PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA IMPLANTACION DE SISTEMAS DE SEGURIDAD LOGICA PARA LAS EDARs

ANTECEDENTES Y OBJETO

Las diversas estaciones depuradoras de aguas residuales (EDARs) de AB albergan sistemas de información que dan soporte al proceso industrial de la depuración. Estos sistemas son considerados OT (Operational Technologies). Estos sistemas soportan la automatización y el control de los procesos y por lo tanto son esenciales para el correcto funcionamiento de las plantas.

Actualmente la compañía se enfrenta a nuevas amenazas en materia de cibercriminalidad. Los sistemas informáticos en general son la base de la mayoría de los procesos de la compañía y defender y protegerlos de las amenazas es la prioridad de la Dirección de Seguridad. En concreto los sistemas OT de las EDARs suponen punto clave y deben estar suficientemente protegidos.

Tras un análisis de riesgos en cada una de ellas se evidenció la urgente necesidad de establecer nuevos sistemas de control y defensa de la infraestructura OT.

Con anterioridad, AB abordó este tipo de proyectos en las ETAPs y en los centros de control operativos. Ya se realizó una inversión en tecnología de ciberseguridad. Esta licitación pretende ampliar estas soluciones ampliando el ámbito protegido extendiendo las soluciones al resto del entorno OT.

Es básico ampliar las infraestructuras ya existentes para lograr eficiencias de inversión y de gestión.

Por ello esta licitación detalla los elementos necesarios por cada una de ellas para lograr una mitigación de riesgos cibernéticos suficiente y dotar de una protección adecuada a cada planta.

1. DESCRIPCIÓN DEL ALCANCE

El alcance comprende las 7 EDARs:

- *Edar Besòs*
- *Edar El Prat de Llobregat*
- *Edar Sant Feliu*
- *Edar Montcada*
- *Edar Gavà*
- *Edar Begues*
- *Edar Vallvidrera*

En cada una de ellas desplegaremos soluciones del tipo:

- Segregación de redes (FW)
- Fortificación servidores y clientes de operación
- Control de accesos *securizados* y zona acceso remoto seguro
- Detección malware avanzado y respuesta a incidentes

2. DESCRIPCION DE LOS LOTES

RESUMEN LOTES;

Lote 1: Segregación de redes y prestación de servicios de implantación y despliegue, así como, soporte técnico y mantenimiento.
Lote 2: Compra de licencias para la fortificación Servidores y clientes de operación, así como, prestación de servicios de soporte técnico y mantenimiento.
Lote 3: Compra de licencias para el control de accesos *securizados* y zona acceso remoto seguro, así como, prestación de servicios de soporte técnico y mantenimiento.
Lote 4: Compra de licencias para la detección de malware avanzado y respuesta a incidentes, así como, prestación de servicios de soporte técnico y mantenimiento.

2.1 Lote 1: Segregación de redes.

Actualmente las 6 Edars cuentan con un FW cada una de la marca Zyxel que cuentan con más de 8 años de antigüedad. Esta tecnología ha quedado totalmente obsoleta de día de hoy y el grado de defensa que suponen estos equipos es totalmente insuficiente.

Adicionalmente el FW actual es único por lo que no contamos con una redundancia, aumentando el riesgo de caída del servicio.

Aigües de Barcelona cuenta, en otras plantas como las Etaps, con un parque de Firewalls de última generación Palo Alto Networks gestionados mediante la consola central Panorama.

A la hora de sustituir los FW Zyxels actuales es imprescindible alinear tecnológicamente la solución con la existente. Estos FW Paloalto son de los denominados "*Next Generation Firewall*" por su capacidad de analizar las 7 capas OSI de la comunicación, dotando al sistema de capacidades de análisis absolutos. Adicionalmente añadir FW de la misma marca supone una innumerable gama de ventajas al respecto de la integración. Recordemos que el tráfico informático atraviesa distintos FW desde que accede al perímetro de AB hasta que llega a su destino. Esta integración entre los diferentes FW asegura el control más alto posible de la seguridad.

Todos los FW de AB estará integrados en la consola Panorama de Paloalto (de la que ya disponemos en la actualidad) centralizando allí todos los eventos y logs consiguiendo un repositorio único. De otra manera sería imposible agregar toda esta información y se deberían desarrollar soluciones de integración a medida desbordando el importe de la inversión muy significativamente.

Por las necesidades anteriormente enunciadas, la solución licitada deberá ser un producto Palo Alto Networks que permita una completa compatibilidad con la infraestructura corporativa ya existente. Se propone como solución más ajustada a nuestras necesidades el firewall PA-220 tras el estudio del dimensionamiento necesario para cumplir con las necesidades tanto actuales como futuras.

- *Edar El Prat de Llobregat* — *Site tipo 4*
- *Edar Sant Feliu* — *Site tipo 4*
- *Edar Montcada* — *Site tipo 4*
- *Edar Gavà* — *Site tipo 4*
- *Edar Begues* — *Site tipo 3*
- *Edar Vallvidriera* — *Site tipo 3*

Habida cuenta de lo expuesto, no es posible establecer alternativas equivalentes que puedan sustituir de forma fiable a FW de la misma marca referenciada en el apartado que precede, por cuanto dicha sustitución o reemplazo podría dar lugar a incompatibilidades o dificultades técnicas de uso y mantenimiento

desproporcionadas que conllevarían la inejecución del sistema.

No obstante lo anterior, procede poner de manifiesto que a pesar de ofrecer el producto con la misma marca se estaría actuando de conformidad con el principio de concurrencia pues podrían suministrarlo diferentes operadores económicos que actúan en el mercado viéndose satisfecho, por consiguiente, el objeto del contrato

La Edar de Besòs (site tipo 4) ya cuenta con 2 PA-220 en alta disponibilidad, por lo que no entra dentro del alcance de este lote.

Características

Características de hardware: Palo Alto Networks PA-220 o similar:

- 500/560 Mbps firewall throughput1
- 150/260 Mbps Threat Prevention2
- 100 Mbps IPsec VPN throughput
- 64,000 max sessions
- 4,200 new sessions per second3
- 1,000 IPsec VPN tunnels/tunnel interfaces
- 3 virtual routers
- 15 security zones
- 500 max number of policies

Características de software necesarias:

- Threat prevention subscription 3 años
- WildFire subscription 3 años

Características soporte anual:

- Partner enabled premium support 3 year

Detalle de equipos por sede

En el ANEXO_1 se puede ver detallado las demandas por sede que el proponente deberá cotizar.

Servicios de implantación y despliegue

El despliegue cubierto en la presente licitación abarcará el suministro del material, la puesta en marcha y configuración básica inicial de cada uno de los equipos.

A continuación, se detallan las principales acciones incluidas en este despliegue:

- **Análisis de la arquitectura actual en explotación**. Estudio a alto nivel de la infraestructura actual, para ello se proporcionará al proveedor la información necesaria extraída de la consola de gestión centralizada corporativa *Panorama de Palo Alto Networks*.
- **Instalación física de los equipos**. Al proveedor contará con la colaboración del personal de Aigües de Barcelona para coordinar las tareas de enracado, cableado, etc. de los equipos físicos que deberá realizar el proveedor
- **Instalación inicial de los dispositivos y puesta en marcha** atendiendo a los criterios previamente establecidos para el resto de la plataforma *Palo Alto Networks* ya en cliente y los requerimientos sugeridos por fabricante:
    - Solicitar las IPs de gestión de los equipos y proceder a su configuración. Aigües de Barcelona gestionará previamente las IPs con el operador correspondiente

  - Instalación y puesta en marcha siguiendo las configuraciones recomendadas por el fabricante tales como configuración del acceso de red, configuración de la interfaz de gestión, hostname, ajustes de DNS, servidor de actualización y servidor proxy, NTP, verificación e instalación de nuevas versiones de software (> 8.0.7), cambio de contraseña para la cuenta de administrador. Todas las configuraciones anteriores se basarán en parámetros proporcionados por Aigües de Barcelona en el momento de la instalación
  - Registro del cortafuegos con el servicio de soporte de *Palo Alto Networks*
  - Activación de las licencias
  - 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 dos equipos suministrados. Definición de las condiciones de balanceo. Pruebas de contingencia para validar la configuración HA.
  - Activar User-ID en las zonas y configurar los agentes de User-Id
  - Colaboración para la integración con la herramienta central de *Panorama* corporativa
  - Creación de perfiles de seguridad según mejores prácticas de *Palo Alto Networks*
  - Configuración de envío de logs a *Panorama*
  - Creación del perfil del reenvío de logs.
  - Colaboración para el envío de los logs de *Panorama* a otros sistemas de análisis (Splunk).

- **Documentación requerida a la finalización del despliegue**: documentación descriptiva de la configuración llevada a cabo, algunos ejemplos:
  - Diagrama físico (formato Visio)
  - Documentación del proceso de despliegue y las configuraciones aplicadas en cada fase.
  - Configuración HA aplicada
  - Usuarios de gestión y las contraseñas asociadas
  - Reporte de las pruebas realizadas para la validación del correcto funcionamiento de HA u otras pruebas realizadas
  - Inventario licencias y mantenimiento en vigor
- **Traspaso y formación al equipo encargado de la explotación de la solución desplegada** (tiempo estimado 2 jornadas de trabajo en total para todos los FWs, Será coordinado con AB la planificación de esta formación pudiéndose fraccionar en función de las necesidades)
- **Tareas no incluidas en la licitación**:
  - Definición y despliegue de políticas de filtrado

Soporte y mantenimiento

La solución propuesta debe contar con soporte por parte del fabricante 24x7. En la presente licitación se requiere el Partner Enabled Premium Support para cada uno de los dispositivos hardware, las principales características son:

- Soporte 24x7x365
- Servicio de reposición de piezas defectuosas durante el siguiente día laborable
- Tiempos de respuesta entre 1h y 8h dependiendo de la criticidad de la incidencia
- Capacidad de interacción con el servicio de soporte para recalificar la criticidad de una incidencia.

En cuanto al SW la oferta debe contemplar el mantenimiento de:

- Threat prevention subscription 3 años
- WildFire subscription 3 años

2.2 Lote 2: Fortificación Servidores y clientes de operación

La protección de los equipos informáticos tiene una de sus mejores soluciones en el antivirus. Pero este tipo de soluciones pueden llegar a ser intrusivas en el rendimiento de las aplicaciones. En el entorno de las Edars es básico respetar el tiempo real para garantizar el control sobre las infraestructuras.

AB ya tiene desplegada en estos momentos la solución "Endpoint Threat Protection" de McAfee para proteger los equipos OT de otras instalaciones. Adicionalmente al Software de antivirus requerimos dos elementos más de la suit de productos McAfee; El controlador de dispositivos y el controlador de aplicaciones.

Añadir más licencias McAfee supone una innumerable gama de ventajas al respecto de la integración con el parque ya instalado. Recordemos que el tráfico informático atraviesa la red desde que accede al perímetro de AB hasta que llega a su destino, saltando de equipo en equipo. Esta integración entre los diferentes agentes instalados en los equipos asegura el control más alto posible de la seguridad. Todos los productos de la Suit McAfee que AB ya tiene están integrados en la consola gestión de McAfee (de la que ya disponemos en la actualidad) centralizando allí todos los eventos y logs consiguiendo un repositorio único. De otra manera sería imposible agregar toda esta información y se deberían desarrollar soluciones de integración a medida desbordando el importe de la inversión muy significativamente.

Por todo lo anterior no se requiere cotizar el proyecto de instalación y despliegue pues añadir las nuevas licencias es sumamente sencillo y rápido. En este sentido, destacar que no es posible establecer alternativas equivalentes que puedan sustituir de forma fiable a sistemas antivirus de la misma marca – Suit McAfee, por cuanto dicha sustitución o reemplazo podría dar lugar a incompatibilidades o dificultades técnicas de uso y mantenimiento desproporcionadas que conllevarían la inejecución del sistema.

No obstante, lo anterior, procede poner de manifiesto que a pesar de ofrecer el producto con la misma marca se estaría actuando de conformidad con el principio de concurrencia pues podrían suministrarlo diferentes operadores económicos que actúan en el mercado viéndose satisfecho, por consiguiente, el objeto del contrato

Características técnicas

Requerimos desplegar esta solución en las Edars. El uso de los diferentes productos de la Suit dependerá de la función del equipo a defender:

- **Servidores:** Los servidores son la parte más crítica del sistema de control de las Edars, por eso debemos prestarle una atención extraordinaria.
    - **McAfee EndPoint Security Threat Prevention (ENS)**
    - **McAfee Device Control (DEC)**

  Si el servidor es virtual no será necesario DEC.

- **Clientes de operación y/o supervisión OT**: Se trata de entornos con SO de PC que, al tener una interacción directa con el usuario, no permiten un nivel de bastionado de sistema operativo tan elevado como el caso de los servidores. El uso habitual y continuado del equipo por parte del usuario lo hace más propenso a recibir ataques o a la ejecución de posibles programas maliciosos (conocidos o no), por este motivo se despliega la solución de control de aplicaciones y de dispositivos en los clientes de operación.
    - **McAfee Application Control (ACD)**
    - **McAfee Device Control (DEC)**

  Si el equipo cliente es virtual no será necesario DEC.

Detalle de licencias

- Sesenta y cinco (65) licencias**: Endpoint Threat Protection (Perpetual):** Suit de productos entre los que se incluyen
    - **Virus Scan Enterprise:** Solución de antivirus de McAfee orientada a servidores industriales

con sistemas operativos WindowsXP o WindowsServer 2003.

- **McAfee EndPoint Security Threat Prevention (ENS):** Solución de antivirus de McAfee orientada a servidores industriales.
- **McAfee Device Control (DEC):** Permite controlar los dispositivos extraíbles que se conectan a un equipo y bloquear los que no estén permitidos.

- Cincuenta y cinco (55) licencias**: McAfee Application Control (ACD) (Perpetual):** Módulo para el congelado de equipos a través de listas blancas de aplicaciones.

Servicios de implantación y despliegue

No se requieren

Soporte y mantenimiento

La solución propuesta debe contar con soporte por parte del fabricante durante el primer año, así como acceso a las nuevas versiones. Gold Software Support.

2.3 Lote 3: Control de accesos *securizados* y zona acceso remoto seguro

El control de acceso a los equipos de manera remota supone uno de los riesgos más importantes, por ello debemos *securizar* al máximo estas conexiones, así como la custodia de las credenciales.

Actualmente tanto los sistemas OT como los IT de AB ya está usando CiberArk. Debemos considerar el control de acceso como básico en el control de seguridad. Por ello es básico centralizar este control en una única solución. De esta manera el registro de accesos es único y está integrado. De otra manera seria imposible agregar toda esta información y se deberían desarrollar soluciones de integración a medida desbordando el importe de la inversión muy significativamente. Las políticas deben ser nativas y transversales.

Aunar la solución tecnológica a su vez facilita enormemente la tarea para los usuarios de modo que no deben gestionar credenciales diferentes para acceder a sistemas distintos.

El despliegue de esta misma solución en las Edars supondrá que únicamente debamos adquirir licencias adicionales ya que ya se dispone de la infraestructura de servidores necesaria para gestionarlas.

Del mismo modo no se requiere cotizar el proyecto de instalación y despliegue pues añadir las nuevas licencias es sumamente sencillo y rápido. En este sentido, destacar que no es posible establecer alternativas equivalentes que puedan sustituir de forma fiable al producto CiberArk, por cuanto dicha sustitución o reemplazo podría dar lugar a incompatibilidades o dificultades técnicas de uso y mantenimiento desproporcionadas que conllevarían la inejecución del sistema.

No obstante, lo anterior, procede poner de manifiesto que a pesar de ofrecer el producto con la misma marca se estaría actuando de conformidad con el principio de concurrencia pues podrían suministrarlo diferentes operadores económicos que actúan en el mercado viéndose satisfecho, por consiguiente, el objeto del contrato

Características técnicas

La solución elegida tendrá las siguientes características técnicas:

- Registrará el mayor nivel de trazabilidad posible, sobre la actividad de los usuarios y accesos, permitiendo visualización en vivo y la grabación de sesiones.
- Permitirá la terminación remota de sesiones a los equipos de seguridad para que puedan cerrar inmediatamente las sesiones privilegiadas sospechosas directamente desde la consola central.
- Permitirá enmascarar las credenciales privilegiadas de los usuarios y garantizar que estas

credenciales nunca lleguen a los puntos finales evitando cualquier mal uso o elevación de credenciales privilegiadas.

- Permitirá el rotado automático y seguro de credenciales de cuentas distribuidas.
- Utilizará algoritmos seguros de cifrado tales como AES-256 o RSA-2048 para el almacenado de contraseñas.

Detalle de licencias

Requerimos la compra de esta solución en las Edars:

- Sesenta (60) licencias **EPV-Business User Licenses for managing personal passwords**
- Diez (10) licencias **PSM** licencias concurrentes.

Es importante notar que no requerimos licencias en suscripción, sino que la licitación adquirirá las licencias con el primer año de garantía.

Servicios de implantación y despliegue

No se requieren

Soporte y mantenimiento

La solución propuesta debe contar con soporte por parte del fabricante durante el primer año, así como acceso a las nuevas versiones.

2.4 Lote 4: Detección malware avanzado y respuesta a incidentes.

Las amenazas de seguridad actuales son cada vez más sofisticadas en la forma en que seleccionan, atacan e infiltran a las organizaciones para robar sus activos principales. Necesitamos una solución para investigar y generar una respuesta ante un incidente que minimice el impacto comercial potencial de ataques cibernéticos cada vez más sofisticados y dirigidos.

Actualmente los sistemas OT de las otras plantas de AB ya están usando FireEye, tanto en equipos de cliente como servidores.

Por ello es básico centralizar este control en una única solución. De esta manera el repositorio de logs y evidencias es único y está integrado. De otra manera seria imposible agregar toda esta información y se deberían desarrollar soluciones de integración a medida desbordando el importe de la inversión muy significativamente.

Aunar la solución tecnológica a su vez facilita enormemente la tarea para los investigadores y los equipos de reacción ante amenazas o ataques, minimizando los tiempos de análisis.

El despliegue de esta misma solución en las Edars supondrá que únicamente debamos adquirir licencias adicionales ya que se dispone de la infraestructura necesaria para gestionarlas.

Del mismo modo no se requiere cotizar el proyecto de instalación y despliegue pues añadir las nuevas licencias es sumamente sencillo y rápido. Ampliaremos el número de licencias reaprovechando la infraestructura base ya desplegada. En este sentido, destacar que no es posible establecer alternativas equivalentes que puedan sustituir de forma fiable al producto FireEye, por cuanto dicha sustitución o reemplazo podría dar lugar a incompatibilidades o dificultades técnicas de uso y mantenimiento desproporcionadas que conllevarían la inejecución del sistema.

No obstante lo anterior, procede poner de manifiesto que a pesar de ofrecer el producto con la misma marca se estaría actuando de conformidad con el principio de concurrencia pues podrían suministrarlo diferentes operadores económicos que actúan en el mercado viéndose satisfecho, por consiguiente, el objeto del contrato

Características técnicas

- Plataforma de investigación única: acelera el proceso de investigación identificando rápidamente las alertas que requieren una investigación exhaustiva y centrando su atención mediante una investigación forense de red centralizada que se inicia desde una sola plataforma.
- Generación de informes: configura FireEye Investigation Analysis System para generar informes basados en períodos de tiempo o en parámetros más sofisticados en función del número de casos. Utilice la función de generación de informes para detectar actividades anómalas en la red y supervisar los eventos de la red.
- Visualización y uso compartido de la información: ahorra tiempo muy valioso durante la investigación y descubra las amenazas ocultas.

Detalle de licencias

Licencias para setenta (70) agentes de FireEye Endpoin Security (HX) versión Power, con soporte Platinum y suscripción DTI para 1 año, compatibles con la plataforma en producción HX Controller nº de serie: FZ1637GC2L4 o el equipo que lo reemplace en caso de RMA.

Es importante notar que no requerimos licencias en suscripción, sino que la licitación adquirirá las licencias con el primer año de garantía.

Servicios de implantación y despliegue

No se requieren

Soporte y mantenimiento

La solución propuesta debe contar con soporte por parte del fabricante durante el primer año, así como acceso a las nuevas versiones.

3. PLAZO DE ENTREGA DEL SUMINISTRO E INSTALACIÓN

En el caso del Lote 1: Segregación de redes, el plazo máximo de para la realización del proyecto incluido el suministro de los materiales es de 3 MESES desde la recepción del pedido.

En el resto de los Lotes, al ser únicamente aprovisionamiento de licencias de software el plazo máximo para el suministro es de 1 MES desde la recepción del pedido.

ANEXO_1: Lote 1. Segregación de redes y control de tráfico.

Edar El Prat de Llobregat:

- 2 x Palo Alto Networks PA-220 en alta disponibilidad (configuración en HA activo-pasivo)

Edar Sant Feliu:

- 2 x Palo Alto Networks PA-220 en alta disponibilidad (configuración en HA activo-pasivo)

Edar Montcada:

- 2 x Palo Alto Networks PA-220 en alta disponibilidad (configuración en HA activo-pasivo)

Edar Gavà:

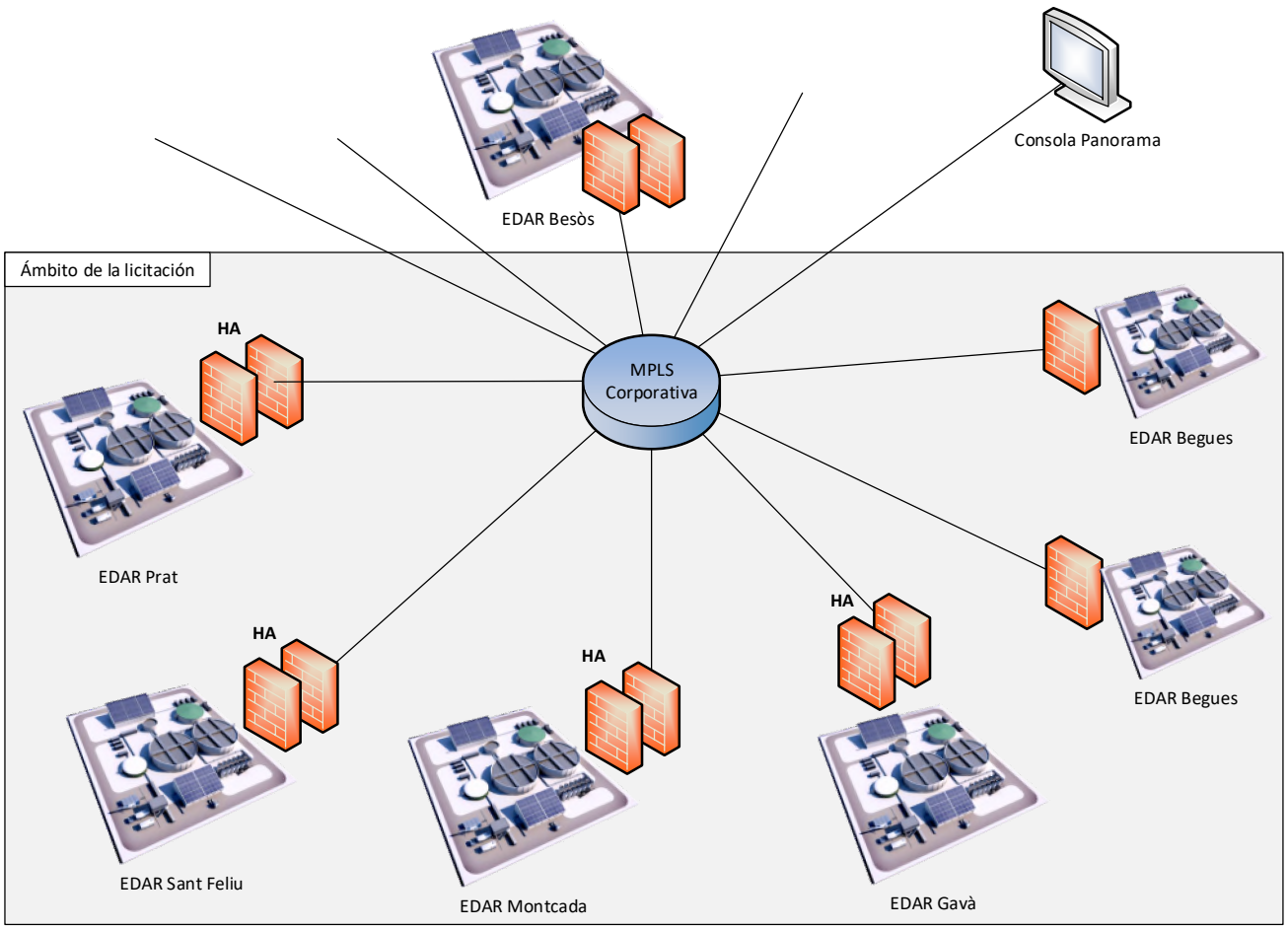
- 2 x Palo Alto Networks PA-220 en alta disponibilidad (configuración en HA activo-pasivo)

Edar Begues:

- 1 x Palo Alto Networks PA-220 en alta disponibilidad

Edar Vallvidriera:

- 1 x Palo Alto Networks PA-220 en alta disponibilidad



ANEXO_2: Equipos servidores

- *Edar Besòs* *5*
- *Edar El Prat de Llobregat* *5*
- *Edar Sant Feliu* *3*
- *Edar Montcada* *2*
- *Edar Gavà* *2*
- *Edar Begues* *0*
- *Edar Vallvidriera* *1*

ANEXO_3 Equipos cliente

- *Edar Besòs* *24*
- *Edar El Prat de Llobregat* *21*
- *Edar Sant Feliu* *2*
- *Edar Montcada* *3*
- *Edar Gavà* *4*
- *Edar Begues* *0*
- *Edar Vallvidriera* *1*