PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE “SUMINISTRO, PUESTA EN MARCHA, OPERACIÓN Y MANTENIMIENTO DE UN SISTEMA PARA LA DETECCIÓN DE ANOMALÍAS, INTRUSIONES Y VULNERABILIDADES EN REDES INDUSTRIALES CON GESTIÓN DE INVENTARIO, DISEÑO DE ARQUITECTURA PARA LA SEGREGACIÓN E IMPLEMENTACIÓN DE REDES EN LOS ENTORNOS DE IT Y SISTEMAS DE CONTROL INDUSTRIAL (OT) DE AGUAS DEL ARCO MEDITERRÁNEO, S.A.”

INDICE

1. ANTECEDENTES

La Empresa Aguas del Arco Mediterráneo, S.A. (en adelante, AGAMED), es una sociedad mixta cuyo objeto social es la gestión de servicios y suministros de aguas en el término municipal de Torrevieja.

La principal actividad de es la gestión del Ciclo Urbano del Agua, desde su compra, la distribución, el mantenimiento de la red de saneamiento, el control de vertidos y la depuración del agua residual.

AGAMED es una empresa comprometida medioambiental y socialmente responsable, contando con los siguientes sistemas de gestión certificados: normas de calidad (ISO 9001); medioambiental (ISO 14001); prevención de Riesgos Laborales (ISO 45001); gestión de la inocuidad del agua (ISO 22000); y sistema de gestión de continuidad de negocio (ISO 22301). De esta forma, los proveedores de AGAMED deben conocer las políticas definidas en nuestros sistemas de gestión e implantar buenas prácticas en esta línea, así como ajustarse a dichos procedimientos.

A raíz de la transposición de la ley NIS (RD 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información) y el RD 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, AGAMED es considerado un operador de servicios esenciales y es necesaria la protección de la empresa implementando las soluciones técnicas pertinentes.

AGAMED como prestador de servicios esenciales, debe considerar las medidas de protección de la información, conforme a la legislación y regulación, tanto española como europea, siendo éste el marco de seguridad a aplicar, tanto como parte del servicio como para garantizar la seguridad y cumplimiento de la legislación.

A destacar entre dicha legislación está el Esquema Nacional de Seguridad (ENS), Ley de Administración Electrónica, Ley Orgánica de Protección de Datos (LOPD), Reglamento General de Protección de Datos europea (GRPD), Ley de Protección de Infraestructuras Críticas (LPIC), Directiva europea NIS, entre otras.

Además, el adjudicatario deberá considerar las disposiciones de desarrollo de las normas anteriores y las que apliquen en materia de seguridad de la información.

Los sistemas de control industrial (en adelante, SCI) constituyen la base de la operación en la mayoría de los procesos de la compañía, por tanto, es prioritario para AGAMED implementar las medidas necesarias para defenderlos y protegerlos de cualquier amenaza relacionada con la seguridad de la información y la ciberseguridad.

2. OBJETO

El objeto del presente contrato es implementar, mediante un plan de mejora continua, las acciones preventivas y de respuesta, así como las medidas necesarias para garantizar la seguridad de nuestro SCI, disminuir vulnerabilidades y proteger el SCI frente a cualquier ataque que pueda comprometer su correcto funcionamiento y, de esta forma, afectar gravemente al servicio de agua y alcantarillado que AGAMED presta al municipio de Torrevieja.

La protección necesaria en AGAMED, para la infraestructura del SCI, requiere el aprovisionamiento de soluciones técnicas y servicios de ciberseguridad que nos permitan asegurar la detección, protección y respuesta frente a los ataques de seguridad de la información.

2.1. DETECCIÓN DE ANOMALÍAS

Desarrollo e implantación de un sistema para la detección de anomalías, intrusiones y vulnerabilidades de las redes industriales, incluyendo: gestión del inventario de componentes y elementos que pertenecen a la red industrial del SCI de agua y saneamiento de AGAMED; diseño de arquitectura e implementación de licencia del sistema de detección. El sistema debe obtener visibilidad sobre los activos existentes en la red del SCI, control de configuraciones, gestión de

vulnerabilidades y alarmas predictivas que nos permitan disponer de mayor control en los activos de comunicaciones del SCI, así como una detección temprana de anomalías.

El sistema debe ser de baja intrusión en las comunicaciones del SCI y en ningún caso debe bloquear acciones de los operadores o interferir en el óptimo tráfico de las redes de comunicaciones. Es un sistema de alertas que garantiza que en ningún caso se introduce tráfico no autorizado o proveniente del exterior de las redes del SCI. El sistema debe ser capaz de identificar aquellas situaciones que puedan suponer un riesgo para la infraestructura del SCI y en la definición de reglas para su detección, partiendo de un análisis previo de reconocimiento de patrones.

La solución debe contemplar los protocolos de comunicaciones industriales, analizando también el payload (datos útiles) de los paquetes, con el objetivo de identificar comandos, descargar o cargar programas en los PLC, escanear la red del SCI para identificar los equipos que forman parte de ella, envío de comandos potencialmente peligrosos DPI (Deep Packet Inspection), o cualquier otra técnica relacionada con el ataque al SCI.

El sistema minimizará los riesgos asociados a la seguridad del SCI en cuanto a:

- Control de acceso a la red SCI
- Control de acceso a los elementos del SCI
- Gestión de vulnerabilidades y actuaciones de seguridad
- Inventario de activos de información
- Propiedad de los activos de información
- Uso aceptable de los activos de información
- Supervisión continua y monitorización
- Respuesta temprana a incidentes

Además, necesitamos que el sistema facilite la elaboración de un inventario de componentes y comunicaciones, que refleje de forma fidedigna la instalación del SCI. Los atributos mínimos necesarios para cada activo deben ser:

- Identificación unívoca (id)
- Categoría del activo
- Nombre del activo
- Descripción de activo / rol
- Propietario del activo
- Versión del sistema, firmware o aplicación
- Software configurado
- Hardware configurado
- Localización física y lógica
- Si existe soporte vigente del proveedor
- Criticidad del activo

Es importante elaborar un procedimiento de actualización del inventario de equipos y control de versionado.

2.2. SEGREGACIÓN DE REDES

El objetivo que se pretende es segregar las redes de IT y OT mediante electrónica de red basada en tecnología Firewall de última generación y alta disponibilidad, siendo capaces de inspeccionar el tráfico en las comunicaciones industriales sobre la capa 7 (capa de aplicación según la torre de protocolos OSI). Debe permitirse filtrar por características propias de un protocolo de comunicaciones, bloqueando o modificando el resultado. Esta tecnología, en conjunto con la propuesta de arquitectura, asegurará la seguridad perimetral de la red del SCI. La solución debe permitir aislar la red de proceso industrial del resto de redes de negocio, mediante el diseño de un juego de reglas de filtrado robusto del tráfico entrante y saliente, entre las diferentes zonas:

- Zona de proceso SCI: donde se ubicarán los equipos pertenecientes al centro de control industrial, necesarios para el funcionamiento y operación del SCI.
- Zona de salto: donde serán ubicadas las máquinas de salto.
- Zona DMZ (Demilitarized Zone) o de intercambio: donde se alojarán las máquinas para la explotación de datos por parte de la red de negocio.
- Zona IT/Red de negocio: segmento de red existente para servidores y servicios de información de la organización.

La segregación de redes debe tener capacidad para filtrar el tráfico en base a puertos y en base a aplicaciones, siendo este último un filtrado más robusto que disminuye considerablemente las capacidades de evasión. La solución debe incluir un juego avanzado de reglas para cubrir las necesidades de seguridad del SCI, por ejemplo: bloqueo de internet; bloqueo de correo; bloqueo de peticiones desde IT, configuración de reglas para realizar consulta de datos al SCI, etc. La definición y configuración de reglas se hará en base a usuarios, logrando así un mayor grado de granularidad aplicando las buenas prácticas definidas como principio del mínimo privilegio (PoLP).

La segregación de redes debe capacitar la detección y bloqueo de amenazas de ciberseguridad, incluyendo APT's, filtrado de URL's y detección de ejecución o existencia de código malicioso.

Así, el sistema propuesto permitirá reducir los riesgos asociados a la seguridad de nuestro SCI, sobre los siguientes conceptos:

- Control de acceso a la red del SCI
- Control de acceso para los elementos que componen el SCI
- Gestión de vulnerabilidades y actualizaciones de seguridad
- Protección zona exterior
- Protección perimetral
- Áreas protegidas
- Protección de áreas o zonas
- Acceso local al SCI
- Acceso remoto al SCI
- Acceso Wireless
- Control de trabajos en zonas seguras
- Protección anti-malware

2.3. OPERACIÓN, SOPORTE, MANTENIMIENTO E INFORMES DE SEGUIMIENTO

El documento de propuesta deberá contar con la descripción del servicio de operación y gestión de las soluciones, que permitirá evolucionar todas las funcionalidades habilitadas, afinar las políticas iniciales, desarrollar nuevas políticas con la granularidad requerida por las necesidades de seguridad de AGAMED, a lo largo de la vigencia del contrato.

3. ALCANCE

En la elaboración de la oferta se ha de considerar como alcance el equipamiento de la infraestructura de red de los sistemas de control industrial (SCI) propiedad de AGAMED, incluyendo el centro de proceso de datos donde existen los sistemas SCADA, centro de control y puesto de operación, puesto de cliente para gestión y explotación del SCI y de todos los dispositivos integrados en la red que conforma el SCI de AGAMED.

La oferta debe incluir todos los módulos, licencias y equipos necesarios para cubrir los requisitos funcionales y técnicos descritos. El licitador debe incluir en su oferta una propuesta de diseño de la arquitectura a implantar sobre el SCI de AGAMED, que refleje el alcance del pliego y recoja la realidad de la infraestructura, proporcionando un diseño real y verídico del sistema propuesto.

Si durante la vigencia del contrato se incorpora alguna instalación adicional a la gestión de AGAMED, esta quedará automáticamente incluida en el ámbito del presente pliego.

Como requisitos de buenas prácticas de operación del SCI, forma parte igualmente del alcance, la conexión e integración de los datos del sistema con el servicio de operación y monitorización para la prestación de servicios de ciberseguridad desde y hacia el SOC360 de SUEZ España.

3.1. DETECCIÓN DE ANOMALÍAS

El alcance de la solución debe permitirnos obtener visibilidad, gestión, detección, identificación y control de todos los activos que conforman la red del SCI, así como identificar anomalías, vulnerabilidades y/o analizar cualquier acontecimiento que se presente en las redes OT pertenecientes al SCI.

Con el fin de poder gestionar la totalidad de los equipos industriales pertenecientes al SCI de AGAMED, la gestión del inventario, detección de intrusiones, detección de anomalías y/o vulnerabilidades, debe realizarse sobre los elementos como sobre el tráfico de los equipos conectados mediante protocolos TCP/IP, así como sobre los equipos conectados mediante otros protocolos de comunicaciones de AGAMED.

3.2. SEGREGACIÓN DE REDES

El alcance consiste en la protección de los sistemas de automatización industrial, propiedad de AGAMED, mediante la segregación de las redes de tecnologías de información (IT) y de las tecnologías de operación (OT). Los servicios deben comprender la electrónica de red basada en tecnología de cortafuegos de alta disponibilidad, las correspondientes licencias, el análisis de la infraestructura, la implantación, configuración y puesta en marca, así como la documentación del proceso y soporte del fabricante. La solución debe asegurar la seguridad perimetral de la red del SCI. El diseño de la solución aislará la red del proceso industrial del resto de redes de negocio, a través de filtrado robusto del tráfico entrante y saliente entre las diferentes zonas.

3.3. SERVICIOS DE OPERACIÓN Y MANTENIMIENTO DE LA SEGURIDAD, NIVEL 1 Y 2

Las soluciones permitirán la realización de las actualizaciones necesarias para el funcionamiento de las plataformas y mantenimiento de estas, además de encargarse de implementar las acciones para garantizar el correcto funcionamiento de la solución y, por tanto, el cumplimiento de su función para la seguridad de AGAMED. Ante cualquier fallo y/o anomalía que presente la solución, se recibirá el apoyo del proveedor a lo largo de la vida del contrato, debiendo acreditar el licitador disponer de Atención postventa y servicios de mantenimiento y soporte anual de la solución a adquirir. Igualmente, soporte técnico a usuarios en español y Facilidades para capacitación (ej., presencial, vía web u otros).

4. LUGAR DE EJECUCIÓN

La ejecución de los trabajos se llevará a cabo, tanto en las oficinas y dependencias del adjudicatario, como en las instalaciones donde reside el centro de control industrial de AGAMED, sitas en C/ Caballero de Rodas 41, 2ª Planta de Torrevieja (Alicante).

5. REQUISITOS Y CONDICIONES TÉCNICAS DEL CONTRATO

Los requisitos necesarios para cumplir el alcance anteriormente descrito y que debe satisfacer esta licitación, serán descritos a continuación y estarán conformes con la siguiente normativa:

- Ley 8/2011, de 28 de abril, por la que se establecen medidas de protección para las infraestructuras críticas.
- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.

- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de infraestructuras críticas.
- Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- RD 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

AGAMED, como operador de infraestructuras esenciales, debe considerar las medidas de protección de la información, conforme a la legislación y regulación vigente, tanto española como europea, siendo éste el marco de seguridad a aplicar, tanto como parte del servicio como para garantizar la seguridad y cumplimiento de la legislación. A destacar, el Esquema Nacional de Seguridad (ENS), la Ley de Administración Electrónica, Ley Orgánica de Protección de Datos (LOPD), Reglamento General de Protección de datos (RGPD), Ley de Protección de Infraestructuras Críticas (LPIC), Directiva Europea NIS, entre otras. Además, el adjudicatario deberá considerar las disposiciones de desarrollo de las normas anteriores y las que apliquen en materia de seguridad de la información durante la totalidad del periodo de vigencia del contrato.

5.1. DETECCIÓN DE ANOMALÍAS

La detección de anomalías en procesos industriales es un tema de alto impacto que ha sido analizado y estudiado por diversas áreas de investigación. La mayor parte de los métodos de detección actualmente disponibles posibilitan el análisis de irregularidades sobre el historial de uno o varios procesos, ayudando a extraer información significativa en una amplia variedad de aplicaciones. Entre los sistemas que ayudan a detectar, responder e informar de forma temprana las posibles amenazas, se encuentran los sistemas de detección de intrusos y anomalías de red, de tipo “no invasivo”, que son específicos para entornos de tecnologías de operación. Estos sistemas supervisan de forma pasiva el tráfico de los sistemas de control industrial, aprenden el funcionamiento de la red de operación y establecen cuál es el procedimiento normal de operación. Cuando el sistema detecta algún comportamiento en la red que no corresponde con lo aprendido, inmediatamente lanza una alerta informando de anomalías. En esta línea, nuestra organización requiere de una solución para la detección de intrusiones y/o anomalías, que posibilite el inventario en tiempo real, detección de vulnerabilidades y gestión de las mismas, para toda la red e instrumentación del SCI.

5.1.1. REQUERIMIENTOS DEL SISTEMA

Nuestro objetivo es disponer de una solución que nos permita obtener visibilidad, gestión, detección y control de las anomalías, activos del SCI, detectar vulnerabilidades y/o cualquier acontecimiento que se presente en las redes de OT. Por tanto, la solución debe contemplar, como mínimo, los siguientes requisitos:

a) Requisitos técnicos generales:

- La solución técnica no debe ser invasiva. Los fabricantes de sistemas de control industrial no permiten la instalación de agentes no certificados sobre sus plataformas. Además, el sistema no debe afectar de ninguna forma a las comunicaciones entre el centro de control y la instrumentación. Por lo anterior, el licitador debe indicar claramente cómo la solución ofertada realiza el proceso de detección de anomalías y la gestión de vulnerabilidades sobre ecosistemas OT.
- Madurez de la solución, con al menos 3 años de presencia en el mercado.
- Debe permitir la detección y gestión de activos del SCI.
- Realizará detección y gestión de amenazas, tanto sobre la instrumentación como sobre la red del SCI.
- Con capacidad para obtener las relaciones entre los dispositivos existentes en el SCI, en tiempo real.
- La solución tendrá capacidad de autoaprendizaje.

- Solución no intrusiva y pasiva, cuyo diseño nos permita recibir una copia del tráfico de red de la infraestructura OT.
- Debe detectar elementos no autorizados en la red.
- Debe permitir establecer reglas estándar y/o configurables, para facilitar la detección de intrusiones.
- La solución permite identificar y categorizar las anomalías detectadas.
- La solución permite establecer alertas de anomalías de funcionamiento, para el control de la infraestructura.
- La actualización de las reglas de detección de amenazas podrá actualizarse de forma manual o automática.
- La solución permite identificar y categorizar las vulnerabilidades detectadas sobre los activos del SCI, mediante análisis pasivos de la información circulante en la red de OT y/o mediante la inspección interna remota del activo.

También debe proveer la solución y/o mitigación de las vulnerabilidades identificadas, según su categorización.

- La solución cuenta con un sistema de monitorización y control centralizada de los eventos.
- La solución puede implementarse tanto en entornos físicos, como sobre entornos virtuales, o mixtos.
- Para entornos virtualizados, la solución tendrá capacidad para soportar al menos 300 dispositivos/activos, con un consumo no superior a 16 GB de RAM y/o cuenta con una solución hardware para ahorro de recursos del SCI.
- Permite la integración de dispositivos de campo de distintas marcas y modelos.
- La solución incluye la consola de gestión local física y la conexión para gestión
- y administración remota desde una consola centralizada.

b) Requisitos funcionales:

La funcionalidad de la solución entendida como “la capacidad del software de proveer y cumplir las funciones necesarias para satisfacer las necesidades específicas de AGAMED, en relación con la visibilidad, gestión y control de las anomalías, activos, vulnerabilidades y cualquier acontecimiento que se presente en nuestras redes OT”.

- La solución debe integrarse sobre software y protocolos de comunicaciones industriales de más de 15 fabricantes.
- La solución debe integrarse y puede operar sobre diferentes plataformas de sistema operativo.

5.1.2. REQUERIMIENTOS DE LA PUESTA EN MARCHA

A continuación, se plasman los requisitos y actividades concretas a desarrollar en la puesta en marcha del contrato.

a) ENTREGA DE EQUIPOS

El suministro de los equipos se recibirá en el lugar de ejecución mencionado anteriormente, para su instalación en AGAMED. El plazo máximo de suministro de los equipos será de **6 semanas** a contar a partir de la formalización del contrato.

b) IMPLANTACIÓN, PRUEBAS Y PUESTA EN PRODUCTIVO

El adjudicatario llevará a cabo las siguientes tareas de puesta en marcha, durante

la ejecución el contrato:

- Montaje y pruebas de funcionamiento. La fecha límite para la ejecución del montaje y las pruebas será de **8 semanas** a partir de la fecha de entrega de los equipos.
- Es indispensable conocer la arquitectura completa de la red del SCI de AGAMED para poder implementar las diferentes medidas de protección y entender los riesgos de

acceso a las instalaciones industriales de forma remota. Para ello, el adjudicatario deberá documentar la arquitectura de seguridad del SCI, incluyendo:

  - Diagrama de red lógico: flujo de información existente en nuestra red OT y la forma en que se comunican entre sí los dispositivos, incluyendo subredes, dispositivos de comunicaciones, protocolos de red, dominios, topología de red, etc. Deben contemplarse las diferentes zonas de seguridad.
  - Diagrama físico: diseño de los elementos físicos de la red, como switches, routers, incluidos cables y hardware. Debe indicarse los puertos de conexión, información VLAN, rangos de IP, etc.
  - Diagrama de flujo de datos: incluyendo las comunicaciones que se establecen entre los diferentes activos de la red OT.
  - Arquitectura de servidores.
  - Diagrama del sistema de Backup.
- Desarrollo de un procedimiento que asegure el mantenimiento de la documentación actualizada de la arquitectura del SCI.
- Formación al equipo encargado de la gestión y explotación de la solución desplegada, coordinándose y consensuándose esta formación con AGAMED.

c) DOCUMENTACIÓN DE LA IMPLANTACIÓN

El licitador deberá presentar, una vez finalizadas las fases de implantación, pruebas, puesta en marcha e integración, la documentación técnica justificativa del cumplimiento de las especificaciones técnicas requeridas en el presente pliego de prescripciones técnicas particulares, que nos asegure la correcta configuración de la herramienta, un rendimiento de redes adecuado, pruebas de estrés con carga de tráfico a analizar, presencia de ataques o vulnerabilidades, equipamiento de control y servidores con análisis de tráfico, y cualquier documentación que sea necesaria para garantizar que se ha realizado correctamente la implantación, configuración y puesta en productivo de la solución propuesta.

5.2. SEGREGACIÓN DE REDES

Consiste en la instalación, diseño y puesta en productivo del equipamiento de electrónica de red, basada en tecnología Firewall High Availability (alta disponibilidad), con licenciamiento y software necesario, que permita implantar políticas y herramientas que protejan la red del SCI, realizando filtrado de URL, protección de phishing, ejecución de comandos maliciosos, ransomware, tráfico no deseado, análisis y detección de malware conocido o desconocido, falsificación de respuestas a una consulta DNS para un dominio o URL malicioso, etc.

5.2.1. REQUERIMIENTOS DEL SISTEMA

Las características mínimas que debe cumplir la solución propuesta por el licitador para la segregación de redes del SCI de AGAMED son las siguientes:

- Debe aislarse la red de OT, controlando el tráfico entrante y saliente, del resto de segmentos de la red de negocio, proporcionando un filtrado robusto.
- Basado en tecnología Next Generation, que trabaje a nivel de capa 7 del modelo OSI, filtrando el tráfico en base a las aplicaciones, además del filtrado a nivel puertos y protocolos. Para ello, deberá contar con los siguientes módulos:
  - Advance Persisten Threat (APT): capacidad para detector y bloquear amenazas de forma avanzada, puede evadir las detecciones y controles tradicionales. Al mismo tiempo, ofrece visibilidad total del tráfico para detectar intentos de evasión, como: uso de puertos no estándar, encriptación SSL y otras opciones que puedan poner en riesgo la gestión y operación de nuestro SCI.
  - Filtrado de URLs: permite controlar el tráfico web aplicando restricciones a nivel URL o categorías de URLs. Cuenta con bases de datos de categorización propia con capacidad para integrarse con bases de datos de terceros, de esta forma

pueden adquirir millones de URLs categorizadas que ya existen actualmente y que son actualizadas de forma periódica por terceros.
    - Descifrado de tráfico SSL: permite obtener visibilidad sobre el tráfico cifrado e incorporar políticas de seguridad personalizadas, según el tipo de tráfico analizado, ayudando a conocer y encontrar amenazas ocultas, y otorgando una visión amplia de los riesgos a los que nos enfrentamos.
    - Detección de robo de credenciales y posibilidad de doble factor de autenticación (MFA): que brinda una capa de seguridad adicional y permite garantizar la veracidad y autenticidad del usuario que accede al sistema.
- Integración con nuestro directorio activo que nos permita desplegar políticas de seguridad específicas para el usuario detectado.
- Solución robusta frente a fallos, que proporcione alta disponibilidad. En el caso de caída no debe existir afectación al servicio productivo y debe disponer de fuente de alimentación redundada.
- Permite realizar backups de las configuraciones realizadas.
- La administración de la solución se puede realizar de forma centralizada, ofreciendo visibilidad del tráfico que se produce en cada nodo y pudiendo gestionar los aspectos de configuración para cada uno de ellos, aplicar políticas globales y generar reportes específicos de patrones de tráfico, amenazas de seguridad, entre otros.
- Capacidades de sandboxing para la ejecución y detección de código malicioso basado en "comportamiento", que permite testear y bloquear tráfico con contenido malicioso desconocido.
- Debe integrar los eventos generados a un sistema de monitorización y control de eventos centralizado (SIEM).
- La solución permitirá configurar monitorización por protocolo simple de administración de red (SNMP).
- Para proteger el entorno crítico de operación, la solución puede bloquear el acceso a internet y al correo electrónico a la red del SCI.
- Restricción de acceso a la red del SCI a un listado concreto de activos, imposibilitando el acceso a cualquier activo que no esté previa y debidamente autorizado.
- Impedir que los equipos de la red del SCI puedan ofrecer servicios fuera de la propia red directamente.
- Permite configurar un diseño robusto y seguro para el intercambio de datos y comunicación entre la red del SCI y la red de negocio.
- Los equipos Firewall a instalar deben disponer de las siguientes capacidades:
    - Pueden soportar más de 500 Mbps de ancho de banda de análisis de tráfico a nivel aplicación (capa 7 modelo OSI).
    - Pueden soportar más de 200 Mbps de ancho de banda en prevención de amenazas.
    - Pueden soportar más de 4.000 conexiones por segundo.

5.2.2. REQUISITOS DEL DISEÑO DEL SISTEMA A INSTALAR

El diseño definitivo de la arquitectura securizada será el obtenido del propio análisis inicial que se ha llevado a cabo en la primera fase del proyecto. Dicho diseño diferencia las siguientes partes:

- Diseño de la segregación de entornos IT/OT basado en zonas y best practises.
- Diseño de la red de ciberseguridad.

a) DISEÑO DE LA SEGREGACIÓN DE ENTORNOS IT/OT BASADO EN ZONAS Y BEST PRACTISES.

- En base a las protecciones, se definen los siguientes módulos a implementar:

- Módulo de identificación de vulnerabilidades y amenazas en las comunicaciones: permite bloquear el tráfico en función de la categorización y criticidad asignada. Detecta ataques de denegación de servicio (DDOS), virus, vulnerabilidades, etc., de los equipos en función de la correlación de eventos de tráfico.
- Módulo para analizar ficheros detectados en las comunicaciones: en caso de detectar un fichero malicioso debe generar firmas para bloquearlo en las siguientes comunicaciones. Los registros de actividad (logs) que genera este módulo deben permitir detectar posibles infecciones.

- En base a la revisión actual de las comunicaciones de la infraestructura, se diseñará la mejor arquitectura securizada, diferenciando al menos las siguientes zonas:
  - Zona de proceso SCI: donde se ubican todos los equipos propios de la rede de control industrial, necesarios para el funcionamiento y operatividad del SCI.
  - Zona de salto: donde se ubican las máquinas de salto.
  - Zona DMZ o de intercambio: donde se alojan las máquinas para la explotación de datos, por parte de la red de negocio.
  - Zona insegura IT/Red de negocio: corresponde al segmento de red existente para los servidores y servicios de los sistemas de información de AGAMED que corresponden a negocio (IT).

b) DISEÑO DE LA RED DE CIBERSEGURIDAD

- El diseño debe disponer de una red dedicada y asilada, para alojar las herramientas de ciberseguridad, proporcionando independencia del resto de redes y sistemas, tanto de la red corporativa IT, como de la red de OT del SCI.

  Este diseño debe configurarse para que pueda adaptarse a posibles adquisiciones futuras de plataformas de seguridad.

- Esta zona, llamada *red de ciberseguridad*, debe ser bastionada y securizada de forma que no pueda ser comprometida desde las redes de OT o de negocio:
  - El control de acceso será provisto por el cortafuegos, quien controlará el acceso a los activos de la red de OT.
  - La seguridad de autenticación proporcionada por los propios sistemas.
  - El sistema de gestión de credenciales desplegado en AGAMED.
  - Se podrá enviar una copia del tráfico de la red del SCI a la red de ciberseguridad, de forma unidireccional.
  - La red de ciberseguridad debe albergar todos aquellos sistemas/componentes de gestión de las diferentes soluciones de ciberseguridad desplegadas. Entre ellas, pueden estar:
  - Consola de gestión de los Firewall.
  - Consola de gestión de antivirus, listas blancas y bloqueo de dispositivos externos.
  - Colector de eventos del SIEM.
  - Sistema de gestión y detección de intrusiones y anomalías.
  - Sistema de gestión continua de vulnerabilidades (CIS).
  - Sistema de detección de malware avanzado, respuesta ante incidentes (IR) y análisis forense.
  - Sistema de gestión de ticketing.
  - Sistema de gestión de credenciales.
  - Sistema de autenticación remota.
  - Sistema de transferencia de ficheros entre zonas.

5.2.3. REQUISITOS DE LA PUESTA EN PRODUCTIVO DEL PROYECTO DE SEGREGACIÓN DE REDES

Las actividades concretas para desarrollar la puesta en marcha serán las siguientes:

a) ENTREGA DE LOS EQUIPOS

El suministro de los equipos que conforman el sistema objeto de licitación se efectuará, para su instalación en AGAMED, en un plazo máximo de **6 semanas** a contar a partir de la formalización del contrato.

b) IMPLANTACIÓN, PRUEBAS Y PUESTA EN MARCHA

Las principales tareas serán las siguientes:

- Análisis de la arquitectura actual existente.
- Estudio en alto nivel de la infraestructura actual, para ello se proporcionará al licitador la información necesaria, extraída de la consola de gestión centralizada corporativa.
- Instalación física de los equipos. El adjudicatario contará con la colaboración del personal de AGAMED para coordinar las tareas de ubicación, enracado, cableado, etc., de los equipos físicos, sobre la actual infraestructura de AGAMED. Tareas que deberá realizar el adjudicatario.
- Instalación inicial de los dispositivos y puesta en marcha, atendiendo a los criterios previamente establecidos para el resto de la solución y los requerimientos sugeridos por fabricante:
  - Solicitar las IPs de gestión de los equipos y proceder a su configuración. AGAMED gestionará previamente las direcciones IP con el operador.
  - Instalación y puesta en marcha, siguiendo las configuraciones recomendadas por fabricante, tales como: configuración de acceso a la red, configuración de la interfaz de gestión, hostnames, ajustes de los DNS, servidor de actualización y servidor PROXY, Network Time Protocol (NTP), verificación e instalación de nuevas versiones de software y cambio de contraseña para administradores. Todas las configuraciones anteriores se basarán en parámetros proporcionados por AGAMED en el momento de la instalación.
  - Registro del cortafuegos con el servicio de soporte de fabricante.
  - Activación de las licencias pertinentes.
  - Gestión de la actualización de contenidos dinámicos. Verificación e instalación de nuevas versiones y configuración de las actualizaciones automáticas.
  - Conexión y configuración de las interfaces-zonas y routing necesario (según instalación actual).
  - Configuración HA (activo-pasivo) de los equipos suministrados. Definición de las condiciones de balanceo. Pruebas de contingencia para validar la configuración de alta disponibilidad.
  - Activar User-ID en las correspondientes zonas y configurar los agentes de User-ID.
  - Colaboración para la integración con la herramienta de gestión centralizada corporativa.
  - Creación de perfiles de seguridad según las mejoras prácticas del fabricante.
  - Configuración de envío de logs a la herramienta de gestión centralizada corporativa.
  - Creación de un perfil de reenvío de logs.
  - Colaboración para el envío de los logs de la herramienta de gestión centralizada corporativa a otros sistemas de análisis (Splunk).

Además de la solución aportada, el adjudicatario debe llevar a cabo las siguientes tareas de puesta en marcha, durante la duración del contrato:

- Montaje y pruebas de funcionamiento. La fecha límite para la ejecución de esta segunda fase será de **8 semanas** a partir de la fecha de entrega de los equipos.
- Para implementar las diferentes medidas de protección que se pueden adoptar en nuestro SCI, entender los riesgos para acceder a nuestras instalaciones industriales de forma remota y adaptar las soluciones en un escenario seguro, es necesario conocer la arquitectura completa de la red de control. Para ello, el adjudicatario debe documentar la arquitectura de seguridad del SCI, incluyendo como mínimo la siguiente información:
  - Diagrama de red lógico: flujo de información existente en nuestra red OT y la forma en que se comunican entre sí los dispositivos, incluyendo subredes, dispositivos de comunicaciones, protocolos de red, dominios, topología de red, etc. Deben contemplarse las diferentes zonas de seguridad indicadas anteriormente.
  - Diagrama físico: diseño de los elementos físicos de la red, como switches, routers, incluidos cables y hardware. Debe indicarse los puertos de conexión, información VLAN, rangos de IP, etc.
  - Diagrama de flujo de datos: incluyendo las comunicaciones que se establecen entre los diferentes activos de la red OT.
  - Arquitectura de servidores.
  - Diagrama del sistema de Backup.
- Desarrollo de un procedimiento que asegure el mantenimiento de la documentación actualizada de la arquitectura del SCI.
- Formación al equipo encargado de la gestión y explotación de la solución desplegada, coordinándose y consensuándose esta formación con AGAMED.

c) DOCUMENTACIÓN DE LA IMPLANTACIÓN

El licitador deberá presentar, una vez finalizadas las fases de implantación, pruebas, puesta en marcha e integración, la documentación técnica justificativa del cumplimiento de las especificaciones técnicas requeridas en el presente pliego de prescripciones técnicas particulares, que nos asegure la correcta configuración de la herramienta, un rendimiento de redes adecuado, pruebas de estrés con carga de tráfico a analizar, presencia de ataques o vulnerabilidades, equipamiento de control y servidores con análisis de tráfico, y cualquier documentación que sea necesaria para garantizar que se ha realizado correctamente la implantación, configuración y puesta en productivo de la solución propuesta.

La documentación requerida a la finalización del despliegue de la segregación debe contener, al menos:

- Diagrama físico (formato Visio o similar).
- Documentación del proceso de despliegue y las configuraciones aplicadas en cada fase.
- Configuración HA aplicada.
- Usuarios de gestión y contraseñas asociadas.
- Reporte de las pruebas realizadas para la validación del correcto funcionamiento de HA y otras pruebas realizadas.
- Inventario de licencias y mantenimiento en vigor.

5.3. OPERACIÓN, SOPORTE, MANTENIMIENTO E INFORMES DE SEGUIMIENTO

Una vez definido el despliegue, el documento de propuesta deberá contar con la descripción del servicio de operación y gestión de las soluciones, que permitirá evolucionar todas las funcionalidades habilitadas, afinar las políticas iniciales, desarrollar nuevas políticas con la granularidad requerida por las necesidades de seguridad de AGAMED, a lo largo de la vigencia del contrato.

La solución propuesta debe contar con soporte por parte de fabricante. En el caso de los componentes de hardware, el soporte in situ deberá quedar cubierto con el servicio de 24x7, con un tiempo máximo de respuesta de 4 horas. Para el caso del software, además del soporte, la solución propuesta deberá permitir el acceso a nuevas versiones de los productos.

La solución propuesta, una vez puesta en productivo, deberá ser operada por el adjudicatario, facilitando la formación continua del personal técnico de AGAMED.

a) CARACTERÍSTICAS GENERALES DEL SERVICIO
    a. Servicio 8x5
    b. Recepción de incidencias en plataforma 24x7
    c. Duración 36 meses desde la firma del contrato
b) GESTIÓN DE LA INFRAESTRUCTURA PLATAFORMA

El servicio comprenderá el mantenimiento necesario de las soluciones desplegadas, entendiendo como tal, la realización de las actualizaciones que sean necesarias para el funcionamiento de las plataformas. Además:

- Comprobación proactiva de las plataformas, soporte y mantenimiento, con la generación de tickets de seguimiento y aplicación de correcciones con el fabricante.
- Mantenimiento de los perfiles de administración necesarios.

c) OPERACIÓN DE LA SOLUCIÓN

Además del mantenimiento necesario sobre la plataforma, el servicio ha de encargarse de implementar las acciones que correspondan en cada momento, para garantizar el correcto funcionamiento de la solución y, por tanto, el cumplimiento de su función dentro del esquema general de seguridad de AGAMED. Entre estas acciones se encuentran:

1. Reportar cualquier comportamiento inusual detectado
2. Clasificación de incidentes de seguridad
3. Eliminar falsos positivos
4. Generar las alertas pertinentes
5. Valorar el impacto de los incidentes de seguridad
6. Comunicar al SOC corporativo
7. Seguimiento del incidente
8. Proteger la evidencia de un incidente
9. Mantener una base de datos histórica de incidentes
10. Adaptar las best practices de las políticas actuales y/o futuras
11. Generación de informes:
    a. Seguimiento operativo del servicio (periodicidad mensual). Debe reportarse, con periodicidad mensual, un informe con los indicadores más importantes de la solución ofertada, que incluirá, entre otros aspectos: los detalles de uso, alertas generadas, incidentes de seguridad creados y resueltos, número de tickets generados y resueltos, incidencias que afecten al buen funcionamiento de la solución y recomendaciones que se estimen oportunas. Los aspectos y formato del informe se consensuarán entre el proveedor y AGAMED.
    b. Informe de resultados de actuación sobre un ataque o incidente gestionado (incidente clasificado como grave).

5.4. CRITERIOS DE SOLVENCIA TÉCNICA

Los criterios mínimos de solvencia técnica que deberá justificar el licitador serán:

- Acreditar antigüedad de la representación y partnership de la solución en España (mínimo seis meses).
- Experiencia de la empresa ofertante, de al menos un año, como usuario de tecnologías del tipo ofertado.

- Acreditar que se cuenta con un staff de profesionales cualificados y certificados por la marca, que sustentan la capacitación y soporte técnico en España.
- Certificación ISO 27001 y/o equivalente y/o acreditación de trabajos en el entorno de dicha norma.
- Disponer de la Certificación Esquema Nacional de Seguridad o acreditación de trabajos en el entorno de dicha norma.

5.5. CRITERIOS DE SOLVENCIA ECONÓMICA

AGAMED requerirá al adjudicatario provisional la acreditación de la solvencia económica y financiera conforme a lo siguiente:

- El criterio para la acreditación de la solvencia económica y financiera será el volumen anual de negocios del licitador o candidato, que referido al año de mayor volumen de negocio de los tres últimos concluidos deberá ser al menos una vez y media el valor estimado anual medio del contrato.
- El volumen anual de negocios del licitador o candidato se acreditará por medio de sus cuentas anuales aprobadas y depositadas en el Registro Mercantil, si el empresario estuviera inscrito en dicho registro, y en caso contrario por las depositadas en el registro oficial en que deba estar inscrito. Los empresarios individuales no inscritos en el Registro Mercantil acreditarán su volumen anual de negocios mediante sus libros de inventarios y cuentas anuales legalizados por el Registro Mercantil.

6. PRESUPUESTO DEL CONTRATO

El valor estimado del total del contrato asciende al importe **de CIENTO DIECISEIS MIL CIENTO DIECISIETE EUROS Y TRENTA Y CINCO CÉNTIMOS DE EURO (116.117,35 €)**, IVA no incluido, para la vigencia total del contrato (36 meses). El desglose del presupuesto

Concepto	**Valor estimado del contrato (en euros)**
Suministro, puesta en marcha, operación y mantenimiento de un sistema de detección de anomalías, intrusiones y vulnerabilidades en redes industriales con gestión de inventario; y suministro de electrónica de red basada en tecnología Firewall y puesta en marcha, operación y mantenimiento de un proyecto de diseño de arquitectura, segregación e implementación de redes en los entornos de TI y OT (Sistema de Control Industrial) en Aguas del Arco Mediterráneo, S.A.	
Detección de anomalías: sistema CLAROTY o equivalente	43.979,17 €
Segregación de redes: sistema PALO ALTO o equivalente	15.438,18 €
Operación y mantenimiento de la seguridad nivel 1 y nivel 2 (3 años)	56.700,00 €
TOTAL VALOR ESTIMADO DEL CONTRATO	**116.117,35 €**

Los gastos derivados de los trabajos descritos, desplazamientos, alojamiento y manutención quedan incluidos en dicha oferta.

Estos importes se incrementarán con el IVA vigente.

7. PLAN DE EJECUCIÓN Y CRONOGRAMA

En la oferta, el licitador debe incluir la programación justificada de las actuaciones, donde se incluirá con detalle la programación de trabajos y tareas que se desarrollarán en el proyecto.

En la programación, para su definición, se tendrán en cuenta el conjunto de instalaciones y medios auxiliares precisos, así como las situaciones provisionales que deban establecerse.

Se indicarán las interrelaciones entre las diversas tareas y actividades, el plazo parcial de cada una de ellas y sus trabajadores asociados, las unidades que se consideren críticas, el plazo total de la ejecución, así como la seguridad que se adoptará en cada una de las instalaciones.

8. EJECUCIÓN DE LAS MEDIDAS CORRECTORAS

Será responsabilidad del adjudicatario la realización de todos aquellos trabajos adicionales que sean necesarios para la no afección al normal funcionamiento o imagen de AGAMED, tanto durante la realización de los trabajos, como una vez finalizados estos. Cualquier actuación adicional necesaria y su coste, no contemplados en el proyecto, correrá a cargo del adjudicatario. Si por cualquier motivo relacionado con actuaciones derivadas de la presente licitación, se vieran afectados los trabajos, será la empresa adjudicataria la responsable de las consecuencias que se deriven. Los importes que se deriven de estas actuaciones serán detraídos de las certificaciones a abonar al adjudicatario, y/o de los avales presentados.

9. AUTORIZACIÓN DE VISITA A INSTALACIONES

Al objeto de que las empresas licitadoras puedan realizar adecuadamente sus ofertas, podrán solicitar autorización de visita a la sede de AGAMED, para verificar in situ las características de las instalaciones y equipos existentes, y así concretar el estudio del proyecto a ejecutar.

10. MEDIOS TÉCNICOS Y HUMANOS

La empresa licitadora deberá relacionar y justificar en su oferta el personal que destinará al desempeño de los trabajos objeto del presente proyecto, que deberá ser el suficiente y necesario para la realización de los trabajos con la calidad exigida en el mismo.

Todos los trabajos deberán ser realizados por personal con amplia experiencia en trabajos similares. La instalación y puesta en marcha debe realizarse por un equipo certificado por la marca y con experiencia demostrable en ciberseguridad, para el sector de agua/energía.

Si el personal previsto se demostrara insuficiente para la correcta prestación de los trabajos objeto del proyecto, el adjudicatario tendrá que asumir el coste que fuera necesario para corregirlo.

El adjudicatario deberá designar un jefe de proyecto, con titulación técnica universitaria competente, junto con la cualificación y experiencia demostrable en trabajos similares. Además, tendrá capacidad suficiente para ostentar su representación cuando sea necesaria, en orden a lo estipulado en el contrato y en relación con la buena marcha de los trabajos. El jefe de proyecto asumirá las tareas de interlocución con la persona designada por AGAMED, en calidad de jefe de proyecto por parte de AGAMED. Esta figura de interlocutor, o la persona que le sustituya, se mantendrá durante toda la duración del contrato. Este jefe de proyecto tendrá las siguientes funciones:

- Servir de interlocutor entre el equipo que presta el servicio objeto del contrato y el responsable del contrato.
- Garantizar el control de la correcta prestación del servicio y horarios del personal que presta los servicios objeto del contrato.
- Resolver incidencias tales como ausencias imprevistas, necesidad de refuerzos urgentes, etc.
- Asistir a las reuniones que sean necesarias a solicitud del responsable del contrato.
- El/la jefe/a deberá disponer de una línea de teléfono móvil y dirección de correo electrónico para las comunicaciones que sea necesario realizar debiendo estar disponible como mínimo en horario laboral.
- Remitir al/la responsable del contrato con carácter mensual, dentro de los primeros diez días de cada mes, a partir del primer mes de prestación del servicio, un informe con las incidencias más relevantes detectadas durante la prestación del servicio durante el mes en cada dependencia.

Se entregará currículum vitae del personal técnico adscrito al contrato, que incluya: identificación, titulación y experiencia en trabajos similares. De entre ellos, se identificará al jefe de proyecto, que ejercerá asimismo las funciones de jefe de seguridad y salud, y quien firmará el documento de aceptación de responsabilidad técnica y contractual.

La empresa adjudicataria dispondrá de la maquinaria, herramientas y utillaje, así como los medios técnicos precisos, para llevar a buen término los trabajos objeto del contrato. Dichos medios podrán ser propios o alquilados, siempre que aseguren la efectiva prestación de los medios en el momento en que sean requeridos.

Ante cualquier fallo y/o anomalía que presente la solución, se recibirá el apoyo del proveedor a lo largo de la vida del contrato, debiendo acreditar el licitador que dispone de servicio de atención postventa, servicios de mantenimiento y soporte anual de las soluciones adquiridas. Igualmente, soporte técnico a usuarios en castellano y facilidades para la capacitación (por ejemplo: presencial, vía web u otros).

11. ACTA DE RECEPCIÓN

Una vez hayan concluido la totalidad de las actuaciones objeto del contrato, se procederá a redactar el Acta de Recepción de los trabajos realizados.