)* |

D. Características técnicas

**D.1 CARACTERÍSTICAS TÉCNICAS**

El presente apartado tiene por objeto proporcionar a las empresas participantes en la licitación las características técnicas **mínimas** que deberán cumplir las soluciones y/o equipos y su licenciamiento a ofertarse, excepto en aquellos casos en los que se especifique, expresamente, una característica determinada.

La propuesta técnica deberá incluir, en **las partidas que así lo requieran**, todos los componentes, accesorios y características detallados en el presente anexo. La omisión de cualquiera de ellos, podrá ser motivo para desechar su propuesta.

**“CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS Y/O SOLUCIONES”**

Las siguientes fichas técnicas tienen la finalidad de proporcionar a las empresas participantes las características técnicas de las soluciones y/o equipos de cada partida, objeto de la presente adquisición.

|  |
| --- |
| **PARTIDA 1***Secure Web Gateways, Reporteador y Administración Centralizada BlueCoat* |
| **SUBPARTIDA 1.1** |
| *Solución Secure Web Gateways con antivirus de marca BlueCoat* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.**EN APEGO A LA NORMATIVA VIGENTE, EL ÁREA TÉCNICA HA SUSTENTADO LA NECESIDAD DE ADQUIRIR POR MARCA DETERMINADA (BLUECOAT) LA SOLUCIÓN DE FILTRADO WEB; ELLO, A EFECTO DE ASEGURAR LA COMPATIBILIDAD, CONECTIVIDAD, IDONEIDAD Y HOMOGENEIDAD TECNOLÓGICA CON LA PLATAFORMA QUE YA SE ENCUENTRA INSTALADA EN EL CONSEJO DE LA JUDICATURA FEDERAL. |
| **Núm.** | **REQUERIMIENTO MÍNIMO**Los enlaces de internet propios del Consejo de la Judicatura Federal deberán contar con equipo de seguridad web como se detalla a continuación. |
|  | **Características:**  |
|  | **Rendimiento.** | * 1 equipo que soporte 500 Mbps y al menos 10000 usuarios para el enlace de internet CCA Ciudad Judicial, Zapopan.
* 1 equipo que soporte 500 Mbps y al menos 5000 usuarios para el enlace de internet CCP Canoa 79.
* 1 equipo que soporte 300 Mbps y al menos 3000 usuarios para el enlace de internet Edificio Sede.
* 1 equipo que soporte 300 Mbps y al menos 5000 usuarios para el enlace de internet San Lázaro.
 |
| **Todos los equipos que integran la solución deben cumplir con los siguientes parámetros de integración y operación.** |
|  | **Puertos de operación.**  | Puertos integrados:- 1000 Base – T Puertos de cobre (con *bypass*).- 1000 Base – T Puertos de cobre (sin *bypass*).- 10/100 Base – T Cobre, puerto de administración  |
|  | **Parámetros Generales.** | Proveer una solución de filtrado de contenido y seguridad Web para los enlaces de internet, basada en appliance con sistema operativo y software específico para este propósito; el cual debe contener las siguientes características:1. Arquitectura de proxy escalable para asegurar las comunicaciones Web.
2. Soportar los siguientes métodos de implementación: implícito (en línea, policy based routing-, WCCP) y explícito (WPAD, archivos PAC).
3. Operación como proxy para los siguientes protocolos: HTTP, HTTPS (HTTP sobre SSL), FTP, DNS, CIFS, MAPI, SOCKS(v4/v5), RTSP/QuickTime, RTMP, RTMPE, MMS, TCP-tunnel, S-TUNNEL.
4. Administración de ancho de banda, soporte de media stream splitting y almacenamiento de caché para la optimización de entrega de multimedios y contenido. Manejo de cuotas por volumen y tiempo.
5. Geolocalización del tráfico.
6. Clasificación del contenido web en al menos 80 categorías de Filtrado de Contenido.
7. Deberá realizar filtrado para las categorías de YouTube, es decir, podrá habilitar únicamente YouTube educacional.
8. Reconocimiento y categorización de contenido web en diversos idiomas, incluido completamente el idioma español.
9. Base de datos de la solución de filtrado web que contenga al menos un mil millones de URLs.
10. Categorización dinámica en tiempo real para sitios nuevos, que permita el análisis y categorizar nuevos sitios con una precisión del 98%.
11. Protección directa y automática con servicios basados en la nube que permitan la protección proactiva para sitios nuevos que contengan o no, amenazas de seguridad informática (malware) o requieran categorización de contenido.
12. Deberá de tener la capacidad de brinda runa seguridad por capas para correo electrónico protegiendo contra amenzas conocidas, desconocidas y ataques dirigidos, con la capacidad de incluir firmas de al menos dos antivirus reconocidos en la industria, lista blanca y los servicios de reputación de archivos, análisis de código estático y dinámico.
 |
|  | **Filtrado e intercepción de contenido Web en protocolos de capa de aplicación, HTTP y HTTPS.** | 1. Detección y bloqueo de amenazas web en tiempo real.
2. Lenguaje (visual o de línea de comando) para aplicación de políticas de seguridad sobre el contenido web, esquemas de autenticación, envío de mensajes/alertas, entre otros.
3. Soporte para usuarios con Windows (7 o superior) y Mac OS X (10.0 o superior).
 |
|  | **Control de aplicaciones** | 1. Habilitación de búsquedas seguras en navegadores web.
2. Control granular sobre redes sociales y sus aplicaciones como: “publicar mensajes”, “envío de email”, “email”, “subir fotografías”, “subir videos”, “juegos”, “mensajería instantánea”.
3. Control de correo electrónico web, clips de audio y video, mensajería instantánea web, y aplicaciones web generales.
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de todos los equipos deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física de los equipos, la configuración y puesta a punto de cada uno de ellos realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por cada una de las instalaciones realizadas. |

Adicionalmente a lo señalado en estas bases para estos equipos, se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | Los equipos que se solicitan deberán contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La(s) solución(es) será(n) distribuida(s) e instalada(s) acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar las licencias activadas, a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 1***Secure Web Gateways, Reporteador y Administración Centralizada BlueCoat* |
| **SUBPARTIDA 1.2** |
| *Solución de Software de Reporteo de navegación web de marca BlueCoat.* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que la solución considere la última versión disponible en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.**EN APEGO A LA NORMATIVA VIGENTE, EL ÁREA TÉCNICA HA SUSTENTADO LA NECESIDAD DE ADQUIRIR POR MARCA DETERMINADA (BLUECOAT) LA SOLUCIÓN DE SOFTWARE DE REPORTEO DE NAVEGACIÓN WEB; ELLO, A EFECTO DE ASEGURAR LA COMPATIBILIDAD, CONECTIVIDAD, IDONEIDAD Y HOMOGENEIDAD TECNOLÓGICA CON LA PLATAFORMA QUE YA SE ENCUENTRA INSTALADA EN EL CONSEJO DE LA JUDICATURA FEDERAL. |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características:** |
|  | **Reporteador de Navegación Web** | Para consolidación de reportes web que permita tener la visibilidad y control sobre la actividad de los usuarios en la web, tanto para trafico web general como el relacionado a video. La solución debe ser completamente adaptable y ofrecer características de interfaz de visualización amigable e intuitiva que permitan mostrar reportes de seguridad, cumplimiento, administración de ancho de banda, entre otros, asimismo debe contar con los siguientes parámetros:* Capacidad de ocultar datos para los reportes.
* Contar con los siguientes reportes predefinidos:
	+ Tablero con navegación en tiempo real que muestre la actividad web y los eventos de seguridad actuales e históricos.
	+ Actividad web de spyware y malware, uso de video, aplicaciones web, términos para búsquedas, categorías filtradas, contenido web, sesiones, perfiles de tráfico, usuarios y autenticación.
	+ Reportes que interpreten la actividad web histórica correlacionando la información con grupos como uso en Negocios, responsabilidad legal, pérdida de ancho de banda, riesgos de seguridad, entre otros.
	+ Acceso y reportes personalizados para administradores que contengan vistas predefinidas como vista de seguridad, vista para administración de redes y vista de administración.
* Debe ser capaz de procesar las líneas de LOGs (para el reporteo de un tráfico dependiendo el enlace de internet, señalados en el punto 1 de la SUBPARTIDA 1.1, y ser almacenados por 6 meses).
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de toda la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación, la configuración y puesta a punto de la solución, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica de la instalación realizada. |

Adicionalmente a lo señalado en estas bases para esta solución, se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | La solución de software solicitada deberá contar con una garantía en sitio por el período mínimo de 3 años. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra con una garantía mínima de 36 meses, y en caso de reinstalación o reconfiguración del software, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La(s) solución(es) será(n) distribuida(s) e instalada(s) acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 1***Secure Web Gateways, Reporteador y Administración Centralizada BlueCoat* |
| **SUBPARTIDA 1.3** |
| *Administración centralizada de Secure Web Gateway de marca BlueCoat* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.**EN APEGO A LA NORMATIVA VIGENTE, EL ÁREA TÉCNICA HA SUSTENTADO LA NECESIDAD DE ADQUIRIR POR MARCA DETERMINADA (BLUECOAT) LA ADMINISTRACIÓN CENTRALIZADA DE SOLUCIÓN WEB; ELLO, A EFECTO DE ASEGURAR LA COMPATIBILIDAD, CONECTIVIDAD, IDONEIDAD Y HOMOGENEIDAD TECNOLÓGICA CON LA PLATAFORMA QUE YA SE ENCUENTRA INSTALADA EN EL CONSEJO DE LA JUDICATURA FEDERAL. |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características:**  |
|  | **Administración Centralizada de Solución Web** | Contar con una consola de administración centralizada para la configuración de la solución de filtrado de contenido con las siguientes características y funcionalidades:* Creación de políticas locales que puedan ser distribuidas globalmente; a través de un esquema de jerarquías que incluyan políticas maestras, políticas regionales o locales, que puedan ser adecuadas para los requerimientos de configuración de cada uno de los equipos que componen la solución.
* Autentificación de administradores de la consola a través usuarios locales del sistema, LDAP, Radius y TACACS+.
* Acceso a la consola de administración centralizada a través de Web o línea de comandos de forma segura.
* Respaldo y archivado de configuraciones en automático.
* Automatización de tareas calendarizadas para el mantenimiento, actualización de políticas, respaldos, actualizaciones del sistema operativo y de licencias.
* Automatización de entrega de contenido a través de la calendarización de tareas.
* Monitoreo en tiempo real de los dispositivos a administrar agrupados por severidad, métrica, estado, status y tiempo de los componentes de hardware y software de la solución como: utilización de CPU, estado de los discos duros, memoria, interfaces de red, utilización de licenciamiento, expiración de licenciamiento, distribución de tráfico, procesamiento y throughput por tipo de protocolo empleado, entre otros.
* Entrega de bitácoras que permitan rastrear a detalle (perfil, IP, comando) de los cambios de configuración realizados, respaldos de configuración, modificación de tareas calendarizadas, entre otras.
* Solución basada en appliance de propósito específico en modalidad de hardware o virtual appliance.
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física, configuración y puesta a punto de la solución realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica de la instalación realizada. |

Adicionalmente a lo señalado en estas bases, para esta solución se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | La solución que se solicita deberán contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La(s) solución(es) será(n) distribuida(s) e instalada(s) acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 2***Kits móviles de informática forense y servidores de análisis y borrado de discos duros* |
| **SUBPARTIDA 2.1** |
| *Kits móviles de informática forense* |
| **CANTIDAD SOLICITADA: 6** |
| Es indispensable que los kits consideren hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Laptop para recuperación y análisis de evidencia** |
|  | * Sistema operativo Windows 10 o superior
	+ Tipo Sistema: 64 bits, edición: Pro o Enterprise.
	+ Idioma: español
* Procesador: Intel® Core™ i7-7700K o superior.
	+ 4 Número de núcleos mínimo.
	+ Cache de 6 MB o superior.
	+ Velocidad @ 3.5 GHz o superior.
* Memoria RAM de 32 GB
* Almacenamiento:
	+ Disco duro para sistema 256 GB SSD
	+ Disco duro para cache 256 GB SSD
	+ Disco duro para datos 1TB 7200 rpm
* Lector de memorias 6-in-1 (MMC/RSMMC/SD/Mini-SD/SDHC/SDXC up to UHS-II)
* Conectividad:
	+ Puertos de red de datos RJ45 1Gb mínimo.
	+ Conexión Inalámbrica Banda dual 802.11ac
	+ Bluethoot 4.2.
* 3 puertos USB 3.0 y 1 eSATA/USB 3.0.
* Controladora de video integrada con memoria de 1GB.
* Puerto HDMI.
* Lector externo USB de blu-ray BR-RE/CDRW/DVDRW.
* Software encase (última versión).
* Maletín para trasportación segura para alto impacto con organizador de cables.
 |
|  | **Bloqueadores de escritura** |
|  | * Bloqueador para
	+ USB 3.0
	+ IDE/SATA
	+ SAS
	+ USB 3
	+ FireWire
	+ Lector de tarjetas
* Adaptadores
* Interface para computadora
* Maletín rígido de transporte
* Fuente de alimentación
 |
|  | **Duplicador de discos duros** |
|  | * Soporte para discos:
	+ USB 3.0
	+ SATA
	+ IDE
	+ SAS
* Adaptadores de corriente para discos duros
* Fuente de alimentación
* Interface para computadora
 |
|  | **Dispositivos externos y enclosures** |
|  | * Case USB 3.0 con switch de lectura/escritura
* Lector de tarjetas de memoria con switch de lectura/escritura
 |
|  | **Características adicionales** |
|  | * Adaptadores:
	+ Disco duro 2.5” y disco duro de 1.8”
	+ Disco duro TDA3-1 micro SATA
	+ SATA LIF
	+ Blade tipo SSD
	+ FireWire 9 a 4 pines y de 9 a 6 pines
	+ Micro/mini SD a SD
* Disco duro SATA 2 TB
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de todo el kit deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física de los kits; la configuración y puesta a punto de cada uno de ellos, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por cada una de las instalaciones realizadas. |

Adicionalmente a lo señalado en estas bases, para estos kits se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | Los kits que se solicitan deberán contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, los componentes de los kits deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá otorgar una transferencia de conocimientos de los componentes de los kits para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en los componentes de los kits objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar los componentes de los kits para su reparación, el proveedor deberá proporcionar un componente de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al componente sustituto, toda la configuración de trabajo generada hasta ese momento. El componente reparado deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 5x8. |
|  | En caso de sustitución definitiva del componente o kit, el proveedor entregará uno nuevo de la misma marca, de características iguales o superiores al sustituido, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al componente o kit sustituto toda la configuración de trabajo generada hasta ese momento, componente o kit que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 5x8.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado el componente o kit a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | Los kits deberán ser distribuidos e instalados acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de los kits, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 2***Kits móviles de informática forense y servidores de análisis y borrado de discos duros* |
| **SUBPARTIDA 2.2** |
| *Servidor en formato torre para solución centralizada y análisis de evidencia de informática forense* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que el equipo considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
| **Sistema operativo** |
| Tipo Sistema  | 64 bits. |
| Versión | Windows 10 o superior. |
| Edición | Pro o Enterprise. |
| Idioma | Español |
| **Procesador** |
| Tipo de procesador | Intel Xeon E5-2640 v4 o superior. |
| Número de Núcleos | 10  |
| Cache | 25 MB o superior. |
| Velocidad del bus frontal | @ 2.4 GHz o superior. |
| **Memoria**  |
| Tipo de Ranura  | 8 DDR4-1600/1866/2133 EEC  |
| Memoria Solicitada/Máxima | 64 GB de memoria. |
| Ranuras ocupadas de Memoria | Las mínimas necesarias para una configuración de 64 GB. |
| Ranuras de expansión de Memoria | Las ranuras necesarias para expandir como mínimo a 128 GB. |
| **Almacenamiento**  |
| Almacenamiento disco para sistema. | 256 GB SSD o superior. |
| Almacenamiento disco Cache | 256 GB SSD o superior |
| Almacenamiento para datos | 2TB 7200rpm |
| Arreglo de discos RAID | 1 de 2TB como mínimo |
| Ranura de memoria | 2-in-1 SD(UHS50)/MMC |
| **Red** |
| Puertos de red de datos RJ45 | 1 de 1Gb mínimo. |
| **Entrada/salida** |
| Unidades ópticas | BD-R/BD-RE/DVD±RW/CD±RW quemador de Blu-ray Dual-Layer Combo Drive |
| Puertos USB | Puertos USB 3.0, mínimo. |
| **Video** |
| Controlador de video  | Controlador de video dedicada, 1 GB o superior. |
| **Hardware forense** |
| Bloqueador de escritura de disco duro |
| Adaptadores de discos duros:* IDE
* SATA
* SAS
* FireWire
* USB3.0/2.0
 |
| 2 bahías de disco duro extraíble IDE |
| 3 bahías hotswap IDE/SATA |
| **Accesorios** |
| Monitor con altavoces |
| Teclado y mouse |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto del equipo deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física, la configuración y puesta a punto del equipo, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica para la instalación realizada. |

Adicionalmente a lo señalado en estas bases, para este equipo se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | El equipo que se solicita deberá contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software. |
|  | Al reporte de la falla, el equipo deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación. |
|  | Se deberá otorgar una transferencia de conocimientos del equipo para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en el equipo objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar el equipo para su reparación, el proveedor deberá proporcionar un equipo de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al equipo sustituto, toda la configuración de trabajo generada hasta ese momento. El equipo reparado deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 5x8. |
|  | En caso de sustitución definitiva del equipo, el proveedor entregará uno nuevo de la misma marca, de características iguales o superiores al sustituido, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al equipo sustituto toda la configuración de trabajo generada hasta ese momento, equipo que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 5x8.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado el equipo a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | Será distribuido e instalado acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto del equipo, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 2***Kits móviles de informática forense y servidores de análisis y borrado de discos duros* |
| **SUBPARTIDA 2.3** |
| *Servidor en formato torre para borrado seguro de discos duros* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que el equipo considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | Bahías | 8 |
|  | Tamaño | 3.5” |
|  | **Red** |
|  | Puertos de red de datos RJ45 | 1Gb mínimo. |
|  | Cantidad | 2 |
|  | **Entrada/salida** |
|  | Puertos USB 3 | 9 Puertos tipo A |
|  | Puertos USB 2 | 4 puertos tipo A |
|  | Interfaz de usuario | Display touch. |
|  | **Fuente alimentación** |
|  | Interna a AC 120/230 V |
|  | **Accesorios** |
|  | Adaptadores:* IDE 2.5/3.5”
* IDE 1.8”
* 1.8“ IDE ZIF
* Extensión SAS/SATA
* mSATA
* MicroSATA
* eSATA
* Extensión SAS/SATA
* Kit de lectores y kit de adaptadores para memorias
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto del equipo deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física, la configuración y puesta a punto del equipo, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por cada una de las instalaciones realizadas. |

Adicionalmente a lo señalado en estas bases, para estos equipos se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | Los equipos que se solicitan deberán contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software. |
|  | Al reporte de la falla de los equipos, esta deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá otorgar una transferencia de conocimientos de los equipos para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en los equipos objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar los equipos para su reparación, el proveedor deberá proporcionar un equipo de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al equipo sustituto, toda la configuración de trabajo generada hasta ese momento. El equipo reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 5x8. |
|  | En caso de sustitución definitiva del equipo, el proveedor entregará uno nuevo de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al equipo sustituto toda la configuración de trabajo generada hasta ese momento, equipo que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 5x8.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado al equipo a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | Los equipos serán distribuidos e instalados acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de los equipos, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 3** |
| *Solución integral de protección horizontal contra amenazas de malware* |
| **CANTIDAD SOLICITADA: 2** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características** |
|  | **Descripción** | El Consejo de la Judicatura Federal requiere una solución de seguridad y monitoreo integral para tener visibilidad de tráfico interno malicioso y amenazas avanzadas que puedan poner en riesgo los activos información, bases de datos, usuarios finales, clientes móviles, que puedan ocasionar un daño a la confidencialidad, integridad de la información y disponibilidad de los servicios informáticos.Dicha solución debe de ser capaz de detectar malware de día cero, polimórfico y exploits dentro de la red, así como comunicación de tipo comando y control o tráfico TOR hacia el exterior de la misma. La arquitectura deberá estar basada en el concepto del despliegue de trampas, honeypots o sensores al interior de la red, que permitan identificar el movimiento lateral del malware y primeros signos de las amenazas avanzadas o comportamientos anómalos desde el interior de la red.La tecnología deberá incorporar el mecanismo de análisis de archivos binarios bajo un ambiente controlado a través de la ejecución virtual conocido como sandboxing, así como el análisis forense para entender la interacción del código malicioso, con el ambiente de la entidad.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Sitio*** | ***Cobertura de Red*** | ***Internet/Mbps*** | ***Usuarios*** |
| A | 50 VLANS | Si/500Mbps | 5000 |
| B | 50 VLANS | Si/500Mbps | 10000 |

 |
|  | **Requerimientos Generales** | 1. La solución debe estar basada en la red sin necesidad de emplear agentes.
2. La solución debe ejecutarse sobre hardware que soporte un throughput de al menos 1Gbps y debe ser capaz de escanear al menos 40 Vlans por localidad, cada una de ellas con máscara de red de 23 bits.
3. La solución debe estar basada en un sistema operativo endurecido y cerrado.
4. La solución debe de emplear trampas, honeypots o sensores de red que deberán ser desplegados estratégicamente al interior de la red para la identificación de amenazas que se propagan lateralmente al interior de la entidad.
5. La solución podrá permitir desplegar al menos 100 trampas, emulaciones o sensores por localidad donde se encuentre un Appliance/hardware instalado.
6. La solución debe tener la capacidad de monitorear la comunicación entre VLANS y el tráfico de salida a internet en las localidades donde se requiera.
7. La solución no debe requerir licencias de sistemas operativos para las emulaciones, trampas, honeypots o sensores desplegados mediante tecnología de engaño o Deception Grid.
8. La solución debe mezclar las trampas, sensores o emulaciones falsas con los activos del entorno productivo de la entidad creando un entorno de detección basado en el engaño.
9. La solución debe contar con una gestión centralizada.
10. La solución debe de incorporar la capacidad identificar visualmente el movimiento lateral de las amenazas generados desde la propagación del malware, actividad humana o cualquier actividad maliciosa detectada desde los sensores o trampas y desde ahí brincar al detalle de la alerta.
11. La solución deberá permitir emplear mecanismos de autenticación mediante una base de datos local o el directorio activo de Microsoft en caso de ser requerido.
12. La solución debe ser capaz de realizar un autodescubrimiento de la red para facilitar el despliegue de sensores o trampas al interior de la red, de igual forma, detectar cambios en el número de recursos informáticos.
13. La solución debe tener la capacidad de integrarse con un sistema SIEM, mediante SYSLOG u ODBC.
14. La plataforma debe de incorporar un flujo de trabajo integrado que permita el rastreo de los incidentes para su análisis y resolución.
15. La solución debe permitir generar reportes estadísticos relacionados con malware, eventos de actividad de comando y control, conexión a las trampas, top de direcciones IP destino y fuente con actividad maliciosa, ataques de alto riesgo al menos.
 |
|  | **Inteligencia y Detección de Amenazas** | 1. La solución debe de ser capaz de monitorear el tráfico generado del interior de la red hacia internet, para poder identificar comportamiento basado en botnets, comando y control, así como responder rápidamente ante la identificación de equipos comprometidos.
2. La solución deberá detectar el movimiento lateral en tiempo real, en cualquiera de las VLANs antes referidas de la entidad.
3. La solución debe utilizar al menos los siguientes mecanismos para la detección de malware o ataques, tales como sandboxing, análisis estático, base de Inteligencia contra amenazas o análisis por reputación e Integración con VirusTotal.
4. La solución debe de ser capaz de capturar el código malicioso para su análisis, a pesar de no ser una amenaza conocida previamente.
5. La solución deberá incorporar la capacidad de obtener un reporte del análisis dinámico en caso de ser requerido para las piezas binarias identificadas durante el esparcimiento lateral.
6. La solución debe generar notificaciones inmediatamente después de la detección de posibles amenazas internas o de malware.
7. La solución debe de minimizar los falsos positivos en la generación de alertas.
8. Es deseable que la solución sea alimentada desde múltiples fuentes de inteligencia contra amenazas que proporcionan información y diagnóstico respecto a amenazas previamente detectadas o de la actividad comando y control.
9. La solución debe de ser capaz de identificar no solo ataques o comportamientos basados en malware, sino cualquier actividad de interacción humana o automatizado que haga contacto con los sensores o trampas desplegados.
10. La solución debe incluir la siguiente información relacionada con el ataque:
* IP del atacante y el objetivo.
* Payload.
* Análisis preliminar.
* Captura de tráfico de la sesión en la red (*PCAP*).
* Servicios utilizados durante los ataques o interacción con la trampa.
* Descripción del proceso de mitigación/reparación (Recomendaciones si aplica).
1. La solución debe soportar la administración de VLANs o ser compatible con 802.1Q.
2. La solución debe permitir la extracción del malware original para realizar un análisis forense externo o una retención legal.
3. La plataforma debe permitir identificar y filtrar los eventos generados desde las trampas o sensores por la naturaleza de su actividad:
* Conexión
* Reconocimiento
* Interacción
* Infección
1. La arquitectura deberá incluir análisis forense manual o automatizado que permita obtener mayor detalle de un activo comprometido como memoria infectada, procesos, interacciones de red, etc con el objetivo de responder a un incidente o brecha mayor.
2. Las trampas deben poder simular o emular diferentes sistemas operativos tales como Windows, Linux, MAC y switches de red al menos que sean similares al ambiente de la entidad.
3. La solución debe emular al menos los siguientes servicios para ambientes Windows: Directorio Activo, DNS, DHCP, SMB, FTP, SQL.
4. La solución deberá permitir visualizar el nivel de riesgo y la cantidad de malware detectado basado en su severidad dentro de la entidad.
5. La solución debe permitir emular datos falsos en las trampas Windows para engañar al atacante
6. La solución deberá permitir desplegar artefactos, señuelos o scripts falsos sobre activos reales de IT (usuarios o servidores) que permitan engañar y desviar la atención de los atacantes hacia trampas del ambiente, tales como servicios ODBC o RDP, recursos compartidos ficticios, credenciales en memoria, entradas en los archivos hosts.
7. La arquitectura deberá incluir la capacidad de detección y contención de amenazas del tipo ransomware sobre el usuario final mediante el despliegue de artefactos o señuelos y que permita desconectar automáticamente a cualquier usuario comprometido.
 |
|  | **Monitoreo** | 1. La solución debe de permitir usar un servidor de NTP para sincronización de toda la arquitectura.
2. La solución debe de permitir contar con una vista que permite monitorear todo el ambiente en términos de amenazas internas como salientes.
3. La solución debe de contar con un tablero/vista o reporte que liste los malwares y direcciones IP que propagan el malware al interior de la red de la entidad.
4. La solución debe incluir un tablero/vista o reporte que liste las direcciones IPs involucradas en comunicación C2 o tráfico TOR.
5. La solución debe de incluir un tablero/vista o reporte que liste las IPs destino involucradas en tráfico C2 o TOR.
6. La solución debe de permitir excluir eventos no deseados tales como IP involucrada en la conexión o puerto.
7. La consola de gestión deberá de ser capaz de mostrar su los payloads obtenidos desde las trampas y enviados al sandbox para su análisis, fallaron en su envío, están siendo procesados o si el reporte PDF forense está listo.
 |
|  | **Reportes** | * La consola de gestion deberá incluir al menos la generación de los siguientes reportes para la entidad:
	+ Eventos relacionados con el tráfico saliente como detección de bots al interior.
	+ Resumen de detecciones de malware al interior.
	+ Top de Direcciones IP destino
	+ Top de direcciones IP fuente maliciosas
	+ Resumen de ataques semanales o diarios.
* La consola deberá permitir granularme a la plataforma de correlación al menos los siguientes eventos:
	+ Detecciones TOR en el tráfico saliente
	+ Detecciones C2 y troyanos en el tráfico saliente
	+ Detecciones de infecciones al interior de la red
	+ Detecciones de interacciones sobre la estructura de las trampas o sensores al interior de la red de la entidad.
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de toda la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física de las soluciones; la configuración y puesta a punto de cada una de ellas, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por cada una de las instalaciones realizadas. |

Adicionalmente a lo señalado en estas bases, para estos equipos y/o soluciones se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | Las soluciones que se solicitan deberán contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La(s) solución(es) será(n) distribuida(s) e instalada(s) acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de las soluciones, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 4** |
| *Solución de administración de eventos y seguridad de la información (SIEM).* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características**  |
| 1. | **Correlacionador de eventos** | El servicio debe proveer en términos generales las siguientes capacidades integradas en una misma interface de administración personalizable y basada en web: Monitoreo de Seguridad, Investigación basada en metadatos de eventos de seguridad y captura de tráfico, Reconstrucción de sesiones en el caso de que se requiera un análisis en profundidad forense, Reportes para Cumplimiento normativo.1. La solución de Inteligencia de Seguridad (Security Intelligence) con la que se aprovisione el servicio deberá contar con las siguientes capas en cuestión de arquitectura y diseño:
	1. -Colección
	2. -Administración de Logs (Log Management)
	3. -Administración de Eventos (Event Management)
	4. -Correlación de eventos
	5. -Alarmas
	6. -Manejo de Incidentes y casos
	7. -Manejo de flujos de trabajo con posibilidad de automatización
	8. -Reporteo
	9. -Monitoreo de punto final (Endpoint Monitoring)
	10. -Análisis forense de la red (Network Forensics)
2. Todos los componentes de la solución con la que se aprovisione el servicio, deben tener interoperabilidad, la solución en ningún momento deberá acceder a soluciones de externas para brindar algunas de las funcionalidades aquí expresadas.
3. Deberán de omitirse bases de datos que escriban los datos en claro a archivos planos, ya que se espera que se proporcione, firmado y compresión.
4. Deberá permitir acceder a los logs originales (raw log data), siempre que así se desee, además de contar con la información previamente interpretada por la solución de Inteligencia de Seguridad / Security Intelligence (Eventos, Alarmas e Incidentes).
5. Deberá contar con la posibilidad de que la consola administrativa sea accesible por Internet Explorer/Chrome/Firefox/Safari vía web (HTTPS).
6. El sistema deberá contar con la posibilidad de distribuirse geográficamente en distintas locaciones conteniendo integridad en la información que está siendo analizada.
7. Deberá mantener cifrado en los componentes de autenticación y en las capas de transporte de datos, este cifrado podrá ser desactivado en algunos componentes para proveer funcionalidades de agilización de transferencias de datos.
8. Deberá permitir un modelo de (delivery) entrega basado en: Appliance

1. Deberá estar basado en una plataforma endurecida (Hardened) de sistema operativo (preferiblemente Windows) dicho sistema operativo debe estar en cumplimiento con Common Criteria EAL2 (Methodically designed, tested and checked), en caso de tratarse de soluciones basadas en Linux, deberá validarse el cumplimiento y soporte de los mismos.
2. Se deberán poder aplicar parches al sistema operativo de manera discrecional conforme recomendaciones del fabricante del sistema operativo sin impactar el rendimiento y presentación de la aplicación, el fabricante de la solución de Inteligencia de Seguridad / Security Intelligence no deberá de ninguna manera regular el acceso a los parches de sistema operativo y componentes específicos alternos a la solución ofertada.
3. La colección de logs de las plataformas deberá realizarse en forma “agentless” sin agentes, con agentes o de manera hibrida en un deployment específico.
4. Los agentes deberán estar certificados por el fabricante además de disponibles para plataformas:
	* + Windows Server 2003 (32 Y 64 Bits)
		+ Windows Server 2008 (32 Y 64 Bits)
		+ Windows Server 2008 R2 (64 Bits)
		+ Windows Server 2012
		+ Windows Server 2012 R2
		+ Windows Server 2016
		+ Windows Vista (32 y 64 Bits)
		+ Windows XP (32 Bits)
		+ Windows 7 (64 Bits)
		+ Windows 8
		+ Windows 10
		+ Linux RedHat Enterprise
		+ Solaris
		+ HP-UX
		+ AIX

 1. De manera adicional deberá soportar colección de plataformas ampliamente utilizadas de manera nativa como son:
	1. -Windows Events Remote Collection
	2. -Netflow v1,v5,v9, IPFIX
	3. -Cisco IDS (via SDEE)
	4. -Checkpoint LEA
	5. –Fortinet
	6. -Sourcefire eStreamer
	7. -Nessus API
	8. -Nexpose API
	9. -AS400 (iSeries), z/OS (zSeries), GuardianOS (Tandem), etc
2. La solución de Inteligencia de Seguridad (Security Intelligence), deberá contar con la posibilidad de poder manejar una capa de información viva (live data) para búsquedas avanzadas y detalladas y una capa de información en reposo (cold data) siempre permitiendo utilizar datos viejos archivados fuera de la infraestructura en reportes e investigaciones forenses inclusive hasta 10 años.
3. La solución de Inteligencia de Seguridad (Security Intelligence), deberá acoplarse a utilizar las soluciones de STORAGE que la institución ya ha adquirido NAS/SAN, sin necesidad de sustituirlas por las soluciones propietarias
4. No se deberá presentar ningún tipo de costo extra a la adquisición de STORAGE propietario ni mucho menos representar este costo en la cotización para la utilización del STORAGE ya adquirido por la institución.
5. Los logs archivados deberán tener la funcionalidad de almacenarse y deberán tener la tipificación básica de evidencia legal bajo el concepto (digital chain of custody) todo ello por medio de la no alteración y la custodia de los logs originales.
6. La solución deberá realizar funciones normalización y mediación en su capa de administración de logs (log management) no en su capa de colección para aminorar el impacto a los equipos que realizan las funciones de colección.
7. Se deberán poder separar archivados por entidad e infraestructura con fines de poder gestionar backups de esos archivados de manera separada sin impactar los backups generales de la plataforma, lo anterior tiene el fin de que la solución muestre un arreglo de multi tenencia (Multi-Tenant) donde las bitácoras archivadas se puedan separar de manera general por cliente, edificio o grupo, dependiendo la configuración que el cliente plantee, sin tener que trabajar con la plataforma completa.

 1. Cuando la cantidad de logs recibida sobrepase la capacidad licenciada de logs la solución NO deberá “tirar/borrar” los logs sino encolarlos para su procesamiento futuro cuando su carga baje.
2. Deberá contar con un framework o método sencillo para poder integrar nuevos dispositivos no detectados conforme necesidades futuras de la institución en cuestión de normalización de bitácoras.

 1. El sistema de administración de logs deberá contar con la posibilidad de configurar que es un evento y que no, de todos los logs que se reciben, con fines de maximizar las capacidades de análisis de información importante e información intrascendente.
2. El sistema de administración de logs deberá proporcionar la posibilidad de rotar con funcionalidades de alta disponibilidad y saturación a los agentes entre el pool de manejadores de logs de manera automatizada para que, si los agentes pierden conectividad con el manejador de logs A, el manejador de logs B los reciba sin problema alguno y más tarde sincronicen sus colecciones, cuando el manejador de logs A regrese.
3. El sistema de administración de logs deberá contar con la posibilidad de traducir de manera automatizada y en tiempo real PAISES, ESTADOSy CIUDADESen vez de mostrar solo direcciones IP para los eventos que sean reenviados al sistema de administración de eventos.
4. El producto de Inteligencia de Seguridad (Security Intelligence) deberá poder brindar auto-clasificación de los datos capturados en modo estructurado con fines de brindar funcionalidades de búsquedas estructuradas (structured search), pero también brindar funcionalidades de búsqueda no estructurada, esto quiere decir que el sistema de inteligencia podrá ser consultado en función de estructuras específicas de datos conocidas pero también deberá permitir consultar datos sin conocer su estructura (unstructured search), lo anterior deberá estar presente en un producto único sin necesidad de duplicar la información.
5. El sistema deberá proporcionar funcionalidades de datamasking en caso de que se desee que la información no sea visualizada por personal que no tenga acceso a ella.
6. El sistema de administración de eventos deberá contar con la posibilidad de brindar una consola general para la consulta de la información en tiempo real, para realizar investigaciones forenses al pasado y mostrar una visión de tendencias hacia el futuro sobre los distintos eventos que se presenten en la plataforma.

 1. Deberá permitir diseñar modelos de cálculo de riesgo basado en formulas especificas dictaminadas por la organización donde se pueda ir tabulando por medio de sumatorias, repeticiones o indicadores específicos el verdadero impacto para que el CSOC pueda tomar decisiones acordes con la tipificación especifica de la amenaza en cuestión.
2. La consola de administración en conjunto con el sistema de administración de eventos deberá permitir la visión y búsqueda de más de 60 campos de metadatos normalizados para auto filtrado automatizado en donde puedan seleccionarse condicionales específicas.
3. La consola de administración de la solución de administración de eventos y logs deberá permitir generar Layouts o dashboards específicos por persona e infraestructura que es la que analiza los datos, esto quiere decir que la vista general de la solución debe permitir configuraciones especificas por analista y perfil de búsqueda sin necesidad de re-configurar todo cada vez que se autentica a la misma.
4. La consola de administración debe contar con la posibilidad de mostrar información realmente en tiempo real y no en procesamiento batch, esto quiere decir que la información que está cambiando en un aplicativo, sistema operativo o firewall debe ser virtualmente posible verla inmediatamente reflejada en la consola de administración sin esperar tiempos considerables a realizar esta tarea.
5. La consola de administración deberá permitir ordenar “sortear” la información conforme necesidades específicas en tiempo real sin necesidad de la gestión de consultas o queries complicados.

 1. La consola de administración deberá contar con la posibilidad de agrupar eventos parecidos con fines de verlos de una manera más sencilla y no repetirlos, además de contar con la posibilidad de generar gráficos específicos de tiempo inicial y tiempo final en la que ocurrieron los eventos.

La consola de administración deberá contar con vistas en tiempo real como: * 1. -Estadísticas de eventos comunes
	2. -Estadísticas de eventos con IP originaria
	3. -Estadísticas de eventos con Host originario
	4. -Estadísticas de eventos con IP victima (impactada)
	5. -Estadísticas de eventos con Host victima (impactado)
	6. -Estadísticas de aplicaciones impactadas
	7. -Estadísticas de fuente de logs específicos
	8. -Logs por semana, día y hora
	9. -Logs por tiempo y dirección
1. La consola de administración deberá contar con la posibilidad de utilizar listas de objetos, cosas, direcciones IP, países, ciudades, etc, estas listas deberán poder compartirse entre usuarios y automatizarse dentro de la solución.
2. Deberá promover una integración nativa con información de inteligencia de amenazas (ThreatIntel) de fuentes OpenSource con un formato específico incluyendo STIX/TAXII.
3. Las funcionalidades de correlación y normalización de datos, deberá realizarse en tiempo real de manera comprobable, evidenciando el modelo completo de normalización y tratamiento de los datos, creación de reglas y normalización de tiempo, permitiendo correlacionar datos “fuera de tiempo” incluso.
4. El sistema deberá contar con una funcionalidad de actualización (automática o manual, dependiendo sea la necesidad) de inteligencia de parte del fabricante que por lo menos con una regularidad de 1 día actualice formatos nuevos detectados de bitácoras, eventos nuevos y riesgosos, nuevas políticas de alertamiento, modificaciones en estándares.
5. La consola de administración deberá soportar queries básicos para la gestión de investigaciones sin necesidad de aprender un lenguaje de programación (SQL Like) o expresiones regulares con fines de hacer sencilla la explotación de datos.
6. La consola de administración deberá proveer la funcionalidad de agrupar de manera completa dispositivos, hosts, redes y activos específicos para poder asignar locaciones, dirección de conectividad (inside, outside, local, etc) así como el nivel de riesgo de cada activo el cual estará ligado a la cantidad de eventos e importancia que cada uno de ellos refiera de manera aislada.
7. El sistema de administración de eventos deberá contar con la posibilidad de correlacionar de manera básica eventos por contenido de login, IP, histórico en tiempo.
8. El sistema de correlación de eventos avanzado deberá ser manejado de manera completa por medio de wizards gráficos (drag and drop) sin la necesidad de conocer lenguajes de programación para la gestión de políticas nuevas.
9. El sistema de correlación de eventos avanzado deberá nutrirse no solo de información de eventos (limited subset) sino de flujos de datos (netflow, jflow, sflow, ipfix, etc.), logs nativos, etc. para proveer la máxima capacidad de abstracción posible para la detección de amenazas complejas y advanced persistent threats.
10. El sistema de correlación de eventos avanzado deberá permitir activar y desactivar las políticas durante un tiempo específico con fines de monitorear la utilización de CPU donde se están realizando estas comprobaciones a su vez la utilización de memoria RAM que es gastado en cada función de correlación avanzada.
11. El sistema de correlación de eventos deberá contar con la posibilidad de agrupar las políticas que se ejecutan en tiempo real y ordenarlas para evitar errores de obtención de información una vez que se cumplen X o Y factores.
12. El sistema deberá integrarse de manera nativa con Microsoft Active Directory, con fines de extracción de la base total de usuarios y grupos para realizar correlación multidimensional y jerárquica.
13. El sistema deberá permitir como mínimo a 3 administradores y analistas, acceder a información independiente de manera centralizada y recurrente (al mismo tiempo).
14. El sistema deberá contar con una base de datos local de autenticaciones para manejar usuarios en caso de no desear alinearlo a la infraestructura de Microsoft Active Directory de la institución.
15. El sistema deberá permitir desactivar de manera temporal cuentas sin necesidad de borrar toda la información de autenticación a la plataforma una vez que un empleado se le deniegue el acceso a dicha plataforma.
16. El sistema deberá permitir manejar grupos y roles por grupo para poder manipular con mayor sencillez a los usuarios.
17. El sistema deberá contar con la posibilidad de limitar el nivel de acceso conforme la credencial autenticada y esto concordar con el perfil asignado a cada empleado sobre el tipo de información a la cual se tiene acceso (fuentes de logs, configuraciones, etc).
18. El sistema de administración de eventos deberá permitir configurar que datos deben ser compresos y cuáles no; es decir, el detalle de la base de datos de eventos y el valor de compresión de los índices.
19. El sistema de administración de eventos deberá manejar índices pre-calculados para agilizar las investigaciones.
20. La consola de administración deberá permitir contenidos de visualización tales como mapas de calor (heatmaps), mapas de conectividad (connection maps/contextualization maps), indicadores de compromiso (IOC) y configuraciones completas por el cliente para visualizar cualquier tipo de dato que se encuentre procesado por la solución.
21. La plataforma deberá contar con la posibilidad de brindar API´s para construir interfaces de propósito específico con visualizaciones especificas en tableros de ciberinteligencia (construidos por medio de webservices) con el fin de brindar visibilidad de modo general y particular a gusto del cliente, sin tener que acceder a la solución de correlación de manera separada (SINGLE PANE OF GLASS).
22. El sistema de manejo de alarmas deberá proveer las funcionalidades de alertar en función de observar consideraciones, patrones y condicionales específicas en cualquiera de las capas atrás mencionadas:

 * 1. -Colección
	2. -Administración de Logs (Log Management)
	3. -Administración de Eventos (Event Management)
	4. -Correlación de Eventos
1. Las alarmas deberán de manejarse como datos aislados de incidente promoviendo las funcionalidades de dar seguimiento oportuno por medio de alertas vía correo electrónico, SMS, ejecución de programas específicos o escritura a archivos planos para procesamiento futuro con otras herramientas.
2. El sistema de alarmas deberá integrarse de manera sencilla con Remedy, OTRS u otras herramientas, por medio de correo electrónico, archivo plano o SNMP, con un layout específico declarado para que oportunamente se pueda dar seguimiento a los casos detectados.
3. El sistema de alarmas deberá contar con un sub-sistema de remediación (automático o manual) que cuente hasta con 3 aprobaciones para realizar actividades propias de remediación.
4. El sistema de alarmas deberá proveer funcionalidades para realizar alarmas públicas o privadas y que puedan segregarse en el panel del dashboard principal a placer (layouts)
5. El sistema de alarmas y manejo de incidentes deberá permitir asignar el estatus a una alarma dentro de la misma herramienta con fines de que se mantenga comunicación interna entre el personal que ocupa la herramienta para saber si una alarma ha sido escalada, se está trabajando en ella o se trataba de un falso positivo, ha sido resuelta, se continuara monitoreando o no ha sido ni será resuelta además de permitir al usuario asignar comentarios a cada momento.

1. El sistema de alarmas y manejo de incidentes permitirá conocer cuál es el histórico (quien la toco, quien la abrió, quien la cerró, quien respondió a ella, cuándo) de una alarma con fines de su futura explotación y auditoria.
2. El sistema de alarmas contará con un compendio especifico y un set de condiciones para declarar cosas que salen de cumplimiento, por ejemplo, se deberá contar con alarmas preestablecidas de rompimiento de estándares generales como PCI-DSS, ISO 27001, SOX.
3. La solución de Inteligencia de Seguridad (Security Intelligence), deberá proporcionar un proceso completo desde la captura de las bitácoras, indicadores y demás datos de maquina (machine data) hasta la gestión y documentación del incidente visualizado, donde deberá proporcionar un visor de incidentes en el cual los analistas podrán colaborar asignando evidencias y poniendo sus experiencias sobre un incidente visualizado.
4. La herramienta de manejo de casos (Case Management) deberá poder interactuar por medio de API´s con herramientas de manejo de tickets del SOC con fines de poder realizar interacción bidireccional de las evidencias (logs, screenshots, imágenes forenses de disco, capturas de paquetes).
5. La herramienta de manejo de casos (Case Management) deberá promover un escenario jerárquico de dictaminación de incidentes en el cual se pueda asignar riesgo, colaboradores, analistas y staff que no debe de visualizar un dato específico. Lógicamente la herramienta de manejo de casos debe interactuar con el sistema de remediación para, por medio de flujos, poder responder a un incidente.
6. La solución SIEM deberá contar con la posibilidad de generar reportes avanzados de los siguientes estándares con la adecuación completa a requerimientos de auditoria en caso de existir:
	1. -FISMA
	2. -GLBA
	3. -HIPAA
	4. -ISO 27001
	5. -ISO 27001:2005
	6. -NERC / NERC-CIP
	7. -NRC
	8. -PCI-DSS
	9. -SOX

 1. La solución SIEM deberá contar con reportes de estándares y plantillas modificables por el usuario de categorías como las siguientes:
	1. -Top atacantes
	2. -Vulnerabilidades
	3. -Amenazas
	4. -Alarmas detonadas
	5. -Violaciones de cumplimiento
	6. -Fallos operativos
	7. -Violaciones de auditoria
	8. -Reportes ejecutivos
	9. -Detalles de logs (volumen, detalle, capacidad)
	10. -Estadísticas de los componentes de la solución (Log Management, Event Management)
	11. -Resúmenes y templates específicos
2. La solución de Inteligencia de Seguridad (Security Intelligence), deberá mostrar los reportes en pantalla antes de solicitar cualquier exportación a formatos externos.
3. La solución de Inteligencia de Seguridad (Security Intelligence), deberá guardar un registro completo de que reportes que se producen y almacenar un cache para acceso más tarde sin necesidad de ejecutar nuevamente el reporte lo cual reduce el tiempo de entrega de los mismos.
4. De esos reportes ya previamente producidos es importante que se puedan realizar filtrados sin necesidad de re-ejecutar la consulta que produjo el reporte.
5. La solución de Inteligencia de Seguridad (Security Intelligence), al producir estos reportes debe contar con una funcionalidad de exportación a formatos:
	1. -Excel con datos y detalle
	2. -CSV
	3. -PDF
	4. -XML/HTML
6. Los reportes deben de contar con un análisis discrecional de privilegios dentro de la organización para solo permitir que las personas que puedan verlo sean las únicas que tienen acceso a ellos.
 |
|  | **Monitoreo Forense a Infraestructura de Red** | 1. La solución de monitoreo de red deberá contar con la posibilidad de realizar identificación de aplicaciones (no solo puerto ip) sino tener embebido un engine DPI (Deep Packet Inspection) que deberá tener la capacidad de identificar más de 3100 aplicaciones, el mismo deberá ser actualizable en demanda para soportar más aplicaciones y poder diseñar reglas específicas para interpretación de tramas de red.
2. Deberá proporcionar la posibilidad de inspeccionar hasta 5 gbps de tráfico en puertos de cobre y puertos de fibra.
3. Deberá proporcionar la posibilidad de integrar un de-criptor de sesiones SSL en el futuro cuando la institución así lo defina, además de evidenciar en una lista los fabricantes con los que puede trabajar para realizar esta parte, en caso de que el fabricante cuente con esta funcionalidad incluida deberá especificarlo en su oferta de solución de manera separada.
4. El modulo deberá tener un API con el cual se podrá interactuar con aplicaciones de terceros y con la misma solución de Inteligencia de Seguridad / Security Intelligence, para poder generar automatización de funcionalidades de correlación avanzada.
5. Deberá permitir su acceso a configuración mediante HTTPS asi como SSH (CLI).
6. Deberá permitir desde su interfaz web el poder realizar búsquedas no estructuradas y estructuradas con gran facilidad para poder alcanzar tramas específicas.
7. Deberá contar con la capacidad de mostrar metadatos específicos de aplicaciones detectadas, los mismos podrán ser explotados por funciones de correlación en dispositivos conectados externamente o por medio del SIEM.
8. Deberá permitir la capacidad de realizar la captura de paquetes a nivel sesión (reconstruir la sesión en caso de ser posible), desde la capa 2 hasta la capa 7.
9. Deberá permitir exportar estas capturas de paquetes en archivos PCAP que después podrán ser analizados por herramientas que soporten los archivos mencionados, tales como Wireshark, dichas capturas de paquetes deberán contener la sesión completa capturada.
10. El concepto de captura de paquetes selectivos deberá estar integrada con la plataforma de Security Intelligence, en función de que la plataforma detecte un indicador de compromiso especifico con un riesgo especifico, sea posible de manera integrada el obtener la captura de paquetes de esa transacción o grupo de transacciones, sin suponer realizar una búsqueda en uno y otro producto buscando una consola o producto unificado.
11. El módulo de captura de comunicaciones en red deberá contar con la posibilidad de presentarse en un appliance dedicado y deberá ser completamente pasivo (promisc mode), el mismo se conectará a un puerto SPAN del switch core, no debera trabajar en bridge, para no suponer un riesgo severo a la disponibilidad de la infraestructura en caso de tener una falla.
12. Deberá permitir reconstruir archivos transmitidos por protocolos específicos como SMTP (reconstruir un archivo que se compartió por un correo electrónico y que contenía información confidencial o malware, lógicamente sin que el analista cuente con control del servidor de correo electrónico, el buzón del destinatario o del emisor, todo ello reconstruyendo la trama de datos que ha sido capturada por la solución de Analíticos de Red / Network Analytics), entre otros.
13. Deberá contar con la posibilidad de interactuar con los flujos de captura de paquetes para poder utilizarse a modo de IDS con sets predefinidos de captura y comparación para detectar patrones analíticos en la red que serían de otra manera imposibles de analizar.
14. Deberá proporcionar en conjunto con la solución de Inteligencia de Seguridad / Security Intelligence paquetes de Análisis de amenazas de red (Network Analytics), Detección de Anomalías basadas en comportamiento por sus siglas NBAD en inglés (Network Behavioral Anomaly Detection).
15. Deberá permitir almacenar por lo menos 1 mes de tráfico en *realtime* (captura completa de los paquetes incluyendo “original data” y “metadata” seleccionada y hasta 6 meses en *archives* compresos de metadatos específicos.
16. Deberá contar con la posibilidad de replicar pcaps (capturas de paquetes) capturados en otras plataformas en formato pcap standard para poder analizarlos más tarde.
17. Deberá contar con dashboards predefinidos que permita diagramar la actividad aplicativa, de sesiones y capturas dependiendo el requerimiento específico que se quiera, dichos dashboards deberán estar alineados completamente con la posibilidad de búsquedas no estructuradas o bajo una estructura de metadatos definida.
18. Deberá proporcionar inteligencia “out of the box” detectando por medio de las suites de analíticos propias de la plataforma indicadores complejos que exploten vulnerabilidades en la plataforma operativa de la institución.
19. La solución deberá estar basada en un sistema operativo con base Linux.
20. El appliance deberá proporcionar arreglos redundantes para la información capturada (RAID 0, RAID 5 o similar).
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de toda la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física, la configuración y puesta a punto de la solución, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por la instalación realizada. |

Adicionalmente a lo señalado en estas bases, para esta solución se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | La solución que se solicita deberá contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La(s) solución(es) será(n) distribuida(s) e instalada(s) acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 5***Solución integral de protección contra amenazas avanzadas para el vector web, puntos finales y correo electrónico* |
| **SUBPARTIDA 5.1** |
| *Solución integral de protección contra amenazas avanzadas para el vector web.* |
| **CANTIDAD SOLICITADA: 2** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características** |
|  | **Descripción** | El Consejo de la Judicatura Federal requiere una solución de seguridad y monitoreo integral para tener visibilidad de tráfico interno malicioso y amenazas avanzadas persistentes dirigidas, que puedan poner en riesgo los activos información, bases de datos, usuarios finales, clientes móviles, que puedan ocasionar un daño a la confidencialidad, integridad de la información y disponibilidad de los servicios informáticos.El Consejo de la Judicatura Federal solicita una tecnología específicamente dedicada para la detección y prevención de amenazas avanzadas, mismas que permitan detectar, contener, bloquear y proveer información respecto a los eventos detectados. Para ello se han considerado diversas necesidades tanto técnicas como consultivas que permitan dirigir una estrategia y una mejora continua ante las constantes amenazas persistentes avanzadas (APT) y dirigidas.Es de suma importancia que el fabricante de la solución tecnológica a elegir, cuente con las siguientes capacidades:* Tecnología de punta para detección proactiva, no basada en firmas, diseñada específicamente contra los ataques tipo APT, con inteligencia detrás que permita retroalimentación a nivel mundial a partir de las detecciones y análisis consultivos.
* Estar dedicado a la detección y prevención de amenazas avanzadas.
 |
|  | **Requerimientos Generales** | La solución requerida tendrá por objetivo el detectar y prevenir de amenazas avanzadas que sean identificadas como entrantes a la red del Consejo de la Judicatura Federal vía la navegación Web, así como detectar y bloquear la extracción de información y/o comunicación al exterior que pudiera presentarse en equipos que cuenten con amenazas, sean conocidas o desconocidas.* La solución deberá detectar y proteger contra amenazas avanzadas con un equipo de propósito específico (appliance), todas las funcionalidades descritas en esta sección deberán llevarse a cabo internamente en el mismo appliance, sin necesidad de soluciones, módulos, agentes y/o servidores externos.
* La solución a ofertar no debe ser parte o módulo de otras soluciones como IPS, Filtradores de Contenido (Proxies/Web Gateways) o Firewalls. Debido a la naturaleza de los ataques, el appliance debe estar solo dedicado a la detección y prevención de amenazas avanzadas.
* La solución debe estar basada en la red sin necesidad de emplear agentes.
* La solución debe ejecutarse sobre hardware que soporte un throughput de al menos 1Gbp
* Dicha solución debe de ser capaz de detectar malware de día cero, polimórfico y exploits dentro de la red, así como comunicación de tipo comando y control hacia el exterior de la misma
* La solución debe ser capaz de ejecutar todo el código sospechoso, URL’s y diversos tipos de archivos en un entorno virtual propietario de inspección dentro del mismo dispositivo. No se aceptan tecnologías que usen hipervisores comerciales.
* La solución debe proporcionar detección y protección en las comunicaciones desde y hacia Internet de vulnerabilidades día cero, polimórfico, botnets y Ataques Persistentes Avanzados (APT).
* El análisis debe detectar con un análisis de flujos múltiple el contexto total de un ataque cibernético: exploit, infección a partir de un código malicioso y comunicación a servidores de comando y control.
* La solución debe poder bloquear comunicaciones de salida a Internet hacia servidores de externos para control de los dispositivos comprometidos.
* La solución deberá poderse instalar en 2 modos diferentes de operación: modo en línea (capa 2) y fuera de banda (puerto espejo), con capacidad de bloqueo.
* La solución debe identificar amenazas usando tecnología local sin depender de enviar muestras a analizadores en la nube.
* La solución no deberá basar su análisis en firmas, así como también evitar apoyarse en otras tecnologías como Proxies o IPS para el envío específico de análisis de amenazas avanzadas.
* En el entorno virtual de análisis, el malware deberá ser inspeccionado y examinado en diversas máquinas virtuales correspondientes a varios sistemas operativos, aplicaciones, navegadores y complemento de navegadores. No se aceptan emuladores, solo máquinas virtuales completas.
* Las máquinas virtuales deberán estar instrumentadas de fábrica para el análisis de las amenazas avanzadas.
* La solución debe ser capaz de retroalimentarse automáticamente ante nuevas amenazas para de manera proactiva obtener nuevas posturas e inteligencia de las amenazas avanzadas, todo ello sin necesidad de interacción humana.
* La solución deberá ser instalable en un tiempo no mayor a una hora sin requerir configuraciones adicionales como políticas o afinación de reglas de algún tipo.
* La solución debe eliminar casi en su totalidad los falsos positivos para evitar al máximo realizar trabajos innecesarios.
* La solución deberá generar de manera dinámica inteligencia acerca de las amenazas para proteger localmente y conectarse a una red global para compartir información de amenazas detectadas deteniendo APT y ataques día-cero.
 |
|  | **Inteligencia y Detección de Amenazas** | * La solución debe de ser capaz de monitorear el tráfico generado del interior de la red hacia internet, para poder identificar comportamiento basado en botnets, comando y control, así como responder rápidamente ante la identificación de equipos comprometidos.
* La solución debe de ser capaz de capturar el código malicioso para su análisis, a pesar de no ser una amenaza conocida previamente.
* La solución debe generar notificaciones inmediatamente después de la detección de posibles amenazas internas o de código malicioso.
* La solución debe de minimizar los falsos positivos en la generación de alertas.
* Es deseable que la solución sea alimentada desde una nube de inteligencia global contra amenazas que proporcionan información y diagnóstico respecto a amenazas previamente detectadas.
* La solución debe incluir la siguiente información relacionada con el ataque:
	+ IP del atacante y el objetivo.
	+ Payload.
	+ Análisis preliminar.
	+ Captura de tráfico de la sesión en la red (*PCAP*).
	+ Servicios utilizados durante los ataques o interacción con la trampa.
* La solución debe permitir la extracción del código malicioso original para realizar un análisis forense externo o una retención legal.
* La solución deberá poder entregar un análisis forense que permita obtener mayor detalle de las amenazas detectada como memoria infectada, procesos, interacciones de red, etc.
 |
|  | **Monitoreo** | * La solución debe ser capaz de analizar archivos DLL y scripts JavaScript, así como archivos comprimidos ZIP, RAR, ZIP y archivos comunes para usuario como lo son documentos de Word, Excel, PDF, PowerPoint, Flash o HTML.
* La herramienta debe soportar reglas estáticas de análisis YARA.
* La solución debe utilizar técnicas de análisis de amenazas codificadas mediante técnicas tipo XOR.
* La solución debe soportar de manera nativa el encabezado XFF (X-Forwarded-For).
* La solución deberá poder entregar notificaciones mediante los siguientes protocolos: Syslog, SMTP, HTTP y SNMP.
* El equipo propuesto deberá enviar notificaciones a través de correo electrónico.
 |
|  | **Reportes** | * La solución deberá proporcionar información forense que pueda ser usada para proteger la red local. Como mínimo deberá contener la siguiente información
1. Fecha y hora del ataque.
2. URL de infección.
3. Hash MD5 o SHA-1 de los binarios maliciosos.
4. Tipo de archivo malicioso detectado.
5. Captura de tráfico en formato PCAP
6. Encabezados de la navegación
7. Capacidades nocivas de la amenaza: robo de información, comportamiento malicioso, cambios al sistema operativo.
8. La solución debe poder brindar el Malware en archivo comprimido. También si es parte de la amenaza, entregar el sitio de infección de la misma manera.
* La solución propuesta deberá proveer la siguiente información del host afectado como mínimo:
1. Número de incidencias.
2. Tipo de alerta detectada.
3. Severidad.
4. Dirección IP y/o nombre del servidor al cual se comunica (cuando aplique).
5. Puertos.
* La solución propuesta deberá contar con un módulo de Reporteo que emita reportes de al menos:
1. Reportes sobre las principales Alertas (actividad actual o históricos)
2. Reportes en un rango de fechas, Sensor/Site y rango de direcciones IP.
3. Reportes detallados de llamadas a casa, identificando cuando sea posible la geo localización de la IP..
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de toda la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física de las soluciones; la configuración y puesta a punto de cada uno de ellos, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por cada una de las instalaciones realizadas. |

Adicionalmente a lo señalado en estas bases, para estos equipos y/o soluciones se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | La solución que se solicitan deberá contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La(s) solución(es) será(n) distribuida(s) e instalada(s) acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 5***Solución integral de protección contra amenazas avanzadas para el vector web, puntos finales y correo electrónico* |
| **SUBPARTIDA 5.2** |
| *Solución integral de protección contra amenazas avanzadas para el vector correo electrónico.* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características** |
|  | **Descripción** | El Consejo de la Judicatura Federal requiere una solución de seguridad y monitoreo integral para tener visibilidad de tráfico malicioso y amenazas avanzadas persistentes dirigidas vía correo electrónico, que puedan poner en riesgo los activos información, bases de datos, usuarios finales, clientes móviles, que puedan ocasionar un daño a la confidencialidad, integridad de la información y disponibilidad de los servicios informáticos.El Consejo de la Judicatura Federal solicita una tecnología específicamente dedicada para la detección y prevención de amenazas avanzadas dirigidas vía correo electrónico, mismas que permitan detectar, contener, bloquear y proveer información respecto a los eventos detectados. Para ello se han considerado diversas necesidades tanto técnicas como consultivas que permitan dirigir una estrategia y una mejora continua ante las constantes amenazas persistentes avanzadas (APT) y dirigidas.Es de suma importancia que el fabricante de la solución tecnológica a elegir, cuente con las siguientes capacidades:* Tecnología de punta para detección proactiva, no basada en firmas, diseñada específicamente contra los ataques tipo APT, con inteligencia detrás que permita retroalimentación a nivel mundial a partir de las detecciones y análisis consultivos.
* Estar dedicado a la detección y prevención de amenazas avanzadas.
 |
|  | **Requerimientos Generales** | La solución requerida tendrá por objetivo el detectar y prevenir de amenazas avanzadas que sean identificadas como entrantes a la red del Consejo de la Judicatura Federal vía correo electronico, así como detectar y bloquear el ingreso de correos electronicos que cuenten con amenazas, sean conocidas o desconocidas.* La solución deberá detectar y proteger contra amenazas avanzadas con un equipo de propósito específico (appliance), todas las funcionalidades descritas en esta sección deberán llevarse a cabo internamente en el mismo appliance, sin necesidad de soluciones, módulos, agentes y/o servidores externos.
* La solución a ofertar no debe ser parte o módulo de otras soluciones como AntiSPAM, IPS, Filtradores de Contenido (Proxies/Web Gateways) o Firewalls. Debido a la naturaleza de los ataques, el appliance debe estar solo dedicado a la detección y prevención de amenazas avanzadas.
* La solución debe ejecutarse sobre hardware que soporte un rendimiento de 300,000 correos al dia y debera incluir licenciamiento para proteccion de 25,000 buzones de correo electronico.
* La solucion debe ser capaz de ejecutar todo el código sospechoso, URL’s y diversos tipos de archivos en un entorno virtual propietario de inspección dentro del mismo dispositivo. No se aceptan tecnologías que usen hipervisores comerciales.
* La solución debe identificar amenazas usando tecnología local sin depender de enviar muestras a analizadores en la nube.
* La solución no deberá basar su análisis en firmas, así como también evitar apoyarse en otras tecnologías para el envío específico de análisis de amenazas avanzadas.
* La solución debe ser capaz de retroalimentarse automáticamente ante nuevas amenazas para de manera proactiva obtener nuevas posturas e inteligencia de las amenazas avanzadas, todo ello sin necesidad de interacción humana.
* La solución deberá generar de manera dinámica inteligencia acerca de las amenazas para proteger localmente y conectarse a una red global para compartir información de amenazas detectadas deteniendo APT y ataques día-cero.
 |
|  | **Inteligencia y Detección de Amenazas** | * La herramienta de detección y protección para amenazas avanzadas en correo electrónico debe ser capaz de analizar archivos adjuntos incluidos en los correos electrónicos así como direcciones URL que se encuentren en el cuerpo del correo, todo dentro de un entorno virtual propietario de inspección dentro del mismo dispositivo.
* La solución a ofertar no debe ser parte o módulo de otras soluciones como Antivirus o AntiSPAM. Debido a la naturaleza de los ataques, el appliance debe estar solo dedicado a la detección y prevención de amenazas avanzadas.
* En el entorno virtual de análisis, las amenazas deberán ser inspeccionadas y examinado en diversas máquinas virtuales correspondientes a varios sistemas operativos, aplicaciones, navegadores y complemento de navegadores.
* Las máquinas virtuales deberán estar instrumentadas de fábrica para el análisis de las amenazas avanzadas. Sólo se permitirá configurar los tipos de archivos que se quieran analizar en los correos, para máxima efectividad.
* La solución debe permitir colocar en cuarentena aquellos correos que presenten alguna amenaza cuando el equipo se encuentre ubicado en modo en línea, para evitar que éstas entren en la organización.
* La solución debe permitir la opción de liberar un correo puesto en cuarentena por el administrador de la solución.
* La solución debe permitir también el envío de notificaciones para las detecciones de infecciones realizadas, así como un envío de la copia del correo identificado como malicioso hacia los correos que se definan para su análisis.
* Debe permitir operar el equipo en los modos en línea (modo MTA), o bien en modo monitoreo vía configuraciones SPAN/TAP o en modo de Copia de Correo cuando la plataforma de correo se encuentre fuera de la instalación física o bien sea un servicio arrendado a un tercero.
* La inspección a archivos adjuntos debe incluir tipos de archivo como son PDF, archivos de Office, vCards, contenido multimedia como son MP3 y video, por citar algunos.
* La solución deberá poder revisar correo cifrado mediante el protocolo TLS.
* La solución deberá poder entregar notificaciones mediante los siguientes protocolos: Syslog, SMTP, HTTP y SNMP.
* La solución deberá poder interactuar con la solución contra amenazas avanzadas basada en Web, mismo que permitan en conjunto identificar y contener ataques de tipo Spearphishing.
* La solución debe de ser capaz de capturar el código malicioso para su análisis, a pesar de no ser una amenaza conocida previamente.
* La solución debe generar notificaciones inmediatamente después de la detección de posibles amenazas de codigo malicioso.
* La solución debe de minimizar los falsos positivos en la generación de alertas.
* Es deseable que la solución sea alimentada desde una nube de inteligencia global contra amenazas que proporcionan información y diagnóstico respecto a amenazas previamente detectadas.
* La solución deberá ser capaz de interactuar con soluciones de amenazas avanzadas en red para realizar análisis de correos electrónicos con URLs incluidas
* La solución deberá ser capaz de intercambiar indicadores de compromiso de las amenazas detectadas a soluciones de protección de puntos finales.
 |
|  | **Consola de Gestion** | Con la finalidad de obtener una gestión unificada, el Consejo de la Judicatura Federal requiere de un repositorio central para gestionar las soluciones y las alertas generadas, por ello se solicita una consola. Esta contará con las siguientes características:* El equipo deberá fungir como consola de administración centralizada para los equipos dedicados al análisis y detección de amenazas avanzadas distribuidas en los entornos de ingreso a la red (Web/correo electronico).
* Debe permitir la administración y envío de actualizaciones a los equipos que gestiona.
* Debe tener la capacidad de almacenar todos los eventos generados en los equipos distribuidos en el entorno de red, así como la capacidad de generar reportes basados en la información almacenada.
* El equipo debe contar con la capacidad de integración con dispositivos de monitoreo y/o correlación de eventos (SIEM) mediante los estándares SNMP, SMTP HTTP y RSYSLOG, teniendo definidos parámetros de configuración para los más comunes, como LEEF y CEF.
* El sistema de gestión debe tener la capacidad de ser colocado en modo Alta Disponibilidad.
* El equipo debe existir en un equipo de propósito específico.
* La gestión de la consola de administración debe hacerse mediante uno o más protocolos seguros.
* La consola debe poder proveer la correlación entre los dispositivos Web y Mail para detección de ataques combinados (Spearphishing)
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de toda la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física, la configuración y puesta a punto de la solución, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por la instalación realizada. |

Adicionalmente a lo señalado en estas bases, para esta solución se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | La solución que se solicita deberá contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La solución será distribuida e instalada acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 5***Solución integral de protección contra amenazas avanzadas para el vector web, puntos finales y correo electrónico* |
| **SUBPARTIDA 5.3** |
| *Solución integral de protección contra amenazas avanzadas para puntos finales.* |
| **CANTIDAD SOLICITADA: 1** |
| Es indispensable que la solución considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Características** |
|  | **Descripción** | El Consejo de la Judicatura Federal requiere una solución de seguridad y monitoreo integral para tener visibilidad de tráfico malicioso y amenazas avanzadas persistentes dirigidas a equipos de cómputo o “puntos finales”, que puedan poner en riesgo los activos información, bases de datos, usuarios finales, clientes móviles, que puedan ocasionar un daño a la confidencialidad, integridad de la información y disponibilidad de los servicios informáticos.El Consejo de la Judicatura Federal solicita una tecnología específicamente dedicada para la detección y prevención de amenazas avanzadas dirigidas a puntos finales, mismas que permitan detectar, contener, bloquear y proveer información respecto a los eventos detectados. Para ello se han considerado diversas necesidades tanto técnicas como consultivas que permitan dirigir una estrategia y una mejora continua ante las constantes amenazas persistentes avanzadas (APT) y dirigidas.Es de suma importancia que el fabricante de la solución tecnológica a elegir, cuente con las siguientes capacidades:* Tecnología de punta para detección proactiva, no basada en firmas, diseñada específicamente contra los ataques tipo APT, con inteligencia detrás que permita retroalimentación a nivel mundial a partir de las detecciones y análisis consultivos.
* Estar dedicado a la detección y prevención de amenazas avanzadas.
 |
|  | **Requerimientos Generales** | La solución requerida tendrá por objetivo el detectar y prevenir de amenazas avanzadas que sean identificadas en equipos de computo o puntos finales en la red del Consejo de la Judicatura Federal.* La solución deberá detectar y proteger contra amenazas avanzadas con un equipo de propósito específico (appliance) y agentes instalados en los puntos finales, todas las funcionalidades descritas en esta sección deberán llevarse a cabo internamente en el mismo appliance, sin necesidad de soluciones, módulos, agentes y/o servidores externos.
* La solución a ofertar no debe ser parte o módulo de otras soluciones como AntiSPAM, IPS, Filtradores de Contenido (Proxies/Web Gateways) o Firewalls. Debido a la naturaleza de los ataques, el appliance debe estar solo dedicado a la detección y prevención de amenazas avanzadas en puntos finales.
* La solución debe ejecutarse sobre hardware que soporte un rendimiento de 100,000 puntos finales y debera incluir licenciamiento para proteccion de 45,000 puntos y soportar los siguientes sistemas operativos:
* Windows XP SP3
* Windows 2003 SP2
* Windows Vista SP1 or newer
* Windows 2008 R2
* Windows 7
* Windows 2012
* Windows 8
* Windows 8.1
* Windows 10
* OSX
* La solución deberá funcionar utilizando dispositivos on premise y como software de agente para endpoints, para detectar y prevenir exploits, así como supervisar la actividad de los endpoints remotos y dentro de la red, lo que permite una respuesta rápida a amenazas conocidas y desconocidas.
* Debe tener la capacidad de detectar de manera automática amenazas en al menos: dynamic link libraries (\*.dll files), object linking y archivo embebidos (\*.ocx), archivos del sistema (\*.sys) y ejecutables (\*.com y \*.exe), asi como tipos de archivos adicionales por medio de un API.
* La solución debe ser capaz de retroalimentarse automáticamente ante nuevas amenazas para de manera proactiva obtener nuevas posturas e inteligencia de las amenazas avanzadas, todo ello sin necesidad de interacción humana.
* La solución deberá permitir evalúar fácilmente todas las actividades de los endpoints con capacidades de triage y auditoria por medio de una única interfaz, identificando y neutralizando los incidentes para su análisis, y facilitando la contención, además de tomar las mejores decisiones sobre la respuesta
* La solución debe tener la capacidad de identificar ataques avanzados y amenazas persistentes avanzadas (APT) y ser capaz de aislar los dispositivos que están en riesgo para que los atacantes no puedan acceder a los sistemas. Al mismo tiempo, se permita la investigación a distancia.
 |
|  | **Inteligencia y Detección de Amenazas** | * La solución deberá colectar de forma automática la evidencia de los eventos en los usuarios finales que estén siendo identificados vía Web y correo electrónico para el inmediato análisis.
* La solución debe monitorear los Endpoints en tiempo real siendo capaz de protegerlos utilizando, como mínimo, los siguientes indicadores de actividad sospechosa:
	+ Uso no autorizado de cuentas de usuario válidas
	+ Rastreo de archivos de evidencia
	+ Actividad de Comando y Control
	+ Malware conocido y no conocido
	+ Tráfico de red sospechoso
	+ Uso de programas válidos para propósitos maliciosos
	+ Acceso no autorizado a archivos
	+ Exploits y otros ataques online
	+ Malware commodity
* La evidencia colectada deberá contar con la capacidad de crear una línea de tiempo previa al evento detectado vía Web y correo electrónico.
* La solución deberá poder identificar e investigar en los puntos finales en cuestión de minutos amenazas y determinar:
	+ Qué vectores de ataque se han empleado para infiltrarse en el endpoint.
	+ Si se ha producido un ataque en un endpoint concreto (y si prevalece).
	+ Si se ha producido la propagación lateral y a qué endpoints ha afectado.
	+ Cuánto tiempo ha durado el ataque al endpoint.
	+ Si se ha filtrado propiedad intelectual.
	+ Qué endpoints y sistemas deben controlarse para evitar futuros ataques.
* La solución deberá contar con la capacidad de realizar búsquedas en todos los dispositivos, utilizando información como puede ser:
	+ - * Browser name
			* Browser versión
			* Cookie flags
			* Cookie name
			* Cookie value
			* DNS hostname
			* Driver device name
			* Drive module name
			* Executable injected
			* Executable PE type
			* File download type
			* File full path
			* File name
			* File SHA256 hash
			* File Signature Exists
			* Local port
			* Local IP address
			* Process name
			* Service name
			* Task name
* Los indicadores de riesgo de la solución deben incluir, como mínimo, análisis basados en las siguientes actividades: actualizaciones de las claves de registro, modificación de archivos, búsquedas de DNS y modificación de cuentas de usuarios permitiendo también la creación de indicadores de riesgo personalizados; y en ambos casos debe notificar a los usuarios que el dispositivo está en riesgo.
 |
|  | **Consola de Gestión** | Con la finalidad de obtener una gestión unificada, el Consejo de la Judicatura Federal requiere de un repositorio central para gestionar las soluciones y las alertas generadas, por ello se solicita una consola. Esta contará con las siguientes características:* El equipo deberá fungir como consola de administración centralizada para los equipos dedicados al análisis y detección de amenazas avanzadas distribuidas en los entornos de ingreso a la red (Web/correo electronico).
* Debe permitir la administración y envío de actualizaciones a los equipos que gestiona.
* Debe tener la capacidad de almacenar todos los eventos generados en los equipos distribuidos en el entorno de red, así como la capacidad de generar reportes basados en la información almacenada.
* El equipo debe contar con la capacidad de integración con dispositivos de monitoreo y/o correlación de eventos (SIEM) mediante los estándares SNMP, SMTP HTTP y RSYSLOG, teniendo definidos parámetros de configuración para los más comunes, como LEEF y CEF
* El sistema de gestión debe tener la capacidad de ser colocado en modo Alta Disponibilidad.
* La consola debe existir en un equipo de propósito específico.
* La gestión de la consola de administración debe hacerse mediante uno o más protocolos seguros.
* La consola debe poder proveer la correlación entre los dispositivos Web y Mail para detección de ataques combinados (Spearphishing)
 |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de toda la solución deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |
|  | El participante será responsable de la instalación física, la configuración y puesta a punto de la solución, realizando las pruebas pertinentes; así mismo, deberá elaborar y entregar al Consejo de la Judicatura Federal una memoria técnica por la instalación realizada. |

Adicionalmente a lo señalado en estas bases, para esta solució se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | La solución que se solicita deberá contar con una garantía en sitio por el período mínimo de 3 años, para el hardware y software que componen la solución. |
|  | Al reporte de la falla, la solución deberá ser atendida en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. |
|  | Se deberá considerar Servicios Profesionales (Onsite Resource Service) para la configuración solicitada por la convocante. |
|  | Se deberá otorgar una transferencia de conocimientos de la solución para cuatro personas asignadas por el Consejo de la Judicatura Federal. |
|  | El servicio de garantía consistirá en la reparación de fallas en la solución objeto de la presente, incluyendo mano de obra, refacciones las cuales deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | En caso de ser necesario retirar la solución para su reparación, el proveedor deberá proporcionar una solución de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. La solución reparada deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 24x7. |
|  | En caso de sustitución definitiva de la solución, el proveedor entregará una nueva de la misma marca, de características iguales o superiores a la sustituida, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento, solución que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 24x7.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado la solución a sustituir. |
|  | Los servicios de garantía que se presenten durante la vigencia establecida, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | La solución será distribuida e instalada acorde a lo señalado en el apartado **F.**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.**  |
|  | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, así como de proporcionar licencias activadas a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico. |

|  |
| --- |
| **PARTIDA 6** |
| **Servidores de datos para servicios críticos**  |
| **CANTIDAD SOLICITADA: 170** |
| Es indispensable que los equipos consideren hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
|  | **Especificaciones** |
| 1. | Tipo de Procesadores  | Intel® Xeon® E7-4820 V4 2.0 GHZ .La tarjeta principal deberá ser de la misma marca del equipo. |
| 2. | Número de Procesadores | 2 Procesadores de diez cores. |
| 3. | Cache | Caché de 25 M. |
| 4. | Velocidad del bus frontal | 6.40 GT/s QPI. |
|  | **Memoria** |
| 5. | Tipo de memoria ECC  | DDR4 RDIMM. |
| 6. | Memoria Solicitada | 64 GB de memoria. |
| 7. | Ranuras ocupadas de Memoria | Las mínimas necesarias para una configuración de 64 GB. |
| 8. | Ranuras de expansión de Memoria | Las ranuras necesarias para expandir como mínimo a 64 GB. |
|  | **Almacenamiento** |
| 9.. | Controlador de disco duro | Controladora de disco con soporte para RAID 0, 1, 5. |
| 10. | Compartimientos  | Los compartimientos mínimos, para soportar la configuración solicitada, unidades de disco duro “*hot plug*”. |
| 11. | Unidades de disco duro  | Discos SAS 10k rpm en Raid 1, usable 300 GBDiscos SAS 10k rpm en Raid 5, usables 1 TB. |
| 12. | Capacidad de almacenamiento interno. | Capacidad de 5 TB de almacenamiento interno. |
|  | **Red** |
| 13. | Puertos de acceso a la red de datos |
| 14. | Puerto para administración |
|  | **Entrada/Salida** |
| 15. | Ranuras de expansión PCI |
| 16. | Unidades ópticas |
| 17. | Puertos USB |
|  | **Fuente de poder** |
| 18. | Tolerancia a fallos |
|  | **Video** |
| 19. | Controlador de video |
|  | **Características adicionales** |
| 20. | Chasis para Rack cerrado en altura máxima de 4U, con rieles para rack universal. |
| 21. | Ventiladores redundantes. |
| 22. | Un juego de manuales por servidor para la instalación, configuración y operación, en español, puede ser en CD, USB, o impreso. |
| 23. | Llave de seguridad |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación y puesta a punto de los equipos deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, instalación, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |

Adicionalmente a lo señalado, para estos equipos se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
| 1 | Los equipos que se solicitan deberán contar con una garantía en sitio por el período mínimo de 3 años. |
| 2 | Los servicios de garantía se deberán atender en horario laboral de lunes a viernes de 09:00 a 18:00 hrs., con respuesta al siguiente día hábil.  |
| 3 | El servicio de garantía consistirá en la reparación de fallas en los equipos objetos de la presente, incluyendo mano de obra, refacciones que deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal . |
| 4 | En caso de ser necesario retirar el equipo para su reparación, el proveedor, deberá proporcionar un equipo de respaldo, de la misma marca, de características iguales o superiores, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al equipo sustituto, toda la configuración de trabajo generada hasta ese momento. El equipo reparado deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 12 horas con servicio 5x8. |
| 5 | En caso de sustitución definitiva del equipo, el proveedor, entregará uno nuevo de la misma marca, de características iguales o superiores al sustituido, debiendo proporcionarse una vez que se haya retirado el dañado, configurado con las mismas características de hardware y software al originalmente instalado, y será el responsable de transferir al equipo sustituto, toda la configuración de trabajo generada hasta ese momento, equipo que deberá restituirse a la misma unidad de asignación original en un tiempo máximo de 48 horas con servicio 5x8.Asimismo, el proveedor, deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del área administrativa a la que estuviera asignado el equipo a sustituir. |
| 6 | Los servicios de garantía que se presenten durante la vigencia de la misma, el proveedor que resulte adjudicado deberá acreditar plenamente el servicio mediante las hojas de servicio firmadas por el ingeniero local, siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General de Tecnologías de la Información, designara a los servidores públicos responsables de la supervisión del contrato adscrito a la misma. |
| 7 | Los equipos serán distribuidos e instalados acorde a lo señalado en el apartado **F**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G. *Cuadro de Distribución*.** |
| 8 | Los equipos deberán tener instalado Windows Server 2012 R2 (La media y la licencia será proporcionada por el Consejo de la Judicatura Federal) y con tres máquinas virtuales montadas en rol de” Hyper-V” configuradas de manera inicial con 6 procesadores virtuales, 12 GB de RAM y dos unidades de disco, una de 120 GB para sistema operativo y otra de 300 GB para datos. |
| 9 | El licitante adjudicado será responsable de la configuración, migración, integración y puesta a punto de la solución, derivada de la presente licitación, así como de proporcionar las licencias activadas para los citados equipos, a fin de garantizar el cumplimiento de los requerimientos mínimos descritos en el anexo técnico |

|  |
| --- |
| **PARTIDA 7** |
| **Monitor LCD de 70 pulgadas** |
| **Cantidades solicitada: 1**  |
| Es indispensable que el equipo considere hardware y software vigente en el mercado; así mismo, **es necesario que en la propuesta técnica se detalle de manera específica las características y marca de los elementos que lo integran. Se les informa a los participantes que las adjudicaciones se asignarán por partida completa.** |
| **Núm.** | **REQUERIMIENTO MÍNIMO** |
| **Especificaciones** |
| 1 | Monitor LCD | 70”, LCD, calidad Full HD (1920x1080), sistema de montaje VESA, al menos una entrada USB, entrada Ethernet, WiFi opcional, tiempo de respuesta 6 a 10ms, operación de 24X7  |
| 2 | Sistema de Video | NTSC/PAL |
| 3 | Duración de la lámpara del panel | Por lo menos 60,000 horas |
| **Especificaciones para la entrada** |
| 4 | Video  | HDMI, DisplayPort, DVI, S-video, VGA opcional. |
| 5 | Audio | RCA análoga opcional y 3.5mm stereo jack opcional. |
| 6 | Voltaje | 120 V |
| **Especificaciones para la salida** |
| 7 | Bocinas de Salida | 10W + 10W |
| **Varios** |
| 8 | Deberá traer: la marca y modelo del fabricantetroquelada o impresa en el chasis, la capacidad claramente indicada y visible en el equipo y en su empaque. No se acepta que dichos datos se presenten en calcomanías, etiquetas o engomados; no se aceptarán alteraciones o correcciones de ingeniería. |

|  |
| --- |
| **Otros** |
|  | Incluirá todos los cables, accesorios y software necesarios para su puesta en operación (v.g.: cables de alimentación, de red, de consola, etc.) |
|  | Incluirá los manuales de usuario para la instalación, configuración y operación. |
|  | Todos los aditamentos, materiales y demás accesorios necesarios para la completa instalación deben ser proporcionados por el participante. |
|  | Los gastos de operación, transporte, mantenimiento, viáticos y cualquier otro gasto implícito o explicito para cumplir con el objetivo de esta propuesta corren a cargo del participante. |

Adicionalmente a lo señalado en estas bases, para este equipo se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS** |
|  | El equipo que se solicita deberá contar con una garantía en sitio por el período mínimo de 36 meses, para el hardware y software  |
|  | El servicio de garantía consistirá en la reparación de fallas en los equipos objeto de la presente, incluyendo mano de obra, refacciones que deberán ser partes nuevas y originales, iguales o superiores en marca y modelo, totalmente compatibles a los instalados y contemplados dentro de la presente, con una garantía mínima de 36 meses, y en caso que el repuesto ocasione la reinstalación o reconfiguración del software de sistema operativo, del firmware, o de los aplicativos, estas labores deberán ser realizadas por el proveedor, sin costo adicional para el Consejo de la Judicatura Federal.  |
|  | Los servicios de garantía que se presenten durante la vigencia de la misma, el proveedor que resulte adjudicado deberá acreditarlos mediante las hojas de servicio firmadas por el ingeniero local siempre y cuando se haya brindado a entera satisfacción del Consejo de la Judicatura Federal.La Dirección General Tecnologías de la Información, designará al servidor(es) publico(s) responsable(s) de la supervisión del contrato adscrito a la misma. |
|  | El equipo será distribuido acorde a lo señalado en el apartado **F**, numeral **F.5.1** **Entrega e instalación de los bienes materia de la presente licitación** y el **G *Cuadro de Distribución*.**  |

**E. Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante.**

**E.1 CARTAS COMPROMISO Y DOCUMENTOS COMPROBATORIOS**

De conformidad a lo establecido en el cuerpo de las bases de licitación y según corresponda, los participantes deberán anexar a su oferta técnica la siguiente documentación y cartas compromiso por cada partida en que participe:

|  |  |  |
| --- | --- | --- |
| **Partida** | **Modelo de carta (apartado I)** | **Descripción** |
| **Todas** | **1** | **Carta de entrega de bienes idénticos.** |
| **2** | **Carta de componentes y partes originales.** |
| **3** | **Carta de certificación de calidad.** |
| **4** | **Carta de distribuidor autorizado (En caso de que el participante sea el fabricante no se requiere esta carta).** |
| **1, 2, 3, 4, 5 y 6** | **5** | **Carta de Instalación.** |
| **Todas** | **6** | **Carta de cumplimiento de términos y condiciones de las garantías y servicios.** |
| **7** | **Carta de cumplimiento de términos y condiciones de entrega de bienes.** |
| **8** | **Cartas de los Centros de servicios que apoyarán para brindar los servicios de garantía.** |
| **1, 2, 3, 4, 5 y 6** | **9** | **Carta de Personal capacitado y especializado** |
| **Todas** | **No aplica modelo o formato de carta** | **Copia simple del certificado vigente correspondiente al fabricante (NOM-019-SCFI-1998).** |
| **Copia simple de la certificación por parte del fabricante o marca, del personal que realizará la instalación y configuración.** |
| **Documentación técnica del fabricante** Nota: Podrá presentarse documentación en idioma del país de origen, pero deberá ir acompañada de una traducción simple al español, subrayando o marcando las características técnicas solicitadas con su numeral correspondiente a la partida en la que participe. |
| **Copia simple del certificado vigente correspondiente al fabricante (NOM-001-SCFI-1993) conforme los establece(n) la(s) dependencia(s) gubernamental(es) responsable(s) de su emisión y vigilancia.** |
| **Número telefónico del tipo larga distancia automática nacional (lada 01-800 o equivalente)** |
| **Formato 1** | **Descripción de los bienes y servicios objetos de su oferta.** |
| **Formato 2** | **Relación de centros de servicio.** |
| **6** | **Formato 3** | **Relación de centros de servicio para las ciudades restantes.** |

E.1.1 NORMA OFICIAL MEXICANA

Todos los equipos deberán cumplir con la Norma Oficial Mexicana que cubre(n) o satisface(n) [conforme lo establece(n) la(s) dependencia(s) gubernamental(es) responsable(s) de su emisión y vigilancia], y a falta de éstas, de las Normas Internacionales, de conformidad con lo dispuesto por los artículos 53 y 55 de la Ley Federal sobre Metrología y Normalización.

E.2 DOCUMENTACIÓN TÉCNICA DEL FABRICANTE

La propuesta técnica deberá incluir la **documentación técnica del fabricante** en donde se pueda comprobar que las características que ofrece el participante sean iguales o superiores a las características solicitadas por el Consejo de la Judicatura Federal, debiendo ser catálogos, folletos y documentos impresos de páginas de Internet, donde aparezca la dirección URL (Uniform Resource Locator) y la fecha de impresión en este último caso, **el no presentar documentación técnica, será motivo para desechar su propuesta.**

La documentación antes descrita deberá permitir validar las características solicitadas, en caso contrario, **podrá ser motivo para desechar su propuesta**. Cabe mencionar que en caso de que existan dudas acerca de la información técnica presentada, la convocante podrá consultar las páginas en internet de los fabricantes o proveedores de los bienes con la finalidad de comprobar y validar las características requeridas.

Las propuestas y todo lo relacionado con las mismas deberán presentarse en idioma español. Los anexos técnicos y folletos podrán presentarse en el idioma del país de origen de los bienes, **acompañados de una traducción simple al español**, subrayando o marcando las características técnicas solicitadas con su numeral correspondiente, **la omisión de la referida traducción, será motivo de descalificación de la propuesta.**

La documentación técnica del fabricante, mencionada en el párrafo anterior, deberá incluirse en la sección II Cartas compromiso, documentos comprobatorios y documentación técnica del fabricante, subíndice II.6 Documentación técnica del fabricante, señalado en el apartado C. Estructura de la propuesta.

F. Características de las garantías y servicios

**F.1 Carta de cumplimiento de términos y condiciones de las garantías y servicios,** el participante a la licitación deberá presentar carta compromiso en la que manifieste que ha leído, entendido y está de acuerdo en prestar servicios solicitados conforme a lo establecido en el presente apartado, **deberá ser entregada en la Sección III “*Garantías y servicios de los bienes solicitados”*, subíndice III.1, señalado en el apartado *C. “Estructura de la propuesta”*.**

**F.2** De acuerdo a lo que se establece en las presentes bases de licitación, los participantes deberán considerar en su oferta para el Consejo de la Judicatura Federal lo siguiente:

1. Entrega de los bienes materia de la presente licitación.
2. Cobertura nacional para la entrega y prestación de la garantía de los bienes materia de la presente licitación.
3. Cobertura en Ciudad de México y área metropolitana para la entrega y prestación de la garantía de los bienes materia de la presente licitación.
4. Instalación, configuración y puesta a punto de los bienes de **las partidas que así lo requieran.**

Los servicios y garantías contemplados en el **subíndice F.2, puntos “1”, “2”, “3” y “4”,** se proporcionarán en sitio por el(los) participante(s) que resulte(n) adjudicado(s) o por sus representantes certificados y autorizados, coordinados y bajo los procedimientos que establezca la convocante.

En los siguientes rubros se establecen de manera particular los lineamientos a los que se sujetará la prestación de los diversos servicios y garantías, así como los requisitos mínimos que deberán cumplirse por el(los) participante(s) que resulte(n) adjudicado(s).

**F.2.1 Carta de cumplimiento de términos y condiciones de entrega de bienes. -** El participante a la licitación deberá presentar carta compromiso en la que manifieste que ha leído, entendido y está de acuerdo en prestar los servicios de entrega de bienes conforme a lo establecido en el presente Anexo “1”, **deberá ser entregada en la Sección III “*Garantías y servicios de los bienes solicitados”*, subíndice III.2, señalado en el apartado *C. “Estructura de la propuesta”*.**

F.3 Bitácora de seguimiento de garantías.

La aplicación de garantías deberá registrarse por el participante que resulte adjudicado y éste se encargará de elaborar los reportes diarios de servicio y atención de fallas. Asimismo, será su responsabilidad el seguimiento de todos y cada uno de los eventos de garantía.

F.4 Informes.

El participante que resulte adjudicado deberá entregar a la Dirección General de Tecnologías de la Información del Consejo de la Judicatura Federal, los siguientes documentos o informes que reflejen todos los eventos de garantía prestados, con la periodicidad que se requiera:

* Un informe de incidentes donde se describa el tipo de falla que se atendió durante el periodo que establezca la convocante y de acuerdo a los requerimientos de ésta. Se deberán anexar los reportes de servicio debidamente requisitados como comprobantes de la atención proporcionada.
* En cada reporte o cédula de servicio de mantenimiento o falla se deberán especificar claramente las series, las marcas, modelos y números de inventario de todos los bienes a los que se haya aplicado el servicio, así como el domicilio en que estén instalados; se deberá recabar el sello de adscripción y la firma de conformidad del usuario responsable del bien entregándoles una copia de la cédula debidamente requisitada.

F.5 Garantía de satisfacción total.

De conformidad con lo establecido en el presente Anexo Técnico, los participantes deberán:

* Cumplir con las condiciones y tiempos establecidos para la(s) garantía(s) y servicios.
* Generar los diversos reportes asociados a las garantías y servicios que se solicitan.

Cabe mencionar que, una vez llevada a cabo la adjudicación e iniciada la prestación de los servicios y garantías, la información proporcionada por el participante que resulte adjudicado en los documentos, informes y bitácoras se corroborará comparándolos con la información que proporcione el responsable del área de Seguridad Informática al que se le proporcionó el bien o servicio.

F.5.1 Entrega e instalación de los bienes materia de la presente licitación.

Para todas las partidas, la entrega se deberá realizar de conformidad con los procedimientos establecidos por la Dirección de Almacenes (**DAL**), dependiente de la Dirección General de Recursos y Materiales (**DGRM**), con base a los cuadros de distribución que le serán proporcionados por la Dirección General de Tecnologías de la Información.

Para efectos de control en la prestación de garantías y servicios referentes a la adquisición realizada, previamente a su entrega, **todos los bienes** serán debidamente identificados con una etiqueta indeleble y polimetalizada, que contenga los datos de la empresa, número telefónico nacional a diez dígitos o servicio “01-800”, (*sin cargo para el Consejo de la Judicatura Federal*), número de licitación, así como el periodo de garantía, considerando mes y año de inicio, y mes y año de conclusión; dicha etiqueta deberá ser suministrada por el participante que resulte adjudicado y la deberá colocar o pegar en cada bien o componente, definiéndose con la convocante, el lugar exacto de su colocación.

Si en el periodo entre la fecha de adjudicación y el plazo de entrega de los bienes a satisfacción del Consejo de la Judicatura Federal, las soluciones y/o equipos ofertados tuvieran alguna variación en sus características técnicas, el participante presentará una carta suscrita por el fabricante donde se justifique el cambio de características y anexar un cuadro comparativo de éstas con el bien ofertado inicialmente. El mismo que deberá ser de la misma marca, de características iguales o superiores al inicialmente ofertado y será evaluado por el área técnica.

Para **las partidas que así lo requieran, se deberá considerar su completa instalación**, **configuración** y puesta a punto en una fecha no posterior al **29 de diciembre**, en el inmueble que determine la convocante. La empresa adjudicada deberá coordinar con el personal de Seguridad Informática de la Dirección General de Tecnologías de la Información las fechas en las que se realizarán los trabajos, no excediendo la fecha establecida con anterioridad. La DGTI proporcionará a la empresa adjudicada el directorio de los ingenieros que estarán encargados de estas tareas.

F.5.2 Garantía de mantenimiento preventivo y correctivo de los bienes materia de la presente licitación.

El participante deberá prestar los servicios de garantía a través de su mesa de ayuda para la administración de los servicios que se generen; que contemple la retroalimentación en línea para conocer el estado de cada reporte por medio telefónico y mediante acceso por internet, que permita análisis históricos del comportamiento de cada bien, reportes por clasificación de fallas, por ciudad y por fechas.

El participante deberá proporcionar un número telefónico nacional a diez dígitos o servicio “01-800”, sin cargo para el Consejo de la Judicatura Federal, **deberá ser entregado en la Sección III “Garantías y servicios de los bienes solicitados”, subíndice III.3, señalado en el apartado C. “Estructura de la propuesta”**, con el objeto de brindar tanto soporte técnico como levantamiento de los reportes de servicio de garantía.

De no especificar el número lada 01-800 o equivalente en su propuesta, deberá manifestar por escrito el compromiso de que, en caso de resultar adjudicado en cualquiera de las partidas donde se solicita este servicio, el número estará disponible al inicio de la instalación de los bienes para el reporte y seguimiento del servicio de mantenimiento preventivo y/o correctivo.

El servicio de soporte técnico incluye el apoyo a los usuarios o a los ingenieros del Consejo de la Judicatura Federal con dudas o problemas suscitados en la instalación y operación de los bienes adquiridos (armado, configuración del equipo, configuración de políticas, etc.)

El participante que resulte adjudicado deberá cumplir con la prestación del servicio de mantenimiento preventivo y/o correctivo como servicio incluido dentro de la garantía para las partidas que así lo requieran, de acuerdo a los siguientes rubros:

* Ante la falla de cualquiera de las soluciones y/o equipos objeto de la presente licitación los servicios de garantía serán proporcionados en sitio, excepto en los casos que expresamente se señale.
* El participante que resulte adjudicado, ante cualquier reporte de falla deberá proporcionar un número de control para el seguimiento de la garantía, registrando la fecha y hora del mismo.
* Al reporte de la falla, las soluciones y/o equipos deberán ser atendidos en un máximo de 1 hora dada la criticidad de la operación de los centros de datos. Para las partidas que así lo requieran, las soluciones y/o equipos deberán ser atendidos en un periodo máximo de 12 horas en un esquema 24x7 o 5x8 según sea el caso. En caso de ser necesario retirar el equipo y/o solución para su reparación, el participante que resulte adjudicado deberá proporcionar un equipo y/o solución de respaldo de la misma marca, de características iguales o superiores invariablemente dentro de los límites de tiempo anteriormente señalados, configurado con las mismas características de hardware y software al originalmente instalado y será el responsable de transferir a la solución sustituta, toda la configuración de trabajo generada hasta ese momento. El equipo y/o solución reparado deberá restituirse a la misma unidad de asignación original.
* Para las partidas que así lo requieran, cuando la aplicación de la garantía exceda del tiempo señalado, y de no haber proporcionado el respaldo del componente dañado, el participante que resulte adjudicado deberá sustituir de manera parcial o total el equipo y/o solución, de tal manera que se asegure la continuidad del servicio dentro de las siguientes 48 horas.
* Para la reparación de los bienes deberán utilizarse partes nuevas y originales de la misma marca, de características iguales o superiores, totalmente compatibles.
* En caso de sustitución definitiva de los bienes, el participante que resulte adjudicado considerará que: el equipo y/o solución de sustitución deberá ser nuevo, de la misma marca, de características iguales o superiores al sustituido, debiendo proporcionarse invariablemente dentro de los límites de tiempo anteriormente señalados, configurado con las mismas características de hardware y software al originalmente instalado y será el responsable de transferir a la solución sustituta toda la configuración de trabajo generada hasta ese momento; también será el responsable de identificar el nuevo equipo y/o solución para lo cual deberá entregar mediante escrito la etiqueta del bien dañado y solicitar su reposición a la Dirección de Almacenes de la Dirección General de Recursos Materiales. Así mismo, el participante que resulte adjudicado deberá presentar una carta donde conste el cambio, indicando claramente los números de serie y demás características, así como los datos del inmueble al que estuviera asignado el equipo y/o solución a sustituir.

Los servicios de garantía para las partidas que así lo requieran se prestarán por el periodo que se solicita (acorde a la descripción de los requerimientos establecidos en el apartado **D. Características Técnicas**) bajo un esquema 24x7 o 5x8; las partidas que no requieran el esquema 24x7 prestarán el servicio de lunes a viernes en un horario de 9:00 a 18:00 hrs., iniciando tales servicios a partir de la instalación de cada uno de los bienes y tomando como referencia para su terminación la fecha de presentación ante el Consejo de la Judicatura Federal, de la última remisión-resguardo con la que se concluye el proceso de entrega/instalación de los bienes.

F.5.3 Cobertura nacional para prestación de la garantía y entrega de los bienes materia de la presente licitación

Además de la carta compromiso que deberá ser entregada en la Sección III “*Garantías y servicios de los bienes solicitados*”, subíndice III.1 “Cumplimiento de términos y condiciones de las garantías y servicios”, señalado en el apartado C. “Estructura de la propuesta” el participante a la licitación deberá entregar una relación que indique la ubicación, señalando domicilio y teléfonos de los centros de servicio a 10 dígitos (código de área y número) correspondiente, que estarán a cargo de la prestación de las garantías deberá ser entregado en la Sección III “*Garantías y servicios de los bienes solicitados”*, subíndice III.4, señalado en el apartado C. “Estructura de la propuesta”, los cuales deberán ubicarse, como mínimo, en las localidades que se relacionan en el cuadro siguiente y mantener cobertura en el resto de las localidades relacionadas en el apartado G. “*Cuadro de distribución”*.

|  |  |
| --- | --- |
| **Partida** | **Localidades donde deben contar con centros de servicio**  |
| **6** | **Ciudad de México; Guadalajara, Jal.; Tijuana, B.C.; Monterrey, NL; Villahermosa, Tab.; Xalapa, Ver.; y/o sus áreas metropolitanas** |
|  **2, 7** | **Ciudad de México y/o su área metropolitana.** |
| **1, 3, 4, 5** | **Ciudad de México y Zapopan, Jalisco; y/o sus áreas metropolitanas** |

Se aceptará que los centros de servicio se ubiquen en todas las ciudades solicitadas o sus zonas conurbadas.

Además de la relación anterior, el participante a la licitación deberá presentar una carta por cada Centro de Servicio que le apoyará en la asistencia y que brindará servicios de garantía, en cada carta se deberá indicar claramente que el centro cumplirá con el apoyo para brindar los servicios de garantía, que tiene conocimiento de la licitación y que otorgará dichos servicios conforme a lo estipulado en las presentes bases. Estas cartas deberán ser firmadas por el representante legal del Centro de Servicio, **deberán ser entregadas en la Sección III “*Garantías y servicios de los bienes solicitados”*, subíndice III.5, señalado en el apartado *C. “Estructura de la propuesta”*.**

**Adicionalmente**, el participante presentará una relación donde indique claramente la forma en que dará la cobertura de la garantía para las ciudades restantes, en donde no se solicita Centro de Servicio, indicando desde que ciudad y centro de servicio dará el apoyo y que cumplirá con los tiempos y condiciones estipulados, **la cual** **deberá ser entregada en la Sección III “*Garantías y servicios de los bienes solicitados*”, subíndice III.6, del apartado C. “Estructura de la Propuesta”.**

Lo anterior, independientemente de que la responsabilidad en la prestación de los servicios estará a cargo del participante que resulte adjudicado. En el caso de que algún Centro de Servicio llegase a modificar su domicilio o teléfono, o que se cambie un Centro de Servicio por otro, el participante que resulte adjudicado deberá comunicar oportunamente tal situación a la Dirección General de Tecnologías de la Información, a efectos de mantener actualizados los directorios correspondientes.

G. Cuadro de distribución

**Generales**

1. Los bienes solicitados serán destinados para el robustecimiento de seguridad y deberán ser distribuidos por el (los) participante (s) que resulte (n) adjudicado (s) de acuerdo a las necesidades del Consejo de la Judicatura Federal, considerando lo especificado en el apartado ***F. 5.1. Entrega e instalación de los bienes materia de la presente licitación.***
2. Para efectos de distribución y garantía en sitio solicitada, los datos completos de los destinatarios (área o inmueble del Consejo de la Judicatura Federal, con nombres de funcionarios, teléfonos y domicilios completos) serán proporcionados en formato electrónico por la convocante al día siguiente hábil a la firma del contrato.
3. Las cantidades por destino y los destinos podrán variar, conforme a las necesidades de la convocante.
4. El participante que resulte adjudicado deberá presentar, en un plazo no mayor a **15 días naturales** posteriores a la firma del contrato, un plan de trabajo que contenga todas las actividades que desarrollará hasta la conclusión de lo requerido en este anexo técnico. Dicho plan de trabajo deberá ser avalado por el fabricante dado que la instalación de los bienes deberá ser aprobada, de acuerdo a las mejores prácticas, expresamente por personal técnico del mismo.
5. Los bienes deberán entregarse, instalarse y ponerse a punto para las partidas que así se requiera y configurarse en una fecha no mayor al **29 de diciembre de 2017.**
6. La transferencia de conocimientos para el personal designado por la Dirección de Seguridad Informática se deberá presentar mediante un plan de implementación, el mismo que se debe entregar a **más tardar en 30 días naturales de la firma del contrato.**
7. La transferencia de conocimientos se realizará directamente sobre los equipos instalados en sitio en un plazo no mayor a 15 días naturales una vez concluida la configuración y puesta a punto.

|  |
| --- |
| **PARTIDA 1** |
| **SUBPARTIDA 1.1** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |
| **2** | Zapopan | Ciudad Judicial periférico Pte. S/n, Col. El Colli, a inmediaciones del cerro del Colli, Zapopan, Jal. C.P. 45036 | 1 |
| **3** | Ciudad de México | Edificio Sede / Insurgentes Sur 2417, Col. San Ángel, Ciudad de México., Álvaro Obregón, C.P. 1000 | 1 |
| **4** | Ciudad de México | Eduardo Molina No. 2, Col. Del Parque, Ciudad de México, Venustiano Carranza, C.P. 15960 | 1 |

|  |
| --- |
| **PARTIDA 1** |
| **SUBPARTIDA 1.2** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |

|  |
| --- |
| **PARTIDA 1** |
| **SUBPARTIDA 1.3** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |

|  |
| --- |
| **PARTIDA 2** |
| **SUBPARTIDA 2.1** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Carretera Picacho -Ajusco No. 170, Col. Jardines en la Montaña, Ciudad de México, Tlalpan, C.P. 14210. | 6 |

|  |
| --- |
| **PARTIDA 2** |
| **SUBPARTIDA 2.2** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Carretera Picacho -Ajusco No. 170, Col. Jardines en la Montaña, Ciudad de México, Tlalpan, C.P. 14210. | 1 |

|  |
| --- |
| **PARTIDA 2** |
| **SUBPARTIDA 2.3** |
| **Csvo.** | **Ciudad** | **Domicilio** |  |
| **1** | Ciudad de México | Carretera Picacho -Ajusco No. 170, Col. Jardines en la Montaña, Ciudad de México, Tlalpan, C.P. 14210. | 1 |

|  |
| --- |
| **PARTIDA 3** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |
| **2** | Zapopan | Ciudad Judicial periférico Pte. S/n, Col. El Colli, a inmediaciones del cerro del Colli, Zapopan, Jal. C.P. 45036 | 1 |

|  |
| --- |
| **PARTIDA 4** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |

|  |
| --- |
| **PARTIDA 5** |
| **SUBPARTIDA 5.1** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |
| **2** | Zapopan | Ciudad Judicial periférico Pte. S/n, Col. El Colli, a inmediaciones del cerro del Colli, Zapopan, Jal. C.P. 45036 | 1 |

|  |
| --- |
| **PARTIDA 5** |
| **SUBPARTIDA 5.2** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |

|  |
| --- |
| **PARTIDA 5** |
| **SUBPARTIDA 5.3** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Edificio Canoa 79 / Calle Canoa No. 79, Col. Tizapán San Angel, Ciudad de México, Álvaro Obregón, C.P. 1090 | 1 |

| **PARTIDA 6** |
| --- |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| 1 | ​Acapulco | Blvd. De Las Naciones No. 640, Granja 39 Fracción A, Fraccionamiento Granjas del Marques, C.P. 39890 | 2 |
| 2 | Aguascalientes | Av. Aguascalientes Sur # 603, Fracc. Jardines de Aguascalientes, Aguascalientes, Ags, C.P. 20270 | 1 |
| 3 | Aguascalientes | Av. De La Convención de 1914 Norte # 111, Fracc. Circunvalación Norte, Aguascalientes, Ags, C.P. 20020 | 1 |
| 4 | Boca del Rio | Av. Habaneras 315, Fraccionamiento Jardines de Virginia, Boca Del Rio, Veracruz, C.P. 94294 | 1 |
| 5 | Campeche | Av. Patricio Trueba Número 245 Colonia San Rafael San Francisco de Campeche, Campeche. C.P. 24090. | 1 |
| 6 | Campeche | Av. Adolfo López Mateos Número 408 Colonia Bosques de Campeche, San Francisco de Campeche, Campeche. C.P. 24030. | 1 |
| 7 | Cancún | Av. Andrés Quintana Roo No. 245, Supermanzana 50, Manzana. 57, Lote 1, Torre A, Planta Baja, Cancún, Q. Roo., C.P. 77533, | 2 |
| 8 | Cd. Juárez | Av. Tecnológico No. 1670, Col. Fuentes del Valle, Cd. Juárez Chihuahua, C.P. 32505 | 1 |
| 9 | Cd. Obregón | Calle Juan Álvarez No. 940 Altos, Col. Campestre, C.P. 85160 | 1 |
| 10 | Cd. Obregón | Calle Sahuaripa Esquina Nainari, Col. Cuauhtémoc, Ciudad Obregón, Son. C.P. 85110 | 1 |
| 11 | Celaya | Quetzalli No. 901, 1Er. Nivel, Col. Los Álamos, Celaya, Gto., C.P. 38020 | 1 |
| 12 | Chetumal | Av. Álvaro Obregón 232 Esq., Av. Independencia, Col. Centro, C.P. 77000 | 1 |
| 13 | Chihuahua | Av. Mirador No. 6500, Pb. Ala Sur, Col. Fraccionamiento Residencial Campestre, Washington, C.P. 31236 | 1 |
| 14 | Chilpancingo | Calle 5 de mayo No. 9, 3Er. Piso, Col. Centro, C.P. 39000 | 1 |
| 15 | Chilpancingo | Av. Álvarez No. 78, Centro, Chilpancingo, Guerrero, C.P. 39000. | 1 |
| 16 | Chilpancingo | Blvd. Vicente Guerrero Km. 274, Fracc. La Cortina (Lateral de la Carretera Federal No. 95), Chilpancingo, Gro. | 1 |
| 17 | Chilpancingo | Av. Juarez No. 24, Centro, Chilpancingo, Guerrero, C.P. 39000. | 1 |
| 18 | Cintalapa | Centro de Readaptación Social, (Cereso No. 14, “El Amate”), Rancho “San José”, Col. Lázaro Cárdenas, C. P. 30410, Municipio de Cintalapa, de Figueroa, Chiapas | 1 |
| 19 | Ciudad de México | Revolución No. 1508, Col. Guadalupe Inn, Deleg. Álvaro Obregón, Ciudad de México, C.P. 01020, Olimpo. | 2 |
| 20 | Ciudad de México | Insurgentes Sur 2417, Col. San Ángel, Del. Álvaro Obregón, C.P. 01000. | 4 |
| 21 | Ciudad de México | Camino al Ajusco 170, Col. Jardines En La Montaña, Del. Tlalpan, C.P. 14210 | 3 |
| 22 | Ciudad de México | Periférico Sur Número 4124 Edificio “Zafiro”, Colonia Jardines del Pedregal, Ciudad de México, Álvaro Obregón, C.P. 1900 | 1 |
| 23 | Ciudad de México | Edificio Prisma / Av. Insurgentes Sur No. 2065, P.B., Col. San Ángel, Ciudad de México, Álvaro Obregón, C.P. 1000 | 4 |
| 24 | Ciudad de México | Edificio Las Flores / Blvd. Adolfo Lopez Mateos 2321, Col. Tlacopac, San Angel, Ciudad de México, Álvaro Obregón, C.P. 1760 | 2 |
| 25 | Ciudad de México | Av. Insurgentes Sur 1888 , Florida, Ciudad de México, C.P. 01030. | 1 |
| 26 | Ciudad de México | Antiguo Camino a Culhuacán No. 202, Col. Santa Isabel Industrial, C.P. 9820, Deleg. Iztapalapa, Ciudad de México. | 1 |
| 27 | Ciudad de México | Bucareli 22 Y 24, Col. Centro, Delegación Cuauhtémoc, C.P. 06040, Ciudad de México. | 1 |
| 28 | Ciudad de México | Blvd. Adolfo López Mateos 1950, Col. Tlacopac San Ángel, Del. Álvaro Obregón, C.P. 01049 | 1 |
| 29 | Ciudad de México | Av. Canoa No.79, Tizapan San Angel, Delegación Álvaro Obregón, Ciudad de México, C.P. 01090.  | 5 |
| 30 | Ciudad de México | Sidar Y Rovirosa S/N, Esq. Eduardo Molina, Colonia Del Parque, Del. Venustiano Carranza, Ciudad de México C.P. 15960. IJF | 4 |
| 31 | Ciudad de México | Av. Blvd. Adolfo López Mateos No. 2321, Col. Tlacopac San Angel, Del. Álvaro Obregón, Ciudad de México, C.P. 01760. | 1 |
| 32 | Ciudad de México  | Revolución No. 1340, Col. Guadalupe Inn, Del. Álvaro Obregón, Ciudad de México, C.P. 01020. | 1 |
| 33 | Ciudad Victoria | Blvd. Praxedis Balboa No. 1813, entre calles Mártires de Río Blanco Y F. De La Garza, Col. Miguel Hidalgo, Ciudad Victoria, Tamaulipas, C.P. 87090. | 1 |
| 34 | Coatzacoalcos | Av. Universidad (antes Antigua Carretera Minatitlán) Km 12 Col. Reserva Territorial, Coatzacoalcos, Veracruz | 1 |
| 35 | Xalapa | Av. Culturas Veracruzanas No. 120, Col. La Reserva, Xalapa, Ver., C.P. 91096. | 1 |
| 36 | Córdoba | Av. 3, N° 1309, esquina Calle 13, Col. Centro, C.P. 94500, Córdoba, Veracruz. | 1 |
| 37 | Cuernavaca | Blvd. Del Lago No. 103, Villas Deportivas, Cuernavaca, Morelos, C.P. 62370. | 1 |
| 38 | Cuernavaca | Av. General Salazar No. 22, Centro, Cuernavaca, Mor, C.P. 62000. | 1 |
| 39 | Culiacán | Carretera a Navolato 10321, Sindicatura de Aguaruto, Culiacán, Sinaloa, C.P. 80308. | 1 |
| 40 | Durango | Carretera a Torreón Km. 6., Col. Ciudad Industrial, Palacio Federal, Durango, C.P. 34208 | 1 |
| 41 | Durango | Blvd. Luis Donaldo Colosio, esquina con Blvd. José María Patoni (Av. San Antonio), No. 101, Predio El Tule, Durango, Dgo. C.P. 34217. | 1 |
| 42 | Durango |  Av. Hierro Y Cobalto, 1Er. Piso, Carretera a Torreón Km. 6 Col. Ciudad Industrial, C.P. 34221 | 1 |
| 43 | Ensenada | Av. Álvaro Obregón No. 389 Esq. Calle Cuarta, Centro, Ensenada, B.C., 22800. | 1 |
| 44 | Ensenada | Calle Cuarta No. 450, entre Av. Ruiz Y Gastelum, Centro, Ensenada, B.C., 22800. | 1 |
| 45 | Estado de México | Sor Juana Inés de la Cruz No. 302 Sur, Col. Centro C.P. 50000 Toluca, Edo. Méx. | 1 |
| 46 | Guanajuato | Carretera Cuatro Carriles Guanajuato-Silao, Glorieta Santa Fe No. 5, Edificio B, 2Do. Piso, Col. Yerbabuena, Guanajuato, Gto., C.P. 36251. | 1 |
| 47 | Guanajuato  | Calle Tierra Colorada No. 117, Col. Jardines del Moral, León, Gto. | 1 |
| 48 | Hermosillo | Boulevard Luis Encinas Johnson N° 253, esquina con Monteverde, Col. San Benito, C.P. 83190, Hermosillo, Son. | 1 |
| 49 | Hermosillo | Paseo Rio Sonora # 159, Col. Hacienda de la Flor, C.P. 83090, Hermosillo, Son. | 1 |
| 50 | Hermosillo | Calle Dr. Paliza No. 44 esquina con Calle Londres, Col. Centenario, Hermosillo, Son., C.P. 83260. | 1 |
| 51 | Iguala | Mariano Matamoros No. 27, Centro, Iguala, C.P. 40000. | 1 |
| 52 | Iguala | Joaquín Baranda No. 47, Esq. García de la Cadena, Col. Centro, Iguala, Gro., C.P. 40000. | 1 |
| 53 | Irapuato | Prolongación Avenida Vicente Guerrero No. 3149, Fracc. Las Plazas, Irapuato, C.P. 36620, Gto. | 1 |
| 54 | Jalisco | Km. 17.5 de la carretera libre a Zapotlanejo, Colonia Complejo Penitenciario en Puente Grande,Jalisco, Puente Grande, C.P. 45427 | 1 |
| 55 | Jalisco | Periférico Pte S/N, Col. El Colli, A Inmediaciones del cerro El Colli, En El Municipio De Zapopan, Jal. C.P. 45036. | 4 |
| 56 | Jalisco | Av. Patria No. 1725, Piso 2, Col. Agraria, Guadalajara, Jal., C.P. 44667. | 1 |
| 57 | Jalisco  | Filadelfia Núm. 1297, Mezzanine 1Er. Piso, Col. Providencia, Sector Hidalgo, Guadalajara, Jal. C.P. 44620. | 1 |
| 58 | La Paz | Calle Concha Nacar No. 4520. entre Mar Caribe, Caracol Y calle Sin Nombre, Ala B, cuarto piso., Col. El Conchalito, La Paz, B.C.S., 23090. | 1 |
| 59 | León | Blvd. Adolfo López Mateos No. 1137 Ote., Colonia Coecillo, León, Guanajuato, C.P. 37260. | 1 |
| 60 | León | Blvd. Adolfo López Mateos 915, Oriente, Coecillo, León, Gto., C.P. 37260. | 1 |
| 61 | Los Mochis | Edificio Terranova, Blvd. Adolfo Lopez Mateos 2213 Norte | 1 |
| 62 | Matamoros | Av. Pedro Cárdenas N215 Esq. Av. Longoria, Col. Fracc. Victoria Matamoros Tamaulipas  | 1 |
| 63 | Mazatlán | Rio Baluarte No. 1000, Fraccionamiento Telleria, Mazatlán, Sin. C.P. 82017 | 1 |
| 64 | Mazatlán | Rio Baluarte No. 1220 Fraccionamiento Telleria, Mazatlán, Sin. C.P. 82017 | 1 |
| 65 | Mazatlán | Rio Quelite No. 31 Fracc. Telleria, Mazatlán, Sin. C.P. 82017 | 1 |
| 66 | Mazatlán  | Rio Quelite 27. Fraccionamiento Telleria, Mazatlán, Sin. C.P. 82017 | 1 |
| 67 | Mérida | Calle 47 No. 575H Por 84ª, Col. Santa Petronila, Yucatán, Mérida, C.P. 97070  | 1 |
| 68 | Mexicali | Calle Hospital No 594, Col. Zona Industrial, Centro Cívico, C.P. 2100. Mexicali. B.C. | 1 |
| 69 | Mexicali | Av. L. Montejano No. 1342, Fracc. Fovissste Torres Del Sol, Mexicali, B.C. | 1 |
| 70 | Monclova | Calle Hermosillo No. 5 Esq. Blvd. Benito Juárez No. 601 , 2 Piso, Palma, Monclova, 25730. | 1 |
| 71 | Monterrey | Av. Constitución No. 241 Pte., Zona Centro, Monterrey, N.L., C.P. 64000. | 1 |
| 72 | Monterrey | Av. Chimenea No. 201, Fracc. Centrika, Segundo Sector, C.P. 64550, Monterrey, Nuevo León. | 1 |
| 73 | Monterrey | Mariano Escobedo 201 Sur / con Modesto Arreola, Zona Centro, Monterrey, N.L., C.P. 64000. | 1 |
| 74 | Monterrey | Diagonal Santa Engracia No. 221, Col. Lomas de San Francisco, Monterrey, N.L., C.P. 64710 | 2 |
| 75 | Morelia | Calle Lacas de Uruapan No 31, Colonia Vasco de Quiroga, Morelia, Mich., C.P. 58000. | 1 |
| 76 | Morelia | Av. Camelinas No. 3550 Planta Baja, Col. Club Campestre, Morelia, Mich., C.P. 58270. | 1 |
| 77 | Naucalpan | Blvd. Toluca No. 4, Col. Industrial Naucalpan, Edo. De México, C.P. 53370. | 2 |
| 78 | Naucalpan | Av. 16 de Septiembre No.784, Col. Industrial Alce Blanco, Naucalpan, C.P. 53560. | 1 |
| 79 | Naucalpan | Calle Cuatro No. 25, Fracc. Industrial Alce Blanco, Naucalpan de Juárez, C.P. 53370. | 1 |
| 80 | Nogales | Plutarco Elías Calles Y Lopez Mateos 3Er Piso., Col. Centro, Nogales, Son., C.P. 84000. | 1 |
| 81 | Nuevo Laredo | Av. Paseo Colon 3360, Col. Jardín, Nuevo Laredo., C.P. 88260. | 1 |
| 82 | Nuevo Laredo | Avenida Ocampo No. 1701, 1er. Piso, Fracc. Ojo Caliente, Nuevo Laredo, Tamps., C.P. 88040. | 1 |
| 83 | Oaxaca | Privada de Aldama No. 106, Col. Paraje El Tule, Municipio San Bartolo Coyotepec, Oaxaca, Oaxaca. | 2 |
| 84 | Pachuca | Blvd. Luis Donaldo Colosio No. 1209, Edificio A, Planta Baja, Reserva Aquiles Serdán, Pachuca, Hgo., C.P. 42084. | 1 |
| 85 | Piedras Negras | Calle Rio Lerma No. 2610, Nueva Americana, Piedras Negras, Coah., C.P. 26070. | 1 |
| 86 | Poza Rica | Av. Palmas Preparatoria esquina Tajín S.N., Fracc. Palmas, Poza Rica, Ver., C.P. 93230. | 1 |
| 87 | Puebla | Av. 23 Poniente No. 2509, Los Volcanes, Puebla, C.P. 72410. | 1 |
| 88 | Puebla | Av. Osa Menor No. 82, Ala Norte, Ciudad Judicial Siglo XXI, Reserva Territorial Atlixcáyotl, Puebla, C.P. 72810. | 1 |
| 89 | Puebla | Blvd. Hermanos Serdán No. 2, Segundo Piso, Colonia Real Del Monte, Puebla, C.P. 72060. | 1 |
| 90 | Querétaro | José Siurob No. 13, Alameda, Querétaro, C.P. 76040, Querétaro, Qro.  | 1 |
| 91 | Querétaro | Av. Fray Luis de León No. 2880, Col. Centro Sur, Ciudad De Querétaro, Qro. C.P. 76090. | 1 |
| 92 | Querétaro | Allende Norte No.1, Centro, Querétaro, C.P.76000. | 1 |
| 93 | Reynosa | Calle Oriente 2 No. 725 Col. Aztlán, Reynosa, Tamaulipas, C. P. 88740. | 1 |
| 94 | Reynosa | Av. De Los Encinos No. 800, casi esquina con Boulevard Hidalgo, Col. Loma Real de Jarachina Norte, Reynosa, Tamaulipas. | 1 |
| 95 | Reynosa | Calle Francisco I. Madero No. 500 esquina con Terán, Zona Centro, Reynosa, C.P. 88500. | 1 |
| 96 | Reynosa | Blvd. Morelos esquina con Occidental No. 2340, Ampliación Rodríguez, Reynosa, Tamaulipas, C.P. 88630. | 1 |
| 97 | Reynosa | Dr. Jose Luis Gonzalez No.391, Fracc. Electricistas, Reynosa, C.P. 88690. | 1 |
| 98 | Salina Cruz | Av. Tampico Núm. 106, Colonia Centro, Salina Cruz, Oaxaca, C.P. 70600. | 1 |
| 99 | Saltillo | Boulevard Nazario Ortiz Garza No. 910, Col. Saltillo 400, Edificio 3, Piso 1, Saltillo, Coahuila, C.P. 25290. | 1 |
| 100 | San Luis potosí | Calle Palmira S/N Frente Principal Y Derecho De Vía, C.F.E. Fraccionamiento Desarrollo del Pedregal, San Luis Potosí, S.L.P. C.P. 78295 | 1 |
| 101 | San Luis Potosí | M. Abasolo No. 414 Segundo Piso, Zona Centro, Ciudad Valles, S. L. P., C.P. 79000 | 1 |
| 102 | San Luis potosí  | Av. Muñoz No. 650 (Plaza Muñoz, Planta Alta), Matehuala (antes Fracc. La Loma), San Luis Potosí, S.L.P., C.P. 78170. | 1 |
| 103 | Sinaloa | Avenida Olas Altas 1300, Torre Principal 1° Y 2° Pisos, Centro, Mazatlán, Sinaloa, C.P. 82000. | 2 |
| 104 | Sonora  | Calle 9 No. 3801, Avenida 38 Esq., Col. Luis Donaldo Colosio, Agua Prieta, C.P. 84270. | 1 |
| 105 | Tampico | Calle Altamira No. 611 Poniente esquina con Alfredo E. Gochicoa, Zona Centro, Tampico, Tamps., C.P. 89000. | 1 |
| 106 | Tapachula | Tercera Calle Oriente No. 23 Esq. Tercera Avenida Norte, Col. Centro, Tapachula, Chiapas, C.P. 30700. | 1 |
| 107 | Tepic | Calle Álamo No. 127, San Juan, Tepic, Nayarit, C.P. 63130. | 1 |
| 108 | Tepic | Avenida Insurgentes No.868 Pte, Fracc. La Huerta Residencial, Tepic, Nayarit, C.P. 63070. | 1 |
| 109 | Tepic | Av. México No. 308, Col. San Antonio, Tepic, Nay.  | 1 |
| 110 | Tepic | Blvd. Tepic-Xalisco No. 521 Sur, Caja de Agua, Tepic, Nayarit, C.P. 63158.  | 1 |
| 111 | Tepic | Cefereso No. 4 de Tepic, Carretera Libre Tepic, Mazatlán, Km.10.6, Ejido El Rincón, Tepic, Nayarit. | 1 |
| 112 | Tepic | Av. Las Brisas No. Ext. 40, Interior 42., Fracc. Las Brisas, Plaza Comercial Fiesta Tepic., C.P. 63117. | 1 |
| 113 | Tijuana | Leona Vicario Y esquina con Vía Rápida Poniente Número 1426, Zona Río Tijuana, B.C., C.P. 22010 | 1 |
| 114 | Tijuana | Av. Paseo de los Héroes No. 10105 9No. Piso, Zona Río Tijuana, B.C., C.P. 22010 | 1 |
| 115 | Tijuana | Dr. Atl, Numero 2084, 7Mo. Piso Zona Rio, Tijuana, B.C., C.P. 22010 | 1 |
| 116 | Tijuana | Av. Paseo De Los Héroes No.10540, 2º. Piso, Zona Rio, Tijuana, B.C., C.P. 22010 | 1 |
| 117 | Tlaxcala | Municipio de Apizaco, Tlaxcala, ubicado en Carr. 136, Libramiento A Huamantla, pasando El Puente Rio Zahuapan, Manzana IV, Lote 1. | 2 |
| 118 | Tlaxcala | Benito Juárez No 53, Col. Centro, Tlaxcala, Tlaxcala C.P. 90000 | 1 |
| 119 | Tlaxcala | Calle Miguel Hidalgo No. 36 Col. Centro Tlaxcala, Tlax. C.P. 90000 | 1 |
| 120 | Tlaxcala | Avenida Ocotlán N° 9, Ocotlán; Tlaxcala, Tlax. C.P. 90100 | 1 |
| 121 | Tlaxcala | Carretera a Ocotlán N° 21, San Gabriel Cuahutla, Tlaxcala, Tlax. C.P. 90117 | 1 |
| 122 | Tlaxcala | Segunda Privada de Cedros N° 9, San Buenaventura Atempan, Tlaxcala, Tlax. C.P. 90010 | 1 |
| 123 | Tlaxcala | Av. Guerrero Lote No. 56 Esq. Mariano Sánchez, Col. Centro, Tlaxcala, Tlaxcala, C.P. 90000. | 1 |
| 124 | Toluca | Dr. Nicolás San Juan No.104, 1Er. Piso Col. Ex-Rancho Cuauhtémoc Toluca, Edo. de México. C.P. 50010 | 1 |
| 125 | Torreón | Blvd. Independencia No. 2111 Ote., Colonia San Isidro, Torreón, Coahuila, C.P. 27100. | 1 |
| 126 | Tuxpan | Avenida Independencia (Calle Manuel Maples Arce) No. 188, Col. Rodríguez Cano, Tuxpan, Ver., C.P. 92880. | 1 |
| 127 | Tuxtla Gutiérrez | Edificio del Poder Judicial de Tuxtla Gutierrez, Boulevard Angel Albino Corzo N°2641, Col. Las Palmas, Tuxtla Gutierrez, Chis. C.P. 29040 | 1 |
| 128 | Tuxtla Gutiérrez | Segunda Sur Oriente No. 990, Barrio San Roque, Tuxtla Gutiérrez, Chiapas, C.P. 29000. | 1 |
| 129 | Uruapan | Carretera Uruapan-Pátzcuaro No. 1380 Col. Fracc. Lomas del Valle Uruapan, Mich. C.P. 60110 | 1 |
| 130 | Veracruz | Avenida S.S. Juan Pablo II No. 646 Esq. Tiburón, Colonia Fraccionamiento Costa de Oro, Boca del Río, Veracruz, C.P. 94299. | 1 |
| 131 | Villahermosa | Av. Malecón Lic. Carlos Alberto Madrazo Becerra No. 729, Col. Centro, Villahermosa, Tab. C.P. 86000 | 1 |
| 132 | Villahermosa | Av. Adolfo Ruíz Cortines No. 917, casi esquina con Av. Pagés Llergo, Villahermosa, Tabasco. | 1 |
| 133 | Villahermosa | Calle Reforma No. 100 esquina con Av. Gregorio Méndez Magaña, Col. Atasta de Serra, Villahermosa, Tabasco., C.P. 86100. | 1 |
| 134 | Villahermosa | Av. Malecón Leandro Rovirosa Wade S/N Esq. Juan Jovito Pérez Col. Gaviotas, Villahermosa, Tab. C.P. 86090 | 1 |
| 135 | Xalapa | Av. Culturas Veracruzanas No. 120, Col. La Reserva, Xalapa, Ver., C.P. 91096. | 1 |
| 136 | Xalapa | Cefereso No. 5, Lerdo de Tejada S/N Congregación Cerro de León, Villa Aldama, Ver. C.P. 91345 | 1 |
| 137 | Xalapa | Ruiz Cortines # 1628 Col. Ferrer Guardia Xalapa, Ver. C.P. 91020 | 1 |
| 138 | Zacatecas | Calle Lateral No. 1202, Planta Baja Torre A, Col. Cerro del Gato, Ciudad Gobierno, C.P. 98160, Zacatecas, Zac. | 1 |
| 139 | Veracruz | Heroico Colegio Militar No. 401 Y 403 esquina Ignacio Zaragoza, Col. Centro, Coatzacoalcos, Ver. C.P. 96400 | 1 |
| 140 | Veracruz | Libertad No. 12, Esq. Av. Cuauhtémoc, Col. Burocrática, Tuxpan, Veracruz, C.P. 92880. | 1 |
| 141 | Tijuana | Paseo de los Héroes No. 10093, Esq. José Clemente Orozco, Local 9, Zona Río, C.P. 22320, Tijuana, B.C. | 1 |
| 142 | Colima | Calzada Pedro A. Galvan N° 239 Norte, Col. Centro, C.P. 28000 Colima, Col. | 1 |
| 143 | Colima | Av. Tercer Anillo Periférico 672, Fracc. Valle Dorado | 1 |

|  |
| --- |
| **PARTIDA 7** |
| **Csvo.** | **Ciudad** | **Domicilio** | **Cantidad** |
| **1** | Ciudad de México | Antiguo Camino a Culhuacán No. 202, Col. Santa Isabel Industrial, Delegación Iztapalapa, C.P. 09820. Ciudad de México. | 1 |

H. Evaluación técnica de prototipos

H.1 PRESENTACIÓN DE MUESTRAS O PROTOTIPOS

Los bienes de las **partidas 1 a la 7** serán objeto de evaluación mediante la documentación solicitada en el presente Anexo Técnico, sin que se requiera la presentación de muestras o prototipos.

H.2 PROCESO DE EVALUACIÓN DE MUESTRAS O PROTOTIPOS

**En el presente procedimiento no se requiere la presentación de muestras o prototipos.**

I. Modelos de cartas

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 1**

**Entrega de bienes idénticos**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No.\_\_\_, manifiesto que los bienes y servicios ofertados se entregarán, en caso de resultar adjudicado, de la marca y con características idénticas a aquellas contempladas tanto en nuestra propuesta como en las especificaciones técnicas establecidas en el presente Anexo Técnico.

(Razón social)

**Nombre, Firma y Cargo.**

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 2**

**Componentes y partes originales.**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No. \_\_\_, manifiesto que, en caso de ser adjudicado, los bienes y/o servicios ofertados se entregarán con todos y cada uno de sus componentes y partes, originales de fábrica, nuevos y certificados por el fabricante.

Así mismo, garantizamos a ustedes la existencia y surtimiento, por un período mínimo de tres años, de todas las partes y refacciones originales y certificadas por el fabricante que sean requeridas para que los bienes ofertados, en caso necesario, puedan ser reparados debidamente.

(Razón social)

**Nombre, Firma y Cargo.**

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 3**

**Certificación de calidad**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No. \_\_\_, manifiesto que los [bienes / productos] ofertados, cumplen con las normas o estándares de calidad \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [p.e- ISO 9001:2000 **o** ISO 9001:2008 **o** NMX-CC-9001-IMNC-2000 **o** NMX-CC-9001-IMNC-2008 **o** superiores **o** las correspondientes internacionales], anexando a la presente copia simple del documento vigente.

(Razón social)

**Nombre, Firma y Cargo.**

(Papel membretado del fabricante)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 4**

**Distribuidor Autorizado**

Por medio de la presente y en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No. \_\_\_, confirmamos que la empresa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, es *Distribuidor Autorizado* de nuestros Productos y servicios, encontrándose capacitada para proporcionar asistencia técnica, así como los servicios relacionados con tales productos.

En virtud de lo anterior, le otorgamos a nuestro distribuidor el más amplio respaldo para que en su caso, esté en aptitud de entregarles el número de bienes y/o servicios ofertados, así como respecto a la asistencia técnica que les deberá proporcionar, reiterando las garantías con que cuentan de fábrica, entrega y prestación de los bienes y/o servicios correspondientes a las soluciones y/o equipos de que se trata o las que dicho distribuidor se haya comprometido a otorgar en su propuesta técnica. Lo anterior conforme a lo establecido en las bases de adquisición y su Anexo técnico.

Así mismo, manifestamos a ustedes nuestro compromiso de mantener en el mercado, por un mínimo de cinco años a partir de la fecha, las partes y refacciones necesarias para que los equipos ofertados puedan ser, en caso necesario, debidamente reparados.

(Razón social del fabricante)

**Nombre, Firma y Cargo.**

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 5**

**Instalación**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No. \_\_\_, manifiesto que, en caso de ser adjudicado, la instalación y puesta a punto de los bienes y/o servicios ofertados se realizará a satisfacción del Consejo de la Judicatura Federal.

(Razón social)

**Nombre, Firma y Cargo.**

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 6**

**Carta de cumplimiento de términos y condiciones de las garantías y servicios**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No.\_\_\_\_\_\_\_\_\_\_ descripción\_\_\_\_\_\_\_:

1. Manifiesto que he leído, entendido y estoy de acuerdo en cumplir con los términos y condiciones solicitados para las garantías y servicios, conforme a lo establecido en estas bases de adquisición.
2. Así mismo, en caso de aplicación de la garantía, seré responsable del retiro, traslado y seguimiento de la reparación o sustitución de dichos bienes, todo esto sin que represente costo adicional alguno para el Consejo de la Judicatura Federal.

A t e n t a m e n t e

(Razón social)

**Nombre, Firma y Cargo.**

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 7**

**Carta de cumplimiento de términos y condiciones de entrega de bienes**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la(s) partida(s) No. \_\_, manifiesto que he leído, entendido y estoy de acuerdo en prestar los servicios de entrega de bienes y/o servicios, conforme a lo establecido en el presente Anexo técnico.

(Razón social)

**Nombre, Firma y Cargo.**

(Papel membretado del Centro de Servicio)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 8**

**Carta del Centro de Servicio que apoyará para brindar los servicios de garantía**

El que suscribe C. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en mi carácter de representante legal, en relación con el procedimiento de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, manifiesto que en caso de adjudicación a la empresa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ participante en la adquisición, la apoyaremos y brindaremos los servicios de garantía a los bienes y/o servicios de la(s) partida(s) No. \_\_\_ (\_\_\_\_\_\_\_\_\_\_descripción\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) a través de nuestro centro de servicio ubicado en (\_\_\_\_\_\_\_\_\_\_\_domicilio completo, ciudad y teléfonos\_\_\_\_\_\_\_\_\_\_\_\_). Así mismo reitero que tenemos conocimiento de la adquisición antes mencionada y que brindaremos los servicios señalados conforme a lo estipulado en el presente Anexo técnico.

(Representante legal)

**Nombre, Firma**

(Papel membretado de la empresa)

Ciudad de México, a \_\_\_ de \_\_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

**Carta No. 9**

**Personal capacitado y especializado**

Por medio de la presente y en relación con el proceso de adjudicación No. \_\_\_\_\_\_\_\_\_\_\_, para las partida \_\_\_\_\_\_\_\_\_\_, confirmamos que la empresa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, cuenta con personal capacitado y especializado para la instalación y configuracíón de los bienes y soluciones solicitados en el presente procedimiento.

**(Razón Social)**

**Nombre, Firma y Cargo**

J. Formatos

**FORMATO 1**

**Descripción detallada de los bienes ofertados**

(Papel membretado de la empresa)

Ciudad de México, a \_\_ de \_\_\_\_\_\_\_\_ de 20\_\_

CONSEJO DE LA JUDICATURA FEDERAL

**P R E S E N T E**

Se presenta la propuesta de bienes ofertados por la empresa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de acuerdo a lo solicitado en las bases de la Licitación Pública Nacional No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, para la Partida No.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Descripción) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Marca: (La marca ofertada) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Modelo: (El modelo ofertado) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cantidad de bienes ofertados: \_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Núm.** | **DESCRIPCIÓN DEL BIEN OFERTADO POR EL PROVEEDOR** |
|  |  |
| **1** |  |
| **2** |  |
| **3** |  |
| **…** |  |
| **N** |  |

Para estos bienes, acorde con lo señalado en bases de licitación, se proveerán los siguientes servicios:

|  |  |
| --- | --- |
| **Núm.** | **SERVICIOS OFERTADOS POR EL PROVEEDOR** |
| **1** |  |
| **2** |  |
| **…** |  |
| **N** |  |

El Representante Legal

(Razón social)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Nombre y Firma**

**FORMATO 2**

**Relación de centros de servicio**

**INSTRUCTIVO:** Completar la Razón Social, Domicilio (deberá contar con todos los datos de la ubicación del centro de servicio, incluyendo ciudad y estado invariablemente) y teléfonos del centro de servicio a diez dígitos, nacional o 01-800 (sin cargo para el Consejo de la Judicatura Federal). Anexar **en la Sección III, subíndice III.5*,* señalado en el apartado**“***C. Estructura de la propuesta*”, UNA CARTA POR CADA CENTRO DE SERVICIO.**

|  |  |  |
| --- | --- | --- |
| **Partida** | **Ciudades que deben contar con centros de servicio** | **CENTRO DE SERVICIO OFERTADO POR EL PARTICIPANTE** |
|
| **Partida N** |  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |

**FORMATO 3**

**Relación de centros de servicio para las ciudades restantes (“*Cuadro de distribución*”)**

**INSTRUCTIVO:** Completar la Razón Social, Domicilio (información completa de la ubicación, incluyendo ciudad y estado, invariablemente), además, número telefónico a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal), indicando cual(es) centro(s) brindará(n) atención a cada ciudad que no cuente con centro de servicio en la localidad.

|  |  |  |
| --- | --- | --- |
| **Partida** | **Ciudades restantes del apartado G** | **ATENDIDA DESDE** |
| **Partida N°.** |  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |
|  | Razón social:Dirección:Teléfono(s) a diez dígitos o 01-800 (sin cargo para el Consejo de la Judicatura Federal): |

K. Penas y deductivas

**J.1 PENAS Y DEDUCTIVAS**

Para el presente procedimiento de adquisición, la pena convencional se aplicará de conformidad con lo dispuesto en los artículos 409 y 410 del *“Acuerdo General del Pleno del Consejo de la Judicatura Federal, que establece las disposiciones en materia de actividad administrativa del propio Consejo”*.

El incumplimiento de cualquiera de las obligaciones adquiridas por parte del proveedor en los contratos o pedidos, dará lugar a la imposición de una pena convencional.

En caso de incumplimiento parcial, la pena se ajustará proporcionalmente al porcentaje incumplido.

Las penas convencionales en ningún caso podrán ser superiores, en su conjunto, al monto de la garantía de cumplimiento.

La pena convencional se calculará tomando como base el importe de los bienes y servicios que únicamente se encuentren pendientes de entrega, en la fecha fijada para el cumplimiento. Esta base se multiplicará por diez al millar diario hasta el cumplimiento total. El importe resultante de la base será ajustado de manera proporcional al cumplimiento pendiente aplicando la misma fórmula.

**L. Supervisión, control y seguimiento**

L.1. SUPERVISIÓN, CONTROL Y SEGUIMIENTO.

Considerando las condiciones de entrega de bienes y/o servicios y garantías solicitadas en el presente anexo técnico, se informa a los participantes que, los rubros sujetos a supervisión, para los bienes y software solicitados, serán los siguientes:

* Plazo de entrega.
* Validación de las características técnicas de los bienes y/o servicios y sus componentes, así como del software.
* Entrega de los bienes y sus componentes, así como del software.
* Instalación, configuración y puesta a punto de los bienes y sus componentes.
* Seguimiento a la atención de garantías.

Los mecanismos de supervisión y medios documentales para acreditar el cumplimiento de las obligaciones contractuales y la validación de los bienes para efectos de pago se realizarán de la siguiente forma:

* Una vez adjudicados los bienes, se revisarán de manera conjunta por parte de la Dirección de Almacenes (**DAL**) y la Dirección de Seguridad Informática (**DSEI**), conforme a sus atribuciones, debiendo ésta última como área técnica, revisar que los bienes y sus componentes, así como el software, sean idénticos en sus características, marca y modelo, a lo conforme al Anexo Técnico.

Una vez realizada la revisión, el personal de la **DAL** integrará un acta, a la cual se anexará la(s) cédula(s) de verificación de las características técnicas realizada(s) por **DSEI**.

* **El participante adjudicado** entregará e instalará (**en las partidas que así lo requieran**), los bienes dentro del plazo establecido de acuerdo a lo solicitado en el **apartado G. “Cuadro de distribución”** del presente Anexo Técnico, y deberá ajustarse a los procedimientos que defina la Dirección de Almacenes (**DAL**), la documentación que entregue el proveedor, deberá contar con los siguientes datos como mínimo, cantidad, descripción, marca, modelo, número de parte, números de serie e inventario, respetando los lineamientos que indique la **DAL**, el trámite de pago será de acuerdo a las directivas que establezca la Dirección antes mencionada.
* Personal de la Dirección de Seguridad Informática **(DSEI),** recibirá los bienes, en el sitio correspondiente, de acuerdo a la logística de entrega-recepción definida por la **DAL**.
* El participante adjudicado, realizará la instalación y configuración de los bienes para **todas las partidas que así lo requieran** y será el responsable de remitir los resguardos originales a la **DAL**, personal designado de la Dirección de Seguridad Informática **(DSEI)** supervisará la instalación de los bienes para todas las partidas que así lo requieran.

**Supervisión y seguimiento de garantías.**

Los rubros sujetos a supervisión y seguimiento serán:

* Una vez que el proveedor entregue los bienes y/o servicios, deberá cumplir con los términos y condiciones establecidas en el apartado **F. Características de las garantías y servicios**.

Los mecanismos de supervisión y medios documentales para acreditar el cumplimiento de las obligaciones contractuales se realizarán de la siguiente forma:

* De acuerdo a lo descrito en el apartado F., el participante que resulte adjudicada deberá entregar a la **DGTI,** los informes y órdenes de servicios que reflejen los eventos de garantía prestados, los cuales serán validados por el personal de la Dirección de Seguridad Informática **(DSEI),** en caso de incumplimiento, se le notificará de manera oficial (correo electrónico o en su caso vía oficio) al participante adjudicado, para que subsane la incidencia; de no atender la solicitud, la **DSEI** notificará la situación por oficio a la **Dirección General de Recursos Materiales**, para que procedan las sanciones que correspondan (penalizaciones).

|  |  |
| --- | --- |
| Elaboró**Lic. Luis Francisco Villa Freyssisnier** Subdirector de Plan de Recuperación de Desastres | Revisó**Ing. Eduardo César Mendoza Ramírez**Encargado de la Dirección de Seguridad Informática. |
| Validó**Lic. Felipe de Jesús Hernández Medina.**Coordinador de Soporte y Continuidad Operativa. |