Pliego de Cláusulas Técnicas para la contratación del servicio de implantación, mantenimiento y soporte técnico de algunas soluciones de seguridad del Excmo. Cabildo Insular de Tenerife

1. CARACTERÍSTICAS TÉCNICAS

Lote I: Implantación y pago por uso de una solución de seguridad para puestos de usuarios, dispositivos móviles y servidores (físicos y virtuales)

1. Situación actual y necesidad

El Excmo. Cabildo Insular de Tenerife (en adelante ECIT) dispone actualmente de una solución de antivirus para puestos de usuario y servidores físicos, que no es suficiente para garantizar la seguridad de los sistemas de información y que se debe complementar con:

- Solución de seguridad para servidores que soporte tanto servidores físicos como virtuales.
- Solución de seguridad para dispositivos móviles.
- Ampliar la cobertura de puestos usuario puesto que el número de equipos a proteger ha aumentado.

2. Objeto

Este lote relacionado con la solución de seguridad integral (equipos de usuarios, servidores y dispositivos móviles) tiene por objeto la implantación y pago por uso (modelo suscripción) de una nueva solución de seguridad, diferente a la solución existente actualmente, para equipos de usuarios, servidores (físicos y virtuales) y dispositivos móviles.

En el anexo técnico, cuyo acceso se describe en el procedimiento de **Consulta de documentación para la elaboración de ofertas**, del apartado de **Información adicional del presente PPT**, se indica el detalle de la solución actual.

En concreto se requieren las siguientes prestaciones:

- Activación de los derechos de uso (suscripciones) y el soporte técnico de la solución propuesta.

  Se contemplan en este apartado la activación de los derechos de uso de una nueva solución completa de seguridad, que se deben mantener durante la ejecución del contrato, así como la prestación del soporte técnico correspondiente.

  La nueva solución, y el servicio de soporte técnico, deberán cumplir las funcionalidades y especificaciones que se detallan en el apartado de características técnicas.

- Servicio de implantación, configuración y puesta en funcionamiento.

  La adjudicataria dispondrá de un plazo máximo de **dos meses desde la fecha de adjudicación del contrato** para la implantación completa de la nueva solución.

- Servicio de formación

- Otros servicios requeridos:

- Disponibilidad de parches y nuevas versiones de todos los componentes de la solución.
- Actualización, con frecuencia al menos diaria, de la base de datos de patrones de virus y código malicioso.
- Soporte en la planificación de migración de versiones, instalación de productos y parches y consultas de configuración.
- Comunicación proactiva por parte del fabricante de avisos de malware y ataques sucedidos en otros clientes.
- Establecimiento de un procedimiento de recogida de incidencias en equipos sospechosos, posiblemente infectados para ser analizados por el laboratorio del fabricante a fin de ofrecer un remedio desarrollando un parche en caso de encontrar código malicioso. Dicho procedimiento se activará cuando se detecte una situación de afección importante y siempre de forma manual.
- Revisión técnica in situ, con una frecuencia mínima de seis meses, de las soluciones de seguridad: Análisis de la configuración, búsqueda de soluciones a problemas pendientes o reiterativos, aclaraciones, recomendaciones, propuestas de mejoras y actualizaciones.

En el coste ofertado, se entenderán incluidas, todas las posibles ampliaciones que solicite el ECIT, sobre el parque inicial indicado en el siguiente apartado, durante toda la ejecución del contrato, lo que incluye sus posibles prórrogas, hasta los siguientes porcentajes de incremento máximo:

- Un 15% de incremento del parque para la solución de seguridad en puestos de usuario.
- Un 10% de incremento del parque para el resto de casos.

3. <u>Infraestructura a soportar:</u>

A continuación se detalla el parque informático inicial para la contratación:

- Puestos de trabajo y servidores físicos:
  - 1400 equipos de usuario.
  - 20 servidores físicos.
- Dispositivos móviles (smartphones, tablets):
  - 500 móviles.
- Plataforma virtual
  - Infraestructura virtual VmWare
  - Dimensionamiento:
    - 9 hosts con 2 CPUs cada uno
    - Soporte para 300 servidores virtuales

4. <u>Características técnicas</u>

- <u>Requeridas</u>

- Protección contra virus, malware, ransomware y cualquier otro de tipo de software malicioso. Esta protección no podrá estar basada solo en firmas, sino que debe proveer otros métodos (basado en comportamiento, machine learning, otras tecnologías antiransomware y antiexploit)
- HIPS (Host Intrusion Prevention System), permitiendo la protección contra amenazas conocidas y desconocidas.
- Prevención de pérdida de datos.
- Cifrado de disco para servidores y puestos de trabajo.
- Control de dispositivos USB, discos duros.
- Control de aplicaciones. Listas blancas y negras.
- Integración con directorio activo (Microsoft DA) para el despliegue.
- Análisis en remoto configurables.
- Análisis bajo demanda y a recursos específicos.
- Definición de política en función de ubicación y en función de usuarios.
- Mínimo impacto en el rendimiento y uso reducido de recursos. El consumo de CPU y recursos de la máquina en la que se encuentre instalado el o los productos, no debe tener un impacto significativo en el funcionamiento del equipo y la operativa normal del usuario del mismo.
- Actualización de agentes de forma automática, desatendida y deben ser transparentes para el usuario. Las actualizaciones se deberán poder realizar de forma indistinta desde los servidores centrales o desde Internet.
- Consola de gestión centralizada e intuitiva.
    - Consola de gestión local o en la nube, en cuyo caso los servidores donde se aloje deberán estar ubicados en la unión europea.
    - Notificaciones de eventos y alertas.
    - Generación de informes y cuadros de mando con el estado general de la seguridad (puestos actualizados y sin actualizar, amenazas detectadas, eliminadas, en cuarentena, etc)

o <u>Requisitos específicos para puestos de trabajo:</u>

- Soporte multiplataforma (Windows, Linux).

o <u>Requisitos específicos de la solución móvil:</u>

- Soporte Android e iOS.
- Bloqueo en caso de pérdida o robo.
- Bloqueo completo o selectivo.
- Detección jailbreak.

o <u>Requisitos específicos de la solución para servidores virtuales:</u>

- Antivirus sin agente (uso de vShield) o agente ligero.
- Soporte multiplataforma (Windows, Linux)
- Integrable con VDI de VmWare Horizon.
- Soporte entorno híbrido (máquinas virtuales, físicas y VDI)

Características técnicas consideradas mejoras:

- Soporte para puesto de trabajo Mac.
- Generación de informes avanzados, basados en los identificadores de vulnerabilidades más comunes (CVE, boletines de seguridad de Microsoft).
- Protección contra vulnerabilidades conocidas hasta que puedan ser parcheadas.
- Evaluación de vulnerabilidades y gestión de parches.
- Apoyo al análisis e investigación de incidencias de seguridad (localización de los activos implicados, identificación de las vulnerabilidades utilizadas, comportamiento del ataque,…)
- Para dispositivos móviles: contenerización de aplicaciones que permita separar los datos y aplicaciones corporativos de los personales.
- En relación con los análisis independientes de reconocido prestigio, se tendrán en cuenta las siguientes clasificaciones:
  - AV-TEST (https://www.av-test.org/es/antivirus/empresas-windows-client/windows-7/febrero-2017):
    - Al menos una puntuación de 4.5 sobre 6 en los apartados de protección, carga del sistema y utilidad.
  - AV-comparatives (http://chart.av-comparatives.org/awards.php?year=2017):
    - Clasificación Advanced o Advanced + en los últimos test de rendimiento y protección de malware.

5. Instalación y configuración y puesta en funcionamiento.

El contratista tendrá que prestar el servicio de instalación, configuración y puesta en marcha de la solución completa.

Se tendrán que realizar al menos las siguientes tareas, que deberán detallarse en un plan de trabajo:

- Instalación y configuración de las herramientas/consolas de gestión.
- Despliegue en servidores
- Despliegue en equipos de usuario
  - Despliegue de un piloto en un grupo de 15 usuarios. Se deberá realizar de forma automatizada, y silenciosa para los usuarios, la desinstalación del producto anterior y la instalación del nuevo.
  - Despliegue en el resto del parque informático

- Despliegue en móviles.
- Definición de política y configuraciones adecuadas.
- Formación a los administradores del sistema. (presenciales 2 jornadas)

Servicios complementarios:

- Desinstalación de la protección agente correspondiente al cliente actual antivirus en los servidores y equipos de usuarios.
- Instalación del nuevo cliente ofrecido por el adjudicatario en los equipos y del nuevo software de gestión.

6. Soporte y horario de atención:

- Horario 24x7x365 para la resolución de problemas relacionados con la infraestructura, prevención, protección y desinfección frente a software malicioso. Para las incidencias leves o consultas el servicio de soporte se prestará de lunes a viernes dentro del horario laboral de 8:00 a 20:00.
- Canales: Teléfono, web, correo electrónico.
- Acceso a todas las actualizaciones de los componentes de la solución: actualización de motores, reglas, consolas, etc.
- En caso de incidencia crítica, se podrá acordar el soporte in-situ para la solución del problema.

Para el soporte se tendrá en cuenta las siguientes características:

Tipología de incidencias.

Se asignará por parte del responsable del ECIT un nivel de criticidad para cada caso, que determinará los tiempos de respuesta y resolución:

- Crítica: se han dejado de proveer totalmente los servicios que proporciona la infraestructura soportada, no estando disponibles los sistemas de backup ni los sistemas redundantes, ocasionando un impacto crítico en la actividad.
- Grave: los servicios prestados por los elementos o aplicaciones soportadas están seriamente dañados, ocasionando un impacto significativo en la operación.
- Leve: los servicios prestados por los elementos o aplicaciones soportadas se encuentran degradados, no quedando interrumpida la prestación de los servicios.

Tiempos de respuesta y resolución.

Se requerirán los siguientes tiempos de respuesta y resolución:

Consultas técnicas	Tiempo de respuesta Tiempo de resolución	12 horas 48 horas
Incidencia leve	Tiempo de respuesta Tiempo de resolución	2 horas 24 horas

Incidencia grave	Tiempo de respuesta Tiempo de resolución	1 hora 8 horas
Incidencia crítica	Tiempo de respuesta Tiempo de resolución	1 hora 4 horas

Los tiempos superiores a 24 horas (1 día), se contabilizan como días hábiles, sin contar sábados, domingos y festivos.

Se entiende por:

- Tiempo de respuesta: el transcurrido desde el escalado hasta el inicio de la atención efectiva de la incidencia.
- Tiempo de resolución: el transcurrido desde el escalado hasta la resolución de la incidencia. Se requerirá el cumplimiento de los tiempos de resolución establecidos en los casos en los que la incidencia sea causada por la infección de un virus conocido, así como ante el fallo de alguno de los productos instalados. En otros casos que supongan nuevos tipos de ataques de seguridad, se requerirá el compromiso de realizar el escalado al fabricante para su análisis y desarrollo de solución. Simultáneamente el adjudicatario deberá proponer alternativas que permitan la solución temporal del problema a fin de poder mantener los niveles de servicio.

7. Acuerdo de nivel de servicio

Con el objetivo de garantizar la correcta prestación del servicio, se establecen una serie de acuerdos de nivel de servicio. Para ello se definen los distintos elementos de servicio y para cada uno de ellos los indicadores, el grado de cumplimiento o nivel de servicio y las deducciones aplicables a su facturación. Los elementos de servicio definidos en este apartado se considerarán el mínimo exigible que debe cumplir el adjudicatario en su prestación del servicio.

La revisión del cumplimiento del ANS especificado en este apartado, se realizará coincidiendo con la facturación del contrato, para lo que se deberá aportar, de forma anexa a la factura el informe detallado correspondiente.

Los acuerdos de nivel de servicio exigidos acorde a la severidad de las incidencias son los siguientes:

Elemento del servicio	Severidad	Nivel de servicio aceptable sin deducción	Penalización
Tiempo de respuesta	Crítica < 1 h Grave < 1 h	>= 99% >=95%	1% facturación bimestral por cada nivel de servicio no cumplido
Tiempo de resolución	Crítica < 4 h Grave < 8 h	>=99% >=95%	2% facturación bimestral por cada nivel de servicio no cumplido

Para incidencias de severidad leve o consultas técnicas no se establecen deducción aplicable a la facturación, ya que no suponen la degradación de ningún servicio o aplicación en producción.

Otras penalizaciones:

- Si se supera el plazo máximo de dos meses para la implantación del servicio, por causas imputables a la empresa adjudicataria, se establecerá una penalización de 500€ por cada semana de retraso.

Las diferentes penalizaciones descritas se aplicarán en la facturación de algunos de los meses siguientes al de la revisión.

Lote II: Antispam, Lote III: Copias, Lote IV: Auditoría, Lote V: Acceso seguro a la Intranet

El objeto de estos lotes incluye:

- Servicio de mantenimiento de licencias y soporte técnico.
- Servicio inicial de actualizaciones a las últimas versiones y parches de seguridad del fabricante.

El soporte técnico deberá tener las siguientes características:

Tipología de incidencias a considerar en el tratamiento de incidencias:

- Crítica: se han dejado de proveer totalmente los servicios que proporciona la infraestructura soportada, no estando disponibles los sistemas de backup ni los sistemas redundantes, ocasionando un impacto crítico en la actividad.
- Grave: los servicios prestados por los elementos o aplicaciones soportadas están seriamente dañados, ocasionando un impacto significativo en la operación.
- Leve: los servicios prestados por los elementos o aplicaciones soportadas se encuentran degradados, no quedando interrumpida la prestación de los servicios.

Tiempos a controlar en el ANS:

- Tiempo de respuesta: el transcurrido desde el escalado hasta el inicio de la atención efectiva de la incidencia.
- Tiempo de resolución: el transcurrido desde el escalado hasta la resolución de la misma.

Sistemas/Productos a incluir:

El detalle de los productos, versiones y licencias de cada solución de seguridad se incluye en el anexo técnico cuyo acceso se describe en el procedimiento de **Consulta de documentación para la elaboración de ofertas** del apartado de **Información adicional del presente PPT**.

En todos los casos se requiere el mantenimiento de licencias con acceso directo al soporte técnico del fabricante.

Sistema antispam y antivirus del correo electrónico

- Descripción:
    - Acceso telefónico, correo electrónico y web a ingenieros de soporte en horario 24x7x365.

- Acceso a web para descarga de actualizaciones, parches de seguridad y documentación de soporte técnico del fabricante.

Sistema de copias de seguridad de servidores:

- Descripción:
  - Acceso al soporte en horario 24x7x365.
  - Acceso a la documentación del software publicada por el fabricante.
  - Actualización de las licencias a la última versión publicada por el fabricante.
  - Acceso a las actualizaciones y corrección de errores de software publicados por el fabricante.

Sistema de auditorías de seguridad de servicios básicos (Directorio Activo, Correo electrónico, servidores de ficheros y servidores de terminales)

- Descripción:
  - Acceso soporte en horario al menos 8x5.
  - Acceso a la documentación del software publicada por el fabricante.
  - Actualización de las licencias a la última versión publicada por el fabricante.
  - Acceso a las actualizaciones y corrección de errores de software publicados por el fabricante.

Sistema de acceso seguro a la intranet

- Descripción:
  - Acceso soporte en horario al menos 8x5.
  - Acceso a la documentación del software publicada por el fabricante.
  - Actualización de las licencias a la última versión publicada por el fabricante.
  - Acceso a las actualizaciones y corrección de errores de software publicados por el fabricante.

2. CONFIDENCIALIDAD

Protección general de la información

Con carácter general la empresa adjudicataria queda expresamente obligada a mantener absolutamente confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del presente contrato.

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados. Con carácter general deberá prestarse especial atención a la observancia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la anterior, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El adjudicatario estará obligado a la realización y al mantenimiento de los registros de evidencias del cumplimiento, durante al menos todo el periodo de ejecución del contrato, de las actividades relacionadas a continuación:

- Definir, implementar y mantener una política de seguridad de la información.

- Implementar los análisis, ingeniería y contramedidas de seguridad con el objeto de proteger los datos, infraestructuras, servicios y sistemas de información, mediante la ejecución de los controles que den respuesta a los requisitos especificados en este clausulado; todo ello integrado en una gestión de análisis y gestión del riesgo.

Extender lo especificado en el punto anterior a los posibles contratos o relaciones con terceros vinculados a sistemas de información, productos y servicios que estén relacionados con la prestación del servicio objeto del contrato.

Protección de datos de carácter personal

De acuerdo con el artículo 12 de la Ley Orgánica 15/1999 del 13 de diciembre, sobre Protección de Datos de Carácter Personal, la empresa adjudicataria asumirá las siguientes obligaciones respecto de los datos de carácter personal a los que pudiera acceder para la prestación del servicio indicado:

1. Efectuar el tratamiento de los datos de carácter personal siempre de acuerdo con las instrucciones del ECIT y con la finalidad señalada en el contrato o servicio pactado, no pudiendo aplicarlas o utilizarlas con un fin distinto, ni comunicarlos, ni siquiera para su conservación, a otras personas.

2. Aplicar a los datos transferidos las medidas de seguridad de índole técnica y organizativa que les sean aplicables de acuerdo con su carácter y naturaleza y que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

3. Asegurarse y responsabilizarse de que en el acceso de sus empleados, reciban los datos únicamente en la medida en que sea necesario su conocimiento para la prestación del servicio pactado, y siempre que éstos se comprometan a garantizar la utilización de la información en los mismos términos del contrato o servicio.

4. No realizar, sin la previa autorización del ECIT, copias totales o parciales y en cualquier soporte, excepto las estrictamente imprescindibles para desarrollar el servicio contratado.

5. Una vez finalizado el servicio por el que era necesario el acceso a los datos de carácter personal, o en caso de resolución contractual por cualquier causa, y en el plazo que determine el ECIT, devolver o destruir todas las copias que se hayan podido generar.

6. En caso de que la empresa adjudicataria destine las datos de carácter personal a otra finalidad, las comunique o los utilice incumpliendo las estipulaciones del contrato o servicio, o incumpla las medidas de seguridad legalmente exigibles de acuerdo con el tipo de datos objeto de tratamiento, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Protección del acceso a los recursos TIC del ECIT

En los supuestos de prestación de un servicio que requiera o se estime conveniente el acceso local o remoto a los recursos TIC del ECIT, se establecen las siguientes limitaciones y responsabilidades específicas:

1. Condiciones técnicas:

    a. Acceso remoto:

        i. La comunicación se realizará punto a punto entre las dependencias del prestador del servicio y las del ECIT empleando un canal de datos seguro (cifrado).

        ii. Si existe la mediación de un tercero, la empresa adjudicataria será la única responsable de asegurar la confidencialidad del intercambio y de las consecuencias de su incumplimiento.

        iii. El medio técnico preferente de conexión para accesos puntuales será el establecimiento de una conexión VPN. Para ello, con independencia del presente clausulado se deberá cursar la petición expresa correspondiente ante el ECIT una vez iniciada la prestación.

2. Recursos TIC accesibles:

    a. Solamente se dará acceso remoto a los servidores de aplicaciones, bases de datos, etc estrictamente necesarios para el cumplimiento del objeto contractual.

    b. No se permitirá con carácter general el acceso al escritorio o entorno gráfico de los servidores salvo por necesidades extraordinarias del servicio ante incidencias críticas y no exista otra alternativa viable (requerirá de forma obligatoria la validación expresa del ECIT).

3. Características del acceso local:

    a. El acceso local a recursos TIC de equipos de las empresas prestadoras de servicios se deberá integrar y cumplir con las medidas de seguridad de la red del ECIT (control de acceso a la red, disponibilidad de antivirus actualizado, parches seguridad, etc).

4. Potestad de control

    a. El personal autorizado del ECIT, teniendo como finalidad la protección, optimización y mejora de los servicios, monitorizará el tráfico cursado en este tipo de conexiones para la detección de actuaciones anómalas.

5. Deberes y obligaciones para la empresa adjudicataria:

    a. Solamente deberá tener acceso a los recursos del ECIT los usuarios de la prestadora de servicios autorizados y que sean estrictamente necesarios para los fines previamente autorizados por el ECIT.

    b. Los usuarios de la empresa prestadora de servicios deberán hacer un uso adecuado de la conexión, utilizándola eficientemente con el fin de evitar en la medida de lo posible la congestión de la misma, la interrupción de los servicios de red o del equipamiento de la infraestructura conectada.

    c. Se deberá acceder desde equipos y/o redes protegidas que garanticen unas condiciones de seguridad adecuadas sobre todo en lo referente al control de accesos al personal autorizado y la protección de los activos del ECIT a los que se tenga acceso (lo que requiere el uso de soluciones actualizadas, antivirus, antispyware, etc…).

    d. La empresa adjudicataria será la responsable directa de todas las actividades realizadas bajo su nombre.

    e. Las incidencias de seguridad detectadas por el personal del ECIT o comunicadas por entidades externas serán trasladadas al usuario que pueda originarla para la aplicación de las medidas que se estimen oportunas.

    f. Los usuarios deberán reportar al ECIT aquellas incidencias de seguridad de las que tuviesen conocimiento (p.e.: pérdida o compromiso de las credenciales, etc).

6. Uso no adecuado: el servicio de acceso remoto no debe ser usado para:

    a. Cualquier transmisión de información o acto que viole la legislación vigente que le sea de aplicación.

    b. Fines privados, personales o comerciales, no relacionados con las actividades propias y autorizadas por el ECIT.

    c. Transmisión de material que infrinja la legislación sobre propiedad intelectual (software, imágenes, video, audio, películas, etc.). En general el usuario se compromete a no hacer uso de los recursos informáticos y de comunicación para publicar o divulgar material obsceno, difamatorio u ofensivo que pueda suponer una violación de los derechos legales de terceros.

    d. Creación, utilización y transmisión de cualquier tipo de material que perjudique la dinámica habitual de los usuarios del ECIT o redes externas (virus, difusión de correo publicitario, cadenas de correo-e, etc.).

    e. Actividades deliberadas con alguna de las siguientes finalidades:

        i. Congestión de los enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.

        ii. Escanear puertos de equipos sin autorización del titular/es del mismo.

        iii. Búsqueda de vulnerabilidades en equipos pertenecientes al ECIT o redes externas.

iv. Denegación de servicios y desconexión de equipos.

v. Destrucción o modificación de la información de otros usuarios o sistemas de información.

vi. Violación de la privacidad e intimidad de otros usuarios.

vii. Intentar o conseguir acceder de forma no autorizada a equipos.

f. Bajo ningún concepto el usuario atentará contra la integridad, funcionamiento o disponibilidad de los recursos informáticos que componen la red del ECIT. Se considera un atentado contra la integridad de los recursos informáticos las acciones que no tomen las medidas pertinentes contra la inclusión y/o ejecución de software pernicioso (virus, sniffers, etc.) en los equipos a los que tienen acceso, así como el acceso a los recursos informáticos fuera de las condiciones autorizadas por el ECIT.

3. Información adicional

Consulta de documentación para la elaboración de ofertas.

El presente pliego dispone de un anexo técnico, con el detalle de las soluciones de seguridad que se incluyen dentro del objeto contractual, y que podrá ser consultada bajo demanda durante el proceso de licitación, suscribiendo previamente el correspondiente clausulado de confidencialidad específico.
Para el acceso a esta información, los interesados deberán cursar la correspondiente solicitud al correo electrónico: adminf@tenerife.es. Dicha solicitud, deberá incluir los datos personales y de contacto del interesado, así como de la entidad o persona que le represente.
En respuesta a esta solicitud, se contactará con el interesado por igual medio, a la mayor brevedad posible, para coordinar la firma de un clausulado de confidencialidad, que podrá ser en electrónico o presencial, y que deberá ser realizada por el representante de la entidad, para otorgar finalmente el acceso al anexo indicado.

En Santa Cruz de Tenerife a 7 de agosto de 2017.

Natalia Bello Figueroa, Analista Superior de Sistemas de Información

Pedro Melo Peña, Analista Superior de Sistemas de Información

Clemente Barreto Pestana, Jefe del Servicio