PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

SUMINISTRO, INSTALACION Y MANTENIMIENTO DEL SISTEMA DE SECURIZACIÓN PERIMETRAL DE INSTALACIONES PERIFERICAS DE LA RED DE ABASTECIMIENTO DEL CABB

Índice

1 Definición general del proyecto.

1.1 Objeto del proyecto

El objeto de este pliego es el suministro, instalación y mantenimiento del sistema de securización perimetral de las instalaciones periféricas de la red de abastecimiento del Consorcio de Aguas. En adelante CABB.

El objetivo es securizar las instalaciones mediante la instalación de un equipamiento que nos aporta visibilidad del tráfico entre las diferentes redes y delegaciones del CABB además de examinar dicho tráfico a nivel 7 (aplicaciones, antivirus, IPS). Con los cortafuegos se controlan los accesos desde y hacia Internet y entre centros, filtrado de amenazas IPS y control de aplicaciones a nivel 7.

Asimismo, se pretende reforzar la seguridad de CABB mediante la segmentación de las redes internas de estas instalaciones en diferentes capas, para poder aplicar las medidas de seguridad y revisión de tráfico de los servicios críticos para CABB (redes de servidores, DMZs... separadas de las redes de usuarios) limitando mediante reglas específicas el tráfico de los distintos servicios para permitir únicamente las comunicaciones necesarias para el correcto funcionamiento de las instalaciones periféricas. Para ello, habrá que además suministrar la electrónica de red asociada a la segmentación en VLANs.

Los objetivos del presente concurso consisten en el suministro, instalación, puesta en marcha y asistencia posterior de equipos de securización, en alta disponibilidad, y de los equipos necesarios de administración y segmentación de red.

El proyecto puede dividirse en los siguientes puntos:

1. Suministro, instalación y configuración de equipos de securización de capa 7, dos para cada centro. Con un mínimo de dos fases de configuración diferenciadas:
    a. En una primera fase se instalarán los equipos con una configuración genérica en la que la mayor parte del tráfico esté permitido.
    b. En una segunda fase pasado un tiempo prudencial para el análisis, se estudiará el tráfico originado y se presentarán los datos en un informe al CABB para que determine las reglas definitivas a configurar por el adjudicatario del contrato.
2. Integración de los equipos de securización de capa 7 en la infraestructura actual del CABB tanto para la administración centralizada de los mismos como para la gestión de sus logs, así como la configuración de ambas herramientas según indicaciones de CABB, siendo imprescindible que dicha gestión pueda quedar aislada de los equipos que gestionan actualmente
    a. En el caso de que la infraestructura actual del CABB para la gestión centralizada de los equipos y la gestión de los logs, no pudiera abarcar los nuevos equipos por razones de HW, SW o de licenciamiento, la empresa adjudicataria sería la encargada de ampliar, actualizar o incluso proveer de nuevo equipamiento físico (no virtual) para realizar estas funciones.
    b. En el supuesto de que el equipamiento propuesto no sea compatible con la infraestructura actual del CABB para la administración centralizada de equipos y gestión de sus logs, la empresa adjudicataria deberá proveer de nuevo equipamiento físico (no virtual) para realizar estas funciones
3. Suministro, instalación y configuración de equipos de segmentación de red para IT, uno para cada centro e integración de cada equipo en las herramientas de gestión de CABB basadas en SNMP y syslog
4. Suministro, instalación y configuración de equipos de segmentación de red para OT, uno para cada centro e integración de cada equipo en las herramientas de gestión de CABB.
5. Servicio del proveedor en 24x7x4 durante toda la duración del contrato.

6. Servicio del fabricante 24x7 durante toda la duración del contrato, será necesario además disponer del siguiente stock
    a. 1 equipo de cada modelo de cortafuegos ofertado, 1 equipo de cada modelo de segmentación de red para IT y 1 equipo de cada modelo de segmentación de red para OT ofertados en las dependencias del CABB
    b. 1 equipo de cada modelo de cortafuegos ofertado, 1 equipo de cada modelo de segmentación de red para IT y 1 equipo de cada modelo de segmentación de red para OT ofertados en las dependencias de la empresa adjudicataria
7. Suministro, instalación y configuración de Switches industriales, donde sea requerido e integración de cada equipo en las herramientas de gestión de CABB.
8. Bolsa de 50 horas a consumir por año de contrato para la optimización de las políticas de optimización iniciales y resolución de incidencias.
9. Formación del personal del CABB y documentación de proyecto
10. Monitorización 24x7x4 del equipamiento al que hace referencia el presente pliego junto los enrutadores actualmente ubicados en cada sede y algún equipo de segmentación de red OT ya presentes en las sedes. Dicha monitorización se realizará en dependencias externas a CABB y mediante herramientas de gestión basadas en SNMP o syslog propias de la empresa adjudicataria pero que serán accesibles por CABB. Ante la activación de una alarma con motivo de dicha monitorización
11. Suministro de equipamiento auxiliar entre los que destaca principalmente:
    a. Suministro e instalación de Rack de comunicaciones
    b. Instalación de protecciones eléctricas y UPS con tarjeta de red
12. Trabajos de obra civil, eléctricos, etc.

Asimismo, comprende el suministro, instalación y configuración de todos los elementos necesarios no incluidos en este listado para que el sistema quede funcionado plenamente. Por ejemplo, rack de comunicaciones, protecciones eléctricas, pasacables, cableado UTP, fibra óptica, patch panels de UTP y fibra óptica y cuantos elementos sean necesarios. Debe considerarse el presente proyecto como un proyecto "llave en mano".

1.2 Generalidades del proyecto

El proyecto se considera "llave en mano", acometiendo el contratista todos los trabajos y suministros que sean necesarios para el correcto funcionamiento de los equipos con la configuración y programación necesarias.

El contratista deberá de dar soporte de optimización de la parametrización inicial según los equipos vayan conociendo las características del tráfico con Internet y entre los centros, creando o modificando las políticas.

Se deberá realizar configuración de toda la red. Esto supone considerar la red como un todo (incluyendo los equipos no suministrados en este contrato) y su configuración (VLAN, netflow, SMNP, redundancia STP, monitorización, etc.) para que funcione con los equipos instalados. Se deberá de indicar y valorar todo elemento que se considere necesario para el correcto funcionamiento de la red según las prescripciones indicadas e incluso las que no se hayan contemplado en este Pliego indicándose en la oferta.

1.3 *Descripción de los servicios*

Las instalaciones que se van a securizar en el presente pliego se citan a continuación:

ETAP Oleta (Lekeitio)

ETAP Lekue (Galdakao)

ETAP San Miguel (Bakio)

ETAP Salinillas (Balmaseda)

ETAP Gartxeta (Orduña)

ETAP Jarralta (Sopuerta)

ETAP Gorozika (Ondarroa)

ETAP Iparraguirre (Markina)

ETAP Garaizar (Durango)

ETAP San Cristobal (Igorre)

ETAP San Salvador (Abadiño)

ETAP Sollano (Sollano)

Presa Undurraga (Zeanuri)

Presa Ordunte (Valle de Mena)

A continuación, a modo de referencia, se muestra una tabla con los equipos, servicios y licencias a instalar y mantener durante la duración del contrato:

ID	REFERENCIA	DESCRIPCIÓN	CANT.
		APPLIANCE SECURIZACIÓN IT (FIREWALL)	
1		Appliance securización IT (Firewall)	28
2		Licencias durante la duración del contrato de los equipos suministrados**	28
3		Soporte 24x7 fabricante anual por 3 años	28
4		Soporte integrador 24x7x4 anual por 3 años de los equipos suministrados	28
		SWITCH PARA SEGMENTACIÓN DE RED IT	
5	C9200L-24T-4G-E	Switch Catalyst 9200L 24-port data, 4 x 1G, Network Essentials o similar	14
5.1	PWR-C5-125WAC/2	125W AC Config 5 Power Supply - Secondary Power Supply	14
5.2	CAB-TA-EU	Europe AC Type A Power Cable	14

ID	REFERENCIA	DESCRIPCIÓN	CANT.
5.3	C9200-STACK-BLANK	Catalyst 9200 Blank Stack Module o similar	14
6		SFPs 1G monomodo original y nuevo del fabricante del switch para segmentación de red IT	14
7		SFPs 1G multimodo monomodo original y nuevo del fabricante del swicth para segmentación de red IT	14
8		Soporte 24x7 fabricante anual por 3 años (C9200L Network Essentials, 24-port license o similar)	14
9		Soporte integrador 24x7x4 anual por 3 años de los equipos suministrados	14
10		Licencias switch durante la duración del contrato (C9200L Cisco DNA Essentials, 24-port, 3 Year Term license o similar)	14
		SWITCH PARA SEGMENTACIÓN DE RED OT	
11		Switch para segmentación de red OT	14
12		SFPs 1G monomodo original y nuevo del fabricante del fabricante de switch para segmentación de red OT	14
13		SFPs 1G multimodo original y nuevo del fabricante del swicth para segmentación de red OT	14
14		SFP RJ45 Multimodo SW OT	14
15		Soporte NBD fabricante anual por 3 años	14
16		Soporte integrador 24x7x4 anual por 3 años de los equipos suministrados	14
17		Licencias switch durante la duración del contrato	14
		CUADRO ELÉCTRICO	
18		Salida tipo 5 B - alim serv varios 10-25 A	14
19		Trafo de mando 230/230 V c.a.	14
20		Protector de Sobretensiones	14
21		Rack de Comunicaciones	14
22		Sensor de temperatura	14
23		Servicios auxiliares	1
24		Pequeño material	1

ID	REFERENCIA	DESCRIPCIÓN	CANT.
25		Sistema de alimentación ininterrumpida	28
26		Alimentación control 24Vcc	14
27		Montaje Cuadro	1
		REPUESTOS	
28		Appliance securización IT (Firewall)	2
29		Switch para segmentación de red IT	2
30		Switch para segmentación de red OT	2
31		SFP FO Monomodo SW OT	2
32		SFP FO Multimodo SW OT	2
33		SFP RJ45 Multimodo SW OT	2
34		Switch Industrial con FO Multimodo	2
35		Switch Industrial con FO Monomodo	2
		ADECUACIÓN DE INSTALACIONES	
36		Switch Industrial con FO Multimodo	16
37		Soporte para panel de operador 15"	1
38		Desmontaje	1
39		Cable de 3x2,5 mm2/3x4 mm2	445m.
40		Cable Ethernet	2075m.
41		Conectores RJ45	106
42		Fibra Óptica Multimodo	250m.
43		Patch Panel y fusiones de FO multimodo	12
44		Cable de antena	500m.
45		Cable de telefono	830m.
46		Canalización tubo 25	355m.

ID	REFERENCIA	DESCRIPCIÓN	CANT.
47		Canalización bandeja PC+ABS 100x60	335m.
		SERVICIOS GENERALES	
48		Replanteo	14
49		Parametrización de los equipos y puesta en marcha	14
50		Bolsa de horas (150 horas) a distribuir anualmente por 3 años según necesidades (50h/año).	1
51		Formación de 10 jornadas de 5 horas cada una	1
52		Servicio de monitorización de red de las instalaciones anual por 3 años	1
53		Ingeniería y documentación	1
54		Servicio de configuración de PLCs	112h
55		Licencias de firmas industriales para 6 firewalls fortigate 1500D durante la duración del contrato	6

En cuanto a la ubicación de los equipos, los equipos deberán instalarse en distintas instalaciones distribuidas por toda la provincia de Bizkaia y Ordunte.

**Deben incluir licencias de firmas industriales.

2 Situación actual

En estos momentos se puede considerar que las instalaciones a securizar no disponen en estos momentos de equipos cortafuegos ni de electrónica de red gestionable y con capacidad de segmentación en VLANs.

Se requiere que los equipos a instalar tengan, como mínimo, una serie de funcionalidades y licencias durante toda la duración del contrato para las mismas:

- Control de aplicaciones, incluidos protocolos de entornos industriales
- IPS, con firmas para protección de entornos industriales
- Antivirus
- Threat protection
- IP reputation & antibotnet security
- Sandbox cloud
- Doble factor de autenticación integrado en la misma plataforma y del mismo fabricante
- Comprobación de firmas de Antivirus en tiempo real contra una base de datos de inteligencia global del fabricante, sin esperar a recibir el paquete de actualización de firmas
- Capacidad para eliminar contenidos dinámicos de un documento para poder analizarlo entregando al usuario un primer archivo sano, sin contenido dinámico.

- Posibilidad de configuración de routing dinámico, en especial BGP y OSPF con las distintas opciones de filtrado de rutas que permiten ambos protocolos
- La solución debe proveerse en alta disponibilidad física.
- Control de la navegación Web por categorías de URL
- Control DLP de descarga/subida de archivos
- Inspección SSL del tráfico
- Identificación/navegación por identificación de usuario/grupo de usuarios
- Identificación en equipo de multiusuario
- Traffic shapping
- Control horario para aplicación de políticas
- Integración con Active Directory

Los centros se encuentran conectados a la red del CABB a través de una MPLS a diferentes velocidades, normalmente de relativamente baja transferencia que se debe de tener en cuenta a la hora de actualizar las firmas o versiones del equipamiento, para no interferir con el funcionamiento normal de cada planta. Se valorará positivamente la mejora que puedan introducir estos equipos en términos de calidad de servicio o aceleración de tráfico ante líneas de baja transferencia. Cada instalación tiene sus peculiaridades y deben estudiarse de distinta manera. Algunas tienen salida de operador redundante mediante Tetra, otras una única salida. Además, disponen de distintas tecnologías de comunicaciones para conectarse a dicha MPLS.

3 Alcance del proyecto.

El proyecto debe contemplar el suministro, instalación y posterior mantenimiento de un sistema de securización para las instalaciones que conciernen a dicho proyecto. Para ello, se ha considerado que el sistema debe constar de al menos:

Una pareja en alta disponibilidad de cortafuegos de NGFW para entorno IT

Un switch para IT con capacidad de SD-WAN.

Un switch para OT.

Un par de UPSs con tarjeta de red Ethernet, gestionables vía SNMP dotadas de la capacidad de asegurar la alimentación de las dobles fuentes independientes de los equipos para los equipos que dispongan, o en caso de no disponer, como en el caso de cortafuegos y swithces de OT, para alimentar la fuente de cada uno de los elementos con una UPS diferente a fin de dotar al sistema de la máxima disponibilidad y fiabilidad.

Las UPSs deberán contar con esquema de control para su Bypass, a fin de asegurar la disponibilidad y que no se produzcan cortes de la alimentación eléctrica cuando se realicen labores de mantenimiento de las UPSs o sustitución de las mismas.

Protecciones eléctricas con diferenciales superinmunizados para cada uno de los elementos que componen el sistema objeto del proyecto.

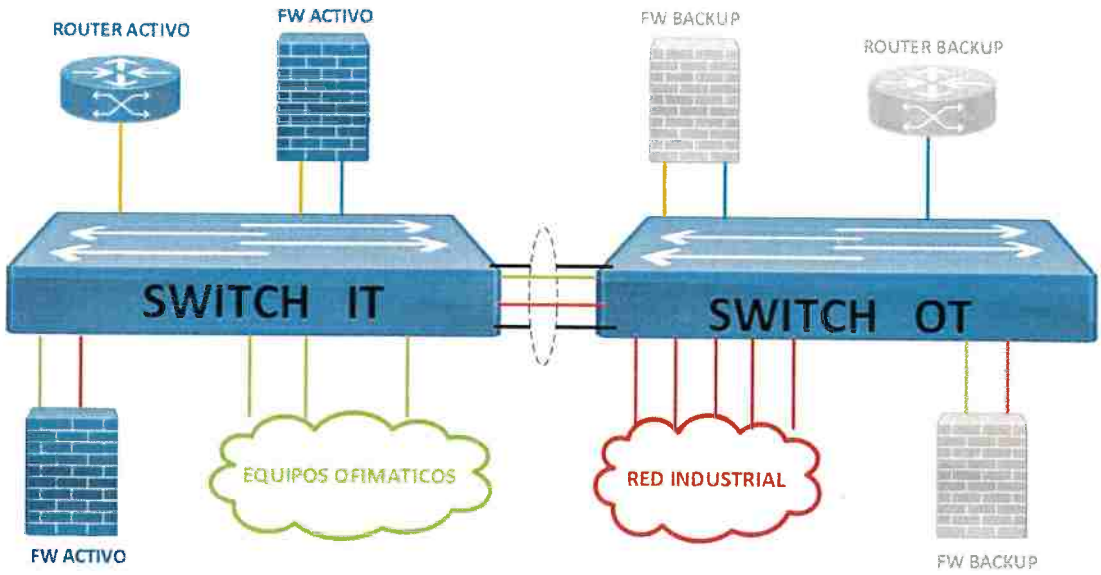
Un armario rack de comunicaciones que albergará todos los elementos de seguridad y comunicaciones.

Al menos, y no únicamente, deberá constar el armario de comunicaciones con cuantos pasahilos, paneles patch panels de UTP, paneles patch panels de fibra óptica, latiguillos de UTP, latiguillos de fibra óptica, etc. sean necesarios para la correcta instalación de todos los elementos de dicho rack.

El armario debe albergar en su interior un sensor de temperatura, así como disponer de cerradura

electrónica para apertura de puerta del rack mediante tarjeta electrónica. Se deberán suministrar al menos 10 llaves electrónicas.

El esquema inicial a alto nivel requerido por el CABB es el siguiente:



A continuación, se indican los requisitos mínimos a cumplir para todo el equipamiento del sistema de securización.

3.1 Firewalls

Como se ha indicado anteriormente el proyecto consiste en el suministro de equipos firewalls, dos para cada centro que se instalarán en clúster; el presupuesto contemplará su instalación, configuración y seguimiento de la configuración inicial para su optimización. Se deberá realizar la configuración de reglas, informes, redes virtuales, routing, etc. es decir, el sistema deberá cumplir las todas las funcionalidades requeridas.

Todo el equipamiento incluido en la oferta por parte del licitador debe ser perfectamente compatible entre sí y con el equipamiento disponible actualmente en las redes del CABB., especialmente con los equipos actuales para la gestión centralizada de las configuraciones y de logs

No se admitirán propuestas de soluciones de menores características y funcionalidades de los que se citan a continuación: (Fortigate 61E, Fortigate Rugged 90D, fortianalyzer 1000E y fortimanager 200F) y debe considerarse que sean capaces de funcionar teniendo todas las funcionalidades habilitadas durante toda la vida del contrato, sin verse afectado el rendimiento de los equipos de manera que pueda verse mermada la calidad del servicio (CPU <20% y memoria <40%).

Los firewalls deberán enrracarse ocupando 1RU del armario que viene descrito posteriormente en el pliego, en caso de que el equipo propuesto tenga unas dimensiones menores, deberá venir acompañado por una

bandeja adicional, preferiblemente propia del fabricante para ocupar 1RU del armario.

Los equipos ofertados deberán de ser además administrados por una consola de gestión centralizada (con acceso por interfaz web y por CLI) que permita la distribución simultánea de políticas a diferentes equipos y la creación de una base de datos de objetos común para todos los dispositivos administrados (ver apartado 3.1.17)

Además de la gestión centralizada de configuraciones será necesario que la solución disponga un servidor centralizado de logs (con acceso por interfaz web y por CLI) a donde los equipos puedan enviar todos sus logs de tráfico en tiempo real y ser almacenados por un periodo mínimo de entre 3-6 meses para su posterior exportación a un servidor externo. También será necesario que dicho servidor central pueda realizar informes personalizados y enviar alarmas por correo ante la recepción de cierto tipo de eventos (ver apartados 3.1.14, 3.1.15 y 3.1.16)

Se han considerado las siguientes características y funcionalidades mínimas para los equipos a ofertar:

3.1.1 Características de gestión y administración

- Arquitectura hardware separada para gestión y servicio, con recursos hardware dedicados.
- Administración por GUI y CLI directamente en el equipamiento, sin necesidad de instalar un cliente en máquina externa al firewall para su administración y / o cualquier otra función del firewall.
- Creación de perfiles y roles de administración con diferentes niveles de privilegio para poder administrar ciertas funcionalidades.
- Posibilidad de aplicar cambios en configuración pendientes, visualizar dichos cambios antes de aplicarlos, así como validarlos antes de aplicarlos en configuración. Se debe también almacenar diferentes versiones de configuraciones, así como descartar cambios en configuración realizados.
- Envío de logs vía SYSLOG, FTP, SCP y TFTP para retención y posterior tratamiento, con posibilidad de envío de logs selectivos según niveles de severidad y también según atributos como por ejemplo los tipos de amenaza.
- Soporte SNMP incluyendo la posibilidad de obtener estadísticas relativas a los procesos de recolección de logs y del estado de salud de las funciones de alta disponibilidad.
- Aplicación de cambios de forma inmediata, sin ninguna espera en su aplicación.
- El sistema debe de disponer de una auditoría de cambios. Cuando se realice un cambio en la configuración, políticas, etc. debe quedar registrado en el sistema de gestión de cambios que será almacenado para poder ser consultado con posterioridad. Deberá quedar registrado en el log como mínimo la siguiente información: quién ha realizado el cambio, fecha, hora, descripción del cambio.
- El sistema debe ser capaz de enviar alertas por correo electrónico ante fallos de sistema, HA, eventos categorizados como prioridad alta o crítica, cambios de configuración, etc.
- Se debe poder configurar todas las prestaciones del cortafuegos mediante línea de comandos.
- Sistema configurable de alertas a través de SNMP y email. Deben, además, los equipos soportar de forma configurable un sistema de alertas a través de SNMP y email.
- Deben disponer soporte de SFlow.

3.1.2 Características generales

Se requiere que los equipos a instalar tengan, como mínimo, una serie de funcionalidades y licencias durante toda la duración del contrato para las mismas:

- Control de aplicaciones, incluidos protocolos de entornos industriales
- IPS, con firmas para protección de entornos industriales
- Antivirus
- Threat protection
- IP reputation & antibotnet security
- Sandbox cloud
- Doble factor de autenticación integrado en la misma plataforma y del mismo fabricante
- Comprobación de firmas de Antivirus en tiempo real contra una base de datos de inteligencia global del fabricante, sin esperar a recibir el paquete de actualización de firmas
- Capacidad para eliminar contenidos dinámicos de un documento para poder analizarlo entregando al usuario un primer archivo sano, sin contenido dinámico.
- Posibilidad de configuración de routing dinámico, en especial BGP y OSPF con las distintas opciones de filtrado de rutas que permiten ambos protocolos
- La solución debe proveerse en alta disponibilidad física.
- Control de la navegación Web por categorías de URL
- Control DLP de descarga/subida de archivos
- Inspección SSL del tráfico
- Identificación/navegación por identificación de usuario/grupo de usuarios
- Identificación en equipo de multiusuario
- Traffic shapping
- Control horario para aplicación de políticas
- Integración con Active Directory
- Modelo de licenciamiento no basado en el número de usuarios. No limitación de usuarios debido a licenciamiento
- Visualización de número de usos y cantidad de tráfico de cada regla. Así como de la última vez que se ha utilizado
- Activación y desactivación automática de las reglas por fecha y hora
- Reparto de carga dinámico de conexiones TCP entre diferentes servidores. Balanceo de carga entre servidores internos con chequeo de estado de estos y aplicación de algoritmos de balanceo avanzados:
    - Source IP Hash
    - Round Robin
    - Weighted Round Robin
    - First Aliveo Least RTT
    - Least Session

- Posibilidad de realizar balanceo de tráfico entre las líneas de salida del cortafuegos en base a distintos algoritmos
- El sistema debe ser capaz de proporcionar redundancia de enlaces WAN monitorizando el estado de las líneas
- Los equipos deben disponer de al menos 6 dominios virtuales incluidos en el cortafuegos
- Arquitectura en Alta disponibilidad, permitiendo el despliegue tanto en modo Activo-Pasivo como Activo-Activo, sin necesidad de licencia
- Alta disponibilidad con sincronización de configuraciones y sesiones
- Interfaces reservados para gestión
- Posibilidad de configurar interfaces HeartBeat redundantes
- Identificación geográfica y posibilidad de aplicar políticas en función de esta, tanto de entrada como

salida del tráfico internet

- Clasificación de todas las defensas frente a amenazas en base a riesgo y nivel de amenaza
- Posibilidad de definición de excepciones por defensa/firma, perfil, origen, destino y puerto.
- Capacidades de traffic shaping y priorización del tráfico, por aplicación, por política e interfaz y subinterfaz, tanto para el tráfico saliente como para el entrante siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP
- Capacidad de proxy cache integrado en el mismo cortafuegos
- Opción de configuración de proxy explícito por interface, con posibilidad de hacer caching en caso de ser necesario
- Posibilidad de disponer de la funcionalidad de optimización WAN integrada en el propio cortafuegos
- Licencias ilimitadas
- Debe disponer de múltiples dominios de gestión (dominios administrativos) asociados a la estructura de dominios virtuales que se esté utilizando, ofreciendo tanto políticas específicas para cada dominio como políticas globales a todos los dominios
- Aplicación simultanea de políticas de seguridad en diferentes sistemas, dominios virtuales o clusters
- Sistema de revisión, chequeo y comprobación de la consistencia de las reglas de las políticas de seguridad, pudiendo verificarse la existencia de:
  - Duplicación de reglas y objetos
  - Reglas y objetos que son "ocultados" por otros
  - Reglas y objetos que son parcialmente sobreescritos por otros
  - Objetos definidos no utilizados

3.1.3 Características de red básicas

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión y administración de la propia plataforma, entendiéndose como funcionalidades mínimas a cumplir:

- Debe soportar varios modos de funcionamiento:
  - Modo transparente.
  - Modo routed y / o modo sniffer.
- Los interfaces del firewall deben soportar los siguientes modos de funcionamiento: modo TAP para monitorizar tráfico de forma pasiva a través de puertos mirror, modo transparente para inspección de tráfico en el flujo de datos y despliegues "in line", modo layer 2 o switching y modo layer 3 o routing.
- Soporte de IEEE 802.1Q y agregación de interfaces mediante 802.1AX.
- Soporte de protocolos dinámicos RIP v1 y v2, OSPF, ISIS, BGP y Multicast para IPv4 e IPv6, así como routing estático.
- Soporte de DHCP, NAT y PAT.
- Debe realizar detección de fallos bidireccional entre Firewall y Router para aplicar a protocolos de routing dinámicos o rutas estáticas.
- Debe realizar policy base routing en base a ip o red de origen, o también basado en usuarios/grupos o por tipo de aplicación.
- Debe soportar arquitecturas de alta disponibilidad de tipo activo/pasivo o activo/activo
- Capacidad de realizar VPN "Site to Site" o "SSL VPN".
- Routing basado en política.
- Soporte Dual Stack IPv4 e IPv6 simultáneamente.
- Network address translation NAT IPv4, NAT64 y NAT66.
- DHCP server / DHCP Relay

- DNS Server y DNS Proxy
- NTP Server
- 802.1Q VLANs
- Routing basado en contenidos: ICAP y WCCP
- Point-to-Point Protocol over Ethernet (PPPoE).
- Capacidades de virtualización: Los equipos deben disponer de al menos 10 dominios virtuales incluidos en el cortafuegos sin coste adicional.
- 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos.
- Capacidad de balanceo de servidores, con posibilidad de hacer SSL off-loading para el tráfico HTTPS.
- Session helpers y ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- Soporte para tráfico VoIP: SIP/H.323 /SCCP NAT trasversal, RTP
- Soporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Funcionalidad integrada del mismo fabricante de doble factor de autenticación vía token hardware o software, asi como por SMS, integrado en la misma plataforma de seguridad
- Funcionalidad de reconocimiento del tipo de dispositivo del cliente (Iphone, Ipad, Android, etc ...) y poder hacer políticas en función del tipo de dispositivo, sin la instalación de ningún agente en el dispositivo remoto
- Detección y bloqueo de botnets en base a listas de reputación globales
- Capacidad para definir múltiples reglas de seguridad en las interfaces origen / destino, incluyendo "año"

3.1.4 Integración e identificación de usuarios

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión e identificación de usuarios, entendiéndose como funcionalidades mínimas a cumplir:

- Aplicación de políticas basadas en usuarios y grupos en vez de por ip.
- Integración con sistemas de directorios para obtención de usuarios y grupos, incluyéndose Microsoft Active Directory, Novell y eDirectory.
- Integración con sistemas multiusuario como Citrix o Microsoft Terminal Server para identificación de usuarios. Es decir, que el equipo sea capaz de identificar los múltiples usuarios conectados a un sistema de Microsoft Terminal Server o similar.
- Soporte de mensajes Radius Accounting para SSO.
- Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+.
- Capacidad de analizar mensajes de syslog con información de login y logout para identificación de usuarios.
- Posibilidad de inyectar usuarios mediante aplicaciones de terceros a través de API XML.
- Capacidad de poder identificar usuarios mediante portal de autenticación propio haciendo uso de protocolos como Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente o autenticación local.

3.1.5 Características generales de seguridad

Los equipos ofertados deben cumplir con los siguientes requerimientos mínimos en cuanto a funcionalidades relativas a seguridad:

- Arquitectura basada en interfaces, para la aplicación de políticas de seguridad.

- Capacidad de identificación de aplicaciones a nivel 7 con un mínimo de 4000 identificadas (incluyendo aplicaciones Web 2.0), así como la identificación de subfunciones dentro de una aplicación como por ejemplo "compartir escritorio de webex", "chat dentro de webex", "transferencia de ficheros en webex", etc.
- Posibilidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.
- Posibilidad de identificar las aplicaciones no solamente si utilizan los puertos tcp/udp por defecto o estándar sino en cualquier puerto que se utilice para dicha aplicación.
- Deben identificar aplicaciones propietarias que usen los protocolos HTTP, HTTPS y TCP.
- Capacidad para identificar las aplicaciones bajo túneles HTTPS
- Deben identificar aplicaciones que vayan bajo túneles encriptados SSL.
- Capacidad de definición de aplicaciones personalizadas.
- El Equipo de seguridad debe de permitir la creación de Aplicaciones personalizadas en función de atributos de capa7, para poder personalizar las posibles aplicaciones propietarias.
- Debe descifrar tráfico SSH y detectar aplicaciones no legítimas sobre este protocolo.
- Posibilidad de crear reglas de calidad de servicio según las aplicaciones que se usen en el tráfico.
- Posibilidad de aplicar políticas de NAT de forma independiente a las políticas de seguridad ante vulnerabilidades y de protección de la red interna.
- La solución debe incluir firmas, actualizaciones y tecnología propietaria. Como por ejemplo para las urls, malware, virus, firmas IPS, etc.
- Inspección de la identidad de la aplicación en cada establecimiento de conexión entrante o saliente
- Posibilidad de disponer de categorías master para facilitar la gestión de las políticas de filtrado.

3.1.6 Protección ante ataques de denegación de servicio

Los cortafuegos ofertados deben contar con medidas de protección ante ataques de Denegación de Servicio de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico.

Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.

3.1.7 Protección ante vulnerabilidades

Los cortafuegos ofertados deben contar con la posibilidad de aplicar políticas de protección ante vulnerabilidades y exploits tanto al tráfico entrante como al saliente, debiendo cumplir con las siguientes funcionalidades:

- Deberá incluir firmas específicas para proteger entornos industriales, incluidas al menos 1500 firmas para entornos OT.
- Se debe poder aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten en el tráfico bien entrante o saliente de Internet sin incurrir en latencia superior a 1 milisegundo para no penalizar la sensación del usuario, efectuando el análisis en una única pasada para todo tipo de amenazas.

- En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas.
- Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades.
- Las vulnerabilidades deben estar categorizadas por tipos y por niveles de riesgo, de forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.
- Se debe poder permitir usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.
- Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando.
- Más de 11000 firmas disponibles para la funcionalidad de IPS.
- Funcionamiento como IPS basado tanto en patrones como en "Rated based". Posibilidad de crear firmas de IPS customizadas
- Definición de las políticas de IPS por perfiles.
- Deberá permitir la creación de firmas específicas de IPS.

3.1.8 Filtrado de URL

Los equipos ofertados deben filtrar la navegación http o https según la URL que se desea visitar basándose en diferentes criterios:

- Deben de definir manualmente listas estáticas de URL o de IP permitidas y no permitidas para la navegación, con posibilidad de definir para las no permitidas la acción a realizar (bloquear, permitir pero advertir, generar solamente un log, etc.).
- Monitorizar y controlar la navegación web pudiendo trabajar con listas blancas y negras de URLs.
- Permitir la navegación basándose en categorías de URL, siendo dichas categorías actualizadas periódicamente a través de un servicio en la nube que permita al menos categorías de URL como "malware", "phising", "hacking", etc.
- Posibilidad de incluir listas de URL o IP dinámicas, de forma que los equipos puedan ser configurados para que de forma periódica consulten listas disponibles en servidores públicos reconocidos en los que se incluyen aquellas IP o URL relacionadas con amenazas y sean bloqueadas de forma automática.
- El equipo debe de proporcionar capacidades contra el robo de credenciales por ataques de Phising. De esta manera debe de ser capaz de:
  - ✓ Bloquear sitios categorizados como phising.
  - ✓ Alertar o Bloquear cuando una credencial de usuario interno vaya a ser publicada en un servicio externo a la red corporativa.
  - ✓ Forzar doble factor de autenticación para las aplicaciones críticas, sean o no basadas en web.

Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.

- El equipo debe de ser capaz de mostrar una página de reemplazo personalizable para las páginas bloqueadas tanto en la navegación HTTP como HTTPS.
- El equipo debe de ser capaz de poder modificar los umbrales de configuración de alerta de un

ataque de fuerza bruta.
- Base de datos de al menos 120 millones de URL.

3.1.9 Detección de equipos comprometidos en la red

Los cortafuegos ofrecidos deben de detectar mediante firmas posibles equipos comprometidos en la red que intenten establecer comunicación con servidores de comando y control, permitiendo realizar acciones predeterminadas como bloquear o monitorizar y registrar mediante log este tipo de tráfico.

Entre las acciones posibles, se debe tener la capacidad de interceptar las peticiones de resolución de dominios realizadas desde servidores propios DNS internos a la red o hacia servidores DNS externos de forma que se identifique los equipos internos comprometidos por algún tipo de malware.

3.1.10 Antivirus

Los cortafuegos propuestos deben de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.

El sistema antivirus debe de ser propietario del fabricante, de tal modo que no dependa de un tercero para la actualización de firmas.

Se debe poder aplicar políticas que permitan aplicar el motor de antivirus sobre protocolos como ftp, http, imap, pop3, smb o smtp, definiendo para cada uno de estos protocolos la acción a realizar (permitir los ficheros, descartar los ficheros, desconectar la sesión o registrar mediante logs) ante la detección del fichero malicioso por el motor de antivirus, adicionalmente, se debe poder tener la posibilidad de enviar el fichero que se inspecciona a un servicio en Internet que permita el análisis de dicho contenido y emita un veredicto en caso de que el fichero sea malicioso que permita realizar al cortafuego las acciones oportunas.

Los cortafuegos deben permitir la aplicación de políticas de antivirus de forma granular, permitiendo por ejemplo la aplicación de dichas políticas a ciertos usuarios de determinados grupos o a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.

3.1.11 Bloqueo de ficheros y datos sensibles

Los cortafuegos propuestos deben de identificar ficheros no basándose en su extensión sino en el tipo de contenido del archivo, permitiendo al menos 100 tipos de ficheros identificables.

Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes.

Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.

Los equipos deben poder buscar patrones sensibles como combinaciones de números de tarjetas de crédito

de forma que se evite la filtración de este tipo de datos.

- Detección del tipo de fichero por cabecera independientemente del tipo de extensión
- Capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como a asociaciones concretas
- Soporte de lenguaje de descripción de datos para la personalización de DLP
- Posibilidad de definición de los tipos de dato en función de palabras clave, palabras clave ponderadas, expresiones regulares, atributos de fichero, diccionario, plantillas corporativas
- Detección e identificación de documentos mediante "Fingerprint"
- Posibilidad de añadir marcas de agua en los documentos de office
- Soporte de más de 75 categorías de filtrado de contenidos

3.1.12 Descifrado de tráfico SSL

Los equipos ofertados deben realizar como mínimo de las siguientes funcionalidades:

- Configuración de las autoridades certificadoras (CA) de confianza para la inspección de tráfico https.
- Identificar aplicaciones propietarias que usen los protocolos HTTP, HTTPS y TCP.
- Identificar aplicaciones que vayan bajo túneles encriptados SSL.
- Los cortafuegos ofertados deben descifrar tráfico SSL y SSH de forma granular, de manera que se puedan establecer políticas de descifrado basándonos en las zonas por las que viaja el tráfico, según las direcciones IP origen o destino del tráfico enviado, los usuarios que generan dicho tráfico o los puertos que se están usando para el envío de tráfico, pudiendo excluir categorías de sitios de internet a las que se accede del tráfico a descifrar.

3.1.13 Tecnología de Sandboxing

Los cortafuegos propuestos deben tener la capacidad de disponer de un servicio en la nube o en on-premise capaz de analizar ficheros de tipo desconocido o enlaces URL recibidos en correos electrónicos, de forma que se permita el envío de dicha información para análisis atendiendo a criterios como:

- Tipo de aplicación que se está usando para transferir el fichero.
- Tipo de fichero que se está transfiriendo.
- Dirección de transferencia (descarga o subida de ficheros).

El servicio en la nube será capaz de analizar los siguientes tipos de ficheros: paquetes de aplicaciones Android, ficheros flash, applets java, ficheros de Microsoft office, ficheros ejecutables con formate PE incluyendo dll, ficheros pdf y enlaces HTTP y HTTPS incluidos en correos electrónicos recibidos por SMTP y POP3. El análisis realizado por este servicio en la nube en caso de que la información enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad deberá generar las firmas apropiadas en un plazo de 5 minutos que se utilizarán para actualizar los motores propios de antivirus y filtrados URL de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas por dichos cortafuegos.

Los cortafuegos deben tener la capacidad de enviar también al servicio de sandboxing en la nube no solamente aquellos ficheros de tipo sospechoso sino aquellos que hayan sido bloqueados por su propio sistema de firmas, con objeto de poder analizar variantes de malware e incorporar esas variantes al sistema de firmas de los propios motores del equipo, además se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.

3.1.14 Informes

Los equipos cortafuegos deben enviar todos los logs a un único equipo físico externo dedicado a generar y unificar los informes tanto predefinidos como personalizados.

Asimismo, los equipos cortafuegos proporcionados deben también tener la capacidad de generar informes tanto predefinidos como personalizados utilizando los logs generados por los propios equipos sin necesidad de equipos externos adicionales, limitándose dicha funcionalidad exclusivamente por la cantidad de logs que dichos equipos cortafuegos sean capaces de almacenar en su propio almacenamiento permanente.

Se debe disponer de la capacidad de generar informes de actividad por usuario, incluyendo aplicaciones utilizadas, sitios web visitados.

Se debe poder generar los informes de forma automática, así como agrupar varios informes en un único documento con formato PDF y que estos puedan ser enviado por correo electrónico a un grupo de distribución.

Entre los informes disponibles, se debe disponer de informes sobre los anchos de banda consumidos por las diferentes aplicaciones, informes sobre los orígenes y destinos geográficos de las amenazas detectadas, e informes sobre el análisis de comportamiento de tráfico observado que permita detectar equipos comprometidos participantes de botnets.

Los cortafuegos proporcionados deben permitir programar el momento en el cual se desea la generación del informe correspondiente y su envío a través de correo electrónico, así como el intervalo de fechas entre las cuales se desea la información de dicho report, dentro de las limitaciones de almacenamiento de los propios equipos.

Deberá ser fácil la generación de informes, y poder configurarlos en detalle. Se deberán identificar los enlaces (interlocutores, consumo, protocolos, etc) en tiempo real.

3.1.15 Procesamiento de logs

Los equipos cortafuegos deben enviar todos los logs a un único equipo físico externo dedicado a generar y unificar los informes tanto predefinidos como personalizados.

Los cortafuegos ofertados deberán tener la capacidad de almacenar los logs localmente con la única restricción de la capacidad de almacenamiento local del propio dispositivo o bien enviar los logs a una plataforma de gestión y procesamiento externa especializada con objeto de mantener dichos logs a largo plazo, el sistema de procesamiento de logs deberá cumplir con las siguientes características:

- Disponer de un cuadro de mando personalizable por usuario que accede al sistema con al menos la siguiente información: Aplicaciones más usadas, Aplicaciones de alto riesgo, Información general del sistema, Estado de los Interfaces, Logs relativos a las amenazas más observadas, Logs de filtrados URL o Recursos del sistema.
- Cuadro de mando de aplicaciones generado a partir de los logs, personalizable por usuario que permita disponer de información como los usuarios que más generan tráfico, las reglas de seguridad que más se usan, vulnerabilidades que más se han detectado y bloqueado, equipos que navegan hacia dominios maliciosos, virus detectados, información enviada a los servicios de sandboxing o host comprometidos en la red interna.
- Deben usar el motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs recibidos se pueda obtener información de alto nivel como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado con

indicación de tiempos, usuarios, direcciones ip y vulnerabilidades o amenazas detectadas.

- Posibilidad de filtrar cada una de las vistas o cuadros de mando de forma que la información esté restringida a ciertos criterios para poder realizar análisis más exhaustivos.
- Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites, etc.), para su visualización.
- Esta visualización tiene que ser tipo "Drill-down", es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo.

3.1.16 Plataforma de gestión de logs y reporting consolidado

Con objeto de cubrir la retención y procesado de logs a largo plazo, la solución propuesta debe ser totalmente compatible con el sistema actual de gestión de logs y reporting del CABB siendo este un Fortianalyzer 1000E.

La solución propuesta debe incluir toda la configuración necesaria para la integración de los firewalls de las instalaciones, elaboración de informes y alertas para las instalaciones a securizar. Así como cualquier trabajo no contemplado necesario para la correcta integración de las instalaciones en el sistema actual.

En caso de que la solución propuesta no sea compatible con el recolector actual de logs de CABB o sea necesario algún tipo de actualización HW, SW o de licenciamiento del mismo para poder soportar el nuevo equipamiento, la empresa adjudicataria deberá hacerse cargo de dichas actualizaciones y en caso de que sea necesario la adquisición de un nuevo equipo para realizar dichas funciones, éste debe ser un dispositivo físico y debe poseer las mismas prestaciones que el actual de CABB

3.1.17 Plataforma de configuración centralizada

Para poder administrar los nuevos equipos de forma centralizada, la solución propuesta debe ser totalmente compatible con el sistema actual de gestión centralizada del CABB siendo este un FortiManager 200F.

Para la integración de los nuevos equipos en la herramienta de CABB, se deberá realizar en un ADOM independiente al en que actualmente se encuentran los equipos de CABB, además una vez configuradas las reglas definitivas en cada equipo se realizará de forma que se

En caso de que la solución propuesta no sea compatible con el gestor centralizado actual de CABB o sea necesario algún tipo de actualización HW, SW o de licenciamiento del mismo para poder soportar el nuevo equipamiento, la empresa adjudicataria deberá hacerse cargo de dichas actualizaciones y en caso de que sea necesario la adquisición de un nuevo equipo para realizar dichas funciones, éste debe ser un dispositivo físico y debe poseer las mismas prestaciones que el actual de CABB

3.1.18 Otras funcionalidades

Los cortafuegos propuestos deberán disponer de funcionalidades adicionales entre las que se encuentran:

- Posibilidad de definir aplicaciones y/o vulnerabilidades propias mediante diferentes parámetros como los puertos tcp o udp que se usan en dicha aplicación y combinaciones de patrones dentro de las cabeceras de los paquetes o en los propios payloads de dichos paquetes que se deben cumplir para que se reconozca la aplicación y/o vulnerabilidad.
- Los cortafuegos ofertados deben descifrar tráfico SSL y SSH de forma granular, de manera que se establecezcan políticas de descifrado basándonos en las zonas por las que viaja el tráfico, según las

direcciones ip origen o destino del tráfico enviado, los usuarios que generan dicho tráfico o los puertos que se están usando para el envío de tráfico, siendo posible excluir categorías de sitios de internet a las que se accede del tráfico a descifrar.

- Deben descifrar tráfico que pasa a través del cortafuegos destinado a sitios web que utilicen certificados de curva elíptica (ECC).
- Captura de tráfico. Los cortafuegos propuestos deben tener la capacidad de realizar capturas del tráfico que atraviesa sus interfaces en formato pcap, de forma que se puedan establecer criterios de la captura como capturar el tráfico originado por un cierto origen ip o destino, cierto puerto o también capturar tráfico de una aplicación en concreto independientemente del origen o destino del tráfico o incluso aplicar filtros de captura de tráfico exclusivamente cuando se detecte un virus o un ataque en los motores de protección.
- Los equipos cortafuegos deben de poder aislar los equipos que se encuentren en una DMZ, haciendo que el tráfico pase por el firewall y a través de sus reglas se permita cierto tráfico entre ellos. Por defecto los equipos, aunque estén en una misma VLAN no se verán entre sí.
- Los equipos deben de poder realizar microsegmentación, equipos que se encuentren en la misma red, con mismo rango de direccionamiento IP pertenezcan a distinta VLAN y el ARP se lleve hasta el firewall, sin necesidad de cambio de direccionamiento de los equipos ni configuración de private vlans, de modo que se pueda gestionar y limitar el tráfico entre ellos.
- Se requiere que el fabricante propuesto, figure en el apartado de líderes del cuadrante mágico de gartner, durante los últimos 5 años y/o que cuente con guías de configuración del CCN-CERT en cuanto a:
  - ✓ Configuración general de cortafuegos
  - ✓ Configuración de protección ante ataques DDoS

3.1.19 Especificaciones de capacidad firewalls

Cada firewall ofertado deberá cumplir como mínimo con las siguientes especificaciones:

- Throughput de Firewall para paquetes de 1518,512 y 64 bytes: 3 Gbps
- Prestaciones o capacidad en tráfico real con las funcionalidades habilitadas de IDS/IPS, Antivirus y AntiSpyware (adicionalmente a identificación de aplicaciones) :
  400 Mbps
- Rendimiento de IPSec VPN: 2Gbps
- Rendimiento de IPS: 400 Mbps
- Rendimiento Threat prevention (malware protection donde está el antivirus, firewall, IPS, control de aplicaciones): 200 Mbps
- Nuevas sesiones TCP por segundo: 30.000
- Sesiones concurrentes: 1.300.000
- Latencia: 3 µs

3.1.20 Características Hardware de los equipos

Cada firewall ofertado deberá cumplir como mínimo con las siguientes especificaciones:

Firewall IT

- 7x GE RJ45 Ports

- 2x GE RJ45 WAN ports
- 1x GE RJ4 5 DMZ Ports
- Disco duro interno de 128 GB SSD
- Puerto de consola RJ45
- Puerto USB
- Bandeja adicional en caso de ser necesaria, preferiblemente propia del fabricante, para ocupar 1RU del armario
- Fuentes de alimentación redundadas Hot-swap y alimentación requerida de 100–240V AC, 50–60 Hz

Como referencia de características mínimas, para orientación de los ofertantes, se han considerado los equipos de la casa Palo Alto. (modelo estudiado es el PAN 320) y de la casa Fortinet. (modelo 61E + FortiAnalyzer + FortiManager).

Todo el equipamiento ofertado debe ser appliance físico.

3.2 Switch industrial cabecera

Los switches utilizados para el entrono OT deberán cumplir las siguientes funcionalidades mínimas:

La solución propuesta se debe componer de switches Industrial Ethernet compactos para construir topologías eléctricas u ópticas en línea, en anillo y en estrella con velocidades de transferencia de 10/100/1000 Mbits/s.

- SCALANCE X-300 está disponible en las siguientes variantes:
  - Variante con puertos Ethernet eléctricos y ópticos ya integrados
  - Variante semimodular con cuatro puertos Ethernet eléctricos integrados y dos slots modulares que se pueden ocupar con módulos de medio de 2 puertos
- Redundancia rápida del medio de transferencia gracias al gestor integrado al efecto, tanto para Gigabit Ethernet como para Fast Ethernet
- Integración de redes de automatización en redes corporativas existentes gracias al soporte de numerosos estándares de TI: construcción de redes virtuales (VLAN)
- Integración redundante en redes de nivel superior gracias al soporte de métodos de redundancia estandarizados (Rapid Spanning Tree Protocol)
- Diagnóstico PROFINET, acceso SNMP, servidor web integrado y función de envío automático de correo electrónico para diagnóstico remoto y señalización a través de la red

Beneficios:

- Gran disponibilidad de la red gracias a:
  - alimentación redundante
  - estructuras de red redundantes con base de FO o par trenzado (gestor de redundancia, función standby y RSTP integrados)
  - reemplazo fácil del equipo mediante soporte de datos intercambiable C-PLUG enchufable
  - muy rápida reconfiguración de la red en caso de avería
- Menor propensión a fallos y mayor disponibilidad de la red de comunicación, ya que los conectores FastConnect RJ45 quedan encajados en el collar de sujeción de los puertos RJ45
- Protección de la inversión gracias a la integración en sistemas de gestión de redes existentes

mediante acceso estandarizado a SNMP
- Ahorro de tiempo en la ingeniería, puesta en marcha y durante el funcionamiento de una instalación gracias al aprovechamiento de la configuración y del diagnóstico integrados en STEP 7
- Adaptación sencilla a distintas topologías de red y reducción de los costes de almacén gracias a la flexibilidad de las variantes semimodulares

Además de esto deberá de cumplir como mínimo con las siguientes características:

- 16 puertos de comunicaciones RJ45 y como mínimo 8 configurables para diferentes medios (RJ45, Fibra óptica multimodo/monomodo). Puertos delanteros.
- Enracable en rack de 19''. (Si es necesario se deberá suministrar un kit de enracado).
- Fuente de alimentación y ventiladores redundante de las mismas características que los principales.
- Alimentación a 230Vca.
- Tarjeta de memoria para almacenar los datos de configuración y posibles datos de usuario.
- CLI
- Gestión basada en web
- Soporte de MIB
- TRAP vía Email
- Configuración con STEP 7
- RMON
- Portmirroring y mirroring multipuerto
- CoS
- Diagnóstico PROFINET IO
- Gestión de VLAN.
- DHCP.
- Protocolos - Telnet, HTTP, HTTPS, TFTP, FTP, BOOTP, GMPR, DCP, LLDP, SNMP v1, SNMP v2,
- SNMP v3, IGMP.
- Redundancia - HRP, HRS, STP, RSTP, MSTP

Ref.: Siemens 6GK5324-4GG10-4ER2 o similar.

Cada switch instalado deberá suministrarse con una memoria de configuración C-PLUG, para almacenar los datos de configuración y posibles datos de usuario. (Ref. 6GK1900-0AB00 o similar).

Al disponer de puertos configurables, se deberán suministrar los puertos SFP que se requieran en cada caso, recomendados por el fabricante.

Ref.: Siemens 6GK5991-2AC00-8AA0 para puertos monomodo, Ref. Siemens 6GK5991-2AD00-8AA02 o similar para puertos multimodo y Ref. Siemens 6GK5992-2GA00-8AA0 o similar para puertos de cobre.

3.3 Switch Industrial

Donde se solicite se deberá suministrar un Switch industrial a colocar en los CGMs o cuadros de control

situados en las instalaciones. Las características de estos Switches deberán ser las siguientes:

- Puertos Ethernet eléctricos y ópticos ya integrados
- 1 puertos de comunicaciones RJ45 10/100/1000 Mbit/s.
- 7 puertos de comunicaciones RJ45 10/100 Mbit/s.
- 2 puertos de fibra óptica multimodo o monomodo (según la necesidad) con conectores SC a 1000 Mbit/s.
- Para montaje en carril DIN.
- Tarjeta de memoria para almacenar los datos de configuración y posibles datos de usuario.
- Alimentación a 24Vcc.
- CLI
- Gestión basada en web
- Soporte de MIB
- TRAP vía Email
- Configuración con STEP 7
- RMON
- Portmirroring y mirroring multipuerto
- CoS
- Diagnóstico PROFINET IO
- DHCP.
- Protocolos - Telnet, HTTP, HTTPS, TFTP, FTP, BOOTP, GMPR, DCP, LLDP, SNMP v1, SNMP v2,
- SNMP v3, IGMP.
- Redundancia - HRP, HRS, STP, RSTP, MSTP

Ref.: Siemens. 6GK5308-2FM10-2AA3 o similar para Switches monomodo y Siemens. 6GK5308-2FL10-2AA3 o similar para Switches multimodo.

Cada switch instalado deberá suministrarse con una memoria de configuración C-PLUG, para almacenar los datos de configuración y posibles datos de usuario. (Ref. 6GK1900-0AB00 o similar).

Estará dentro del alcance la sustitución de Switches existentes donde así se requiera.

3.4 Switch IT

Las características mínimas que deben cumplir los switches para IT son los siguientes:

Característica	Valor
Downlinks total 10/100/1000:	24 ports data

Característica	Valor
Uplink configuration:	4x 1G fixed uplinks
Default primary AC power supply:	WR-C5-125WAC o similar. 125 W de AC
Fans:	Fixed redundant
Stacking support:	StackWise-80 o similar
Stacking bandwidth support:	80 Gbps
Stacking hardware:	8
Kit de stack	Dos adaptadores de data stack y un cable de data stack. Cable de stack de 1m.
Total number of MAC addresses	16,000
Total number of IPv4 routes (ARP plus learned routes)	11,000 (8,000 direct routes and 3,000 indirect routes)
IPv4 routing entries	3,000
IPv6 routing entries	1,500
Multicast routing scale	1,000

Característica	Valor
QoS scale entries	1,000
ACL scale entries	1,500
Packet buffer per SKU	6 MB buffers for 24- or 48-port Gigabit Ethernet models
Flexible NetFlow (FNF) entries	16,000 flows on 24- and 48-port Gigabit Ethernet models
DRAM	2 GB
Flash	4 GB
VLAN IDs	1024
Total Switched Virtual Interfaces (SVIs)	512
Jumbo frames	9198 bytes
Wireless bandwidth per switch	N/A
IP SGT binding scale	10K
Number of IPv4 bindings	10K

Característica	Valor
Number of SGT/DGT policies	2K
Number of SXP Sessions	200

Debe tener e incluirse en la oferta doble fuente de alimentación y la fuente redundante debe ser idéntica a la principal.

Se debe incluir cable de stack de 1m por cada equipo.

Cada switch debe incluir sus correspondientes transceivers compatibles y recomendados por el fabricante indicados en la tabla de referencia del punto 1.3.

Otras funcionalidades y básicas e imprescindibles que deben cumplir los equipos son:

- Administrable
- SNMP
- Sflow, NetFlow
- SD-WAN

3.4.1 Otras funcionalidades

Algunas funcionalidades que debe disponer el equipamiento para electrónica de red para IT, son las siguientes:

- Capacidad de aplicar parches para corregir errores críticos y vulnerabilidades de seguridad entre las versiones de mantenimiento regulares
- Funcionalidades avanzadas de seguridad que permiten la garantía de autenticidad de hardware y software en la cadena de suministro y una protección contra los ataques de intermediarios al software y el firmware
- Soporte de hasta 80G de Stacking
- Modelos con puertos de Uplink a 10G
- APIs abiertas y programabilidad
- Redundancia de fuentes de alimentación y ventiladores
- MACsec AES-128
- Full Flexible NetFlow
- Posibilidad de simplificar la operación y el despliegue con automatización basada en políticas

- Posibilidad de implementar segmentación basada en políticas
- RFID tag compatible con lectores RFID comerciales para facilitar la gestión de inventario
- LED blue beacon en el frontal y parte trasera para una identificación sencilla de los switches
- Soporte de EEE (Energy Efficient Ethernet) en los puertos RJ-45.
- Posibilidad de configurar el máximo consumo en un puerto determinado
- Soporte hardware para conectar un dongle Bluetooth, para habilitar este interfaz Wireless como un interfaz IP de gestión
- Algunas funcionalidades de routing como RIP, EIGRP Stub, OSPF, PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder

Además, el equipamiento ofertado debe disponer de funcionalidades DNA como:

- Automatización de arranque de la red de día 0: aplicación de red Plug-n-Play, configuración de red, credenciales del dispositivo.
- Gestión de elementos: Descubrimiento, inventario, topología, imagen de software, licencias y gestión de configuración.
- Monitoreo de la red: cumplimiento del Equipo de Respuesta a Incidentes de Seguridad del Producto (PSIRT), informes al final de la vida / final de la venta, cociente de telemetría, cliente 360, dispositivo 360, destinatarios principales / NetFlow / colección y correlación de telemetría de transmisión.
- Configuración y supervisión de QoS estática: aplicación EasyQoS.

En caso de encontrar alguna carencia en este PPTP, indicarlo en la oferta de manera detallada, añadiendo el ítem o ítems correspondientes, su referencia e importe.

Se entiende que el equipo suministrado dispone de administración mediante ssh. Debe admitir VLANs, Spanning-tree, SNMP, etc.

3.5 Elementos auxiliares

3.5.1 Rack de comunicaciones

En cada ubicación descrita del presente proyecto será necesario la instalación de un nuevo rack de comunicaciones, la extensión del cableado estructurado actual de la sede periférica (tanto cableado UTP como fibra óptica) hasta la ubicación del nuevo armario, así como la instalación de otros componentes y traslado de equipos como los routers actuales al nuevo rack.

El rack de comunicaciones que albergará cuantos elementos compone la solución del presente proyecto deberá cumplir los siguientes requisitos mínimos y componentes junto a él a entregar:

- 19 pulgadas 42U
- 750mm ancho x 1070mm fondo x 1991mm alto o similar
- Instalación interior
- Tensión de servicio 230 Vca
- Cerradura electrónica

- Llaves electrónicas
- Llave maestra para apertura de rack convencional
- Pasahilos metálicos, no de cepillos
- Paneles Patch Panels UTP cat 6
- Paneles fibra óptica monomodo y multimodo
- Cableado UTP cat 6
- Latiguillos de fibra óptica
- Posibilidad de enrracado también mediante carril DIN
- Grado de resistencia a impactos Ik10
- Puertas metálicas perforadas o transparentes.
- Color negro

APC 3150 o similar.

Es requisito disponer de un armario rack de comunicaciones que albergará todos los elementos de seguridad y comunicaciones con todo debidamente etiquetado

Al menos, y no únicamente, deberá constar el armario de comunicaciones con cuantos pasahilos, paneles patch panels de UTP, paneles patch panels de fibra óptica, latiguillos de UTP, latiguillos de fibra óptica, etc. sean necesarios para la correcta instalación de todos los elementos de dicho rack.

El armario debe disponer de cerradura electrónica para apertura de puerta del rack mediante tarjeta electrónica. Se deberán suministrar al menos 10 llaves electrónicas. De igual manera, para los mismos racks se facilitará al mismo tiempo una llave maestra tradicional.

Estos criterios pueden ser revisados durante la ejecución y puesta en marcha del proyecto.

Dispondrá de refuerzos y medios necesarios para proporcionar la adecuada rigidez y resistencia del panel, tanto en las condiciones normales de operación como en las de transporte y montaje.

En funcionamiento normal, el cuadro tendrá acceso por la parte frontal y trasera mediante puertas (las traseras divididas) equipadas con bisagras interiores. Los paneles laterales, superiores estarán firmemente sujetos a la estructura mediante tornillería.

Dispondrán de los soportes necesarios para la fijación de elementos frontales, interiores, regleteros de bornas, canaleta de cables, etc. Dichos soportes serán atornillados y permitirán de una forma rápida la sustitución del cualquier equipo.

Normalmente, la entrada de cables exteriores será por la parte inferior por lo que se dispondrá de espacio para el conexionado de dichos cables.

En ningún caso se permitirá que para cambiar un equipo o acceder a sus conexiones se tenga que desmontar otro equipo.

En todos los casos, los cuadros tienen que estar diseñados para soportar los esfuerzos dinámicos y térmicos a los que van a estar sometidos, tanto en funcionamiento normal, a las intensidades y tensiones asignadas, como en caso de falta, del tipo que sea.

En caso necesario, en función de la instalación a realizar, los cuadros deben asegurar la integridad de las personas, incluso con la falta más severa, de modo que no pueda haber proyecciones de elementos sólidos, puertas, paneles, etc. ni proyecciones de gases no canalizadas, ni tensiones diferidas no controladas, ni temperaturas inadmisibles.

Se dispondrán etiquetas de identificación en castellano en el frente y parte posterior de cada columna del

cuadro, estas serán de plástico laminado de color blanco con letras y números de 6 mm de altura grabadas en negro. El etiquetado deberá ser realizado de manera informática evitando los textos escritos "a mano". Estarán fijadas al cuadro mediante remache plástico o tornillo.

Los elementos auxiliares se identificarán internamente de acuerdo con los esquemas desarrollados y con rótulos que no se borren o desprendan, igualmente este etiquetado deberá ser realizado de manera informática evitando los textos escritos "a mano". Se identificará doblemente; sobre elemento y sobre placa o estructura de montaje.

La envolvente exterior de los cuadros eléctricos dispondrá de una toma de tierra, asegurando la continuidad de esta toma a través de todos sus elementos.

Los cuadros dispondrán de un elemento portaplanos con los planos eléctricos funcionales de cada uno de ellos.

En el diseño del cuadro se tendrá en cuenta la disponibilidad de espacio de reserva para posibles ampliaciones futuras, que será como mínimo de un 20% del total.

3.5.2 Sensor de temperatura

El sensor de temperatura utilizado en el CABB es de TH2E. Las principales características que tienen son:

- Medidas de temperatura, humedad y punto de rocío
- Conexión LAN
- Interfaz web interno
- Logging inteligente de los valores de las medidas
- Envío a un servidor externo de los datos medidos
- Envío por correo electrónico de alerta de umbrales establecidos
- Comunicaciones: TCP, SNMP, e-mail, MODBUS TCP, XML, HTTP GET, etc.

No se admitirá uno de menores características y funcionalidades.

Se deberá realizar la programación necesaria para integrar los nuevos sensores con el resto de las sondas instaladas en la actualidad en una aplicación web desarrollada por el CABB.

3.5.3 UPSs y protecciones eléctricas

Un par de UPSs dotadas de la capacidad de asegurar la alimentación de las dobles fuentes independientes de los equipos para los equipos que dispongan, o en caso de no disponer, como en el caso de cortafuegos y switches de OT, para alimentar la fuente de cada uno de los elementos con una UPS diferente a fin de dotar al sistema de la máxima disponibilidad y fiabilidad.

Las UPSs deberán contar con esquema de control para su Bypass, a fin de asegurar la disponibilidad y que no se produzcan cortes de la alimentación eléctrica cuando se realicen labores de mantenimiento de las UPSs o sustitución de las mismas.

Las SAIs deben poseer una tarjeta de red con conexión Ethernet para su gestión vía SNMP.

En general los equipos serán de las siguientes características:

- Montaje en rack de 19''.
- Parámetros de entrada:
  - Tensión: 400/ 230 Vac ±10% - (3F o F+N), en función de la potencia requerida.
  - Frecuencia: 50 Hz ± 5%
- Parámetros de salida:
  - Tensión: 230 Vac ±10% - (F+N)
  - Frecuencia: 50 Hz ± 5%
- Potencia: mínima 3 kVA (con reserva del 20 %)
- Autonomía: 60'
- Rectificador completo con corrección activa del factor de potencia.
- Inversión IGBT controlado por procesador de señales digitales.
- Convertidor CC/CC Booster.
- Cargador de baterías.
- Conmutadores de entrada / salida.
- Conmutadores de by pass manual.
- Conmutador estático.
- Baterías integrales de plomo-ácido sin mantenimiento (integrados en el armario del SAI), de alto rendimiento (8-10 años).
- Interface COM estándar y toma de red. Configuración como cliente en red IP/SNMP.
- Software de apagado de S.O. y monitorización.

Salicru SPS ADVANCE RT2 u otro de similares características.

3.5.4 Fuente de Alimentación 24Vcc

En caso de ser necesario alimentar algún equipo a 24Vcc se suministrará una fuente de alimentación de 24Vcc de como mínimo las siguientes características:

- Tensión de entrada (monofásica) 230 Vac (desde SAI)
- Salida 24 Vcc y como mínimo 10 A.
- Protegida mediante interruptor automático de la Icc adecuada, curva D. Fabricante Schneider, Siemens o similar.

Siemens 6EP1334-2BA20 u otro de similares características.

Los equipos electrónicos alimentados a 24 Vcc se protegerán de manera individual y para ello se instalarán fusibles electrónicos o módulos de corte selectivos de entrada 24 Vcc e intensidad de salida ajustable. Deberá disponer de una señal de estado (diagnóstico) por canal de alimentación.

Siemens SITOP PSE200U, (Ref. 6EP1961-2BA31 o 6EP1961-2BA41) u otro de similares características.

3.5.5 Protecciones eléctricas

La acometida de alimentación al Rack de comunicaciones deberá estar protegida con una salida tipo 5B, alimentación bipolar servicios varios, del estándar de especificaciones eléctricas del CABB, que básicamente

está compuesto por:

- Interruptor automático magnetotérmico II del calibre adecuado, capacidad de corte adecuada según cuadro, con contactos auxiliares de posición y disparo, curva C
  Fabricante Schneider, Siemens o similar.
- Interruptor diferencial bipolar de corte en polos, con contacto auxiliar de posición y montaje en carril DIN, tipo multi 9. Se tendrá en cuenta el tipo de carga a proteger al definir el tipo de diferencial a instalar.
  Fabricante Schneider, Siemens o similar.
- Incluyendo bornas de fuerza y control, cables, canaletas, etiquetas, cualquier modulo necesario para la conexión de los distintos componentes, etc.

Cada uno de los elementos electrónicos que componen la solución deberá estar protegida con diferenciales superinmunizados.

A modo resumen, deberían constar al menos de:

- Diferenciales superinmunizados 25A/30mA y contactos auxiliares de posición.
- Automáticos de 2 polos 16A con reenganchador (2 o 3 veces) con curva de corte acorde a la carga que alimenta (curva z) y contactos auxiliares de posición.

Toda la electrónica de red deberá llevar tierras independientes.

3.5.6 Cableado interno (Cables y canales)

Todos los cables de fuerza en el interior del cuadro serán de cobre, unipolares, de tensión nominal 0,6/1 kV, flexible, clase 5, con características de rápida extinción de la llama, no propagadores de incendios y libre de halógenos, tipo RZ1-K (AS).

Todos los cables de control en el interior del cuadro serán de cobre, unipolares, de tensión nominal 750 V, flexible, clase 5, con características de rápida extinción de la llama, no propagadores de incendios y libre de halógenos, tipo H07Z1-K.

Los cables de control tendrán una sección mínima de 1,5 mm2.

Los cables que alimentan bobinas de interruptores y la conexión a los toroidales, 2,5 mm2.

Para señalizar los distintos circuitos se deben utilizar obligatoriamente el siguiente código de colores para los conductores unipolares:

- Azul claro — Neutros de circuito de potencia
- Negro — Conductores activos de circuitos de potencia en c.a y c.c.
- Rojo — Circuitos de mando en corriente alterna
- Blanco — Circuitos en 24 V.c.a.
- Azul — Circuitos de mando en corriente continua
- Amarillo/Verde — Conductores de protección (Tierra)

Excepciones previstas a la norma:

- Mangueras multiconductoras. En este caso deben ir obligatoriamente identificadas mediante marcas

en los cables u otros colores.

- Dispositivos individuales con un cableado interno que son adquiridos como complementos.
- Conductores que, por su naturaleza, no disponen de aislante superficial del color normalizado. En este caso se deberá identificar claramente mediante inscripciones indelebles.

Todas las puntas de cable serán identificadas de forma clara e indeleble, que no se perderá al desconectar los mismos. El etiquetado deberá ser realizado de manera informática evitando los textos escritos "a mano".

Existirán como máximo dos cables (puntas) por punto de conexión. Las conexiones en los puntos de conexión se deberán realizar siempre con punteras adecuadas en función del número de cables y la sección de estos.

Para el cableado de mando exterior hasta el interior de la envolvente deberán utilizarse obligatoriamente bornas de conexión o combinaciones base-clavija adecuadas.

Los canales de cableado interior de la envolvente deben ser de material aislante, tipo ranurado, libres de halógenos y con tapas fijadas a presión. Se deben poder acceder preferiblemente desde la parte delantera del armario para poder hacer modificaciones; caso de no ser así, será necesario prever el acceso al armario desde la parte posterior mediante puertas o tapas accesibles. Los canales deben prever un espacio libre para reserva del 25% de su volumen.

Se prohíben los empalmes de cualquier tipo entre conductores dentro de canales o conducciones, debiéndose disponer de bornas para estas conexiones debidamente colocadas fuera de los canales.

Cuando sea necesario derivar varios cables de un punto dado para su distribución se utilizarán colectores de barras, bornas puenteables o barras de distribución diseñados para soportar los esfuerzos mecánicos y térmicos de la intensidad de cortocircuito máxima previsible en dicho punto.

Dentro de cada regletero las bornas serán sustituidas por niveles de tensión, formando subregleteros.

Dichos colectores se deben disponer en grupos separados cuando existan colectores de mando y de potencia.

Se prohíbe el uso común del mismo colector para funciones de protección (tierra) y funciones de neutro. El colector de tierra debe ser perfectamente identificable y distinto de cualquier otro colector.

Las mallas o cubiertas de los cables apantallados o blindados no podrán ser utilizados bajo ningún concepto como conductores de protección, aunque si deben estar conectados obligatoriamente a tierra.

Cableado UTP

Se utilizará cable UTP industrial libre de halógenos, par trenzado y categoría 6.

El cableado UTP deberá instalarse con un código de colores diferenciador:

- Blanco para las conexiones con equipos IT
- Verde para las conexiones con equipos OT
- Rojo para las conexiones del FW principal
- Azul para las conexiones del FW de backup

El cableado de parcheo utilizado será de una medida adecuada para que no esté muy tirante ni sobre demasiado, se estima que en la mayoría de las ocasiones valdrán cables de 2 metros, aunque en ciertas ocasiones pueden ser necesarios también algunos de 1 ó 3 metros. Estos cables deben ir perfectamente etiquetadas con las indicaciones del CABB y dichas etiquetas.

3.5.7 Protector de sobretensiones

El Rack deberá estar protegido mediante un protector de sobretensión adecuado en la entrada. Para redes tipo TT, clase de exigencia C, Tipo 2, clase II N/PE, 2 polos y con aviso remoto. Este estará protegido mediante fusibles.

Schneider, Siemens u otro de similares características.

3.5.8 Transformador de aislamiento galvánico 230V/ 230V

También se incluirá un transformador de mando de seguridad, cumplirán con la norma EN 61.558, serán monofásicos de 230/230 Vca y serán encapsulados en resina epoxi. Protegidos mediante interruptor automático de la potencia adecuada y curva D.

Es obligatorio el uso de un sistema de seguridad en los circuitos secundarios de mando para evitar las conexiones o desconexiones involuntarias de las máquinas ante la aparición de derivaciones a masa en puntos distintos del circuito, por lo que aguas abajo del trafo de mando de 230V c.a. se instalará relé diferencial con función de rearme automático.

Polylux u otro de similares características.

3.5.9 Bornas

Las bornas serán de paso 6 mm para cables de control y de al menos 8 mm para el resto. Serán seccionables para circuitos de control y de tensión. Para los circuitos de intensidad serán puenteables.

Los regleteros estarán convenientemente identificados y separados por tensión y función.

3.5.10 Puesta a tierra

Se deberá cumplir lo indicado en el REBT-18 y en al ITC-RAT13 (en caso de que aplique) sobre la puesta a tierra de instalaciones

Todo el sistema de puesta a tierra estará dimensionado de forma que para la máxima corriente de fallo, las tensiones estén dentro de los límites admisibles por el vigente reglamento

Para conseguir la equipotencialidad de todas las masas metálicas de la instalación, que no estén en tensión, se deberá garantizar la conexión a la red general de tierra los siguientes equipos y estructuras:

- Los chasis y bastidores de aparatos de maniobra.
- Las envolventes de los conjuntos de armarios metálicos.
- Las puertas metálicas de los locales que puedan ponerse en tensión a consecuencia de averías, accidentes o sobretensiones.
- Las estructuras y armaduras metálicas del edificio.
- Los blindajes metálicos de los cables.
- Racks y bandejas de cables.
- Las carcasas de los transformadores.

- Los neutros de B.T. de los transformadores.
- Los circuitos de baja tensión de los transformadores de medida.
- Los elementos de derivación a tierra de los seccionadores de puesta a tierra.

3.5.11 Cableado Externo

Cables de Baja Tensión de Fuerza en Zonas NO clasificadas

Los cables de fuerza utilizados en instalaciones eléctricas de baja tensión serán, tipo flexible, con aislamiento nominal 0,6/1kV y libre de halógenos.

Los utilizados para acometidas (s/ITC, BT-015) y los utilizados en canalizaciones subterráneas y sobre bandeja serán tipo RZ1-K (Cca-sb1, d1, a1) y libre de halógenos.

En aquellas instalaciones que se indique expresamente los cables serán armados, libres de halógenos, tipo RZ1MZ1-K (Cca-sb1, d1, a1) para multipolares y RZ1MAZ1-K (Cca-sb1, d1, a1) para unipolares. Generalmente en instalaciones de Saneamiento los cables serán armados, y en instalaciones de Abastecimiento no.

Los conductores de cables aislados cumplirán la norma UNE – EN 60.228 sobre formación y resistencia de los mismos.

Las características físicas, mecánicas y eléctricas del material deberán satisfacer lo previsto en las normas UNE 21.011-2.

Los conductores serán siempre de cobre recocido y la sección mínima a utilizar de 2,5 mm2.

Los cables llevarán impresas las características siguientes:

- Tipo constructivo.
- Tensión nominal del cable en kilovoltios.
- Número, sección nominal, naturaleza y forma de los conductores.
- Identificación de la clase CPR en el cable

Además, los cables llevarán una marca indeleble que identifique claramente al fabricante, su designación completa y las dos últimas cifras del año de fabricación.

El embalaje deberá disponer del marcado CE. El fabricante deberá disponer de la Declaración de Prestaciones (DoP).

Se realizarán los siguientes ensayos:

- Ensayo de rigidez dieléctrica de los aislamientos.
- Medida de la resistencia del aislamiento.
- Medida de la resistencia eléctrica de los conductores.

La tensión de prueba de los cables de 0,6/1kV de aislamiento será de 1.000Vcc - 1 min y la resistencia mínima de aislamiento, a la tensión de prueba será de 2MΩ.

La identificación de los conductores se realizará de acuerdo con la norma UNE 21.089.

Se deberán etiquetar las mangueras, indicando el circuito al cual pertenecen, con idéntica nomenclatura a la utilizada en los esquemas eléctricos desarrollados de la instalación.

Los cables de los variadores cumplirán las especificaciones indicadas por los fabricantes de los variadores en cada caso particular y deberán de ser aprobados por el CABB/BBUP antes de su compra.

Cables de Baja Tensión de Fuerza en Zonas NO clasificadas

Los cables de fuerza utilizados en instalaciones eléctricas de baja tensión serán de tipo flexible de tensiones de aislamiento 0,6/1 kV y libres de halógenos.

Los utilizados para acometidas (s/ITC, BT-015) serán libres de halógenos del tipo RZ1-K (Cca-sb1, d1, a1), y los utilizados en canalizaciones subterráneas y sobre bandeja serán tipo armados y libres de halógenos, tipo RZ1MZ1-K (Cca-sb1, d1, a1) para multipolares y RZ1MAZ1-K (Cca-sb1, d1, a1) para unipolares, con aislamiento nominal 0,6/1kV.

Los conductores de cables aislados cumplirán la norma UNE – EN 60.228 sobre formación y resistencia de los mismos.

Las características físicas, mecánicas y eléctricas del material deberán satisfacer lo previsto en las normas UNE 21.011-2.

Los conductores serán siempre de cobre recocido y la sección mínima a utilizar de 2,5 mm2.

Los cables llevarán impresas las características siguientes:

- Tipo constructivo.
- Tensión nominal del cable en kilovoltios.
- Número, sección nominal, naturaleza y forma de los conductores.
- Identificación de la clase CPR en el cable

Además, los cables llevarán una marca indeleble que identifique claramente al fabricante, su designación completa y las dos últimas cifras del año de fabricación.

El embalaje deberá disponer del marcado CE. El fabricante deberá disponer de la Declaración de Prestaciones (DoP).

Se realizarán los siguientes ensayos:

- Ensayo de rigidez dieléctrica de los aislamientos.
- Medida de la resistencia del aislamiento.

La tensión de prueba de los cables de 0,6/1kV de aislamiento será de 1.000Vcc - 1 min y la resistencia mínima de aislamiento, a la tensión de prueba será de 2MΩ.

La identificación de los conductores se realizará de acuerdo con la norma UNE 21.089.

Se deberán etiquetar las mangueras, indicando el circuito al cual pertenecen, con idéntica nomenclatura a la utilizada en los esquemas eléctricos desarrollados de la instalación.

Los cables de los variadores cumplirán las especificaciones indicadas por los fabricantes de los variadores en cada caso particular y deberán de ser aprobados por el CABB/BBUP antes de su compra.

Cableado UTP

En todas las ubicaciones será necesario desplegar cableado estructurado de categoría 6 desde donde se encuentran los equipos actuales (PCs, clientes y servidores SCADA, HMIs, etc) a la nueva ubicación que se ha pensado para cada rack de comunicaciones. A su vez puede que, en alguna sede periférica con fibra óptica, sea necesario también la extensión de dicha fibra hacia la ubicación del rack de comunicaciones.

Se utilizará cable UTP industrial libre de halógenos, par trenzado, apantallado y categoría 6. Los conectores

utilizados deberán ser metálicos para la conexión de la pantalla.

Fibra óptica

El cable de fibra óptica a instalar tendrá las siguientes características, bien en zonas clasificadas como en no clasificadas:

Tipo:	**Multimodo** 62,5/125 µm, 12 fibras
Protección secundaria:	Tubo holgado de PBT
Relleno:	Gel hidrófugo atóxico ni irritante
Cubierta interior:	Termoplástico no propagador de la llama, cero halógenos y baja emisión humos
Armadura:	Fleje acero con capa copolímero corrugado
Cubierta exterior:	Termoplástico no propagador de la llama, cero halógenos y baja emisión de humos.
Máxima tracción	1500 N en operación, 2700 N en instalación
Máximo aplastamiento	2000 N/10cm
Impacto	5J

Tipo:	**Monomodo** 9/125 µm, 12 fibras
Protección secundaria:	Tubo holgado de PBT
Relleno:	Gel hidrófugo atóxico ni irritante
Cubierta interior:	Termoplástico no propagador de la llama, cero halógenos y baja emisión humos
Armadura:	Fleje acero con capa copolímero corrugado
Cubierta exterior:	Termoplástico no propagador de la llama, cero halógenos y baja emisión de humos.
Máxima tracción	1500 N en operación, 2700 N en instalación
Máximo aplastamiento	2000 N/10cm
Impacto	5J

Canalizaciones

Zanjas

Los tubos en canalizaciones enterradas serán conformes a lo establecido en la norma UNE-EN 50 086 2-4, y sus características mínimas serán las indicadas en la tabla 8 de la ITC-BT-21 del RBT.

La canalización tendrá una profundidad aproximada de 700mm.

En su interior se verterá un lecho de arena de 5 cm, sobre el que se tenderá un tubo de diámetro interior no inferior a 60 mm por donde discurrirán los cables. Sobre el tubo se verterá una nueva capa de arena de 10 cm, y sobre dicha capa se verterán los productos de la excavación, compactándose hasta un próctor modificado del 95 %. La zanja se terminará con la reposición del pavimento existente inicialmente o el proyectado en su caso.

Para las zanjas, en cruzamientos de calzada, se preverá como mínimo un tubo de reserva.

Se colocará una cinta de señalización que advierta de la existencia de cables eléctricos, situada a una distancia mínima del nivel del suelo de 0,10 m. y a 0,25 m. por encima del tubo.

Las zanjas no se excavarán hasta que vaya a efectuarse la colocación de los tubos protectores. Se tomarán las medidas oportunas para dejar el menor tiempo posible abiertas las excavaciones con objeto de evitar accidentes. Si la causa de la constitución del terreno o por causas atmosféricas las zanjas amenazasen derrumbarse, deberán ser entibadas, tomándose las medidas de seguridad necesarias para evitar el desprendimiento del terreno y que éste sea arrastrado por las aguas. En el caso en que penetrase agua en las zanjas, ésta deberá ser achicada antes de iniciar el relleno.

Arquetas de registro

Serán de dimensiones normalizadas, dejando como fondo la tierra original a fin de facilitar el drenaje.

Para facilitar el tendido de los cables, en los tramos rectos se instalarán como máximo cada 40 mts., y por cada columna instalada para las luminarias de los viales.

El marco será de angular 45x45x5 y la tapa, prefabricada, de hormigón de Rk= 160 kg/cm², armado con diámetro 10 o metálica y marco de angular 45x45x5.

Se tomarán las disposiciones convenientes para dejar el menor tiempo posible abiertas las arquetas con el objeto de evitar accidentes.

Se deberán sellar las bocas de los tubos de plástico ocupados con cable para evitar la entrada de roedores y de agua. La espuma de poliuretano a utilizar tendrá las siguientes características:

Resistente a la penetración

Estabilidad térmica hasta 80 ºC

Temperatura mínima de aplicación 5 ºC

Los conductos no ocupados por cables serán obturados mediante tapones.

Bandejas aislantes de interior

Las bandejas deberán ser de material aislante según UNE EN 60.243-1, Rigidez dieléctrica superior a 20 kV/mm). Materia prima base PC + ABS sin halógenos – RoHS (Restriction of Hazardous Substances).

Distancia entre soportes máxima cada 1,5 m para una temperatura de trabajo 40 ºC.

Toda la tornillería será como mínimo de Acero Inoxidable AISI 316. Todos los soportes que no sean del mismo material que la propia canaleta serán como mínimo AISI 316.

Deberá soportar unas cargas para temperatura de servicio a 40ºC y ensayo tipo I (la unión entre dos tramos de bandeja puede quedar situada en cualquier posición entre dos soportes). El sistema de bandejas y soportes deberá soportar sin rotura una carga de 1,7 veces la carga admisible. Condiciones del ensayo según EN 61.537.

Protección contra daños mecánicos IK10 (con anclaje tapa IK10) según UNE-EN 62.262.

Las uniones entre tramos deberán ser de espesor igual o superior al de las bandejas a unir.

Serán no propagadoras de la llama s/ EN 61.537.

Dispondrán de un tabique separador para dividir la canalización en zonas dependiendo de la naturaleza de los circuitos que contenga.

Las curvas y enlaces se realizarán con piezas especiales fabricadas para tal fin.

Se exigirá un correcto acabado de sus superficies y nivelado de canalización y elementos.

Bandejas aislantes de exterior

Tendrán que cumplir con las siguientes características:

Las bandejas deberán ser de material aislante según UNE EN 60243-1:1998, Rigidez dieléctrica igual a 18±4 kV/mm). Materia prima base PVC – RoHS. La propia canaleta y accesorios del fabricante, el resto con aprobación del CABB-BBUP.

Temperatura de servicio, desde -20ºC hasta 60ºC según EN 61537:2001.

Distancia entre soportes (mínimo cada 0,5 m hasta 1,0 m). Temperatura de trabajo 60 ºC.

Toda la tornillería para fijación de AISI 316. Todos los soportes que no sean del mismo material que la propia canaleta y del mismo fabricante, serán de AISI 316.

Cargas para temperatura de servicio a 60ºC (distancia entre soportes 1m) y ensayo tipo I (la unión entre dos tramos de bandeja puede quedar situada en cualquier posición entre dos soportes). El sistema de bandejas y soportes deberá soportar sin rotura una carga de 1,7 veces la carga admisible. Condiciones del ensayo según EN 61537:2001

Protección contra daños mecánicos IK10 (con anclaje tapa IK10) según EN 50102:1996.

Bandeja perforada para la ventilación y fijación de cables. Pero no puede ser de panel de abeja.

Unión entre tramos de espesor igual o superior al de las bandejas a unir.

No propagadoras de la llama y ausencia de goteo incandescente. Inflamabilidad de materiales plásticos ANSI/UL 94:1990 clase UL94:V0. Reacción al fuego UNE 23727:1990 M1 (No inflamable).

IP2X (perforadas) según UNE 20324:1993. Marcado CE. Marcado de garantía de materiales UL. Cumplimiento directiva RoHS. Color gris, RAL 7035.

Se requerirá marca de calidad del producto por organismo reconocido que garantice la aptitud frente a los UV en aplicación exterior. Constará de un informe de ensayo no basado en un ensayo puntual sino cubriendo toda la producción. Contemplará la baja temperatura de -20ºC (que incluye ensayos a impacto a esa temperatura s/ norma de bandejas EN 61537:2007).

Tubos rígidos

Deberán ser no inflamables y no propagadores de la llama, libres de halógenos, serán estancos y estables hasta 60ºC, debiendo soportar esa temperatura sin deformación alguna.

El grado de protección contra daños mecánicos será de 3 a 5, tanto los de pared gruesa como extragruesa.

Serán inalterables a los ambientes húmedos y corrosivos, y resistentes al contacto directo de grasas y

aceites.

Todos los tubos cumplirán con el Reglamento Electrotécnico de Baja Tensión, así como con las normas UNE-EN 61.386-1, UNE 53.027, y UNE 53.315.

Cada tubo llevará impreso las siguientes especificaciones:

- Nombre del fabricante y símbolos de identificación.
- Diámetro nominal.
- Espesor.

Se exigirá que el fabricante tenga las tuercas y contratuercas para su unión a las cajas y piezas de acoplamiento y unión entre dos tramos siendo esta unión estanca.

Los conductos aislantes y compuestos deben ser marcados según un código de tres cifras, la primera cifra indicando las características mecánicas, la segunda y la tercera indicando su resistencia a las temperaturas.

El código debe estar conforme a las tablas de la norma UNE-EN 61.386-1.

Si al tubo se le pide cualquier otra aptitud de las especificadas en la norma UNE-EN 61.386-1 será colocada inmediatamente después de las tres primeras cifras indicadas anteriormente y separadas por un trazo oblicuo.

Los diámetros exteriores y las roscas deben cumplir lo indicado en la norma UNE-EN 60.423.

Todos los tubos que vayan a ser utilizados en ambientes húmedos o en locales que requieran algún tipo de seguridad y vayan vistos, serán roscados.

Se podrán utilizar tubos de aislamiento tipo PVC cuando discurran en canalizaciones enterradas o empotradas en obra civil. Cumplirán lo mismo que lo indicado anteriormente, excepto las condiciones contra incendios.

Tubos flexibles

Deberán ser no inflamables y no propagadores de la llama, libres de halógenos, serán estancos y estables hasta 60 º C, debiendo soportar esa temperatura sin deformación alguna.

El grado de protección contra daños mecánicos será de 3 a 5.

No deberán ser afectados por las lejías, sales, álcalis, disolventes ni petróleos.

Para las canalizaciones de red de voz y datos se utilizarán tubos flexibles de PVC y AFUMEX.

Cumplirán con el Reglamento Electrotécnico de Baja Tensión.

3.5.12 Cajas de interconexión

Serán de material aislante de baja emisión de humos tóxicos y no propagador de la llama en caso de incendio con tapa del mismo material y tendrá taladros troquelados semicortados para las entradas de tubos en las cuatro caras.

Las dimensiones mínimas serán de 100x100x40 mm.

Las cajas para instalación empotrada serán de material sintético antihumedad con junta de estanqueidad IP55 según DIN 40.050, dotada de regleta de bornas y prensaestopas y con borne de puesta a tierra conectado a la red de tierras.

El grado de protección que se exigirá será IP 55 según norma UNE 20.324.

3.5.13 Varios

El contratista deberá llevar a cabo cuantos trabajos sean necesarios para la correcta instalación y conexión de todos los equipos, por lo que debe tener en cuenta, que al tratarse de un proyecto "llave en mano" se requerirán trabajos de obra civil consistentes en anclaje de bandejas para el cableado eléctrico y de datos por el techo, o bien acometer perforaciones en el suelo para llevar el cableado desde una planta inferior al rack de comunicaciones. Se deberá tener en cuenta llevar a cabo trabajos en altura que puedan derivarse de estas necesidades.

En todos los suministros estará incluido las bornas de fuerza y control, cables, cables de conexión de los distintos módulos del controlador canaletas, etiquetas, cualquier modulo necesario para la conexión de los distintos componentes, etc

4 Servicios contratados

Este proyecto abarca los siguientes puntos para los firewalls y switches a suministrar:

- Suministro
- Configuración
- Mantenimiento

Suministro:

El suministro comprende la entrega de todo el material necesario para que la instalación quede en funcionamiento de acuerdo a este PPTP.

Todo el equipamiento incluido en la oferta por parte del licitador debe ser perfectamente compatible con el equipamiento disponible actualmente por el Consorcio de Aguas de Bilbao Bizkaia.

Asimismo, el equipamiento debe entregarse con la imagen y las versiones del resto de equipos del CABB, indicadas en el presente Pliego o las que se indiquen en el momento de la entrega del material por parte del personal responsable del contrato del CABB.

El plazo máximo de entrega del material debe ser de 4 semanas a partir de la firma del contrato, debiendo el contratista asumir la responsabilidad de fechas de entrega del o los fabricantes, suponiendo la demora posibilidad de aplicar penalizaciones contempladas en le pliego administrativo del presente proyecto.

Para la realización de este pliego se ha considerado como características mínimas las del siguiente equipamiento:

Configuración:

Se deberá realizar la configuración de los equipos nuevos, a fin de que tengan a su entrega la misma imagen y versión de firmware que el resto del parque existente.

Mantenimiento:

Esta asistencia comprenderá:

- Resolución de averías en 24 horas cualquier día del año (24x7).
- Servicio Gold del fabricante de los equipos para toda la duración del contrato.

5 Otros aspectos técnicos del proyecto.

El proyecto se considera "llave en mano", acometiendo el contratista todos los trabajos y suministros que sean necesarios para el correcto funcionamiento de los equipos con la configuración y programación necesarias.

El alcance del proyecto incluye el mantenimiento por parte de los fabricantes de la solución en 24x7, así como de la empresa integradora en modo (24x7x4).

El mantenimiento abarca el mantenimiento hardware y software, la instalación y mantenimiento de licencias, así como la asistencia por parte de la empresa por medio de una bolsa de horas establecida para la actuación sobre las configuraciones y parametrización de los equipos a mantener una vez finalizada la puesta en marcha de la solución. Además, deberá incluir todas las licencias tanto hardware como software necesarias para el correcto funcionamiento de los equipos con todas las prestaciones solicitadas.

El contratista deberá de dar soporte de optimización de la parametrización inicial, es decir, la que hay en el equipo actual, creando o modificando las políticas y/o perfiles necesarios. Dentro del alcance de la puesta en marcha de la solución estará incluida la optimización de los perfiles y accesos, es decir, no solo incluirá la migración de la configuración actual, sino que incluirá la mejora y optimización de los mismos.

La empresa adjudicataria del contrato se encargará de realizar todas las gestiones para generar y administrar las RMAs con el fabricante, recogida del material, etc. Deberá hacerse cargo de todos los cargos que puedan generar sin coste alguno para el CABB.

El contratista deberá de presentar un planning detallado de la previsión en el desarrollo de los trabajos.

Los trabajos objeto del proyecto se han de realizar sin interferir con el trabajo normal de los usuarios, por lo tanto, todo trabajo que suponga un corte del servicio se deberá de realizar fuera de la jornada laboral.

La empresa adjudicataria deberá colaborar con el fabricante durante la instalación de la solución, para la realización de tareas conjuntas de análisis, diseño, instalación y configuración de la herramienta.

Todo el equipamiento incluido en la oferta por parte del licitador debe ser perfectamente compatible entre sí y con el equipamiento disponible actualmente en las redes del CABB.

La compatibilidad entre los equipos de electrónica de red deberá ser total permitiendo la realización de configuraciones redundante mediante protocolo STP (Spanning Tree Protocol), VLANs entre centros, monitorización de tráfico y servicios, netflow, etc.

Todo equipamiento ofertado deberá ser nuevo y original del fabricante (tanto equipos activos como equipos pasivos tipo transceptores ópticos), siendo motivo de exclusión del concurso la inclusión de cualquier material no original del fabricante.

El CABB debe aparecer como propietario del equipamiento suministrado y debe constar como tal en las bases de datos del fabricante de dicho equipamiento.

Todo el equipamiento ofertado debe ser appliance físico.

En el caso de que alguno de los equipos (incluido ópticas, cables, memorias y demás componentes solicitados) tuviera anunciado el fin de soporte por parte del fabricante, el licitador deberá realizar su oferta

incluyendo el equipamiento propuesto por el fabricante para su sustitución.

Todo el equipamiento solicitado se entregará con la última versión del sistema operativo recomendada por el fabricante en el momento del suministro y previamente aprobado por el CABB.

Cualquier componente, tanto hardware como software, no descrito en los diferentes apartados de este pliego, y que fueran necesarios para el cumplimiento de los diferentes requisitos funcionales, deberá ser incluido en la oferta.

Durante el periodo de tiempo que cubre el mantenimiento de la presente oferta, toda actualización software debido a motivos de mal funcionamiento, algún tipo de bug o vulnerabilidades de seguridad reconocidos por el fabricante en las versiones de producción, será responsabilidad de la empresa contratada sin gastos adicionales para CABB y en caso de que dichas actualizaciones puedan interferir con el trabajo normal de los usuarios, dichas actualizaciones se deberán de realizar fuera de la jornada laboral, siendo además requerimiento la presencia física en la sede para una rápida intervención en caso de algún tipo de problema

6 Descripción de las tareas a ejecutar para la asistencia

Con carácter general diremos que los trabajos serán fruto de las necesidades originadas en el día a día: resolución de incidencias, implantación de nuevas funcionalidades, generación de informes, etc. Estos trabajos podrán tener que ser llevados a cabo en cualquier instalación del CABB.

El adjudicatario deberá cumplir con los siguientes requerimientos:

Soporte y Mantenimiento:

El periodo de garantía del equipamiento objeto de este expediente se extenderá durante toda la duración del contrato para el hardware y el software, a partir de la fecha de instalación de los elementos.

Se deberá prestar soporte 24x7x4 (modalidad de mantenimiento y soporte), durante la duración del contrato para todos los componentes hardware ofertados.

Igualmente se requiere un soporte 24x7x4 (modalidad de mantenimiento y soporte), durante la duración del contrato en todo el licenciamiento y software ofertado incluyendo garantía de disponibilidad, sin coste adicional, tanto de nuevas versiones y/o revisiones mayores o menores y de firmware de los productos objeto del contrato, en un plazo máximo de un mes a partir de su liberación. El adjudicatario procederá a su instalación de acuerdo con las directrices y planificación del gestor del contrato, incluyendo la posibilidad de que la instalación deba realizarse en sábado, domingo o festivo.

Será requisito necesario la disposición de equipamientos de stock en dependencias de CABB y de la empresa adjudicataria tal y como se ha expuesto en el punto 6 del apartado 1.1 y cubrir las necesidades de actualización SW indicadas en el apartado 5

Instalación:

Se precisa la instalación y configuración del equipamiento ofertado y las pruebas necesarias para su puesta en funcionamiento. Los equipos de securización deberán instalarse y configurarse para trabajar en alta disponibilidad (HA) en modo Activo- Pasivo Específicamente se deberán proporcionar los servicios de instalación y puesta en marcha, incluyendo todas las pruebas y soporte in situ necesarios para asegurar el completo funcionamiento de los equipos.

El hardware objeto de esta adquisición tendrá que ser configurado e instalado por la empresa adjudicataria, además de realizar las conexiones de cableado, todo ello según normas que establezca la Subdirección de Informática del CABB. Se deberá asegurar la no interrupción del servicio, por lo que las intervenciones se realizarán en las fechas y horarios autorizados (fines de semana inclusive). La intervención será in situ y consistirá en la manipulación física del equipamiento, conexionado y su configuración software de forma que el equipo quede perfectamente instalado y operativo de acuerdo con las indicaciones del personal del CABB.

Antes de la distribución, la empresa adjudicataria deberá etiquetar los equipos según normas que facilitará la Subdirección de Informática del CABB, para su posterior inventariado.

La empresa adjudicataria antes de proceder a la instalación deberá entregar un planning detallado de trabajos que deberá ser aprobado por el personal responsable del contrato del CABB.

Documentación:

Se considera necesario la entrega de la siguiente documentación mínima:

- Diseño HLD/LLD de la solución a implementar lo más estándar posible para todas las sedes (necesario incluir equipamiento que pueda ser ajeno al suministrado en la oferta pero que sea necesario utilizar como el gestor de logs y de equipos centralizado)
- Documentación de plan de pruebas a realizar en la sede y plan de migración
- Documentación final específica por sede en la que como mínimo se debe incluir:
    - Esquemas de red a nivel físico y a nivel lógico
    - Inventario del equipamiento instalado y su identificación según el etiquetado proporcionado por CABB
    - Esquemas eléctricos
    - Esquema detallado del armario indicando todos los elementos instalados

**** Todos los esquemas de red y de la disposición final del armario incluidos en la documentación deben de presentarse también en formato Visio*

Compatibilidad con la arquitectura del CABB:

Los elementos hardware ofrecidos deben ser totalmente compatibles con la arquitectura, hardware y software, del sistema de electrónica de red del CABB. Será responsabilidad del adjudicatario la ejecución de todas aquellas adaptaciones, configuraciones y parametrizaciones de productos necesarias para satisfacer dicho requerimiento.

Todos los sistemas propuestos deberán poder integrarse y prestar servicio dentro de la actual arquitectura del CABB.

Monitorización:

Los equipos ofertados deben ser monitorizables y han de gestionar el envío de alertas mediante protocolo SNMP, al menos de versión 2c y 3.

La herramienta de monitorización utilizada en el CABB es Intermapper para la recepción de los traps SNMP.

Los equipos deberán ser monitorizables por la solución Nagios actualmente en producción en el CABB.

El contratista se deberá hacer cargo de configurar los sistemas de monitorización del CABB a fin de integrar sus alarmas y objetos a monitorizar, entregando a su finalización de la integración, la documentación

correspondiente a las configuraciones y elementos utilizados para ello, Por ejemplo, MIBs, probes, parametrización, etc.

Se requerirá también un servicio de monitorización externo detallado en el apartado 6.3

6.1 Mantenimiento correctivo

Resuelve las incidencias o errores derivados del funcionamiento de los equipos o configuraciones.

La forma de prestación del servicio será la siguiente:

- El personal del contratista recibirá especificaciones del error detalladas por parte de los técnicos del Consorcio.
- Dicho personal efectuará las correcciones, gestiones con el fabricante y pruebas necesarias para resolver el problema.
- Finalmente documentará las modificaciones y comunicará la resolución de la incidencia y los cambios efectuados en un plazo máximo de 4 horas para las incidencias urgentes y 5 días laborables para el resto de las incidencias.

6.2 Mantenimiento evolutivo o adaptativo

Surgirá a petición de los usuarios para mejorar o adaptar el sistema a nuevas situaciones.

La forma de prestar el servicio será la siguiente:

- El Consorcio decidirá los cambios o mejoras a realizar determinando la prioridad de las ejecuciones.
- El personal del contratista ejecutará los trabajos.
- Finalmente documentará el trabajo y se lo comunicará e enviará al responsable del Consorcio. En caso necesario redactará las instrucciones de manejo.

6.3 Monitorización 24x7

Se requiere un servicio de monitorización de las instalaciones de los equipos principales: routers, switches, firewalls, UPS, temperatura etc. Para reporte y aviso de alertas e incidencias. Para ello, se necesita un servicio de SOC 24x7x365 en instalaciones del integrador.

Todas estas actividades se realizarán en remoto, debiendo estar habilitadas por parte del CABB las funcionalidades y permisos necesarios que permitan este acceso, siempre de manera segura. En caso de que para habilitar esta monitorización remota sea necesario la adquisición de algún equipo extra o nuevas líneas de comunicación debido a que con la infraestructura actual del CABB no es suficiente o las líneas de comunicación actuales se ven degradadas, será responsabilidad de la empresa adjudicataria adquirir ese nuevo equipamiento/ líneas de comunicación para el correcto funcionamiento de la monitorización

La finalidad de la monitorización es analizar el estado de las instalaciones, así como analizar el estado del servicio en la que se encuentran los equipos instalados buscando:

- Identificar riesgos potenciales y cuellos de botella
- Identificar eventos críticos tales como desconexiones, excesos de errores en los puertos, consumos de memoria, etc. Previamente habrá que determinar la relación de equipos que han de ser especialmente monitorizados.
- Realizar propuesta y ajustes de configuración oportunos.
- Generar alarmas definidas con el CABB, tales como cambios de configuraciones, acceso a un

dispositivo, etc.

- Generar informes detallados que permitan a los responsables del CABB conocer la situación y participar en las acciones de análisis o corrección necesarias.
- Actualizar esquemas de implementación.
- Actualizar el inventario de equipos.

El servicio incluye la monitorización continua remota de las alarmas de red en la herramienta del CABB, como Nagios o Intermapper, así como en las herramientas específicas adicionales que se designe desde la localización remota para la monitorización (Nagios o similar). La detección de un evento o alarma de red deberá derivar en la apertura proactiva de una incidencia y su gestión posterior de acuerdo con el procedimiento de actuación establecido.

Será responsabilidad de la empresa adjudicataria del contrato la realización de dicho procedimiento de actuación contando siempre con las necesidades y consideraciones propuestas por el CABB para su elaboración. También se deben realizar aquellas funciones básicas de operación que el CABB considere apropiadas.

Respecto a la propia a monitorización, además de todos los equipos del presente pliego, será necesario monitorizar cada pareja de routers ubicados en cada sede periférica y puede que algún otro conmutador industrial. Entre las variables a monitorizar deben de figurar como mínimo:

- Uso de memoria, CPU, disponibilidad por ICMP, estado de: fuentes, ventiladores y temperatura
- Estado de interfaces específicos: BW, interfaz caído o levantado, errores de interfaz
- Conexiones concurrentes, estado de HA y routing dinámico (sólo FWs)
- Estado de VRRP y routing dinámico (sólo routers)
- Monitorización estado correcto UPS
- Valores de temperatura de sensores

Gestión de la resolución de la incidencia. Para ello deberá ejecutar las instrucciones programadas a tal efecto en los procedimientos de resolución de incidencias existentes, asignando la incidencia a los resolutores adecuados, en coordinación con los técnicos del CABB, las subcontratas de mantenimiento de cada servicio, y las entidades colaboradoras y alianzas estratégicas de servicio del CABB.

Documentación e informes de progreso de las incidencias, en la aplicación de gestión de incidencias habilitada a tal efecto por el CABB. El servicio puede incluir opcionalmente la puesta a disposición del CABB de una nueva aplicación de gestión de incidencias, que será proporcionada por el adjudicatario al CABB.

Elaboración de informes con periodicidad trimestral y anual con estadísticas obtenidas de la herramienta de monitorización en el que se muestre una evolución a lo largo del tiempo del uso de los equipos en los que se debe incluir: memoria, CPU, BW de interfaces...

Elaboración de informes periódicos de estadísticas del servicio, tanto en lo referente a calidad en la recepción de incidencias como en su resolución.

Elaboración de informes de cumplimientos de SLAs con los clientes del CABB.

Colaboración en la generación y optimización de los procedimientos de resolución de incidencias.

La empresa adjudicataria deberá asegurar la continuidad del servicio. Para ello, deberá, en un plazo máximo de dos meses desde la firma del contrato, haber realizado la integración del servicio, incluyendo la atención y numeración telefónica, y la adaptación a la aplicación de gestión de incidencias. La adjudicataria se deberá encargar de la parametrización de esta aplicación, que deberá contener los campos, categorizaciones e informes que el CABB acuerde con el adjudicatario. Se describirá el detalle de la solución y aplicación propuestas. El coste de esta integración será por cuenta de la adjudicataria.

Se adoptarán los procedimientos actuales de recepción de llamadas, asignación de resolutores, clasificación, líneas de progreso, etc... Se prepararán los informes conforme a lo que se defina con el CABB.

A partir de este punto, e incluso previamente, la adjudicataria y el CABB podrán ir adaptando los procedimientos, actuaciones e informes a las indicaciones del CABB y los medios puestos a disposición por la adjudicataria. Se acordará entre ambas partes un modelo de relación, en el que se definen las funciones, roles, interlocutores y tareas a desarrollar, junto con los SLAs acordados y las penalizaciones correspondientes.

6.3.1 Gestión de incidencias

La siguiente actividad consiste en la gestión de las incidencias recibidas y su tratamiento. Las incidencias recibidas se deben atender, consultar con el personal técnico del CABB para su categorización, documentar y describir en toda su extensión rellenando los campos asociados en la aplicación de gestión de incidencias. Las incidencias pueden ser abiertas por personal del CABB, o contratas de mantenimiento o por proyectos de despliegue. Los cortes programados serán comunicados al CAU, y deben ser atendidos como incidencia, con una clasificación que los distinga. Asimismo, de manera proactiva se pueden generar incidencias de motu propio, tras la consulta con el técnico del CABB si así lo dicta el procedimiento. Uno o múltiples avisos o eventos de red detectados podrán generar una incidencia, que puede clasificarse en avería, preventivo, problema o consulta.

La persona operadora deberá asignar la resolución de la incidencia a la persona técnica del CABB, de guardia, o contrata de mantenimiento, notificándola y comunicándola con el nivel de detalle que se requiera, y realizar un posterior seguimiento de la evolución de la incidencia, anotando líneas de progreso y explicaciones sobre el detalle de la incidencia a medida que se van conociendo.

La explicación y líneas de progreso de la incidencia deberán ser técnicamente fundamentadas y reflejar fielmente lo indicado por el personal técnico del CABB y contratas de 1er nivel. Además, deberán estar correctamente redactadas, resultar de fácil comprensión y carecer de faltas de ortografía. Las siglas y elementos técnicos mencionados deben ser precisos y correctos.

Mantendrá durante la fase de vigencia de la incidencia y hasta su cierre una comunicación fluida con el personal técnico del CABB y las contratas de mantenimiento de 1er nivel, ejerciendo de coordinador de la resolución y persiguiendo siempre la actuación óptima de las intervinientes y la máxima eficiencia en las actuaciones. Atenderá en todo momento a las instrucciones técnicas del CABB, o del personal de guardia en horario no laboral, para asegurar que la evolución de la incidencia satisface sus indicaciones.

En el caso de incidencias críticas, la adjudicataria definirá, junto al CABB, un protocolo de notificación de incidencias críticas específico, en el que se debe comunicar de forma automática a responsables del CABB, determinadas incidencias con corte de servicio sobre un impacto importante que excedan de un determinado tiempo (60 minutos), así como hacer seguimiento y comunicar su resolución. La implantación de los mecanismos automáticos de este procedimiento, así como el seguimiento y su resolución, serán una de las funciones de la adjudicataria.

Una vez resuelta la incidencia, procederá a su cierre, cumplimentando la información adicional requerida, y confirmando dicho cierre con el personal técnico del CABB.

La adjudicataria empleará para la gestión de las incidencias la propia aplicación Service Manager del CABB. No obstante, podrá proponer la implantación de una nueva herramienta para este objeto, que deberá describir adecuadamente en su propuesta, en el apartado de medios materiales. Se deberá justificar adecuadamente las mejoras que esta nueva herramienta aportaría al servicio. Se deberá permitir el acceso a los responsables técnicos del CABB en los diferentes perfiles, de consulta o incluso generación y modificación

y cierre de incidencias, según el modelo de relación acordado con la adjudicataria. Esta aplicación de gestión de incidencias deberá alimentar los informes entregados al CABB. El responsable del CABB deberá tener completa accesibilidad a los datos internos contenidos en la aplicación. Las licencias asociadas a esta nueva aplicación deberán ser suministradas al CABB y deberán poder ser utilizadas por ésta en el futuro sin costes adicionales posteriores. En cualquier caso, el CABB se reserva la decisión de implantar la herramienta propuesta o continuar con la actual.

Se estima que, del personal interno del CABB que deba tener acceso a la aplicación, 2 de ellos deberán tener perfiles operativos/administrativos, y se requerirán 8 perfiles consultivos. La simultaneidad de accesos es baja. No obstante, se debe explicitar en la oferta las posibilidades de ampliación de personal con acceso a la herramienta y su coste económico, si lo tuviera.

La adjudicataria será responsable de la explotación de los datos de la aplicación de incidencias, preparará y entregará al CABB los informes que éste requiera. Estos informes tendrán una periodicidad trimestral y tendrán detalles de desglose de incidencias por día y mes, según tipos de incidencias, etc... También contendrán reportes de cumplimientos de los SLA del CABB, en función de los tiempos y nº de incidencias de cada servicio. La cantidad de informes, su contenido y presentación podrán variar durante la prestación del servicio según las instrucciones del CABB dentro de un proceso de mejora continua.

6.3.2 Monitorización de la red y los servicios

El adjudicatario deberá realizar la monitorización permanente 7x24x365 de la red atendiendo aquellos eventos de mayor criticidad. Ante la detección de nuevos eventos de este tipo, activará el procedimiento de actuación vigente y realizará la apertura de incidencia.

Aquellos eventos de red que sean detectados y conocidos, y no afecten a la operativa de la red, pero se mantengan como activos, deberán ser marcados como "reconocidos" por el adjudicatario para no distorsionar la visibilidad de los eventos que deben ser realmente tratados.

El adjudicatario colaborará también permanentemente con el CABB en el ajuste de la herramienta de monitorización, proponiendo modificaciones o ajustes en función de las experiencias acumuladas. Definirá las posibilidades de integración con sus herramientas propias de monitorización, y las ventajas que podría comportar.

Por todo lo descrito anteriormente, el perfil requerido de los operadores del servicio tiene también una componente técnica significativa.

6.3.3 Elaboración de informes

El adjudicatario elaborará los informes acordados en la definición inicial del modelo de servicio. Estos informes contendrán por lo menos la periodicidad y detalle que se presentan a continuación:

- Informe mensual de tickets pendientes y su distribución por subsistema/servicio.
- Informe trimestral de tickets, tickets con corte, plazo medio de recuperación, tiempos de desplazamiento; todos ellos por subsistema.
- Informes anuales de cumplimiento de SLA del servicio prestado.
- Informes trimestrales y anuales de cumplimiento de SLAs del servicio.

Adicionalmente se elaborarán los informes de SLA relativos al servicio prestado por la adjudicataria al CABB, según los compromisos del contrato.

6.4 *Integridad de la información*

Toda la información que se entregue al contratista es propiedad del CABB y totalmente confidencial.

7 Condiciones técnicas de la prestación del servicio de asistencia

La solicitud del servicio se llevará a cabo de la siguiente manera:

7.1 *Solicitud del servicio*

El Consorcio comunicará a la empresa contratista:

- Las nuevas necesidades
- Los cambios o modificaciones a realizar
- Los errores de las configuraciones

El personal responsable por parte del Consorcio planificará, de forma conjunta con el contratista, las fechas de inicio y fin y los recursos a aplicar a las tareas encomendadas.

7.2 *Aportaciones del Consorcio*

El Consorcio suministrará al adjudicatario toda la documentación de la que disponga para el desarrollo del trabajo.

En todos los casos, será el personal responsable del Consorcio el interlocutor con los usuarios.

7.3 *Aportaciones del contratista*

Deberá entregar a los responsables de la Subdirección de Informática del Consorcio lo siguiente:

- Documentación de los procedimientos a seguir para obtener nuevas prestaciones o corrección de anomalías.
- Un informe mensual con información detallada de los trabajos realizados diariamente cuando proceda.
- Un informe diario breve de los trabajos realizados durante la asistencia.
- Un informe trimestral de la situación de la red del CABB.
- Documentación generada de configurar los sistemas de monitorización del CABB a fin de integrar sus alarmas y objetos a monitorizar, entregando a su finalización de la integración la documentación correspondiente a las configuraciones y elementos utilizados para ello, Por ejemplo, MIBs, probes, parametrización, etc.
- Documentación de las modificaciones realizadas para la resolución de las incidencias y los cambios efectuados.

7.4 *Control y seguimiento del servicio*

El contratista comunicará por escrito la designación de una persona de su organización, encargada de ejercer las facultades de dirección, organización y disciplinarias en lo referente a las personas que prestan los servicios contratados.

Además, se creará un Comité de seguimiento del Servicio formado por una o dos personas del Consorcio,

pertenecientes a la Subdirección de Informática, y el responsable designado por el contratista.

Este Comité de seguimiento resolverá los conflictos que pudieran suscitarse y tendrán las reuniones necesarias para conseguir un servicio satisfactorio.

Para agilizar las labores de control y de seguimiento se confeccionarán unos informes, redactados con la periodicidad que se determine, que serán analizados y aprobados por el Comité de seguimiento. El documento deberá recoger también las incidencias y su resolución.

Las reuniones tendrán, al menos, carácter mensual y en ellas se tratarán los siguientes aspectos:

- Cumplimiento de objetivos e indicadores del nivel de calidad del servicio
- Incidencias del servicio
- Avance de las mejoras
- Planificación de los trabajos

Se realizará una reunión inicial al comienzo del proyecto con el fin de realizar un análisis de la situación actual. En esta reunión se aportará un enfoque para mejorar el diseño actual.

8 Condiciones para la facturación

La operatoria a lo largo de la ejecución del contrato será la siguiente:

La facturación de la asistencia se realizará mediante certificación mensual previa aprobación del informe a entregar por el contratista con las horas ejecutadas y trabajos realizados durante ese periodo.

A la finalización de cada período se computarán las horas de trabajo. Si hubiera desviaciones respecto a lo planificado, se determinará si la causa es imputable al CABB o al adjudicatario.

El adjudicatario deberá dar un servicio efectivo desde el primer día de inicio del contrato, de modo que, si por alguna razón hubiera necesidad de adquirir conocimientos para poder ejecutar el servicio con las garantías necesarias y de forma satisfactoria, deberá realizarlo en un período previo al inicio del contrato y sin ningún tipo de coste para el CABB.

9 Confidencialidad e integridad de la información

El contratista mantendrá la más absoluta confidencialidad sobre los datos y documentos utilizados en la prestación del servicio.

Toda la información que se entregue al contratista es propiedad del CABB y totalmente confidencial.

La propiedad de los productos obtenidos en la ejecución del presente proyecto será exclusiva y en su totalidad del CABB.

El contratista tendrá acceso a diferentes datos del CABB/BBUP con el objeto de prestar los servicios contratados, debiendo tratarlos conforma a las instrucciones del CABB/BBUP.

Asimismo, no podrá utilizar dichos datos con un fin distinto al del contrato, ni los comunicará a otras personas físicas o jurídicas, ni siquiera para su conservación, sin el consentimiento escrito del CABB/BBUP.

Durante la vigencia del contrato, e incluso una vez resuelto el mismo, el contratista se compromete a que ni él ni sus empleados o colaboradores divulguen a terceros, ni utilicen en su beneficio cualquier información confidencial obtenida como consecuencia de la prestación de los servicios objeto del presente contrato, con especial atención a la Ley Orgánica de Protección de datos vigente.

Toda la documentación e información derivada de la ejecución del contrato queda sujeta a normas estrictas de confidencialidad y seguridad debiendo comprometerse el adjudicatario a no utilizar dicha información fuera del ámbito de la ejecución del contrato.

Todo software desarrollado por el adjudicatario en la ejecución del proyecto, así como la totalidad de los datos, será propiedad del CABB/BBUP.

Una vez cumplida la relación contractual, los datos de carácter personal deberán ser devueltos al CABB/BBUP, al igual que cualquier soporte o documento en que conste algún dato de carácter personal sin que el contratista o sus empleados o colaboradores tengan derecho a retener copia alguna de la mencionada documentación.

10 Normativa

Se deberá cumplir con la normativa vigente aplicable a los suministros contemplados en el alcance del contrato.

En caso de discrepancia entre normas o entre éstas y el Pliego, se tomará como documento vigente las normas y reglamentos de obligado cumplimiento, el Pliego, y después la norma más conservadora.

Para todas las instalaciones el suministrador adoptará la última edición de la normativa.

En todo caso, la edición de las normas aplicables al contrato en caso de pedido será la vigente en la fecha de la firma del contrato.

Condiciones ambientales

Los equipos se montarán en las siguientes condiciones:

- Altitud: < 1000 m.s.n.m.
- Temperatura ambiente:
- Mínima: - 5 ºC
- Máxima: + 40 ºC
- Humedad relativa: ≤ 95 %
- Categoría Atmosférica de corrosión: ambiente exterior de zona industrial con elevada humedad y atmósfera agresiva, categoría de corrosión C5-1 muy elevada (industria) s/ UNE EN ISO 12.944:2.

11 Horas de servicio de asistencia y lugar de trabajo

El horario para las acciones que no suponen corte del servicio se realizarán en horas de oficina preferiblemente. Cualquier ampliación de este horario deberá ser acordada con la Dirección del Proyecto.

Los trabajos que supongan corte del servicio se realizarán preferentemente fuera del horario laboral. En ningún caso esto supondrá sobrecosto alguno para el CABB.

Los tiempos de respuesta y resolución solicitados en el presente "Pliego de Prescripciones Técnicas" para los elementos incluyen la realización de los trabajos durante las 24 horas de los 365 días del año.

Los recursos necesarios para prestar el servicio requerido se ubicarán habitualmente en las oficinas del CABB. Cuando la ocasión lo requiera el personal de la empresa contratada podrá realizar su trabajo en las oficinas del contratista.

Los tiempos de respuesta del servicio deberán ser inferiores o iguales 1 hora. El criterio de la gravedad lo determinará el responsable del contrato del CABB.

El tiempo de resolución de incidencias graves será de 4 horas como máximo.

Este servicio puede ser solicitado las 24 horas del día, 365 días del año con los tiempos de respuesta anteriormente indicados.

El horario de prestación del servicio de mantenimiento deberá ajustarse a las necesidades del CABB.

Se podrá dar el caso que por razones del servicio algunos trabajos sea necesario realizarlos fuera de las horas habituales de trabajo.

Se podrá dar el caso, por razones del servicio, que algunas de las jornadas se deban realizar en cualquiera de los centros del CABB o tener que realizar desplazamientos entre los mismos, sin sobrecosto alguno para el CABB.

11.1 Acuerdo de nivel de servicio (ANS/SLA)

Para la atención de las averías de los elementos a mantener:

La forma de actuación por parte de los técnicos del proyecto deberá ser on-site, es decir, todos los trabajos se realizarán in situ en cualquiera de los centros e instalaciones del CABB.

Los trabajos objeto del proyecto se han de realizar sin interferir con el trabajo normal de los usuarios, por lo tanto, todo trabajo que suponga un corte del servicio se deberá de realizar fuera de la jornada laboral.

- Tiempo de respuesta: Se establece en 1 hora.

Este tiempo será el comprendido entre la notificación emitida por Consorcio de Aguas hasta el inicio de la intervención por parte del técnico de mantenimiento.

- Tiempo de resolución: Se establece un tiempo máximo de resolución de 4 horas los 365 días del año.

El tiempo de resolución será el comprendido desde la notificación del aviso a la empresa adjudicataria hasta el momento de su resolución u operatividad del elemento averiado.

El nivel de cumplimiento global debe ser igual o superior al 85 % del volumen de incidencias comunicadas por Consorcio de Aguas y cerradas en el mes evaluado.

Con el fin de garantizar una respuesta y agilidad en el servicio a incluir, la empresa licitadora deberá de garantizar poder dar respuesta según el SLA acordado, esto es, 24x7x4 y el personal técnico adscrito a esta licitación deberá de estar asignado a dicho centro de trabajo.

11.2 Servicio de asistencia técnica planificada

Se requiere una bolsa de 50 horas/año a consumir durante la duración el contrato de asistencia técnica. Esta asistencia consistirá en una atención in situ de 24x7x4 a solicitud del CABB bien por avería o por necesidades del servicio. Además, se utilizarán para mejoras de las prestaciones de las políticas, generación de informes, etc.

Con carácter general diremos que los trabajos de la asistencia técnica serán fruto de las necesidades originadas en el día a día: resolución de incidencias, implantación de nuevas funcionalidades, generación de informes, etc. Estos trabajos podrán tener que ser llevados a cabo en cualquier instalación del CABB.

Durante este tiempo, los equipos se mantendrán actualizados a la última versión tanto del sistema operativo como de parches, librerías, etc.

Este servicio tendrá lugar principalmente en las oficinas de Albia del CABB, aunque podrá ser necesario desplazarse a cualquiera de las instalaciones del CABB donde estén instalados los equipos en función de las necesidades. La función principal será realizar los trabajos cotidianos de mantenimiento, reparación, configuración, modificación y asistencia relacionadas con los trabajos anteriormente descritos.

Este servicio se planificará con el adjudicatario con un día de antelación.

Documentación a entregar durante la ejecución

Una vez finalizada la fase de montaje y configuración de la red el contratista deberá entregar:

- Recomendaciones de mantenimiento, versiones del software instalado en los equipos, etc.
- Documento con la descripción de la red, configuraciones, usuarios y claves.
- Ficheros de configuración de todos los equipos.
- Manuales de todos los equipos instalados.
- Manuales de administración, de guías de usuario, generación de informes, troubleshooting, ingeniería forense, etc. de todos los equipos instalados.

Y toda la documentación complementaria que el contratista considere necesaria para la administración y mantenimiento.

11.3 Servicio de retén

En este apartado se engloban aquellos trabajos urgentes no planificados. Los avisos se podrán dar tanto dentro como fuera del horario laboral, así como en sábados y festivos, para lo cual el contratista deberá facilitar un número de teléfono al que llamar en estos casos.

Se ha considerado tres tipos de servicio: aquellos que se realizan en el horario laboral (8:00-18:00h) y horario extendido (el resto). Dentro de estos últimos se han considerado los urgentes cuyo tiempo de respuesta debe ser no superior a 1 hora.

La facturación de las incidencias se realizará en base al cuadro de precios del pliego de cláusulas administrativas. Las consultas o incidencias que se notifiquen en horario laboral se abonarán al mismo precio que el servicio de asistencia técnica descrito en el punto 1.3 de este pliego y aquellas que se realicen fuera del horario laboral el doble del importe en horario laboral.

La categorización de la urgencia de los avisos será a criterio del responsable del contrato del CABB.

12 Pruebas de rendimiento

El CABB se reserva el derecho a pedir a la empresa que haya presentado la oferta económica más ventajosa, la verificación del correcto funcionamiento de la solución propuesta mediante una prueba de concepto, en el plazo a decidir, sin coste adicional.

La prueba de concepto consistirá en la instalación en una de las instalaciones objeto del presente proyecto, de uno de los cortafuegos propuestos. El equipo se configurará mediante port-mirroring para recibir y filtrar el tráfico real, 1 interface interna y 1 interface de salida a la MPLS.

El equipo en cuestión tendrá que tener todas las suscripciones activadas y con todos los filtros, incluyendo todas las firmas disponibles.

Los filtros deberán registrar todo el tráfico de logs, confirmando su eficacia.

Se monitorizará el uso de todos los procesadores destinados a analizar y gestionar el tráfico, durante el tiempo que dure la prueba.

Se identificarán dos aplicaciones internas corporativas para ser tratadas de manera individual aplicando diferentes filtros a cada una de ellas.

Sobre una de las aplicaciones se aplicará un filtro de bloqueo de archivo que impida la subida de un archivo .pdf a la aplicación pero que permita la subida del resto de tipos de archivo.

La prueba de concepto se considerará superada si se cumplen las dos condiciones siguientes:

- Rendimiento: la empresa deberá entregar un documento con la relación de procesadores del cortafuegos y su descripción. La media de los procesadores destinados a analizar y gestiona tráfico NO supera el 30% que garantiza el rendimiento de los equipos durante todo el período de servicio.

Seguridad Aplicaciones web corporativa: el log tendrá que mostrar el tratamiento de filtros diferenciado para las dos aplicaciones de un servidor a definir y su eficacia impidiendo la subida de archivos .pdf.

Se realizarán pruebas de rendimiento una vez instalados los equipos con todos los servicios activados (firewall, IPS, URL filter, antivirus, traffic shapping, control de DLP, control de aplicaciones, etc.) debiendo mantenerse las prestaciones especificadas.

13 Recepción y seguimiento de las incidencias

El adjudicatario pondrá a disposición de los usuarios un teléfono único para toda la gestión de todas las Incidencias reportadas, así como una cuenta de correo mediante los cuales poder abrir y realizar el seguimiento de las incidencias.

Indicará en la oferta la disponibilidad de realización y seguimiento de las incidencias mediante el acceso a la aplicación WEB de gestión de incidencias del licitante.

Aunque actualmente no esté disponible, se podrá exigir en el futuro al adjudicatario el uso de la aplicación de incidencias del Consorcio para la gestión y documentación de aquellas incidencias que estén relacionadas con el contrato.

14 Visita a las instalaciones.

Durante la fase de concurso las empresas interesadas en presentar oferta podrán visitar las instalaciones para la recolección de los datos que consideren necesarios, previa concertación con la persona que el CABB designe para tal fin.

Si las consultas o dudas son muchas el CABB se reserva la posibilidad de convocar a una reunión a todas las empresas que hayan mostrado interés en el proyecto retirando los Pliegos con la finalidad de aclarar las posibles dudas del Pliego.

15 Formación

Se ofertará la formación del personal del CABB sobre la red instalada, su mantenimiento y su administración.

Se ofertará la formación del personal del CABB sobre la red instalada, su mantenimiento y su administración. Se ha considerar como mínimo una formación de 10 jornadas de 5 horas mínimo cada sesión. Una primera formación a la finalización de la puesta en marcha de duración mínima de 5 jornadas, y una segunda formación a determinar con el personal responsable del CABB la fecha, pero con duración de otras 5 jornadas.

16 Equipo de trabajo

El equipo de trabajo propuesto no podrá ser cambiado en el transcurso del contrato sin previa notificación y conformidad del CABB.

El CABB se reservará el derecho a exigir al adjudicatario la sustitución del personal que no observe un normal rendimiento o mostrase una conducta irregular.

17 Control de calidad, inspecciones y puesta en marcha

El suministrador, al comienzo de la obra, deberá realizar un Programa Detallado de Calidad para su aprobación por el CONSORCIO DE AGUAS que deberá incluir los protocolos de pruebas y programas de puntos de inspección (PPIs) a realizar durante el transcurso de la obra.

17.1 Inspecciones de acopio y fabricación

El Suministrador obtendrá de su proveedor certificados de las características eléctricas y mecánicas de los aparatos y de los resultados de todos los demás ensayos requeridos por las especificaciones aplicables. Estos certificados estarán a disposición de CONSORCIO DE AGUAS.

Todos los aparatos se comprobarán antes de su montaje según la norma correspondiente.

Durante el proceso de fabricación, montaje y cableado de los equipos, éstos serán sometidos a los controles indicados en el Programa Detallado de Calidad.

17.2 Verificaciones

Las verificaciones individuales que se deberán incluir en conformidad con la normativa aplicable son:

- Comprobación visual del grado de protección
- Comprobación visual de las distancias de aislamiento
- Comprobación visual de los componentes integrados (11.5)
- Los equipos coincidirán con lo expresado en la documentación, y el material utilizado con el especificado
    - Verificación de la correcta instalación
    - Distribución de columnas y compartimentos.
    - Disposición del aparellaje.
    - Identificación Referencias de aparatos.
    - Marcado de fases alimentación
    - Marcado de fases salidas
    - Conductores y colores utilizados
- Verificación por muestreo de las conexiones eléctricas
- Comprobación visual de los bornes para los conductores externos
- Comprobación del cableado, comportamiento de empleo y funcional
    - Verificación del marcado, etiquetas colocadas
    - Verificación de la Información relativa al conjunto
    - Control de tensión y secuencia de fases
    - Funcionamiento de los órganos de mando
    - Desconexión de los dispositivos diferenciales por medio del botón de test
    - Pruebas de funcionamiento -Se simularán en la medida de lo posible las condiciones reales de funcionamiento y las eventualidades que pudieran presentarse durante su explotación.

17.3 Documentación final de calidad

Antes de la expedición del equipo, el Suministrador pondrá a disposición del CONSORCIO DE AGUAS para comentarios o aprobación, un "dossier" de calidad que deberá incluir lo siguiente:

- Pedido de CONSORCIO DE AGUAS.
- Programa de Puntos de Inspección cumplimentado.
- Carta de cumplimiento del Suministrador con el Pliego y otros documentos contractuales.
- Certificados de Calidad cuando sean requeridos.
- Protocolos de ensayos en fábrica.

17.4 Comprobación a la salida de fábrica

- Revisión del Dossier de calidad.
- Las partes sueltas estarán bien empaquetadas y protegidas contra la herrumbre y rotura, identificadas y sujetas de forma segura.
- Revisión de embalajes, listas de envío y contenido de bultos.
- Comprobación del cumplimiento de las instrucciones de transporte.

17.5 Comprobación a la recepción en almacén de obra

El Suministrador deberá indicar en las Instrucciones de Transporte las comprobaciones que haya que realizar a la recepción de los equipos en el almacén de obra para asegurar que los equipos y sus componentes no han sufrido daños durante el transporte.

17.6 Pruebas, puesta en marcha, recepción provisional y definitiva

El fabricante de cada equipo suministrador proporcionará una relación de las pruebas que considere necesario realizar después de la instalación de los equipos y antes de su puesta en servicio, para comprobar que no han sufrido daños durante su manipulación, almacenamiento y su instalación.

Terminados los montajes mecánicos, eléctrico, electrónico e introducidos los programas de software en todos los sistemas, incluido redes de comunicación, se procederá a efectuar las pruebas y regulaciones de todas las unidades que componen la instalación, para comprobar en vacío si el montaje ha sido adecuado y si se cumplen los cometidos de funcionamiento y operatividad diseñados. A continuación, se realizarán todas las pruebas necesarias para verificar el correcto funcionamiento de la instalación en carga en local.

En todas las fases de las pruebas deberá asistir personal representante de la empresa adjudicataria de las obras en las instalaciones afectadas por las pruebas.

Si por cualquier causa imputable al contratista no procediese realizar la recepción, se suspenderá esta y se señalará un plazo prudencial para subsanar y corregir los defectos o fallos en el caso de que fueran fácilmente corregibles. Si los defectos o fallos fueran graves y de trascendencia, se elaborará el informe preceptivo correspondiente que se comunicará al contratista para su cumplimiento obligatorio, o en su caso, para la rescisión del contrato.

El final del periodo de puesta en marcha, tras recibir toda la documentación solicitada, será otorgado por la Dirección de Obra por medio del Acta de Recepción. Durante dicho periodo la Dirección de Obra del Consorcio de Aguas solicitará las exigencias de pruebas necesarias y personal de explotación apoyará la vigilancia de maniobras y verificaciones, sin ninguna responsabilidad y siempre bajo la tutela del Adjudicatario, quien estará obligado a enseñar a utilizar directa o indirectamente el modo de explotación de la instalación al personal del Consorcio, que posteriormente de la Recepción se encargará de la explotación.

Para otorgar la Recepción será condición indispensable la entrega de toda la documentación indicada, cuyo contenido deberá ser aprobado por la Dirección de Obra.

18 Documentación

Toda esta documentación se deberá elaborar siguiendo las especificaciones y los estándares entregados en las diferentes fases de la obra.

En general la documentación cumplirá con lo siguiente:

18.1 Esquemas eléctricos. Criterios de representación y elaboración

Normativa

La normativa a aplicar será la siguiente:

- UNE-EN 61.082-1 Preparación de documentos utilizados en electrotecnia.
- UNE-EN 81.346 Sistemas industriales, instalaciones y equipos y productos industriales. Principios de estructuración y designación de referencias
- UNE-EN 60.617 Símbolos gráficos para esquemas

Criterios particulares de representación

Además de lo indicado en la normativa del apartado anterior, los criterios particulares de representación de los esquemas eléctricos serán los siguientes:

- Todos los circuitos sin tensión de alimentación.
- Todos los equipos sin alimentación y sobre "balda"
- Todos los accionamientos en posición intermedia
- Pulsadores de mando sin actuar
- Interruptores abiertos
- Relés diferenciales rearmados

Se deben representar todos los contactos de los aparatos o relés, aunque no se utilicen.

Cada aparato o relé solamente puede figurar en una hoja, las representaciones en las diferentes hojas se harán con referencias cruzadas que indicarán el nº de hoja y columna.

Criterios particulares de representación

La documentación eléctrica a generar y entregar contendrá los siguientes planos:

- Portada
- Índice de planos, indicando revisión, fecha y modificación
- Condiciones de representación
- Simbología
- Condiciones de denominación e identificación
- Hoja de características del armario.
- Planos a escala del frente de los cuadros eléctricos y de control. Disposición equipos
- Planos unifilares
- Planos de distribución de tensiones
- Planos de arquitectura de comunicaciones
- Planos de interconexión interna y externa.
- Listado de mangueras de cables, indicando tipo cables, sección y longitudes.
- Listado de materiales.

18.2 Documentación a entregar

Toda la documentación entregada se deberá entregar en formato original de diseño y en formato PDF, de tal manera que esta siempre pueda ser editada y/o modificada utilizando los correspondientes programas de edición.

Se deberá incluir en el proyecto constructivo definitivo todos los esquemas correspondientes a las instalaciones eléctricas y de control, en esquemas desarrollados y multifilares generados, según la normativa UNE-EN 81.346.

Los documentos, tablas, cálculos, etc, se realizarán preferiblemente en formato DIN-A4. Se utilizará Microsoft Office como soporte informático.

Los catálogos, certificados de ensayos de rutina, documentos informativos, etc., se presentarán en formato original.

Los certificados tipo, si los hubiere, se presentará copia del original.

Toda la documentación se presentará en castellano. Para los catálogos se admitirá el inglés.

La documentación generada se entregará tanto en papel como en soporte informático (1 copia en papel y otra en soporte informático).

Todas los programas y copias de seguridad a todos los efectos serán propiedad del CONSORCIO DE AGUAS. Así mismo se entregarán y serán propiedad del Consorcio todos los módulos software que sean necesarios para la programación de los autómatas (módulos de comunicaciones, funciones de regulación, etc. etc.).

Toda la documentación se deberá entregar actualizada, acorde a como haya quedado tras la puesta en marcha ("As built").

Se entregarán, al menos, los siguientes documentos:

Cuadros

- Esquemas eléctricos desarrollados siguiendo los criterios indicados.
- El desarrollo de los esquemas eléctricos se realizará en Eplan P8 en instalaciones nuevas, en Autocad V.14 (o posterior) o Eplan P8 en instalaciones a remodelar (en función del formato de la documentación existente). En Eplan P8 se deberá entregar una copia de la colección de planos en soporte digital (formato "zw1") y en Autocad una copia de todos los planos en DWG, y en ambos casos una copia en único documento en pdf.
- Certificados de cuadros y componentes principales
- Cálculos (de cables, conducciones, etc....)
- Planos de bancada. Detalle de anclajes
- Libros de instrucciones y mantenimiento de equipos
- Catálogos de componentes
- Esquemas de componentes

Cables y bandejas

- Planos de recorrido de bandejas
- Planos de recorrido de cables
- Listado de cables, indicando: composición, origen, destino, recorrido, longitud, tipo, etc.
- Certificado de cables
- Certificado de materiales

Red de tierras

- Planos de detalle de uniones
- Mediciones de residencia de p.a.t
- Mediciones de tensiones de paso y contacto

Equipos

- Lista de equipos.
- Planos de implantación de equipos en campo.
- Planos de detalle
- Manuales técnicos de los equipos.
- De todos los elementos se deberá entregar un manual de programación de los mismos, programas de programación y parametrización necesarios, un listado de aquellos valores que se han modificado respecto del valor de fábrica y si el dispositivo lo permite, una copia de seguridad en soporte informático.
- En caso de existir equipos que intercambien datos con otros mediante comunicación, se entregará información acerca del protocolo utilizado, mapeado de información, estructura de tramas intercambiadas, ...
- Documentación original de todas las licencias suministradas, justificante de abono y un manual de instalación de las mismas.

Comunicaciones

Se deberá entregar un plano de comunicaciones completo de la instalación, que incluya todos los equipos (estén dentro del alcance del suministro de esta obra o no) de la instalación que dispongan de algún medio de comunicación, incluyendo su direccionamiento IP/Máscara Subred/Puerta de enlace, puertos de conexión, flujos de datos, etiquetado de cada cable, etc. y toda la información relevante que facilite la comprensión de la red de comunicaciones de cada instalación.

Fotos finales

La documentación final será acompañada con las siguientes fotos:

- Alrededores del emplazamiento de los cuadros.
- Interior y exterior de los cuadros suministrados.
- Instalaciones realizadas en cuadros ajenos a los suministrados.
- Resto de equipos suministrados en la obra.

Procedimientos de mantenimiento

El contratista deberá realizar procedimientos para la identificación básica de averías y sustitución de equipos. El primer nivel de mantenimiento lo realizará la empresa contratista de mantenimiento de la red de abastecimiento, y los procedimientos deberán ser suficientes para que los mantenedores sean capaces de identificar la fuente del problema con procedimientos sencillos (identificación de LEDs, pruebas básicas de conectividad, etc). En el caso de que el problema sea de hardware de firewall, los mantenedores deberán ser capaces de sustituirlo con el stock local del CABB. La configuración que se haga de los equipos debe permitir que se realicen estos cambios por personal no especializado. Los procedimientos deberán incluir claramente: cómo identificar el problema, cómo realizar el cambio hardware, comprobaciones de la reposición del servicio y bajo qué circunstancias es necesario activar el servicio de retén del contratista y cómo se debe realizar.

NOTA: Toda la documentación realizada y aprobada en fase de ingeniería deberá ser actualizada con las modificaciones surgidas en puesta en marcha para la elaboración de la documentación "As built" a entregar.

debe estar incluido dentro del alcance de documentación de la obra.

19 Coordinación

Toda la documentación que se describe a continuación se deberá elaborar siguiendo las especificaciones y los estándares entregados en las diferentes fases de la obra.

Aunque en la ejecución de la obra se debe mantener inalterable el orden de ejecución de las fases indicadas, dentro de cada una de ellas la mayoría de las tareas se podrán ejecutar en paralelo minimizando así los tiempos de cada una de las fases.

19.1 Fases de la Obra

Reunión de lanzamiento

En esta fase se definen los datos de partida. Se realizará una reunión inicial en la que se definirán y concretarán los detalles de la obra entre todos los participantes:

- Solicitud/Nombramiento de interlocutores de la obra. (Incluido el interlocutor para coordinación de las labores eléctricas y de control)
- Labores a realizar en la obra.
- Entrega de condiciones complementarias.
- Presentación y validación (certificados y conocimientos requeridos por el CABB/BBUP) de las subcontratas participantes en la obra.

Replanteo y planificación

Con la información del proyecto y la información recogida en la reunión de lanzamiento, el contratista deberá realizar el replanteo de los trabajos de la obra y elaborar un informe con las conclusiones del mismo.

Una vez realizado el replanteo y validado el alcance, será responsabilidad del contratista asumir las diferencias que puedan surgir entre la realidad y la ingeniería obtenida del replanteo.

Una vez aclarado y comprobado el alcance de los trabajos a realizar, el contratista realizará una planificación detallada de todos los trabajos a realizar en la obra, atendiendo a los tiempos de ejecución indicados en su oferta.

La planificación deberá ser validada por el CABB al comienzo de la obra.

IMPORTANTE: Esta planificación deberá ir siendo actualizada y entregada al CABB/BBUP durante todo el transcurso de la obra, siempre que se produzca un desvío sobre la planificación inicial. Cuando las desviaciones afecten a la fecha final de entrega de la obra, según sean detectadas, además de actualizar la planificación, el contratista deberá comunicar obligatoriamente al CABB las causas y el tiempo estimado de desviación.

Documentación de seguridad, medioambiente y calidad

Una de las primeras tareas a realizar por el contratista será la de ir preparando la documentación de seguridad, medioambiente y calidad, ya que será necesaria para el acceso a trabajar en las instalaciones. Este, deberá tener en cuenta todos los participantes de la obra a la hora de elaborar esta documentación (subcontratas...).

El tipo de documentación a generar en esta fase dependerá del tipo y volumen de trabajo a realizar en la obra.

Todo lo relativo a la prevención de riesgos laborales se realizará de acuerdo al procedimiento de actividades empresariales.

Ingeniería básica

Tras el replanteo de la obra, el contratista comenzará con la elaboración de la ingeniería básica. Esta ingeniería básica se elaborará partir de la información recibida en la fase de "Reunión de lanzamiento", "Replanteo y planificación". Generalmente consta de los siguientes documentos:

- Lista de equipos.
- Arquitectura de comunicaciones. Tras su validación el contratista deberá realizar las solicitudes de alta necesarias al CABB para la conexión de las instalaciones a sus redes de comunicaciones.
- Distribución de los cuadros (frentes), esquemas unifilares, planos de implantación, listado de marca y modelo de los principales materiales y cálculos eléctricos.

Toda esta documentación debe ser enviada según se vaya disponiendo de ella al CABB para su revisión ya que será la base para la elaboración de la ingeniería de detalle.

Esta ingeniería deberá ser revisada tantas veces como sea necesario hasta lograr una calidad mínima para avanzar en las siguientes fases.

Ingeniería de detalle

Tras la elaboración y revisión de la ingeniería básica, el contratista comenzará con la elaboración de la ingeniería de detalle.

La ingeniería de detalle se elaborará partir de la ingeniería básica. Generalmente consta de los siguientes documentos:

- Ingeniería de detalle necesaria para construcción de cuadros:
  - Esquemas Eléctricos.
  - Lista de materiales.
- Ingeniería de detalle necesaria para la parametrización:
  - Necesidades de tráfico de comunicaciones.
- Ingeniería de detalle necesaria para el montaje en campo:
  - Red de tierras.
  - Implantación de equipos.
  - Planos de canalizaciones.

Toda esta documentación se deberá elaborar siguiendo las especificaciones indicadas en el apartado "Documentación" y debe ser enviada según se vaya disponiendo de ella al para su revisión ya que será la base para la compra de materiales, fabricación de los cuadros, parametrización de equipos...

Se podrán realizar aprobaciones parciales de la documentación, con el fin de poder ir avanzando con las siguientes tareas a realizar.

Fabricación

Tras la elaboración y revisión de la ingeniería de detalle, el contratista comenzará con la ejecución de las

trabajos en taller/oficina, que generalmente se trata de los siguientes:

- Compra de materiales: Se procederá a la compra de los materiales aprobados en la "Lista de materiales" y "esquemas eléctricos desarrollados" de la fase de "Ingeniería de detalle".
- Construcción de cuadros: A partir de los "Esquemas eléctricos" y de la "Lista de materiales" aprobados en la "Ingeniería de detalle" el contratista construye los cuadros en el taller. Una vez construidos, el CABB (si se considera necesario, o en función de los PPIs definidos) realizarán una inspección visual del mismo, atendiendo (a grandes rasgos) a los siguientes conceptos:
  - Disposición de los elementos: correspondencia con la ingeniería eléctrica
  - Identificación de los elementos
  - Normativa aplicable: constructiva, de seguridad, etc...
  - Reservas, tanto de espacio como de equipamientos.
  - ...
- Parametrización de equipos: A partir de las especificaciones del CABB sobre las necesidades de tráfico de comunicaciones, el contratista realizará la parametrización de equipos en sus oficinas.

Puesta en marcha en taller

Una vez finalizados los trabajos de construcción y parametrización en el taller, el contratista realizara en el taller las verificaciones eléctricas (según normativa) y comprobaciones que considere necesarias para garantizar que la construcción y funcionamiento del suministro eléctrico y de control (programación/parametrización) funciona acorde a lo definido en la ingeniería de detalle.

Montaje en Campo

Una vez finalizada la puesta en marcha en el taller, validados los PPIs (Programa de puntos de inspección) estipulados en el procedimiento de calidad, y tras recibir un consentimiento expreso por parte del CABB para abordar esta fase, el contratista comenzará con los trabajos de montaje en campo, que generalmente se tratan de:

- Traslado y montaje de cuadros en obra
- Montaje de equipos.
- Tendido de bandejas, tubos y cables.
- Conexionado de los cables de fuerza y control.
- Etc...

IMPORTANTE: Todos los trabajos serán realizados de acuerdo a lo indicado en el plan de seguridad.

Puesta en marcha (en la instalación)

Tras la realización del montaje en campo, se procederá a la puesta en marcha final de la instalación, que consta de tres fases:

- Comprobación de instalación de campo: El contratista realizara las verificaciones y comprobaciones que considere necesarias para garantizar que la instalación funciona y se ha realizado acorde a lo especificado en la ingeniería de detalle. Generalmente se trata de:
  - Tendido y conexión de mangueras.
  - Tierras.
  - Conexiones en los equipos externos a los cuadros.

- Comunicaciones con otros equipos de campo y con la red de comunicaciones del CABB.
- ...

El CABB (si se considera necesario y en función de los PPIs definidos) revisará la instalación realizada.

- Puesta en marcha de la instalación: Una vez realizado este primer control por parte del contratista, el contratista procederá a realizar la puesta en marcha completa en conjunto con el CABB. El objetivo de esta fase de proyecto es verificar la operatividad completa (probando todas las posibles situaciones de funcionamiento ideal o anomalías que se puedan dar) de la instalación.

Documentación As-Built

Finalmente, una vez realizada la puesta en marcha en campo y realizados los correspondientes ajustes finales de funcionamiento, el contratista modificará los documentos de proyecto necesarios y preparará la documentación final ("As built") según se describe en el apartado "Documentación".

Seguimiento de los trabajos

Para evitar desviaciones en el planning, se realizarán reuniones y/o se redactarán informes (Semanal-Mensual - frecuencia a acordar en las fases de la obra) con los trabajos realizados y los previstos, así como las incidencias y consultas necesarias a la propiedad.

20 Gestión de residuos

Formará parte de los trabajos a realizar la gestión de todos los residuos generados durante la ejecución de la obra.

La gestión de los residuos se realizará de acuerdo a la legislación vigente, cumpliendo como mínimo las siguientes obligaciones:

- Separación en origen de los residuos generados, según normativa
- Se deberá transportar y depositar en el centro autorizado (punto limpio)
- Se deberá presentar la documentación acreditativa de la correcta gestión de los residuos.

Durante la ejecución de la obra se tomarán las medidas necesarias para conseguir una gestión eficiente de los residuos originados

El contratista será el responsable de redactar un Plan de Gestión de Residuos (PGR) que deberá ser aprobado por la dirección de obra y aceptado por la propiedad.

El material desmontado de las instalaciones existentes, que pueda estar en buenas condiciones (según las indicaciones del CABB/BBUP), será entregado al almacén que sea indicado. Se presentará junto con la documentación final un resguardo del aparellaje en cuestión.

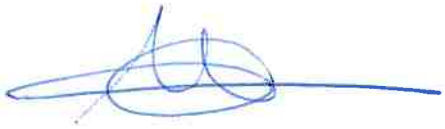
21 Otras tareas

Además de los suministros descritos, se deberán de tener en cuenta el resto de pequeños suministros contemplados en el presupuesto (desmontajes, limpieza de locales, etc.)

Bilbao, 3 de julio de 2019

El Gestor del Contrato

Marian Mena



Subdirector de Informática

Jose Luis Unzueta