ANEXO II

PLIEGO DE CONDICIONES PARTICULARES

PLATAFORMA INTEGRADA DE SEGURIDAD ANTIVIRUS

Artículo 1° – Objeto de la contratación

El objeto de la presente Licitación Pública está destinada a la adquisición de una plataforma integrada que le permita a al Gobierno de la Provincia de Córdoba la actualización, integración y fortalecimiento de las herramientas de análisis de seguridad en equipos de escritorio y servicios informáticos críticos, permitiendo integrar y controlar las incidencias de seguridad de las aplicaciones más utilizadas por los usuarios en la organización como ser correo electrónico, navegación a Internet y el uso de herramientas equipos de escritorio.

Artículo 2º.- Plazo de provisión - Mora

El plazo de provisión del sistema, instalación y puesta en operación con todas las prestaciones mencionadas en el presente Pliego será de noventa (90) días contados a partir del quinto día hábil de la fecha de recepción de la Orden de Compra emitida por el Gobierno de la Provincia de Córdoba.

En caso de incumplimiento del plazo establecido en el presente pliego, la mora se considera automática y sin necesidad de interpelación alguna. La Secretaría de Innovación y Monitoreo de la Gestión podrá aplicar una multa por un importe correspondiente al uno por ciento (1%) del importe total de la Orden de Compra, por cada día de mora. En caso

de persistir esta mora, más allá de los sesenta (60) días, la autoridad de aplicación podrá adjudicar el servicio mencionado a la segunda mejor oferta, previo a rescindir la contratación.

La empresa adjudicataria ante inconvenientes imprevistos que imposibiliten el cumplimiento de los plazos comprometidos para la provisión del sistema ofertado, los deberá comunicar a la Secretaría de Innovación y Monitoreo de la Gestión por escrito y debidamente documentado, dentro de un plazo de cinco (5) días de ocurrido el hecho, los motivos que ocasionan esta situación y a los fines de extender el periodo de implementación y evitar incurrir en mora, quedando tales circunstancias a consideración de la autoridad de aplicación.

Artículo 3° – Seguros y leyes sociales

Estarán a cargo de la empresa adjudicada, además del seguro de vida y por accidente de todo su personal, el cumplimiento de todas las obligaciones que establece la legislación laboral vigente. La adjudicataria antes de la iniciación del servicio deberá presentar a la Dirección General de Administración del Ministerio de Administración y Gestión Pública, constancia de haber contratado un Seguro contra Riesgos del Trabajo (inscripción en A.R.T.) para todo el personal asignado a la prestación del servicio y que cubra las indemnizaciones por concepto de incapacidad total permanente, parciales o absolutas y/o muerte, contratación que deberá mantener en vigencia durante el lapso de vigencia del contrato, en un todo de acuerdo a las previsiones establecidas en la Ley Nacional Nº 24.557 y sus reglamentaciones, en la que deberán constar los nombres y documentos de identidad de las personas que empleará para el cumplimiento del objeto de la presente licitación. En dicha Póliza se agregará una Cláusula de No Repetición, con los siguientes términos:

"ART renuncia en forma expresa a iniciar toda acción de repetición contra el Gobierno de la Provincia de Córdoba, sus funcionarios o empleados, bien sea con fundamento en el Art. 39 Inc. 5 de la Ley 24557 o en cualquier otra norma jurídica, con motivo de las prestaciones en especie o dinerarias que se vea obligado a otorgar o a abonar al personal dependiente de la empresa adjudicataria alcanzados por la cobertura de la presente póliza, por accidentes de trabajo o enfermedades profesionales, sufridas o contraídas por el hecho o en ocasión del trabajo, o en el trayecto entre el domicilio del trabajador y el lugar de trabajo".

Asimismo la firma adjudicataria asume todas las obligaciones laborales y previsionales que en su carácter de empleador emanen de las disposiciones legales y convencionales actuales o futuras.

La dotación del personal afectado a este servicio deberá reunir las siguientes condiciones:

a) *Tener dieciocho (18) años de edad cumplidos como mínimo.*
b) *No registrar antecedentes policiales o penales.*
c) *Guardar debida consideración y respeto en el trato con el resto del personal.*
d) *Antes de comenzar la prestación del servicio, el adjudicatario deberá presentar la nómina de las personas a su nombre o a sus órdenes afectados al mismo, indicando su domicilio debidamente acreditado con el pertinente certificado y acompañando además el certificado de buena conducta de dicho personal extendido por las autoridades competentes. Toda modificación que introdujera en dicho plantel, deberá ser comunicado con debida antelación a la Secretaría de Innovación y Monitoreo de la Gestión. La inobservancia de esta obligación podrá dar lugar a que la*

mencionada repartición no permita la entrada y/o permanencia de toda persona no inserta en la nómina citada. Esta obligación es en caso de que así lo considere por razones de seguridad la Secretaría antes mencionada.

Artículo 4° – Prohibición de Cesión

El adjudicatario no podrá ceder o transferir total ni parcialmente el contrato de provisión sin el previo consentimiento de la Provincia. La violación de esta prohibición podrá ser considerada por la Provincia causal de resolución del contrato por culpa de la contratista.

Artículo 5° – Responsabilidades

El adjudicatario será responsable de los daños y/o perjuicios que por causas imputables a él o a su personal, pudieran sufrir bienes del patrimonio de la Provincia. También le alcanzará la responsabilidad por la desaparición, robo, hurto, daños intencionales y/o accidentales, infidencias, etc. de objetos y/o servicios del Gobierno de la Provincia y/o Personal. Probada la culpabilidad, el adjudicatario deberá reponer lo desaparecido y/o dañado, o bien reintegrar el importe que al efecto determine el Gobierno de la Provincia en su carácter de damnificado.-

Articulo 6° - Sobre la adjudicación

6.1 *La adjudicación se realizará por Renglón completo a la oferta que se encuentre ajustada al Pliego y resulte ser la más conveniente a los intereses del Estado Provincial, a través del dictado del pertinente acto administrativo emanado de Autoridad Competente*

y que se comunicará en alguna de las formas previstas en el Punto 2.8.1 Anexo I del Decreto Nº 1882/80.

***6.2** Garantía de cumplimiento.*

Una vez comunicada la Adjudicación, los adjudicatarios deberán ofrecer una garantía del diez por ciento (10%) del valor total de aquélla, en las firmas y condiciones previstas en el presente Pliego, debiendo en el supuesto de presentación de póliza de seguro de caución ser emitida bajo la calificación "B" o superior para la Compañía como mínimo, según surja de constancias de Calificadoras de Riesgos nacionales e internacionales. Asimismo, deberá cumplimentar para su devolución el total de las prestaciones a su cargo conforme las Condiciones Generales, Particulares y Especificaciones Técnicas que rigen la presente Licitación Pública.

Artículo 7° - Sobre la Ejecución de los Trabajos

El Contratista deberá encargarse, con el esmero y diligencia apropiados, de ejecutar completamente los servicios y actividades de acuerdo a lo establecido en las Especificaciones Técnicas.

El contratista deberá dirigir las actividades, el personal y todos los elementos necesarios para la realización completa de las actividades, de conformidad con el cronograma de desarrollo del servicio. Asimismo, el Contratista deberá emplear para la ejecución de los trabajos personal idóneo, el cual trabajará en relación de dependencia con el Adjudicatario, quien asumirá la responsabilidad laboral, responsabilidad por accidentes y enfermedades de trabajo, cargas sociales y contraprestaciones de cualquier naturaleza, desligando de toda responsabilidad a la Administración Pública Provincial.

Artículo 8º – Forma de Pago – Facturación

La plataforma integrada de seguridad antivirus del Gobierno Provincial objeto de la presente contratación, será facturado por parte de la empresa adjudicataria a partir de la fecha del Acta de Recepción y una vez recibidas y conformadas las facturas por la Dirección de Telecomunicaciones – Subsecretaría Tecnologías Informáticas y Telecomunicaciones, su vencimiento operará a los treinta (30) días hábiles.-

La factura debe estar a nombre de la "DIRECCIÓN GENERAL DE TESORERIA Y CREDITO PUBLICO DE LA PROVINCIA DE CORDOBA – CUIT 34-99923057-3 (Ministerio de Administración y Gestión Pública)" y deberá consignarse, número de expediente, orden de compra, período, y concepto facturado y por los mismos importes que figuran en la Orden de Compra

Al momento del pago de cada factura, por disposición de la Dirección de Rentas deberá cumplimentarse con lo establecido por la Resolución N° 116/00, referente al Certificado Fiscal para Contratar. Para ello deberá solicitar ante la D.G.R. mediante formulario N° 292/00 la emisión del mismo. Es obligación de la Tesorería de la Dirección General de Administración del Ministerio de Administración y Gestión Pública exigir el Certificado previo a cualquier pago que realice.

ANEXO III

PLIEGO DE ESPECIFICACIONES TECNICAS

RENGLÓN ÚNICO

1. OBJETIVO DE LA CONTRATACION

La protección de la información es un proceso altamente dinámico que debe estar a la vanguardia y constantemente actualizado para poder soportar los diferentes tipos de ataques que personas no deseadas o no autorizadas pretenden hacer sobre las plataformas tecnológicas de las organizaciones y de lo cual no se excluye al Gobierno de la Provincia de Córdoba; haciéndose indispensable contar con las soluciones y herramientas que permitan prevenir y mitigar al máximo este tipo de riesgos y exposiciones, y adicionalmente mantener disponible la información de los usuarios finales en el momento en que se requiera.

El objetivo de la presente busca adquirir un sistema que le permita al Gobierno Provincial la actualización, integración y fortalecimiento de las herramientas de análisis de seguridad de usuarios finales, permitiendo integrar las incidencias de seguridad en los servicios más utilizados por los usuarios en la organización como ser correo electrónico, navegación a Internet y el uso de equipos de escritorio. De este modo se brinda continuidad a los nuevos requerimientos tecnológicos permitiendo la disponibilidad y la seguridad de los servicios.

2. DESCRIPCIÓN DEL SISTEMA

2.1 *El Sistema propuesto deberá poseer las siguientes funcionalidades y las mismas deberán ser provistas por el mismo fabricante.*

- *<u>Un SISTEMA ANTIVIRUS PRIMARIO</u> para protección en estaciones de trabajo y servidores de archivos, tanto para Windows como Linux. El sistema deberá funcionar de forma independiente e integrarse para ser administrado desde una única plataforma de Software de gestión.*
- *<u>Un SISTEMA ANTISPAM PRIMARIO</u> para protección ante envío de basura (SPAM) y virus de correo a casillas de usuarios. El sistema deberá funcionar de forma independiente e integrarse para ser administrado desde una única plataforma de Software de gestión.*
- *<u>Un SISTEMA ANTIVIRUS/ANTISPAM SECUNDARIO</u> para protección en cuentas de correo y en servidor del tipo Microsoft Exchange. El sistema deberá funcionar de forma independiente e integrarse para ser administrado desde una única plataforma de Software de gestión.*
- *<u>Un SISTEMA ANTIVIRUS/ANTISPAM TERCIARIO</u> para protección en cuentas de correo y en servidor del tipo Lotus Dominio. El sistema deberá funcionar de forma independiente e integrarse para ser administrado desde una única plataforma de Software de gestión.*
- *<u>Un SISTEMA DE CONTROL DE NAVEGACION</u> para protección y control de contenidos de navegación a Internet. El sistema deberá funcionar de forma independiente e integrarse para ser administrado desde una única plataforma de Software de gestión.*
- *<u>Un SISTEMA DE RESPALDO</u> para recuperación rápida de equipos de escritorio y equipos portátiles basados en Windows. El sistema deberá funcionar de forma independiente e integrarse para ser administrado desde una única plataforma de Software de gestión.*

- *Una PLATAFORMA DE INTEGRACION para monitorear, controlar y administrar todos los sistemas solicitados en una única plataforma tecnológica.*

La oferta debe ser por la Plataforma Integrada de sistemas de seguridad antivirus, antispam, navegación y respaldo, con todos los ítems descriptos en la tabla 2.2 de SISTEMA A PROVEER, los cuales conforman un único renglón, es decir la propuesta será una única solución.

Los ítems indicados en la tabla 2.2, deben ser cotizados como un único renglón, conjuntamente con sus licencias, servicios de capacitación, etc.

2.2 TABLA LISTADO DE SISTEMAS A PROVEER

Ítems	***Bien Ofertado***	***Cantidad***	***Unidad de medida***
1	*Sistema Antivirus Primario*	*10.000*	*Usuarios*
2	*Sistema Antispam Primario*	*10.000*	*Usuarios*
3	*Sistema Antivirus/Antispam Secundario*	*10.000*	*Usuarios*
4	*Sistema Antivirus/Antispam Terciario*	*10.000*	*Usuarios*
5	*Sistema de Control de Navegación*	*10.000*	*Usuarios*
6	*Sistema de Respaldo*	*10.000*	*Usuarios*

7	*Plataforma de Integración de los Sistemas*	*1*	*Sistema*
8	*Licencia de soporte externo del tipo completo provisto por la empresa para todos los sistemas.*	*3 o mas*	*Años*
9	*Licencia de Filtrado URL por 3 años para Sistema de control de navegación*	*3 o mas*	*Años*
10	*Capacitación oficial de la marca para administración completa de la plataforma*	*2*	*Personas*

3. CONDICIONES GENERALES

3.1 *Este proyecto tiene como alcance brindar seguridad en estaciones de trabajo y servicios informáticos comunes de todos los usuarios y los equipos informáticos del Estado Provincial, que formen parte de la red de Gobierno.*

3.2 *El equipamiento será instalado en el Centro de Cómputos de la Provincia en su sitio de equipamiento de redes y seguridad o donde el Gobierno lo requiera.*

3.3*Cada sistema deberá poder ser monitoreado, enviar información referente a eventos de seguridad, e integrarse con la Plataforma de Integración de sistemas.*

3.4 *La plataforma de Integración de sistemas deberá tener la capacidad de administración de todos los sistemas solicitados.*

3.5 *Los equipos que formen parte del sistema solicitado deberán ser todos de la misma marca.*

3.6 *La solución deberá cubrir el licenciamiento de 10.000 puestos de trabajo / usuarios.*

3.7 *La solución deberá proveer directo de la marca el soporte por tres (3) años.*

3.8 *Es requisito que la marca se encuentre entre el grupo THE LEADER en el cuadrante de la consultora Gartner para Endpoint-Protection-Platforms.*

4. REQUISITOS DE LA OFERTA

4.1 *Las ofertas deberán ser presentadas por firmas legalmente constituidas, dedicadas a la provisión y comercialización de servicios similares al que tiene por objeto la presente licitación.*

4.2 *Los oferentes deberán poseer autorización de la marca para comercializar y soportar la versión cotizada o superior, debiendo adjuntar el correspondiente Certificado de Autorización.*

4.3 *Antecedentes de al menos una provisión similar, en los últimos dieciocho (18) meses, por medio de una nota extendida por el cliente final donde se especifique el modelo y cantidad de equipos provistos.*

4.4 *Todos los requerimientos técnicos y funcionalidades esperados de acuerdo a lo solicitado en el presente pliego, deben operar tanto en forma independiente unas de otras como en forma totalmente integrada y/o simultánea, sin limitación alguna.*

4.5 *Todos los elementos necesarios para dar cumplimiento a lo dispuesto por la cláusula anterior y nominada en el cuadro inferior deberán ser ofertados por el oferente como parte integral de su propuesta y entregados en su oportunidad, se hayan requerido expresamente o no en el presente Pliego de Especificaciones Técnicas Básicas, sin costo adicional para el Gobierno de la Provincia de Córdoba.*

4.6 *Toda otra instalación y/u operación que fuera necesaria para la correcta y completa terminación de los trabajos de instalaciones, que deban ejecutarse dentro del plazo expresado anteriormente, aunque no estén expresamente consignadas, pero que resul-*

ten necesarias para ejecutar la prestación de la puesta en marcha de la red durante las 24 hs los 365 días del año de acuerdo al objetivo de la presente contratación, serán a cargo del adjudicatario, sin costo adicional para el Gobierno de la Provincia de Córdoba.

***4.7** El oferente, deberá presentar un esquema de mantenimiento preventivo y correctivo de la totalidad del equipamiento afectado al servicio, incluyendo la sustitución total o parcial cuando fuera necesario para el buen servicio, libre de defectos e interrupciones por el tiempo que dure la garantía, a cago del adjudicatario.*

***4.8** El oferente deberá acompañar su oferta con una descripción técnica y operativa de la solución ofrecida bajo la forma de "Memoria Técnica Descriptiva".*

***4.9** El adjudicatario deberá instalar en cada uno de los puntos indicados en la Tabla 2.2 las licencias del equipamiento que deberán tener una vigencia mínima de tres (3) años.*

***4.10** El oferente, deberá presentar un documento de cierre de proyecto*

***4.11** El adjudicatario deberá realizar la transferencia de conocimientos de la solución implementada con una duración de treinta (30) horas reloj, a definir por la Secretaria de Innovación y Monitoreo de la Gestión.*

***4.12** El adjudicatario deberá brindar la capacitación al personal que disponga la Secretaria de Innovación y Monitoreo de la Gestión y la certificación oficial del equipamiento instalado según detallado en la Tabla 2.2*

***4.13** El equipamiento entregado por el adjudicatario deberá cumplir de manera estricta con el Anexo III - Pliego de Especificaciones Técnicas.*

5. PLAN DE ENTREGA Y CUMPLIMIENTO

5.1 *El plazo de entrega se fijara en noventa (90) días contados a partir del quinto día de recibida por parte de la empresa proveedora la correspondiente Orden de Compra. Todos los bienes serán entregados, instalados y configurados en las dependencias designadas por el Gobierno de la Provincia de Córdoba según lo requiera*

5.2 *El Servicio de Capacitación referido a la configuración, operación y mantenimiento del Sistema Integrado de Sistemas de Seguridad del Gobierno Provincial de todos los elementos (estaciones clientes, dispositivos de seguridad, sistemas de monitoreo, sistema de análisis, etc.) se hará efectivo en oficinas del Proveedor o en algún centro de capacitación ubicado en la ciudad de Córdoba perteneciente al proveedor, dentro de los noventa (90) días contados a partir del quinto día de recibida la Orden de Compra. En caso de realizarse fuera de la Provincia, el oferente se hará cargo de los gastos de transporte y hospedaje de los integrantes que tomaran la capacitación. Todos los equipos deberán ser entregados con la documentación correspondiente a la importación de los mismos, certificados de garantía, licencias de software definitivas de cada producto.*

5.3 *La activación de las licencias e inicio de actividades de soporte (Telefónico o Ticket) empezarán a correr desde el momento de finalización y puesta en funcionamiento del Sistema.*

5.4 *El adjudicatario deberá realizara la instalación y puesta en marcha de todos los software solicitados.*

5.5 *El adjudicatario deberá realizar el diseño e implementación de plataforma de Antivirus*

5.6 *El adjudicatario deberá realizar la disponibilidad y balanceo de carga del servicio.*

5.7 *El adjudicatario deberá realizar el soporte para diez mil (10.000) clientes.*

5.8 *El adjudicatario deberá realizar la implementación de servicios redistribuidores.*

5.9 *El adjudicatario deberá realizar el diseño del plan de desafección del servicio antivirus actual productivo.*

5.10 *El adjudicatario deberá realizar el diseño e implementación de instalación de clientes antivirus.*

5.11 *La implementación será del veinte por ciento (20%) de los clientes, tanto estaciones de trabajo como servidores en los ambientes físicos y virtuales bajo las plataformas Microsoft, Linux, Unix.*

5.12 *El adjudicatario deberá realizar el diseño e implementación de políticas de escaneo respetando las buenas prácticas del destino en cuestión.*

5.13 *El adjudicatario deberá realizar el diseño e implementación de políticas de actualización de firmas las cuales deberán garantizar la descentralización de actualizaciones de clientes de sitios remotos.*

5.14 *El adjudicatario deberá realizar el diseño e implementación de notificaciones y alertas.*

5.15 *El adjudicatario deberá realizar el diseño e implementación de perfiles de seguridad de acceso a la herramienta.*

5.16 *El adjudicatario deberá realizar el diseño e implementación de agentes antivirus para servicio de correo electrónico Lotus Domino. La herramienta deberá soportar agente para bases de datos Microsoft Exchange Server.*

5.17 *El adjudicatario deberá realizar el diseño e implementación de políticas de Actualizaciones y Escaneo aplicando las mejores prácticas correspondientes.*

5.18 *El adjudicatario deberá realizar el diseño e implementación de un antivirus y antispam SMTP el cual deberá garantizar disponibilidad del servicio y balanceo de carga tanto para correos entrantes y salientes del Gobierno de la Provincia de Córdoba.*

5.19 *El adjudicatario deberá realizar el diseño y configuración de reglas de filtrado basados en:*

- *Control de Reputación (listas blancas y listas negras.*
- *Diccionario.*
- *Tipos de archivos.*
- *Diseño y configuración de políticas Antimaleware.*
- *Diseño y configuración de notificaciones, alertas y auditoría.*
- *Diseño y configuración de reportes*
- *Diseño y configuración de perfiles de seguridad de acceso.*

5.20 *El adjudicatario deberá realizar el diseño e implementación de un antivirus Web el cual deberá garantizar disponibilidad del servicio.*

5.21 *El adjudicatario deberá realizar el diseño e implementación de servicio de control de navegación basado en reglas de filtrado de contenido.*

5.22 *El adjudicatario deberá realizar el diseño y configuración de interacción con Microsoft Active Directory.*

5.23 *El adjudicatario deberá realizar el diseño e implementación de Reglas de filtrado antivirus.*

5.24 *El adjudicatario deberá realizar el diseño y configuración de políticas de actualización de firmas.*

5.25 *El adjudicatario deberá realizar el diseño y configuración de notificaciones, alertas y auditoria.*

5.26 *El adjudicatario deberá realizar el diseño y configuración de reportes.*

5.27 *El adjudicatario deberá realizar el diseño y configuración de perfiles de seguridad de acceso.*

6. ESPECIFICACIONES TÉCNICAS GENERALES DE LOS PRODUCTOS A PROVEER

Consideraciones Generales de los productos a proveer deberán ser las siguientes, exceptuando para el Centro de Control y análisis ciertas funcionalidades operativas, no así su licenciamiento y características eléctricas de la República Argentina:

6.1 *Todas las facilidades, features, características y especificaciones del hardware y software ofertado que sean necesarias para que dicho hardware y software se ajuste a los requerimientos de equipamiento y sistemas aquí enunciados, deberán estar disponibles (liberadas al mercado) al momento de la apertura de las ofertas. No se aceptarán facilidades que sólo están disponibles en versiones beta de los paquetes de software o a modo de prototipo en el hardware.*

6.2 *Los elementos, unidades funcionales, dispositivos y accesorios estarán constituidos por unidades nuevas, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso, a que el Gobierno de Córdoba será el primer usuario de los equipos desde que estos salieron de fábrica).*

6.3 *Los equipos a proveer deberán estar vigentes y no poseer fecha de discontinuidad de fabricación a la fecha de presentación de la oferta.*

6.4 *El oferente garantizará por escrito mediante declaración jurada incluida en la oferta, que estará en condiciones de seguir efectuando el mantenimiento, provisión de repuestos y soporte técnico tanto del hardware como del software de todos los bienes a proveer, durante un plazo de por lo menos tres (3) años a partir de la fecha de presentación de la oferta, independientemente de la continuidad de los bienes en el mercado por parte de la empresa fabricante.*

6.5 *Este servicio de mantenimiento del software (upgrade), debe incluir la actualización automática del mismo por nuevas versiones (cualquiera sea el nivel de las mismas) sin cargo alguno para el Gobierno de la Provincia de Córdoba, dichas nuevas versiones deberán ser instaladas en los equipos dentro de los sesenta (60)*

días corridos posteriores a su liberación al mercado en el país de origen del software.

6.6 *El reporte de los Upgrade del sistema operativo debe ser informado por el proveedor en conjunto con la provisión al momento de la oferta de una página WEB u otra vía informativa (revista, news letter), donde el personal técnico de la Dirección de Telecomunicaciones y Seguridad Informática pueda estar informado online de las nuevas actualizaciones del sistemas operativo de los equipamientos ofertados.*

6.7 *También y por el período de tres (3) años, el proveedor deberá brindar un servicio de soporte que permita que los técnicos del Área de Seguridad Informática perteneciente a la Secretaria de Innovación y Gestión Pública efectúen consultas técnicas telefónicas o personales a los especialistas del proveedor.*

6.8 *El Proveedor deberá entregar (para cada tipo de producto) dos (2) copias en CD-ROM del software componente del sistema y las licencias de uso permanente. Para la documentación respectiva dos (2) copias impresas y cinco (5) copias en CD-ROM.*

6.9 *Cada equipamiento deberá contar con diferentes niveles de acceso al sistema (administrador y usuarios) permitiendo la gestión por roles de la infraestructura de red.*

6.10 *Se le entregara al Gobierno de la Provincia de Córdoba el máximo nivel de clave de acceso permitido, lo que posibilite la visualización de los logs del equipamiento.*

7. ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA ANTIVIRUS PRIMARIO (ÍTEM 1).

CARACTERÍSTICAS	***DESCRIPCIÓN***
1. Motor de Exploración del Antivirus.	*El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos.* *Deberá tener integrada una tecnología de Servicio de Mapeo, que permita acceder por debajo del sistema operativo para un análisis y una reparación completo.*
2. Administración Remota.	*Capacidad para acceder a la consola mediante un acceso web.*
3. Acciones posteriores a la detección.	*Capacidad para tomar distintas acciones cuando sea detectado un virus o un ataque, limpiar el archivo infectado, moverlo a cuarentena, no tomar acción, eliminar el archivo, etc.*
4. Exclusiones en la exploración	*Capacidad para excluir de la exploración archivos, carpetas, procesos, etc. específicos.*
5. Exploración de correo	*Capacidad para exploración de mensajes de correo elec-*

electrónico	*trónico utilizando Microsoft Outlook, detección de virus y programas no deseados.*
6. Detección de Programas no Deseados	*El antivirus debe ser capaz de detectar y eliminar diferentes tipos, tales como: adware- spyware- jokeprograms - Keyloggers, trackware,hacktools,remoteaccesstools, dialers.*
7. Instalación remota	*Debe ser capaz de instalarse en clientes de forma remota desde una consola de administración centralizada, de forma transparente para el equipo cliente y con la capacidad de retrasar/suprimir la necesidad del reinicio de este equipo cliente, dependiendo de la tecnología a implementar.*
8. Programación de tareas	*Capacidad para programar tareas de exploración, actualización, etc.*
9. Ahorro de Energía en Equipos Portátiles	*Capacidad para retrasar/dejar en modo espera las búsquedas de virus en caso de que el equipo portátil se encuentre sin alimentación eléctrica directa.*
10. Registro de eventos	*Deberá crear bitácoras por cada uno de los eventos tales como: historial de riesgos, historial de exploraciones, historial de eventos e historial de ataques al antivirus.*

11. Protección & escaneo Acceso Spyware	*Deberá escanear y bloquear en tiempo real cualquier acceso e instalación de cualquier spyware, adware, malware, keylogger, herramientas de administración remota, Dialer,trackware, hacktools, etc, no solamente por escaneo en demanda.*
12. Escaneo de Spyware en Registro	*Deberá escanear llaves del registro y eliminar las llaves creadas por los spyware sin afectar la estructura del registro a nivel de sistema operativo.*
13. Sistemas Operativos	*Deberá poder instalarse en:* • *Windows 2000 Professional/Server* • *Windows XP SP1+ 32-bit/64-bit* • *Windows Vista 32-bit/64-bit* • *Windows Server 2003 32-bit/64-bit* • *Windows Server 2008 32-bit/64-bit.*
14. Reportes	*Deberá proveer reportes gráficos desde la consola de administración centralizada del producto sin necesidad de productos adicionales.* *Deberá clasificar los reportes en categorías como Riesgos, Cumplimiento de políticas, escaneos, estado de los equipos, entre otros.*

15. Único Agente	*La herramienta de protección no deberá requerir aplicaciones adicionales para comunicarse a la consola de administración. Es decir con sólo una vez que se ejecute el instalador la herramienta cubrirá los aspectos de seguridad y comunicación con la consola.*
16. Icono Único	*La herramienta solamente presentará un ícono en el área de notificación de la barra de tareas.*
17. Integración transparente de tecnologías de seguridad	*Debe integrar de forma transparente las tecnologías principales de antivirus, antispyware, firewall, prevención de intrusos y control de dispositivos.*
18. Habilitado Control de Acceso a Red a nivel de auto forzamiento	*Se debe incluir la licencia de Control de Acceso a Red para que el mismo agente de protección pueda establecer políticas mínimas que debe cumplir la estación; caso contrario, la máquina tomará políticas diferentes a las del resto de las PC's.*
19. Interfaz Única	*Debe ofrecer una única interfaz integrada para administrar todas las tecnologías.*
20. Análisis proactivo de amenazas	*Debe contar con protección basada en comportamiento que protege contra las amenazas de día cero y amenazas nunca antes vistas.* *Debe mostrar puntuaciones en base a comportamientos buenos y malos de las aplicaciones desconocidas, para*

	determinar una detección más precisa del software malicioso.
21. Control de las aplicaciones	*Debe permitir a los administradores controlar el acceso a procesos, archivos y carpetas específicos creados por usuarios y otras aplicaciones.* *Debe brindar análisis de aplicaciones, control de procesos, control de acceso de archivos y registro, y control de módulos y librerías DLL.* *Debe permitir a los administradores restringir ciertas actividades consideradas sospechosas o de alto riesgo. Asimismo, si el administrador por política interna de la institución desea controlar la ejecución de aplicaciones mediante el código hash de las mismas, lo podrá hacer.*
22. Control de dispositivos	*Deberá permitir al administrador controlar qué periféricos pueden conectarse a un equipo y cómo se usan.* *Bloquea las estaciones o servidores para impedir que se conecten las unidades thumbdrive, grabadoras de CD, impresoras y otros dispositivos USB.* *Debe igualmente contar con la capacidad no sólo de bloquear en su totalidad un dispositivo, sino de restringir parcialmente actividades en los periféricos, tales como memorias USB; haciendo que sean de sólo lectura, o que no permita la ejecución de aplicaciones desde dichos periféricos.*

	Adicionalmente el administrador podrá definir si restringe el acceso a todos los dispositivos USB o sólo restringe el acceso de acuerdo al identificador del dispositivo.
23. Flexibilidad en administración	*Los administradores deben poder personalizar la interfaz y decidir qué tecnologías ejecutar en los equipos cliente y qué opciones de configuración no estarán disponibles para los usuarios finales.* *Los administradores también tienen la opción de ocultar por completo la interfaz para que los usuarios no la vean.*
24. Jerarquía de Permisos	*La herramienta debe permitir agregar varios usuarios de tipo administrador global, administrador de dominio, revisor global, revisor del dominio. Los revisores tienen acceso de sólo lectura.*
25. Alertas Globales	*La herramienta debe mostrar en la consola el estado actual de alerta sobre amenazas a nivel global.*
26. Adaptabilidad	*La herramienta debe permitir que los clientes no dependan de un solo servidor de actualización, y que en caso de que sean equipos móviles, puedan buscar según prioridad su servidor más cercano.*
27. Integración con LDAP	*Debe permitir integración con LDAP o Active Directory.*
28. Firmas Personalizadas de IDS/IPS	*Debe contar con un IPS/IDS en cuyas características se incluya que el administrador pueda crear reglas personalizadas.*

29. Protección específica para los procesos y archivos propios de la herramienta	*Debe contar con una protección específica para los procesos y archivos propios de la herramienta (tamperprotection).*
30. Políticas por computador o por usuario	*Debe permitir que las políticas sean aplicadas por equipos o por usuarios.*
31. Políticas de acuerdo a la ubicación	*La herramienta debe poder aplicar diferentes políticas a los equipos clientes, de acuerdo a la ubicación de los mismos. Esta ubicación se podrá definir de acuerdo al tipo de conexión (wireless, ethernet, vpn, dial-up), rango de IP, DNS, entre otros.*
32. Proveedor de Actualizaciones para oficinas remotas	*La solución debe permitir que para las oficinas remotas del Gobierno se puedan definir entidades que no necesariamente tengan Sistema Operativo Servidor y cuyo objetivo sea actualizar al resto de máquinas alrededor de esta entidad.*
33. Arquitectura de Ambiente Distribuido	*De acuerdo a la política de tolerancia a fallas del Gobierno, la herramienta de administración estará en la capacidad de replicarse a nivel de: paquetes de instalación de clientes, logs, contenido de seguridad.*
34. Listas de Servidores de Administración para Tolerancia a fallos	*Se debe proveer la capacidad de generar un listado de Servidores con determinada prioridad, los cuales pueden atender requerimientos de actualización de políticas y con-*

	tenido de seguridad de parte de los clientes de protección.

8. ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA ANTISPAM PRIMARIO (ÍTEM 2).

CARACTERÍSTICAS	***DESCRIPCIÓN***
1. Porcentaje permitido de falsos positivos del antispam	*El porcentaje máximo de falsos positivos permitido es del 0.000001 % o uno en un millón (lo anterior auditado por una entidad independiente al fabricante).*
2. Filtro inteligente de idiomas	*Debe contar con filtros inteligentes de idioma para detectar y bloquear Spam en idiomas foráneos.*
3. Listas negras y listas blancas	*Capacidad de crear listas negras/blancas generales para el bloqueo de dominio, email, palabras, etc.* *Capacidad de crear listas negras/blancas individuales por el usuario de red.*
4. AntiSpam basado en reglas	*Capacidad de filtrar correos en base a reglas individuales aplicadas a correos individuales.*
5. Escaneo Heurístico	*Capacidad de escanear por posibles correos basuras que no se encuentren en una lista o regla.*

6. Actualización automática de reglas antispam	*Capacidad para detectar la dirección IP atacante.*
7. Detección de correo basura (SPAM) en tiempo real	*Capacidad de analizar todos los correos entrantes y salientes en tiempo real por contenido SPAM o no deseado.*
8. Detección de correo basura (SPAM) en base al contenido de correos individuales	*Capacidad de aplicar reglas de antispam a cada mensaje que se recibe, donde cada regla está asociada a una calificación. Esto se hace de forma individual por cada correo analizado.*
9. Capacidad de marcar los posibles correos basura (SPAM) que no se desean bloquear	*Permitir añadir un prefijo a la línea de asunto, por ejemplo "SPAM:" a correos con baja calificación para registrarlos y alertar a los usuarios si se desea.*
10. Integración con LDAP	*Debe permitir la integración con los siguientes protocolos de directorio: MS ADS 2000-2003 , SunOneDirectory Server, Exchange 5.5 , Lotus Domino 6.5.*
11. Registros e Informes	*Debe permitir generar informes de estado y eventos al igual que verificar registros de todas las actualizaciones, detecciones, etc.*
12. Capacidad de re-enviar los correos basura (SPAM) a depósito de cuarentena global o de	*Capacidad de enrutar los correos basura (SPAM) a un depósito de cuarentena que pueda ser revisado por usuarios registrados en LDAP, ADS.*

usuarios individuales.	
13. Administración local y remota	*Capacidad de ser administrado mediante su interfaz independiente o a través de su interfaz web de forma remota.*
14. Capacidad de enviar mensajes de alerta	*Capaz de enviar diferentes tipos de alertas (Ej. Vía Email, etc.).*
15. Eficiencia en detección de Spam	*Debe tener una detección no menor del 98% de SPAM sin necesidad de que la herramienta pase previamente por un proceso de aprendizaje o que el administrador deba incorporar reglas manualmente.*
16. Capacidad de actualizarse automáticamente.	*Capacidad de actualizarse periódicamente por conjuntos de reglas antispam mediante una actualización automática que debe de realizarse con una frecuencia de 5 a 20 minutos.*
17. Capacidad de crear políticas de bloqueo de contenido (Ej. Agregar palabra, archivos, etc. a ser bloqueados en los correos o adjuntos)	*Capacidad de analizar los correos y sus adjuntos en busca de contenido no deseado. Se pueden crear reglas que establezcan que palabras o frases no están permitidas en ningún mensaje o adjunto.*
18. Reportes Gráficos	*Capacidad de generar reportes gráficos por detecciones, sumarios, etc.* • *Limpieza de ZIPs infectados: Capacidad de limpiar ZIPs infectados y de eliminar ZIPs de cero bytes.*

	• *Filtrado de adjuntos por contenido: Capacidad de filtrar archivos adjuntos independientemente del tipo de archivo.*
19. Filtrado de correos por destinatario	*Capacidad de filtrar correos por el asunto, cuerpo, remitente, destinatario o recipiente.*
20. Soporte para renuncias (Disclaimers)	*Capacidad de agregar renuncias (Disclaimers) a todos los correos entrantes o salientes.*
21. Políticas basadas por grupos de usuarios del dominio	*Capacidad de crear o modificar políticas por grupos de usuarios del dominio.*
22. Administración automática de Brotes	*Capacidad de administrar posibles brotes a través de acciones, bloqueo de todos los documentos adjuntos, etc.*
23. Administración Segura vía HTTPS	*Capacidad de administrarse vía HTTPS para una comunicación segura.*

9. ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA ANTIVIRUS/ANTISPAM SECUNDARIO (ÍTEM 3).

CARACTERÍSTICAS	*DESCRIPCIÓN*
1. Sistemas Operativos	*Herramienta de análisis sobre Microsoft Exchange 2000, 2003,2007.*
2. Escaneo en tiempo real de correos, carpetas, bases de datos	*Capacidad de manejar el análisis o escaneo en tiempo real (también conocido como análisis en acceso), según accede a ellos el usuario o el sistema. Puede analizar correos o archivos cuando el usuario o sistema los lee o escribe.*
3. Escaneo en demanda de correos, carpetas, bases de datos	*Capacidad de llevar a cabo análisis bajo demanda, de forma manual o planificada, para que se analicen todos los buzones, carpetas y bases de datos por virus o contenido no deseado.*
4. Escaneo en tiempo real y en demanda de archivos comprimidos	*Capacidad para analizar en busca de virus dentro de todos los diferentes tipos de archivos comprimidos como .zip, rar, etc.* *Capacidad de limpiar ZIPs infectados y de eliminar ZIPs de cero bytes.*
5. Bloqueo de correos por contenido (Análisis de contenido)	*Capacidad de filtrar correos por el asunto, cuerpo, remitente, destinatario o recipiente.* *Capacidad para bloquear o detener correos con contenido*

	inapropiado según palabras o frases, asunto y cuerpo del mensaje, en ambientes de Exchange 2000, 2003.
6. *Actualizaciones automáticas de definiciones y motor*	*La tecnología debe permitir descargar las actualizaciones de definición y de motor de forma manual o planificada. Las actualizaciones de definiciones de virus no deben ser mayores a 45 minutos, para mantener la seguridad del Gobierno.*
7. *Administración central y remota*	*Capacidad de administrarse tanto de forma local a través de su consola local (independiente), como de forma remota.*
8. *Filtrado de archivos*	*Capacidad de especificar los nombres, tipos y tamaños de archivos que se deben bloquear mediante reglas de filtrado de archivos.*
9. *Análisis de archivos bromas o sospechosos*	*Capacidad de detectar y eliminar archivos de broma y sospechosos, tales como utilidades de acceso remoto, decodificadores de contraseña, etc.*
10. *Respuesta ante contenido dañado o corrupto*	*Capacidad de filtrar archivos adjuntos independientemente del tipo de archivo.* *Capacidad de detener o eliminar los archivos adjuntos dañados, corruptos o de cero bytes.*
11. *Cuarentena*	*Capacidad de manejar una cuarentena si se desea aislar o poner en cuarentena archivos infectados o sospechosos de estar infectados.*
12. *Detección de virus des-*	*Capacidad de detectar virus conocidos y desconocidos a tra-*

Eliminado: ¶

conocidos (Heurística)	*vés de comportamiento o patrones similares a los de un virus en todos los archivos.*
13. Manejo de Alertas	*Capacidad de manejar varios tipos de alertas para la notificación de eventos como infecciones. Capacidad de enviar mensajes vía Email, etc.*
14. Detección o administración automática de brotes	*Capacidad de detectar y reaccionar ante el caso de una epidemia de virus o la repetición de un evento, enviando mensajes de alerta.* *Capacidad de administrar los posibles brotes a través de acciones bloqueo de todos los documentos adjuntos, etc.*
15. Elementos codificados, firmas digitales (Encrypted Files, digitally-signed)	*Capacidad de permitir o denegar el acceso a los correos o archivos cifrados.*
16. Reportes Gráficos	*Capacidad de generar reportes gráficos por detecciones, sumarios, etc.*
17. Escaneo en Demanda Incremental	*Capacidad de hacer escaneos en demanda programados incrementales.*

18. Soporte de Roles de Microsoft Exchange 2007	*La herramienta podrá ser instalada en Exchange 2007 bajo los siguientes roles: Edge, Hub, Mailbox Server.*
19. Servicio Antispam	*La herramienta deberá tener activo el servicio de antispam.*

10. ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA ANTIVIRUS/ANTISPAM TERCIARIO (ÍTEM 4).

CARACTERÍSTICAS	***DESCRIPCIÓN***
1. Sistemas Operativos	*Herramienta de análisis sobre Lotus Domino 8.5 o superior.*
2. Escaneo en tiempo real de correos, carpetas, bases de datos	*Capacidad de manejar el análisis o escaneo en tiempo real (también conocido como análisis en acceso), según accede a ellos el usuario o el sistema. Puede analizar correos o archivos cuando el usuario o sistema los lee o escribe.*
3. Escaneo en demanda de correos, carpetas, bases de datos	*Capacidad de llevar a cabo análisis bajo demanda, de forma manual o planificada, para que se analicen todos los buzones, carpetas y bases de datos por virus o contenido no deseado.*

4. *Escaneo en tiempo real y en demanda de archivos comprimidos*	*Capacidad para analizar en busca de virus dentro de todos los diferentes tipos de archivos comprimidos como .zip, rar, etc.* *Capacidad de limpiar ZIPs infectados y de eliminar ZIPs de cero bytes.*
5. *Bloqueo de correos por contenido (Análisis de contenido)*	*Capacidad de filtrar correos por el asunto, cuerpo, remitente, destinatario o recipiente.* *Capacidad para bloquear o detener correos con contenido inapropiado según palabras o frases, asunto y cuerpo del mensaje, en ambientes de Lotus Domino.*
6. *Actualizaciones automáticas de definiciones y motor*	*La tecnología debe permitir descargar las actualizaciones de definición y de motor de forma manual o planificada. Las actualizaciones de definiciones de virus no deben ser mayores a 45 minutos, para mantener la seguridad del Gobierno.*
7. *Administración central y remota*	*Capacidad de administrarse tanto de forma local a través de su consola local (independiente), como de forma remota.*
8. *Filtrado de archivos*	*Capacidad de especificar los nombres, tipos y tamaños de archivos que se deben bloquear mediante reglas de filtrado de archivos.*
9. *Análisis de archivos bromas o sospechosos*	*Capacidad de detectar y eliminar archivos de broma y sospechosos, tales como utilidades de acceso remoto, decodificadores de contraseña, etc.*

10. Respuesta ante contenido dañado o corrupto	*Capacidad de filtrar archivos adjuntos independientemente del tipo de archivo.* *Capacidad de detener o eliminar los archivos adjuntos dañados, corruptos o de cero bytes.*
11. Cuarentena	*Capacidad de manejar una cuarentena si se desea aislar o poner en cuarentena archivos infectados o sospechosos de estar infectados.*
12. Detección de virus desconocidos (Heurística)	*Capacidad de detectar virus conocidos y desconocidos a través de comportamiento o patrones similares a los de un virus en todos los archivos.*
13. Manejo de Alertas	*Capacidad de manejar varios tipos de alertas para la notificación de eventos como infecciones. Capacidad de enviar mensajes vía Email, etc.*
14. Detección o administración automática de brotes	*Capacidad de detectar y reaccionar ante el caso de una epidemia de virus o la repetición de un evento, enviando mensajes de alerta.* *Capacidad de administrar los posibles brotes a través de acciones bloqueo de todos los documentos adjuntos, etc.*
15. Elementos codificados, firmas digitales (Encrypted Files, digitally-signed)	*Capacidad de permitir o denegar el acceso a los correos o archivos cifrados.*

16. Reportes Gráficos	*Capacidad de generar reportes gráficos por detecciones, sumarios, etc.*
17. Escaneo en Demanda Incremental	*Capacidad de hacer escaneos en demanda programados incrementales.*
18. Soporte de Roles de Lotus Domino 8.5.3	*La herramienta podrá ser instalada en Lotus Domino 8.5.3*
19. Servicio Antispam	*La herramienta deberá tener activo el servicio de antispam.*

11. ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA DE CONTROL DE NAVEGACIÓN (ÍTEM 5).

CARACTERÍSTICAS	***DESCRIPCIÓN***
1. Protección proactiva contra las amenazas mutantes, dirigidas y nuevas	*Capacidad de detectar amenazas a medida que se crean* *Utilizar el contexto para reducir los falsos positivos y la sobrecarga administrativa.*
2. Protección y prevención contra la pérdida de datos y Web de un solo dis-	*Capacidad de disminuir el riesgo de pérdida de datos mediante la aplicación automática de las políticas de seguridad implementadas por la organización.* *Capacidad de modificar el comportamiento de los usua-*

tribuidor	*rios mediante la educación en tiempo real sobre las políticas.* *Enviar notificaciones sobre las infracciones a las políticas.*
3. *Capacidad de almacenamiento en memoria caché y proxy*	*Capacidad de funcionar como un proxy de red.* *Capacidad de implementar memoria caché HTTP para conservar y reducir consumo de ancho de banda.* *Capacidad de descifrar trafico SSL.* *Capacidad de integrarse a mecanismos DLP de la marca.*
4. *Filtrado de Contenido del Producto*	*Capacidad de contar con software de filtrado de contenido.* *Respaldo de la red y bases de datos de filtrado del fabricante del producto.* *Capacidad de actualizaciones en tiempo real para reforzar la protección.* *Integrarse con el motor de Antivirus de la marca.*
5. *Filtrado de contenido URL*	*Capacidad de utilizar la lista de filtrado de URL de la Marca posibilitando la administración, la supervisión y el bloqueo en el acceso a las direcciones URL catalogadas por la Marca.* *La lista de filtrado de URL de la Marca deberá contar con*

	más de 80 millones direcciones. *La base de la marca deberá contar con más de 60 categorías diferentes.*
6. *Protección contra amenazas basadas en web 2.0*	*Capacidad de detectar y tomar acciones contra direcciones URL maliciosas, spyware, botnets, virus y otros tipos de malware.* *Proporcionar controles de uso de la Web y las aplicaciones.* *Inspeccionar y analizar en tiempo real el tráfico sin retrasos asociados con las arquitecturas basadas en proxy.*
7. *Protección de acceso a sitios web*	*Capacidad de proporcionar medidas defensivas en varios puntos que permitan bloquear sitios web inapropiados o maliciosos, contenido activo, aplicaciones de descarga de archivos, tráfico de VoIP, y otros ataques.*
8. *Protección para distintos protocolos de red*	*Capacidad de análisis en múltiples protocolos para el tráfico de Internet entrante y saliente.*
9. *Protección contra amenazas en la transferencia de archivos*	*Protege contra amenazas de malware en todos los canales de transferencia de archivos.*

10. Integración con Microsoft Active Directory	*Debe permitir la integración con Microsoft Active Directory y la validación con los grupos y las políticas definidas en dicha herramienta.*
11. Registros e Informes	*Deberá proveer un acceso Web integral de informes y alertas.* *Presentación de informes web a nivel de usuario.* *Deberá guardar y programar informes y configurar alertas.* *Deberá permitir exportar informes a través de múltiples formatos.*
12. Creación de políticas flexibles	*Los controles de políticas flexibles deben permitir la creación de políticas sobre los criterios y el control sobre cómo se aplican las políticas en toda la organización.*
13. Inspección Activa e Inactiva de Botnets	*Capacidad para inspeccionar, detectar y bloquear botnets activos e inactivos.*
14. Control de Aplicaciones	*Capacidades de control de aplicaciones avanzadas con capacidad de monitorear y controlar el uso por los usuarios finales que abarcan múltiples aplicaciones.*
15. Administración Se-	*Capacidad de administrarse vía HTTPS para una comuni-*

gura vía HTTPS	*cación segura.*

12. ESPECIFICACIONES TÉCNICAS PARTICULARES DEL SERVICIO A PROVEER PARA EL SISTEMA DE RESPALDO (ÍTEM 6).

CARACTERÍSTICAS	***DESCRIPCIÓN***
1. Sistemas Operativos	• *Windows XP Home Edition (32 bits)* • *Windows XP Professional Edition (32, 64 bits)* • *Windows Vista (x86, x64) Home, Business, Ultimate, Enterprise.*
2. Compatibilidad con ambientes de virtualización	*La solución debe ser compatible con los siguientes ambientes:(anexar matriz de compatibilidad)* • *Microsoft Hyper-V* • *VMWare ESX, VMWare Workstation, WMWare Server* • *Citrix Xen Server*

3. *Tareas de respaldo/generación de imágenes*	• *Debe permitir la creación de imágenes de particiones de Windows por medio de un disco de inicio sin necesidad de instalar el software o un agente.* • *Debe permitir calendarizar tareas para la generación de imágenes de todo el PC o de particiones seleccionadas.* • *Debe permitir, además de la generación de imágenes de todo el equipo o particiones específicas, la generación de respaldos de archivos o carpetas determinados por el usuario.* • *Debe permitir enviar los archivos generados, ya sea por generación de imágenes o por respaldo, a los siguientes tipos de dispositivos:* o *Dispositivos de disco internos de los equipos* o *Dispositivos de almacenamiento en disco con conexión USB* o *Dispositivos de almacenamiento en disco con conexión FireWire* o *Archivo compartido en red* o *CD / DVD* • *Debe manejar diferentes niveles predefinidos de compresión de información* • *Debe permitir cifrar las imágenes generadas en*

	el estándar AES de 128 y 256 bits • *Debe permitir enviar copias de las imágenes generadas a un segundo sitio de almacenamiento que puede ser:* o *Dispositivos de almacenamiento en disco con conexión USB* o *Dispositivos de almacenamiento en disco con conexión FireWire* o *Archivo compartido en red* o *Servidor FTP* • *Debe permitir modificar el consumo de recursos de la tarea de respaldo o generación de imágenes.* • *Debe permitir que tareas de respaldo se lancen automáticamente como respuesta a cualquiera de estos eventos:* o *Instalación de una aplicación* o *Cualquier usuario se conecta al equipo* o *Cualquier usuario se desconecta del equipo* o *La información agregada al equipo supera cierto volumen.* • *Debe permitir ejecutar tareas de generación de imágenes o respaldo de archivos bajo demanda.*

	• *Debe permitir copiar un drive completo a un segundo drive.*
4. *Restauración de respaldos e imágenes*	• *Debe permitir agregar controladores de dispositivos de red y almacenamiento al disco de restauración de los equipos para incrementar su compatibilidad con hardware diferente.* • *Debe permitir recuperar las imágenes de las PCs, incluso en equipos de hardware diferente o en ambientes virtuales soportados.* • *Debe permitir montar (asignar una unidad), explorar y visualizar las imágenes que ha generado; permitiendo incluso recuperar un archivo a una unidad alterna cuando la imagen está montada.* • *Debe permitir convertir las imágenes a discos de máquinas virtuales bajo demanda.*

13. ESPECIFICACIONES TÉCNICAS PARTICULARES DE LA PLATAFORMA DE INTEGRACIÓN (ITEM 7)

Consola centralizada de gestión: es la interfaz que permite de forma integral, manipular cada uno de los componentes de la plataforma (antivirus, antispam, filtrado navegación web), permitiendo el control centralizado y estableciendo políticas transversales a toda la solución. Además posee el módulo de reportes que permiten visualizar las métricas de desempeño y el módulo de monitoreo que permite un seguimiento instantáneo a la situación de todos los activos informáticos protegidos por la suite, mostrando las vulnerabilidades y ataques recibidos con el fin de disponer medidas preventivas y/o correctivas

14. PLAZO DE EJECUCIÓN

14.1 *Duración del Proyecto*

El proyecto deberá tener una duración máxima de noventa (90) días, comenzando a partir del quinto día hábil de la fecha de recepción de la Orden de Compra emitida por el Gobierno de la Provincia de Córdoba.

14.2 *Cronograma General*

Se deberá presentar un plan de trabajo del proyecto que describa sus etapas, tareas planificadas, hitos, tiempos a insumir, recursos asignados y entregables.

14.3 *Hitos del Proyecto. Aprobación y Pago*

Hito es una tarea de mayor relevancia del cronograma general pues indica el comienzo y la finalización de una etapa. Un hito cumplido es la aprobación de los entregables de una etapa del proyecto concretados en tiempo y forma.

En este proyecto el acta de comienzo y finalización de cada etapa es un hito y deberá ser aprobado por el equipo de proyecto designado por el Gobierno de Córdoba, que se expedirá sobre lo recibido en un informe que respaldará la correspondiente conformación de la factura para iniciar con ello la gestión de pago.

15. PLAN DE ENTREGA Y CUMPLIMIENTO

#	Etapa	Entregable / Hito	Desembolso Asociado
1	Licencias	10.000 Licencias de Antivirus Primario 10.000 Licencias de Antispam Primario 10.000 Licencias de Antivirus/Antispam Secundario 10.000 Licencias de Antivirus / Antispam terciarios 10.000 Licencias control de navegación 10.000 Licencias de sistema de respaldo 1 Plataforma de integración de sistemas Licencias de soporte externo por 3 años Licencias de filtrado URL por 3 años	90% al finalizar
2	Implementación, capacitación,	Capacitación oficial de la marca para administración total de la plataforma	10% al finalizar

	documentación y cierre del proyecto	*Aceptación de la documentación del proyecto finalizada y aceptación del cierre del Proyecto.*	