entrerios GOBIERNO

IAFAS INSTITUTO DE AYUDA FINANCIERA A LA ACCIÓN SOCIAL

INSTITUTO DE AYUDA FINANCIERA A LA ACCIÓN SOCIAL

LICITACIÓN PRIVADA Nº 21/2023

Renovación, ampliación e implementación de Solución de Antivirus Corporativo para Sede central I.A.F.A.S., Casinos y Salas Tragamonedas.

PLIEGO de CONDICIONES PARTICULARES

ARTICULO 1°: OBJETO.

El presente llamado a Licitación Privada tiene por objeto la renovación de la solución de Antivirus "Eset" corporativo, ampliando las características de seguridad de la versión actual para implementarse en Sede central I.A.F.A.S., Casinos y Salas Tragamonedas ubicados en la provincia de Entre Ríos.

ARTICULO 2°: DESCRIPCION Y CANTIDADES

En el PLIEGO TÉCNICO de la presente licitación, se determinan las especificaciones técnicas de los bienes a proveer. Allí se describen las características técnicas mínimas y cantidad; pudiendo el OFERENTE presentar ofertas cuyas características superen o mejoren las aquí solicitadas.

ARTICULO 3°: DOCUMENTACION TECNICA.

El OFERENTE junto con su propuesta deberá presentar folletos, catálogos, CDs y/o DVDs informativos, métodos y manuales de instalación, así como cualquier otra documentación técnica que permita evaluar si lo ofertado se ajusta a lo solicitado en el **ARTÍCULO 2°**.

El no cumplimiento de este requisito será motivo suficiente para la no consideración de la oferta.

ARTICULO 4°: PRESENTACION.

La propuesta deberá presentarse en sobre u otro contenedor cerrado y lacrado, señalándose en la cubierta el número y objeto de la Licitación, día y hora de apertura de la misma.

Dicho sobre contendrá el Presupuesto detallado, con cantidades en letras y números coincidentes con el total de la oferta; además de los correspondientes comprobantes de Garantía de Oferta y constancia actualizada de encontrarse inscripto en el Registro de

Proveedores del Estado Provincial (acorde al Art. 2º del P.C.G.) en caso de poseerla de años anteriores, deberá presentar su vigencia para el año en curso.

Será recibida en la División Mesa de Entradas del Instituto, calle 25 de Mayo 255 de la ciudad de Paraná, provincia de Entre Ríos, hasta el día y hora establecidos en la Licitación.

Las ofertas deberán elaborarse, respetando el ordenamiento establecido, punto por punto, especificado en el presente Pliego. El OFERENTE podrá presentar una cotización adicional del equipamiento, que será considerada como alternativa, la que a juicio del I.A.F.A.S. podrá ser tenida en cuenta o rechazada, siempre y cuando presente la Oferta Base.

El no cumplimiento de este requisito será motivo suficiente para la no consideración de la oferta.

ARTICULO 5º: ACEPTACIÓN.

La sola presentación de oferta implica la aceptación lisa y llana de todos y cada uno de los artículos que conforman el presente **Pliego de Condiciones Particulares (P.C.P.) y el Pliego de Condiciones Generales (P.C.G.).-**

ARTICULO 6º: FORMA DE COTIZAR.

En la propuesta económica deberá especificarse claramente el precio unitario y total de lo cotizado de acuerdo al siguiente desglose:
Se deberán incluir además las especificaciones y detalles (marca, modelo, calidad, garantía, etc.) que permitan una correcta evaluación de lo ofrecido.
La cotización por precio unitario y total deberá estar expresada en moneda Argentina y/o Extranjera autorizada, en cuyo caso a efectos de la comparación deberá indicarse con precisión, el tipo de cambio vendedor vigente al cierre del día anterior a la presentación. A los fines de la facturación deberá ser expresada en moneda Argentina, el Instituto es sujeto **EXENTO** frente al Impuesto al Valor Agregado (I.V.A.).-

ARTICULO 7º: GARANTIA de OFERTA.

Para afianzar el cumplimiento de todas las obligaciones, los proponentes deberán presentar una garantía de oferta, que será del **uno (1%) por ciento** del valor total cotizado.

En caso de cotizaciones alternativas, las garantías se calcularán sobre el mayor valor propuesto. La garantía o su comprobante respectivo según el caso, será adjuntada a la propuesta.

A los fines de la aplicación de lo establecido en el presente deberán remitirse a lo establecido en el Pliego de Condiciones Generales Artículos 22° ;24°; 25°; 26° y 27°.-

ARTICULO 8°: VALIDEZ de la OFERTA.

La oferta presentada tendrá validez plena por **treinta (30) días hábiles** contados desde la apertura de la Licitación.

Vencido dicho término sin que se hubiese resuelto la adjudicación, los OFERENTES que se acojan a lo estipulado en este artículo y opten por el desistimiento de sus propuestas lo comunicarán por escrito al Instituto, caso contrario se tendrá por válida la misma.-

ARTICULO 9°: LUGAR y PLAZO de ENTREGA.

En las respectivas propuestas los señores OFERENTES deberán indicar el plazo de entrega de los elementos ofertados, el que no podrá exceder los sesenta **(60) días hábiles** contados a partir de la notificación de la adjudicación mediante la orden de compra pertinente.

La entrega de esta adquisición será controlada y verificada por personal de la Coordinación de Sistemas Informáticos del Instituto.

La contratación incluye todos los gastos que se originen por fletes, acarreos, descargas, entregas e instalaciones.-

ARTICULO 10°: FORMA de ADJUDICACIÓN.

La adjudicación podrá ser otorgada por la totalidad de la compra a un único OFERENTE.

La adjudicación se hará por ítem como consecuencia de la comparación de las ofertas presentadas al acto respectivo y de conformidad a lo previsto en el Pliego de Condiciones Generales.

La presentación de una sola oferta no invalidará el acto licitatorio y podrá ser adjudicado.

ARTICULO 11°: GARANTIA de ADJUDICACIÓN.

El adjudicatario deberá dentro del plazo de **diez (10) días hábiles** contados a partir de la fecha de notificación de la adjudicación, constituir una garantía de adjudicación conforme lo previsto en el Artículo 22° inciso b) del Pliego de Condiciones Generales y por un valor equivalente al **cinco por ciento (5%) del valor total que fuera adjudicado**, en cualquiera de las modalidades previstas por el Artículo 26° del Pliego de Condiciones Generales.

La presente garantía será restituida al adjudicatario dentro de los diez (10) días de la recepción total de lo adjudicado.

ARTICULO 12°: PENALIDADES y/o MULTAS.

Si el adjudicatario no cumpliera con el plazo de entrega estipulado, se le aplicarán las siguientes multas:

- **el equivalente al tres por mil (3 ‰) diario del valor total de la facturación durante los diez (10) primeros días**
- **el equivalente al cinco por mil (5 ‰) diario del valor total de la facturación durante los diez (10) días siguientes**
- **el equivalente al diez por mil (10 ‰) diario del valor total de la facturación durante los diez (10) días siguientes**

Además de las sanciones estipuladas en el Capítulo XIII y Capítulo XIV de la Reglamentación de Contratación del Estado (Decreto N° 795/96 M.E.O.S.P.).-

ARTICULO 13°: SELLADOS e IMPUESTOS.

En oportunidad de hacerse efectivo el pago de las facturas, el Instituto retendrá los impuestos que corresponden de acuerdo a las Leyes Impositivas vigentes, debiendo el adjudicatario acreditar el pago de los Impuestos Provinciales y Nacionales de los cuales fuera responsable.-

ARTICULO 14°: FORMAS de PAGO.

El pago al proveedor se realizará en el Dpto. Tesorería del Instituto previa entrega y aceptación de lo que le fuera adjudicado; en cumplimiento de los trámites administrativos corrientes y presentación por parte del adjudicatario de la pertinente factura con arreglo a las normas impositivas vigentes.

El pago se realizara en Pesos Moneda Nacional, mediante transferencia bancaria a la cuenta de la empresa adjudicataria.

En el caso de que se hubiera efectuado la adjudicación en moneda extranjera autorizada, de acuerdo con el precio que fuera cotizado, a los efectos de la presentación de la factura correspondiente se deberá efectuar la conversión del precio adjudicado en moneda extranjera a moneda nacional, utilizando para ello el tipo de cambio vendedor publicado por el Banco de la Nación Argentina el día anterior al de la emisión de la misma.
Para su realización será indispensable la presentación ante el Instituto , del Certificado de Libre Deuda Fiscal para Proveedores del Estado o Certificado de Regularización de Deuda para Proveedores del estado, emitido por la Administradora Tributaria de Entre Ríos, conforme a las Resoluciones vigentes de ATER

El pago será efectuado dentro de los treinta (30) días corridos de la fecha de recepción de la correspondiente documentación.

Los señores OFERENTES en su propuesta podrán ofrecer descuentos por pronto pago solo para los siguientes plazos:

- **Por pago a los diez (10) días corridos de la fecha de recepción de la correspondiente documentación.-**
- **Por pago a los quince (15) días corridos de la fecha de recepción de la correspondiente documentación.-**
- **Por pago a los veinte (20) días corridos de la fecha de recepción de la correspondiente documentación.-**

El Instituto no reconocerá ningún aumento en el precio de lo cotizado durante el tiempo de mantenimiento de la oferta y/o del plazo de provisión, según corresponda cualquiera sea la denominación que se utilice para aumentar el valor de los bienes cotizados. La presentación de la propuesta implica que el OFERENTE renuncia en forma expresa a cualquier reclamo de aumento en el precio cotizado cualquiera sea su origen, incluidos los acontecimientos imprevisibles o extraordinarios.

ARTICULO 15º: CONSULTAS y ACLARACIONES.

Las consultas y aclaraciones en forma personal, podrán efectuarse en días hábiles administrativos en la ciudad de Paraná – 25 de Mayo N° 255 – Tel: (0343)4201188, durante el horario de 09:00 a 12:00 horas, previamente haber sido informado a la Coordinación de Sistemas Informáticos del I.A.F.A.S.

Las consultas y aclaraciones en forma electrónica podrán efectuarse vía mail a: *mmandel@iafas.gov.ar - abarbera@iafas.gov.ar -*

DOC H8 GAC CPR 002

C.P.N. GUILLERMO A. DUBRA
DIRECTOR
I.A.F.A.S.

Cdor. SILVIO ORESTES VIVAS
Presidente
I.A.F.A.S.

Dra. Victoria V. WOLF
Jefa Dpto. Despacho
I.A.F.A.S.

entrerios GOBIERNO

IAFAS INSTITUTO DE AYUDA FINANCIERA A LA ACCIÓN SOCIAL

PLIEGO DE ESPECIFICACIONES TÉCNICAS

Pliego Técnico

Renovación, ampliación e implementación de Solución de Antivirus Corporativo

El objeto de la presente es contratar la renovación de la solución de Antivirus **"Eset"** corporativo, ampliando las características de seguridad de la versión actual. La presente adquisición debe ser desplegada en la **Sede Central del I.A.F.A.S., Casinos y Salas Tragamonedas ubicados en la provincia de Entre Ríos.**

1. Consideraciones Generales

1.1 Prestaciones Tecnológicas

La solución de software adquirida deberá brindar protección a nivel de servidores, equipos de escritorio y dispositivos móviles por un término de 3 años con posibilidad de renovación por 3 años más. Se pretende un servicio corporativo 24x7x365 para la prevención y protección ante nuevas amenazas o incidentes derivados de estos.

1.2 Cantidad de equipamiento mínimo a Cubrir.

El total de equipamiento a cubrir por parte de la solución de antivirus solicitado, es de un parque informático de 550 equipos. De los cuales se cuenta con: *Equipos Desktop, dispositivos móviles,* ***Notebook con SO Mac OS X 10.x,*** *Servidores Windows y Servidores GNU/Linux*.

1.3 Plazo de ejecución.

El plazo máximo para la recepción, capacitación y puesta en marcha de lo solicitado, será de sesenta días (60) desde la notificación formal de la aceptación de la oferta.

Se debe contemplar como fecha para la implementación de licencias, la fecha de vencimiento de las licencias actuales: 15/03/2023.

1.4 Antecedentes del Proveedor.

El OFERENTE deberá acreditar al menos cuatro (4) años de experiencia en la provisión de soluciones corporativas de Antivirus adjuntando para tal motivo una carta del Fabricante que lo certifique como proveedor comercial habilitado e indicando que el mismo posee la capacidad de brindar los servicios de Soporte Técnico de la solución propuesta como así también la habilitación de escalar incidentes al Centro de Soporte del propio Fabricante.

El OFERENTE deberá incluir al menos tres (3) referencias comprobables de implementación del sistema Antivirus que hayan sido implementadas por el propio OFERENTE. Una de dichas referencias deberán ser sobre redes de más de 250 puestos, el resto podrán ser sobre redes de al menos 100 puestos. Sobre cada referencia deberá indicarse: fecha de la implementación, empresa donde se realizó, teléfono del contacto, cantidad de servidores y números de estaciones de trabajo.

El OFERENTE deberá disponer de personal técnico con Certificación Oficial del fabricante de la solución Antivirus debiendo incluir los certificados que acrediten tal condición.

1.5 Forma de cotizar.

La cotización por precio unitario y total deberá estar expresada en moneda Argentina o extranjera autorizada.

2. Consideraciones Técnicas

2.1 Solución basada en un solo fabricante

Se valorará que lo solicitado sea una solución integral de un mismo fabricante. En caso de ser una integración de productos distintos, el proveedor se hará cargo y

será el único responsable por todos y cada uno de los productos que conformen la solución integrada.

2.2 Compatibilidad de Software.

Sistemas Operativos para Desktop y portátiles	**Sistemas Operativos para Servidores**	**Sistemas Operativos para móviles**
Mac OS X 10.x	Windows 2012 Server (todas las versiones)	Android (4.0 o superior)
Windows 7 (todas las versiones)	Windows 2016 Server (todas las versiones)	
Windows 8 (todas las versiones)	Windows 2019 Server (todas las versiones)	
Windows 10 (todas las versiones)	Windows 2022 Server (todas las versiones)	
Windows 11 (todas las versiones)	GNU/Linux (Kernel 2.6 o superior)	

2.3 Instalación y Configuración.

Se deberán incluir dentro de la cotización las tareas de puesta en marcha, instalación y configuración de los equipos detallados a continuación, dejándolos a todos perfectamente operativos y funcionales.

Los equipos a implementar son:

- Un servidor de Antivirus.
- Una consola de Administración Central.
- Cinco (5) equipos de trabajo clientes, tanto Desktop como Servidores.
- Dos (2) dispositivos móviles corporativos.

Esta solicitud de instalación será realizada conjuntamente por la empresa proveedora y los técnicos de la Coordinación de Sistemas de I.A.F.A.S., para quienes esta práctica será complementaria a la capacitación teórica solicitada. Serán establecidos los días y horas a realizar la misma, por la Coordinación de Sistemas Informáticos del I.A.F.A.S.

Una vez concluida las tareas solicitadas de cada una de las partes intervinientes que conforman la solución de antivirus, será de carácter primordial que todos los equipos queden en condiciones máximas de prestaciones y seguridad (Consolas de Administración, Sistemas de Reportes y mecanismos de actualización con sus distribuciones automáticas). Teniendo como obligación la empresa proveedora de generar documentación que detalle los procedimientos realizados y los responsables intervinientes de ambas partes.

2.4 Métodos de análisis.

La solución de antivirus deberá ser capaz de realizar análisis de virus en tiempo real (poseer módulo residente), bajo demanda, programado o en forma remota. Incluyendo dispositivos de almacenamiento (discos rígidos locales, de red y extraíbles), memoria operativa del equipo, archivos, directorios, etc. Con la posibilidad de hacerlo solo sobre aquellos previamente seleccionados.
Deberá disponer de herramientas de línea de comando (CLI) para la exploración y limpieza de virus.

2.5 Perfiles de seguridad

- La solución debe contar con perfiles de seguridad de manera que haya al menos un grupo administrador y un grupo usuarios, como mínimo. Los perfiles deberán diferenciarse en los privilegios de operación.

- Solo los administradores podrán operar aspectos relacionados con la instalación, configuración y desinstalación del antivirus.
- Los usuarios no podrán deshabilitar ni interrumpir cualquier acción realizada por un administrador.

2.6 Detección y Eliminación de virus

La solución debe poseer capacidad para detectar y limpiar las infecciones mediante: Exploración en acceso, exploración en tiempo real, exploración bajo demanda, y exploración programada.

2.6.1 Debe contar con capacidad de realizar las siguientes acciones al detectar un virus:

- Limpiar, borrar, mover, bloquear el acceso (el archivo seguirá en la máquina pero no se podrá ejecutar), mover a cuarentena, etc.
- deberá poder realizar copia de resguardo, previo a realizar la acción.
- Como mínimo deberá ser capaz de prevenir y eliminar código potencialmente malicioso tipo: Virus, JAVA, ActiveX y VBScrips, Worms, Troyanos, Virus de red, Spyware, Graywares, Adwares, Rootkits, Pishing, Pharming, Hijacking, Jokes Programs, Hawking Tools, Remote-access Tools, Password Cracking, Key Loguers, etc.

2.6.2 Debe contar con capacidad de eliminar los siguientes tipos virus:

- Virus de arranque, virus de archivos, virus de macros, virus de scripting y vulnerabilidades del Sistema Operativo.
- Virus en archivos compactados, sin importar el número de niveles de compresión, en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros.
- Archivos empaquetados y encriptados (p.e., con upx).

- Archivos de intercambio y Archivos en el directorio raíz.

2.7 Actualización automática, programada o remota vía Intranet o Internet.

La solución debe ofrecer la funcionalidad de actualización del motor, de los patrones, de las versiones de firmas, parches y base de datos del antivirus en forma manual, programada y automática desde los siguientes medios como mínimo: unidad magnética, unidades extraíbles, la red interna (LAN), Internet (servidores oficiales y certificados por la empresa desarrolladora del producto antivirus).

Las actualizaciones del motor, patrones, versiones del antivirus deberán poder enviarse a todas las estaciones de trabajo en forma masiva o solo a aquellas estaciones seleccionadas.

La actualización de la base de firmas de virus deberá realizarse al menos una vez por día.

2.8 Administración centralizada por consola.

La solución deberá contar con una consola de administración centralizada que permita gestionar los clientes y servidores, y ser accesible desde cualquier punto de la red.

Sin importar si la instalación fue realizada en una única red local o una red distribuida con muchas locaciones, la solución deberá poder ser administrada en forma centralizada y remota.

Soporte para instalación de servidor/s de actualizaciones que permita realizar en forma descentralizada las actualizaciones de los clientes localizados en la red.

2.9 Consola Central de Gestión.

La solución ofertada de implementar un Soporte de consola central de gestión de servidor de actualizaciones y de clientes conectados a la red con las siguientes prestaciones:

- Capaz de administrar las actualizaciones, parches y actualizaciones del programa a través de la administración central remota.
- Contar con interfaz gráfica compatible con Windows 7 (todas las versiones), Windows 8 (todas las versiones), Windows 10 (todas las versiones), Windows 11 (todas las versiones), Windows 2012 Server (todas las versiones), Windows 2016 Server (todas las versiones), Windows 2019 Server (todas las versiones).
- Permitir la instalación en múltiples servidores, de las consolas y mirrors; facilitando la administración de los clientes.
- Capacidad desatendida de instalación remota de los clientes en un dominio o grupo de trabajo.
- Permitir aplicar la seguridad por protección de contraseña.
- Gestión de los clientes en un ambiente LAN / WAN
- Poseer herramientas de diagnóstico incluidas en la consola de administración remota.
- Capaz de migrar actualizaciones a las estaciones de trabajo y servidores en redes Lan/Wan cuando no estén conectadas a la Consola central: Listado de definiciones de virus, parches del programa y actualizaciones.
- Reporte centralizado del estado de los sistemas operativos de las estaciones de trabajo, servidores y sistemas de antivirus, generando un informe estadístico completo.
- Las actualizaciones automáticas se realizarán desde la Web, sin necesidad de realizar descargas manualmente.
- Las actualizaciones deben ser pequeñas e incrementales tanto para las estaciones de trabajo como para los repositorios de firmas (Mirror).
- Debe permitir actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status "stand-alone".

- El servidor de administración debe tener la posibilidad de integrarse con algunas de las siguientes bases de datos: Access/MSSQL/MySQL
- Capaz de controlar la configuración del sistema operativo del cliente remotamente.
- Ejecución remota de scripts y paquetes MSI con derechos de administrador a través de la consola de administración.
- Generación de informes detallados, tales como: Clientes con mayor porcentaje de alertas, comparativas de alertas (diarias, mensuales y anuales), porcentajes de alertas de las respectivas amenazas, amenazas con mayor intento de incidencia, etc.
- Envío de reportes vía email y/o SNMP.
- La consola de administración deberá permitir el bloqueo, a través de contraseña, de las opciones de configuración en los clientes instalados.
- La administración centralizada no dependerá de la existencia de un Dominio para su correcto funcionamiento. Debiendo permitir la administración de los clientes de antivirus en distintos grupos de trabajo o multi-dominios ya existentes.
- La consola de administración no debe requerir para su funcionamiento del uso de MMC (Microsoft Managment Console).
- El producto, una vez instalado y configurado en los clientes, no debe requerir de agentes adicionales para integrarse a la Consola Central de Gestión.

2.10 Mantenimiento y Soporte.

El producto ofertado deberá brindar soporte de **8hs. x 5 x 365** días del año mientras dure la contratación, tanto preventivo, como correctivo, ya sea en forma telefónica y/o Email de forma ilimitada. Considerando necesario que el OFERENTE presente por escrito un plan de Soporte y Mantenimiento con prioridad de

respuesta inmediata, indicando cómo se llevará a cabo, metodologías de comunicación, alcances y mecanismos de soporte oficiales brindados por la solución de antivirus propuesta y tiempo máximo de respuesta ante contingencias.

En caso de ser requerida la presencia de un especialista en las instalaciones del I.A.F.A.S., el adjudicatario se hará cargo de todos los gastos en que se incurra (viáticos, gastos de movilidad, etc.).

2.11 Modalidad de Contratación y Esquema de Licenciamiento.

Para todas las licencias de software solicitadas, el OFERENTE deberá presentar licencias del tipo para uso por entidades gubernamentales, siempre que la empresa desarrolladora del software posea este tipo de licenciamiento. Como forma alternativa podrán presentarse licencias del tipo empresarial.

Frente a esto, el I.A.F.A.S. tomará la decisión en función al costo monetario de las mismas.

La cantidad de licencias necesarias solicitadas deberán cubrir el equipamiento y servicios detallados, con actualización de motor y firmas de virus, establecidos anteriormente en los puntos **"Prestaciones Tecnológicas"** y "**Cantidad de equipamiento mínimo a Cubrir"**. Teniendo en cuenta las cantidades mínimas solicitadas y los criterios de comercialización del producto ofertado, se podrán cotizar paquetes con mayor cantidad de licencias a las solicitadas.

De los productos de software objeto de la presente contratación se deberán entregar sus originales con sus respectivas licencias y toda la documentación original de los mismos. Los medios permitidos de entrega tanto del software como de documentación deberán ser medios ópticos, tipo CD/DVD-ROM o por medio de sistemas "Electronic Delivery" mediante la identificación única de usuario y contraseña provistas por el adjudicatario.

Al momento de realizarse la propuesta, el OFERENTE deberá dejar, por escrito, claramente explicado el alcance y cobertura del esquema de licenciamiento

respecto a versiones, releases y patch de los productos licenciados; incluyendo los mecanismos de alertas tempranas, avisos de distribución de patchs, nuevas versiones y recomendaciones ante ataques masivos detectados. Se deberá indicar el método de notificación y los tiempos máximos de aviso y de solución de problemas.

También es de suma importancia dejar por escrito, en forma clara y detallada, cuales son los criterios comerciales que la empresa desarrolladora del software dispone a la hora de la "**Renovación de los productos licenciados, tanto para actualización de firma de virus como de motores, por un periodo de tiempo a determinar por el I.A.F.A.S.**"

3. Capacitación y Documentación.

Se deberá brindar capacitación para al menos 10 (diez) personas en el lugar y fecha donde indique la Coordinación de Sistemas Informáticos del I.A.F.A.S.

La cantidad de horas mínimas de capacitación no pueden ser inferior a 6 hs. horas, en los siguientes temas (enumerativo, no taxativo):

- Conceptos generales del Antivirus provisto.
- Estrategias de Seguridad del Antivirus Provisto, configuración, parametrización y herramientas adicionales.
- Antecedentes y estadísticas de ataques de virus
- Tipos de ataque y perfil de los virus
- Conceptos relativos a spam, y otros métodos de ataque
- Modelos y esquemas a instrumentar en políticas antivirus.
- Planes de Contingencia
- Estrategias de contención y neutralización de ataques para respuestas ante incidentes.

- Herramientas de seguridad y auditoria
- Instalación y configuración de servidor de administración centralizada.

La propuesta deberá incluir el temario de los cursos y su duración, perfil de los asistentes y sugerir a criterio del OFERENTE, otros cursos de capacitación que considere conveniente. Se deberá entregar los Manuales Oficiales correspondientes a los cursos ofrecidos en idioma español y Certificado Oficial de Asistencia.
La capacitación brindada por el OFERENTE deberá ser de carácter "Oficial", siendo ésta avalada por el Fabricante, y dictada por un profesional certificado en el producto.

4. ITEM 1: 550 (quinientos cincuenta) Licencias de Software Antivirus Corporativo "Eset" con 3 (tres) años de actualización y soporte.

Características técnicas:

- Acceso a soporte técnico on-line, parches y actualizaciones de versión en forma directa y on-line del fabricante.
- Soporte telefónico para consultas sobre procedimientos habituales y/o de emergencia: número urbano o número gratuito del tipo 0800. El oferente deberá indicarlo en su propuesta.
- El oferente deberá realizar la instalación (o actualización) y configuración de la consola de monitoreo y administración centralizada en un equipo provisto por el Instituto. La configuración deberá realizarse en todos sus componentes (consola de monitoreo y administración, servidores y puestos de trabajos) de manera que se implemente la distribución y actualización de los listados de patrones de virus con la modalidad y frecuencia recomendada por el

fabricante. La configuración deberá ser consensuada con el personal técnico del Área de Sistemas del Instituto previo a la implementación.

- El oferente deberá presentar, conjuntamente con su oferta, un plan de trabajo detallando tiempos y personal afectado para realizar la tarea antes mencionada, debiendo quedar el trabajo finalizado lo antes posible. El oferente debe garantizar la total operatividad del producto antes de la fecha indicada como plazo de entrega.
- El software ofertado, deberá brindar protección de antivirus a nivel de servidores y desktop, soportando el escaneo y limpieza de paquetes de tráfico sobre protocolos POP3, POP3s, IMAP4, HTTP y FTP; tanto en los servidores como en las computadoras personales.
- El software ofertado, deberá brindar protección de antivirus optimizada para plataformas móviles, soportando Anti-Phishing, Filtrado de SMS y llamadas, Control de aplicaciones y funciones de protección antirrobo.
- Funcionalmente debe utilizar un único motor que no requiera la instalación de ningún agente adicional para su operación, tanto para computadoras personales, desktop, móviles y servidores.
- Deberá tener soporte completo para plataformas de 32bits y 64bits.
- El software de antivirus deberá ejecutar como máximo 3 (tres) procesos en segundo plano.
- Soporte para computadoras portátiles con capacidad de posponer tareas cuando se ejecuta con la batería.
- Soporte para dispositivos móviles con capacidad de realizar exploración completa del sistema durante la carga de la batería.
- El producto ofertado deberá tener la capacidad de poder ejecutar desde la consola de administración, acciones básicas como, bloquear, desbloquear, activar una alarma, encontrar en el mapa y borrar los datos del dispositivo en forma remota.

- El producto ofertado deberá tener la capacidad de poder enviar a los centros oficiales de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad que puedan ser analizados y clasificados para su contingencia inmediata.
- El producto ofertado deberá tener la capacidad de generar CDs y/o USB booteables, con los cuales se puedan realizar tareas de análisis para la inspección de código malicioso. Dichos medios deben poder ser actualizados una vez se encuentren compilados o en uso (memoria residente).
- Deberá incorporar chequeo y control de Hotfix de Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.
- Deberá poder realizar control de medios extraíbles de almacenamiento.
- El producto ofertado deberá importar o exportar configuraciones de clientes por medio de archivos XML.
- ***Todo el software deberá entregarse en idioma español y en su última versión liberada al mercado.***
- El producto de software deberá ser "perpetuo", es decir, que el producto deberá seguir funcionando una vez vencidas las licencias adquiridas.

NOTA: Todas las características y servicios solicitados son prestaciones de carácter mínimo a cumplir, pudiendo el OFERENTE incluir en su propuesta mejoras tecnológicas no solicitadas siempre y cuando no representen estas mayores costos para el Instituto.

No se acepta bajo ningún concepto, cargos adicionales o condiciones que no figuren tácitamente en la oferta. Igualmente no se aceptarán problemas o cuestiones emanadas de no haber realizado las consultas pertinentes a la Coordinación de Sistemas Informáticos del I.A.F.A.S., Central Paraná, o por no ser

visitado el lugar de instalación o las ocasionadas por desconocimiento de las instalaciones o recursos.

Por lo tanto es responsabilidad del "OFERENTE" recabar toda la información necesaria para realizar una adecuada cotización.

C.P.N. GUILLERMO A. DUBRA
DIRECTOR
I.A.F.A.S.

Cdor. SILVIO ORESTES VIVAS
Presidente
I.A.F.A.S.

Dra. Victoria V. WOLF
Jefa Dpto. Despacho
I.A.F.A.S.