Verificaciones Industriales de Andalucía, S. A.
CONSEJERIA DE HACIENDA, INDUSTRIA Y ENERGÍA

Nº EXPEDIENTE: CF050-18-097

SUMINISTRO E INSTALACIÓN DE SOLUCIÓN PROXY DE NAVEGACIÓN PARA VEIASA

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETO 3
3. DIVISION EN LOTES 3
4. LUGAR DE ENTREGA DEL SUMINISTRO/SERVICIO 3
5. ASISTENCIA TÉCNICA Y CONTROL DE CALIDAD 4
6. CARACTERÍSTICAS DEL EQUIPAMIENTO 4
   6.1 Características del Suministro Hardware 4
   6.2 Características Técnicas de la Solución 5
      6.2.1 Requisitos Generales 5
      6.2.2 Requisitos de Autenticación de Usuarios 6
      6.2.3 Requisitos de Gestión de Tráfico SSL/TLS 6
      6.2.4 Requisitos de Filtrado de Contenidos y Gestión de Políticas 8
      6.2.5 Requisitos de Optimización y Control de Tráfico 9
      6.2.6 Requisitos de Control de Tráfico de Vídeo 10
      6.2.7 Requisitos de Gestión de Logs e Informes 10
      6.2.8 Requisitos de Integración con otros Sistemas 11
7. SERVICIOS 11
   7.1 Fases del Servicio y Plazos de Ejecución 12
      7.1.1 Instalación y configuración 12
      7.1.2 Periodo de pruebas y verificación 12
      7.1.3 Puesta en marcha en producción 12
      7.1.4 Plazos de Ejecución 12
   7.2 Equipo de Trabajo 13
8. GARANTÍA Y MANTENIMIENTO CORRECTIVO 13
9. ACUERDOS DE NIVEL DE SERVICIO 13

1. INTRODUCCIÓN

Actualmente los usuarios de VEIASA navegan en internet a través de una solución proxy software que presenta graves limitaciones en cuanto a capacidad y seguridad. Internet es hoy día una herramienta esencial y uno de los medios de comunicación más utilizados por los diferentes departamentos en sus tareas diarias, por ello se hace necesario contar con una solución profesional que optimice la experiencia del usuario y que además permita a la Unidad de Mantenimiento de Sistemas de Información controlar la seguridad de estos accesos.

2. OBJETO

El objeto del presente pliego es la contratación del suministro e instalación de una solución de filtrado web (proxy de navegación) basada en 2 nodos físicos que permitan garantizar el uso apropiado de los recursos que ofrece internet y proteger a la organización de las nuevas amenazas actuales. Esta plataforma debe poder ser administrada de forma unificada y sencilla, y ofrecer una completa visibilidad a VEIASA de la protección y control aportado.

Deberá cumplir los siguientes requisitos:

- Control del acceso de los usuarios a Internet.
- Optimización y aceleración de aplicaciones y contenido.
- Deberá integrar funcionalidades avanzadas de filtrado de contenido.
- Gestión multiprotocolo incluyendo al menos: HTTP, HTTPS, FTP, Streaming Media (MSSS, Apple HLS, RTMP), SSL, SOCKS
- Deberá poseer funcionalidades de cifrado/descifrado de tráfico SSL.
- Deberá contar con herramientas propias de reporting.
- La solución debe soportar mecanismos de autenticación avanzada tales como: Integración con Directorio Activo (Kerberos, NTLM), LDAP, autenticación basada en certificados, usuarios invitados, autenticación secuencial, y otros.
- Las licencias suministradas, si fuesen necesarias, pasarán a ser propiedad de VEIASA.

3. JUSTIFICACIÓN DE LA NO DIVISION DEL CONTRATO EN LOTES

El presente contrato no es susceptible de división en lotes, debido a que se licita como un pack único, producto y licencias de uso, conformando una solución integral y única, no siendo asumible una segmentación de las funciones en lotes diferenciados, dada la estrecha interrelación entre las tareas. La ausencia de lotes no discrimina la presentación de ofertas por parte de ningún posible licitador.

4. LUGAR DE ENTREGA DEL SUMINISTRO Y SERVICIOS

El material a suministrar se entregará y los servicios de instalación objeto del contrato se realizarán en la siguiente dirección:

- Servicios Centrales de VEIASA
  Calle Albert Einstein 2
  41092 – Sevilla

5. ASISTENCIA TÉCNICA Y CONTROL DE CALIDAD

La empresa adjudicataria deberá establecer un control de calidad tanto del servicio como de los elementos suministrados, certificando así que se ajustan a las especificaciones técnicas exigidas en el presente documento.

En el supuesto de que algún elemento a suministrar se deteriore o no se ajuste a las especificaciones definidas, aun estando ya suministrado, deberá ser restituido a su correcto estado por cuenta del adjudicatario.

Asimismo, la empresa adjudicataria establecerá un sistema para gestionar el control de las devoluciones. La información derivada de este control ha de estar disponible para VEIASA en el plazo que se establezca.

6. CARACTERÍSTICAS DEL EQUIPAMIENTO

El suministro del material y licencias software a suministrar (si aplicasen) deberán ceñirse totalmente a las características reseñadas en este documento, no existiendo en ninguno de los casos excepciones ni variantes.

6.1 Características del Suministro Hardware

Solución basada en equipos dedicados en las instalaciones de los servicios de VEIASA, ya que es necesaria su interoperabilidad con otros sistemas corporativos ubicados en redes internas, tales como HSM y Directorio Activo que, de acuerdo con la política de seguridad corporativa, no pueden ser accedidas directamente, ni desde red externa (Internet) ni desde zonas DMZ.

Por lo tanto, la solución de control y seguridad de navegación suministrada deberá ajustarse a los siguientes requisitos técnicos, no considerándose como válidas soluciones que no cumplieran estrictamente todos estos requisitos:

- 2 equipos para montaje en modo cluster. Cada equipo cumplirá con los requisitos indicados en los siguientes puntos y deberá funcionar en alta disponibilidad ACTIVO-ACTIVO balanceando la carga sin ningún otro elemento o sistema que los propios equipos ofertados.
- Sistema modelo appliance, no basado en servidor de propósito general
- Doble fuente de alimentación “hot-swap”
- 1 x CPU de 4 cores de capacidad
- Capacidad de al menos 1000 usuarios concurrentes (con sus respectivas licencias si estas fuesen necesarias).
- Un tamaño máximo de 1xU de rack
- Capacidad mínima de 3 discos de 1xTeraByte cada uno con tecnología SAS
- Al menos 16 GBytes de memoria RAM
- Conectividad mínima:
    - 2 x puertos 10GBASE-SR Pass-Through, Fibra Multimodo

La plataforma debe ofrecer características de escalabilidad vertical:

- Sobre el equipo propuesto debe existir la posibilidad de añadir los siguientes componentes:

- Escalar hasta 6 cores
- Escalar hasta 32 GBytes de memoria
- Escalar hasta 8 discos de 1xTB

6.2 Características Técnicas de la Solución

6.2.1 Requisitos Generales

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución deberá obligatoriamente estar basada en una plataforma de control y seguridad de navegación que "simule" el servidor de destino, terminando las sesiones de los usuarios a nivel 7, e iniciando, cuando así lo permita la política definida, una nueva sesión desde la plataforma propuesta al servidor de destino (proxy de navegación). Así mismo todo el contenido descargado deberá ser analizado por la solución propuesta antes de entregar el contenido al usuario.

- Deberá soportar simultáneamente y sobre los mismos interfaces el despliegue como proxy de navegación explícito y transparente desplegando la solución en línea con el tráfico.

- La plataforma propuesta debe incorporar interfaces con hardware bypass integrado.

- La solución propuesta soportará el descubrimiento automático del proxy explícito.

- Deberá ser capaz de alojar múltiples ficheros PAC en la plataforma de control y seguridad de navegación, pudiendo controlar por política qué fichero PAC se entrega a cada usuario.

- La solución debe ser capaz de reenviar las peticiones (proxy chaining/forwarding).

- Deberá contar con capacidades de reporting de alertas mediante la utilización de SNMPv3, SMTP, Syslog, etc.

- Deberá tener capacidad de definir dominios de routing independientes, así como capacidad para definir agregación de interfaces físicos (LACP).

- El equipo debe poder realizar funciones de intercepción y el control de tráfico en nivel en modo full proxy. La solución debe soportar los siguientes servicios de Proxy, para atender a las peticiones realizadas por los usuarios:

    - HTTP con detección de protocolo. El proxy de http debe ser capaz de detectar si la petición es de tipo HTTPS o FTP y derivar dicha petición (handoff) al proxy de aplicación SSL o FTP respectivamente
    - SSL
    - FTP
    - SOCKS (v4/v5). La versión 5 debe permitir además autenticación.
    - Streaming (Flash, http, Windows Media, Real, Quick Time)
    - IM (AIM, MSN, Yahoo Messenger)
    - MAPI

- Webex para el control de las funciones de Login, Host meeting, Join meeting, File Sharing y Desktop Sharing.
- DNS. El equipo debe tener capacidad para interceptar peticiones DNS con funcionalidad de "Firewall de DNS"; por ejemplo, no permitir hacer peticiones a dominios identificados como malware.
- Soporte e intercepción del tráfico de Skype for Business de Office 365

6.2.2 Requisitos de Autenticación de Usuarios

La solución propuesta deberá cumplir con los siguientes requisitos:

- Debe soportar al menos los siguientes métodos de autenticación. Todos estos métodos pueden ser definidos simultáneamente y ser referenciados en la política de control:

  - LDAP (Lightweight Directory Access Protocol), Versión 2, Versión 3 y LDAP sobre SSL.
  - IWA (Basic, NTLM y Kerberos)
  - Radius
  - Novel SSO
  - X509 Certificate
  - Tokens
  - SAML
  - Base de datos Interna

- La solución deberá permitir autenticación transparente por sesión de usuario, cookies o IP. Esto permitirá realizar autenticación de la navegación aun cuándo múltiples usuarios estén navegando tras una misma dirección IP. No se considerarán válidas aquellas propuestas que identifiquen al usuario en base a la dirección IP origen del tráfico.

- La autenticación debe ser compatible con la ubicación de la plataforma de navegación en una DMZ corporativa. Para ello la solución propuesta debe ser capaz de integrarse con Directorio Activo a través de un agente intermedio, pues la política de autenticación corporativa no permite la comunicación directa desde red externa o red DMZ con los controladores de dominio del Directorio. No se considerará válida a cualquier solución que obligara a infligir la política de seguridad corporativa para realizar la autenticación Kerberos de usuarios desde la DMZ.

6.2.3 Requisitos de Gestión de Tráfico SSL/TLS

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución deberá ofrecer funcionalidad de proxy SSL. Esta funcionalidad deberá trabajar en al menos dos modos:

  - Modo túnel: No se descifra el tráfico SSL entre el cliente y el servidor, pero sí se hace validación de certificado del servidor.
  - Modo intercepción: Además de la validación de certificado, el sistema descifra y cifra el tráfico entre el cliente y el servidor

- La intercepción deberá poder realizarse de forma selectiva, en función de parámetros tales como la categoría, destino, usuario/grupo, aplicación, etc.

- La solución deberá ofrecer la posibilidad de funcionar en modo "tap", de tal forma que pueda descifrar el tráfico SSL y enviarlo a fuentes externas a través de un interfaz de red.

- La solución debe permitir la validación de certificado tanto de cliente como de servidor (mutual-SSL authentication). De esta forma el equipo debe ser capaz de presentar el certificado de cliente a un servidor.

- Sólo se considerarán como válidas aquellas plataformas que soporten, al menos, los siguientes algoritmos de cifrado (para la inspección de seguridad de tráfico https):

    - ECDHE-ECDSA-AES128-SHA256
    - ECDHE-ECDSA-AES128-GCM-SHA256
    - ECDHE-ECDSA-RC4-SHA
    - ECDHE-ECDSA-AES128-SHA
    - ECDHE-ECDSA-AES256-SHA
    - AES128-GCM-SHA256
    - AES256-GCM-SHA384
    - DHE-RSA-AES128-GCM-SHA256
    - DHE-RSA-AES256-GCM-SHA384
    - ECDHE-RSA-AES256-SHA384
    - ECDHE-RSA-AES256-GCM-SHA384
    - ECDHE-RSA-AES256-SHA384

- Debe poder inspeccionar el campo de User-Agent en una cabecera HTTPS, funcionando en modo proxy explícito, para de esta forma, establecer políticas en base a dicho User-Agent.

- La solución propuesta debe permitir definir políticas de validación del certificado digital presentado por el servidor de destino en base a criterios de fecha de validez del certificado, coincidencia entre el CN del certificado y el hostname del servidor de destino, verificación de listas de revocación vía OCSP (cuando estén disponibles) y grado de confianza en la CA que emite el certificado.

- La solución debe tener capacidad de identificar tráfico cifrado basado en protocolo TLS-v1.3. Con ello el sistema deberá poder procesar dicho tráfico, bien haciendo un downgrade a TLS-v1.2 o bien procesándolo en TLS-v1.3.

- La solución propuesta debe tener capacidad de interceptar (descifrar/cifrar) tráfico SSL/TLS de dos modos:

    - A través del propio equipo con emulación de certificado y en modo MITM
    - A través de un equipo externo dedicado al procesamiento de tráfico SSL/TLS. Este equipo externo podrá descifrar el tráfico SSL/TLS y enviárselo en claro al proxy, para luego devolverlo y volverlo a cifrar para su destino.

6.2.4 Requisitos de Filtrado de Contenidos y Gestión de Políticas

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución debe permitir el control de la descarga de ficheros, siendo posible definir reglas que impidan la descarga de ficheros en función del usuario/grupo, la categoría del sitio, etc. La solución debe ser capaz de identificar el tipo de fichero a bloquear mediante, al menos los siguientes tres modos:

    - La extensión del fichero
    - El campo Content-Type de la cabecera http
    - Mediante "Apparent Data Type" de tal forma que se lean los primeros 256 bytes del fichero, para así determinar el tipo de archivo.

- Debe incorporar un servicio de categorización web embebido, que realice la categorización en base a URL completa y no sólo en base al sitio web.

- La solución debe ofrecer multicategorización, de modo que una misma URL pueda estar categorizada dentro de varias categorías (al menos hasta 4 categorías diferentes).

- La solución debe proporcionar control de aplicaciones: La solución debe reunir las siguientes características relativas a las aplicaciones Web:

    - Tener capacidad de identificar al menos 22.000 aplicaciones Web.
    - Permitir el control de operaciones sobre estas aplicaciones. Por ejemplo, se podrá permitir el acceso a dichas aplicaciones (sitios de correo personal, redes sociales, almacenamiento on-line, etc.), pero con la posibilidad de bloquear operaciones específicas tales como subida o descarga de ficheros, envío de correos, chat, etc.
    - Tener capacidad de control de atributos sobre estas aplicaciones. Por ejemplo, determinar si una aplicación cumple el ISO-27001 o usa autenticación multi-factor, y en base a estos atributos, definir políticas de control y acceso

- La solución debe incluir una categorización específica de los contenidos de YouTube a través de la API de desarrollo proporcionada por Google. Esta categorización debe incluir categorías tales como "Howto", "Entertainment", de tal forma que se puedan establecer políticas de filtrado en base a estos contenidos.

- La solución debe tener capacidad para aplicar políticas en base al país, tanto en origen como en destino (geolocalización).

- La solución debe permitir mostrar páginas de bloqueo personalizadas, con la posibilidad de que sean diferentes en función de la categoría, grupo de usuarios, hora del día/día de la semana, etc. Asimismo, debe poder ofrecer páginas de coaching de tal forma que el usuario puede acceder a la URL solicitada, previa aceptación.

- La solución propuesta permitirá realizará la actualización automática de las aplicaciones y operaciones Web 2.0 soportadas, sin que para ello sea necesario realizar actualizaciones de software en la plataforma de control y seguridad en la navegación.

- La solución propuesta debe soportar la definición de reglas de control basados en cualquier campo de la cabecera http y https y tanto para peticiones como para respuestas.

- La solución propuesta debe permitir la definición de reglas de control basadas en el contenido del cuerpo de las peticiones y las respuestas http y https.

- La solución propuesta debe soportar la intercepción de Exchange Online de Office 365 a través del proxy MAPI, para protocolo MAPI/HTTPS.

- La solución debe ofrecer una arquitectura de Políticas Flexible. Debe proporcionar flexibilidad, control granular de protección de contenidos, control y aceleración basado en múltiples atributos tales como usuarios, grupos, sitio de usuarios, hora del día, tipo de contenido, tipo de archivo, tipo de URL, agentes, etc.

- Debe tener capacidad para permitir la definición de reglas en base a niveles de riesgo.

- La solución debe ser capaz de definir reglas y políticas de forma simple, a través de un interfaz web o a través de línea de comandos. Además se debe soportar la utilización de lenguaje de programación para la configuración de políticas en línea de comandos.

- La solución debe tener capacidad para permitir la definición de reglas multi-tenant.

- La solución debe permitir definir políticas para el control de cuotas por tiempo de uso y por volumen de tráfico.

- La solución debe permitir definir el acceso a través de la presentación de un código CAPTCHA.

6.2.5 Requisitos de Optimización y Control de Tráfico

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución deberá ofrecer mecanismos para la gestión de ancho de banda. Esta funcionalidad deberá contar con controles que apliquen la política de ancho de banda en base a:
    - Protocolo/Aplicación
    - Origen/Destino
    - Usuarios/Grupo de Usuarios
    - Categoría de URL
    - Franja Horaria

- La solución será capaz de permitir la definición de un mínimo de ancho de banda garantizado, un máximo de ancho de banda, y establecer prioridades, controlando toda la sesión y no únicamente su establecimiento.

- La solución permitirá el control del ancho de banda tanto del lado cliente como del lado servidor, y en sentido entrante y saliente.

- La solución deberá ofrecer funcionalidades avanzadas de caching. La cache podrá ser configurada para determinar qué contenido será cacheado y cuál no.

- La solución incorporará un mecanismo que permita cargar el contenido de una página y/o objetos en la cache, previamente a que se realice la primera consulta a las mismas.

- La solución será capaz de modificar los tiempos por defecto en los cuales los objetos son almacenados en la cache de la solución, independientemente de su valor original.

6.2.6 Requisitos de Control de Tráfico de Vídeo

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución debe identificar de forma clara los siguientes protocolos de vídeo: RTMP, MS Smooth Streaming, Apple HLS y Adobe HDS. Soportará los siguientes protocolos de streaming: Real Networks, Windows Media Player, QuickTime y Adobe Flash Player.

- Dentro de este tipo de tráfico cabe señalar dos tratamientos claramente diferenciados y necesarios en la organización

    - Streaming en Tiempo Real: sobre este tipo de tráfico se debe realizar un splitting del tráfico, de modo que permita compartir a todos los usuarios una única conexión entre el Proxy y el servidor origen del vídeo. De este modo, se reduce la carga sobre el servidor y se reduce el consumo de ancho de banda.
    - Vídeo bajo Demanda (VoD): la solución debe ser capaz de cachear este tipo de objetos de vídeo (incluidos objetos flash video), permitiendo que una vez que un usuario ha accedido a este contenido, el resto de accesos son servidos directamente desde la caché. También sobre este tipo de tráfico, mientras se realiza el cacheo en el primer acceso, la plataforma realizará splitting en el mismo modo que se explicó en el apartado anterior para vídeo en tiempo real.

6.2.7 Requisitos de Gestión de Logs e Informes

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución debe permitir crear logs personalizados, generando múltiples logs simultáneamente.
- La solución deberá soportar diferentes métodos y formatos de fichero de registro de actividad de los usuarios, atendiendo al usuario, grupo, o servicio. Además deberá disponer de métodos de consulta de actividad en tiempo real y diversos mecanismos de extracción con formatos personalizados, que provean reportes gráficos sobre accesos a la web con vistas por usuarios, grupos, categoría de contenido, consumo de ancho de banda, uso de mensajería instantánea e integración con herramientas y software de terceros.
- Los logs deben ser fácilmente accesibles en tiempo real, sin necesidad de equipamiento adicional. La solución deberá proveer la capacidad de analizar dichos logs en tiempo real sobre la propia plataforma. Estos logs deberán recoger toda la información relativa a la conexión, incluyendo usuario, URL, categoría, acción tomada, etc. y con la posibilidad de modificar los campos de dichos logs para incluir otra información de interés.
- Los logs de acceso a su vez deberán poder ser enviados a una máquina externa o un servidor ftp para su archivado sin que sean manipulados.
- La solución incluirá herramientas que permitan realizar reportes específicos sobre detecciones de código malicioso, identificando posibles máquinas infectadas. Los informes deben poder personalizarse en base a usuarios, protocolos, destinos, tipo de tráfico.
- La solución debe tener la capacidad para identificar Adobe Flash Player.

6.2.8 Requisitos de Integración con otros Sistemas

La solución propuesta deberá cumplir con los siguientes requisitos:

- La solución debe tener la capacidad de integrarse a través de protocolo ICAP y Secure-ICAP (ICAPS) con un sistema de análisis de contenidos para la detección de amenazas avanzadas. Este sistema debe reunir las siguientes características:

    - Debe tener capacidad de recibir el 100% de los contenidos enviados desde el módulo de análisis. El resultado del análisis del sistema de anti-malware debe dar un veredicto en tiempo real al módulo de análisis, sobre el resultado del análisis, antes de servir o no el contenido al usuario final.
    - El sistema debe ofrecer tres módulos de análisis independientes: un primer módulo basado en una base de datos de whitelist/blacklist que permita identificar mediante algoritmo de hash contenidos identificados como libres de malware. Un segundo módulo debe poder incluir hasta 2 motores de antivirus para identificar contenidos maliciosos. Los motores de antivirus no pueden ser de tipo "open-source". Un tercer módulo de análisis de código estático con capacidades de machine-learning.
    - El sistema debe incluir además la capacidad de realizar un análisis de comportamiento sobre la muestra analizada, aplicando técnicas avanzadas de sandboxing. Este análisis únicamente debe realizarse cuando ninguno de los 3 módulos anteriores hayan sido capaces de identificar el archivo.

- La solución debe tener la capacidad de integrarse con plataformas de Web-Isolation o Remote-Browsing. La integración debe basarse en funcionalidad de proxy-chaining. Debe tener la capacidad de definir un criterio de selección en base a un origen (usuario/grupo, dirección-IP, User-Agent, etc), y destino (categoría, dirección-IP, URL, etc), el cual permita decidir qué peticiones Web son redirigidas a la plataforma de Web-Isolation y cuáles no.

7. SERVICIOS

Los servicios profesionales, incluidos en la oferta, deberán garantizar la instalación de dicho equipamiento y su correcta configuración final que garantice, sin lugar a dudas, el funcionamiento del conjunto instalado final.

Todas las tareas de instalación y configuración se consensuarán y planificarán con el personal técnico de VEIASA que ésta designe. Todos los trabajos, tanto dentro como fuera de horario, se realizarán de forma que no interrumpan el normal funcionamiento y la disponibilidad de los servicios informáticos de VEIASA.

Se deberán, por tanto, cumplir los siguientes puntos:

- Planificar conjuntamente entre VEIASA y el adjudicatario la fecha de realización del servicio con antelación suficiente.

- Las instalaciones pueden requerir la actuación fuera del horario laboral, si entraña riesgo de afección al servicio que se presta actualmente a los usuarios.

- VEIASA designará un responsable, como punto focal, para toda la comunicación relativa al servicio, facultado para actuar en nombre VEIASA.

- El adjudicatario impartirá al menos una jornada de formación a los administradores de sistemas que VEIASA designe, orientada a la operación de la plataforma en el día a día.

En virtud del artículo 62 LCSP, se designa como responsable del contrato al Jefe de la Unidad de Mantenimiento de Sistemas de Información, a quien corresponderá supervisar su ejecución y adoptar las decisiones y dictar las instrucciones necesarias, con el fin de asegurar la correcta realización de la prestación pactada, dentro del ámbito de facultades que el órgano de contratación le atribuya.

7.1 Fases del Servicio y Plazos de Ejecución

7.1.1 Instalación y configuración

Los materiales a suministrar deberán ser instalados y configurados, realizando las tareas de actualización del firmware y configuración del software, de forma que queden totalmente operativos. Se acordará con VEIASA la planificación y ejecución de estas tareas de forma que no impacten en el normal funcionamiento de los servicios informáticos.

7.1.2 Periodo de pruebas y verificación

Se deberá de contemplar un periodo de pruebas y verificación del suministro e instalación antes de su puesta definitiva en producción. Dicho periodo será igualmente consensuado con los técnicos de VEIASA. En el caso que las pruebas no tengan resultado satisfactorio, el fabricante procederá a realizar las correcciones oportunas hasta que obtenga la validación por escrito de VEIASA.

Durante este periodo se realizará la jornada de formación al personal técnico que VEIASA designe.

7.1.3 Puesta en marcha en producción

Una vez comprobado el perfecto funcionamiento del sistema tras el periodo de pruebas, se procederá a la puesta en producción definitiva del suministro, realizando las labores y ajustes necesarios. Durante esta fase, el personal del fabricante estará presente en las instalaciones de VEIASA, hasta la comprobación definitiva del perfecto funcionamiento del sistema.

7.1.4 Plazos de Ejecución

- Suministro del equipamiento: 25 días, a contar desde la comunicación del pedido al adjudicatario.

A continuación se fijan los plazos de instalación, configuración, pruebas y puesta en marcha, que se computarán a partir de la fecha en que se realice el suministro:

- Instalación física de los equipos: 2 días.
- Pruebas de integración y rendimiento: 2 días.
- Puesta en marcha: 1 día.

7.2 Equipo de Trabajo

El equipo de trabajo asignado por la empresa adjudicataria deberá realizar las tareas descritas en el punto 7.1 relativas a: instalación, configuración, pruebas y puesta en marcha.

Los técnicos asignados deberán aportar experiencia de al menos 3 años en los últimos 5 años en instalaciones similares, entendiendo por similar aquellas realizadas en equipos del mismo modelo o superior al ofertado.

8. GARANTÍA Y MANTENIMIENTO CORRECTIVO

Todos los equipos deberán contar con un servicio de garantía y mantenimiento correctivo durante las veinticuatro horas del día, los siete días de la semana, en la modalidad de 24x7.

Este servicio conjunto de garantía y mantenimiento tendrá una duración mínima de 3 años, y empezará a surtir sus efectos desde el momento en que VEIASA preste su conformidad a la totalidad del suministro, instalación y puesta en funcionamiento de los equipos, conforme a lo establecido en el presente pliego de prescripciones. La empresa adjudicataria deberá suministrar los documentos necesarios que justifiquen dicha garantía.

Así mismo, las licencias adquiridas otorgarán derecho de uso, así como acceso a soporte y actualizaciones durante al menos 3 años.

9. ACUERDOS DE NIVEL DE SERVICIO

A continuación se especifican los requisitos mínimos exigidos por VEIASA en cuanto a los niveles de servicio, que se medirán de forma mensual:

SERVICIO	INDICADOR	DESCRIPCION	VALOR
Plazo Total de Ejecución	I1	Tiempo de puesta en producción de la solución: Suministro, Instalación, Configuración, Pruebas y Puesta en Marcha.	<= 1 mes
Servicio de Soporte	S1	Tiempo de respuesta para Incidencias de alta prioridad o críticas	< 30 minutos
	S2	Tiempo de respuesta para Incidencias de media prioridad	< 2 horas
	S3	Tiempo de respuesta para Incidencias de baja prioridad	< 4 horas

10. SEGURIDAD

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero. En concreto, se deberá asegurar

el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes, considerando que el sistema de información recae en la categoría de seguridad MEDIA conforme a los criterios establecidos en el anexo I del ENS.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccn-cert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.