



29-07-2019

ENTRADA

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES  
PARA LA CONTRATACIÓN DEL MANTENIMIENTO Y EVOLUCIÓN DEL  
SISTEMA DE SUPERVISIÓN ZENOSS DE LA RED DE  
TELECOMUNICACIONES DEL CANAL DE ISABEL II, S.A.**

**Nº 152/2019**

25 de JULIO de 2019

## ÍNDICE

|        |   |    |
|--------|---|----|
| 1.     | OBJETO DEL CONCURSO .....   | 3  |
| 2.     | SITUACIÓN ACTUAL.....   | 4  |
| 2.1    | Entorno tecnológico actual .....  | 4  |
| 2.2    | Sistemas de gestión integrados .....  | 5  |
| 2.3    | Equipos gestionados .....   | 6  |
| 2.4    | Configuración de la situación actual .....  | 6  |
| 2.4.1  | Arquitectura actual .....   | 6  |
|        | Se describe con más detalle cada una de las arquitecturas según la capa lógica..... | 7  |
| 2.4.2  | Arquitectura ZenOSS.....  | 7  |
| 2.4.3  | Arquitectura lógica Docker.....   | 9  |
| 2.4.4  | Arquitectura Control Center .....   | 9  |
| 2.4.5  | Funcionalidades de ZenOSS .....   | 10 |
| 2.4.6  | Configuración de eventos .....  | 12 |
| 2.4.7  | Correlaciones .....   | 14 |
| 2.4.8  | Tools (scripts) .....   | 14 |
| 2.4.9  | Tratamiento de eventos.....   | 15 |
| 2.4.10 | Inventario detallado .....  | 16 |
| 2.4.11 | Gráficas .....  | 16 |
| 3.     | ALCANCE .....   | 17 |
| 3.1    | Mantenimiento preventivo y correctivo.....  | 17 |
| 3.1.1  | Regímenes de servicio.....  | 18 |
| 3.1.2  | Generación de informes semanales y mensuales .....                                  | 20 |
| 3.1.3  | Gestión del servicio .....  | 20 |
| 3.2    | Actualizaciones de software .....   | 20 |
| 3.2.1  | Acceso a correcciones de software .....   | 20 |
| 3.2.2  | Acceso a nuevas versiones de software .....   | 21 |
| 3.2.3  | Realización de pruebas .....  | 21 |
| 3.3    | Bolsa de horas.....   | 21 |
| 3.4    | Formación .....   | 22 |
| 4.     | ACCESO REMOTO.....  | 24 |
| 5.     | FORMATO DE LAS OFERTAS .....  | 25 |



## 1. OBJETO DEL CONCURSO

El objeto del presente concurso es la mantenimiento y evolución del actual sistema de supervisión de la red de telecomunicaciones de Canal de Isabel II, basada en el programa opensource Zenoss.

## 2. SITUACIÓN ACTUAL

Canal de Isabel II cuenta, actualmente con una solución de supervisión y consola única de eventos basada en la solución Open Source Zenoss Core r5.3.0.

### 2.1 Entorno tecnológico actual

La solución actual consta de dos servidores virtuales idénticos en los que se ha instalado la solución de monitorización de red y consola de eventos: Zenoss Core r5.3.0, que monitorizan la red de manera independiente, además de un servidor de desarrollo (o maqueta) para la definición de nuevas integraciones, pruebas de nuevas versiones, actualizaciones, parches, homologación de equipos y nuevas tecnológicas de red... todos están instalados en el entorno de virtualización de Canal de Isabel II (VMWARE en Vsphere 5.5 versión Enterprise Plus.),

Las funciones del sistema de supervisión incluyen:

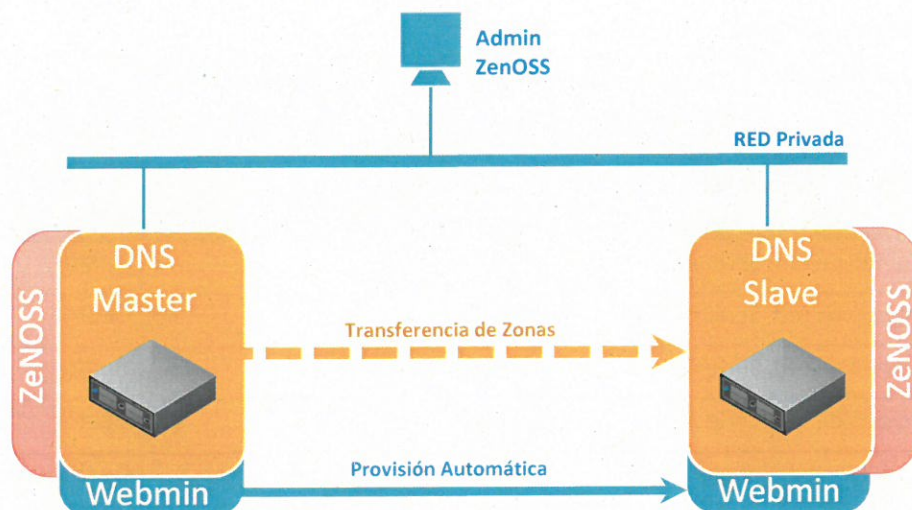
- Recepción de traps / syslog de todos los sistemas de gestión y equipos de la red de telecomunicaciones.
- Consola única de eventos para el entorno de la red de transmisión.
- Monitorización de estado e interfaces de los equipos de la red de telecomunicaciones con direccionamiento IP de gestión.
- Modelado de equipos.
- Gestión de infraestructura.
- Acciones adicionales de consulta sobre equipos y bases de datos de inventarios basadas en scripting y consultas snmp, para enriquecimiento de la información.
- Acciones adicionales de ejecución de comandos sobre equipos basadas en scripting y comandos snmp.

Adicionalmente, los servidores virtuales de Zenoss asumen las funciones de:

- Servidor DNS para la resolución directa e inversa de las direcciones de gestión de los equipos del entorno gestionado. Servicio DNS basado en una implementación de Bind. la aplicación BIND DNS está instalada en ambos servidores en modo Master/Slave. El servidor proclamado como principal, se comporta como Master de las zonas DNS y el secundario como DNS Slave de todas las zonas, el servidor DNS Slave tendrá copia de todas las zonas en caso de fallo del Master.

Diagrama lógico de la solución DNS:





- Servidor NTP para los equipos de la red de Telecomunicaciones.

Herramienta opensource Subversion para el control de versiones.

## 2.2 Sistemas de gestión integrados

En el sistema cuenta con gestores adicionales, ya integrados en el sistema de monitorización:

- PolyView (con 2 servidores virtualizados sobre windows): Gestor de la red radio Ceragon. Asumen las funciones propias del gestor (inventario, monitorización de estado y monitorización de rendimiento) con capacidad para generar eventos propios.

Su función principal desde el punto de vista de la consola única de eventos son:

- Envío – vía SNMP Trap – de los eventos generados como consecuencia de la monitorización.
- Reenvío de traps de los equipos que gestiona.
- ASPEN (con 2 servidores sobre SOLARIS 10): Gestor de la red MPLS de NSN. Asumen las funciones propias del gestor (inventario, monitorización de estado y monitorización de rendimiento) con capacidad para generar eventos propios.

Sus funciones principales, desde el punto de vista de la consola única de eventos son:

- Reenvío – vía syslog- de las notificaciones enviadas por los propios equipos.
- Envío – vía syslog- de los eventos generados como consecuencia de la monitorización realizada.
- CACTI: Monitorización y generación de informes históricos de rendimiento de la infraestructura gestionada.

Actualmente se encuentra parcialmente integrado en la consola única de eventos:

- Envío traps ante superación de umbrales predefinidos.

Consulta de gráficas desde el sistema de supervisión.



## 2.3 Equipos gestionados

A continuación, se describen los equipos gestionados actualmente en ZENOSS.

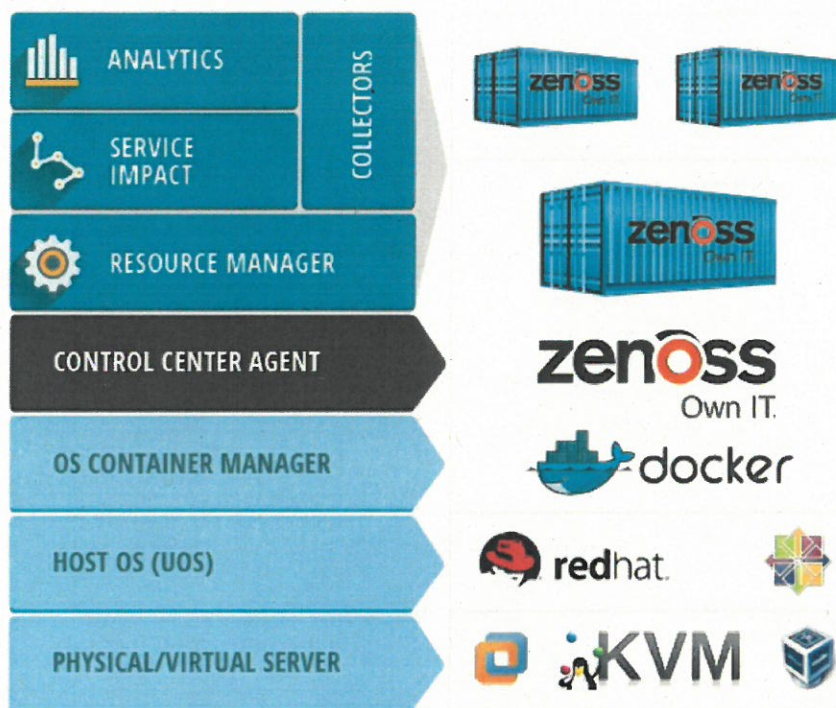
| Gestor  | Tipo Equipo                   | Modelos   | Nº  | Tratamiento eventos enviados por: | Tipo Envío    |
|---------|-------------------------------|---|-----|-----------------------------------|---------------|
| ASPEN   | Equipo de red. Serie A. NSN   | A-8100  | 2   | Gestor                            | Syslog        |
| ASPEN   | Equipo de red. Serie A. NSN   | A-4100  | 46  | Gestor                            | Syslog        |
| ASPEN   | Equipo de red. Serie A. NSN   | A-2140  | 138 | Gestor                            | Syslog        |
| ASPEN   | Equipo de red. Serie A. NSN   | A-2200  | 70  | Gestor                            | Syslog        |
| CERAMAP | Radio Digital. Ceragon        | IP-MAX  | 200 | Gestor y Equipo                   | Traps         |
| CERAMAP | Radio Digital. Ceragon        | IP-10   | 100 | Gestor y Equipo                   | Traps         |
| CERAMAP | Radio Digital. Ceragon        | IP-10G  | 10  | Gestor y Equipo                   | Traps         |
| N/A     | Radio Digital. 4RF            | SR y SR+  | 100 | Equipo                            | Traps         |
| N/A     | Switches                      | Cisco, Allied, Hirschman, Korenix, Jet Net...   | 300 | Equipo                            | Traps/Syslog* |
| N/A     | SAIs                          | Pulsar, APC, Socomec, Energiro..                | 130 | Equipo                            | Traps         |
| N/A     | Equipo rectificador, energia. | Enertel   | 170 | Equipo                            | Traps         |
| N/A     | Equipo rectificador, energia. | Delta   | 35  | Equipo                            | Traps         |
| N/A     | Wimax                         | Breeze Access VL (Cliente y EB), Radwin         | 250 | Equipo                            | Traps         |
| N/A     | Encapsuladores                | Patton 4412, 4522, 4424,...                     | 50  | Equipo                            | Traps         |
| N/A     | Centralitas                   | Mitel, Ericsson,, Asterisk                      | 40  | Equipo                            | Traps         |
| N/A     | Videocámaras                  | Axis, On-Safe                                   | 25  | Equipo                            | Traps         |
| N/A     | Otros                         | Centrales de alarmas, conversor protocolos,.... | 20  | Equipo                            | Traps         |
| N/A     | Servidores Virtuales          |   | 20  | Equipo                            | Traps         |
| N/A     | Otros                         | Varios  | 50  | Equipo                            | Traps         |

## 2.4 Configuración de la situación actual

### 2.4.1 Arquitectura actual

La solución actual presenta diferentes capas en su arquitectura, es una solución bajo VMWare en la capa de virtualización y RHEL 7.x como Sistema Operativo (OS). A continuación, se describe mediante una ilustración cada una de las capas en las que se compone la arquitectura lógica de la solución:



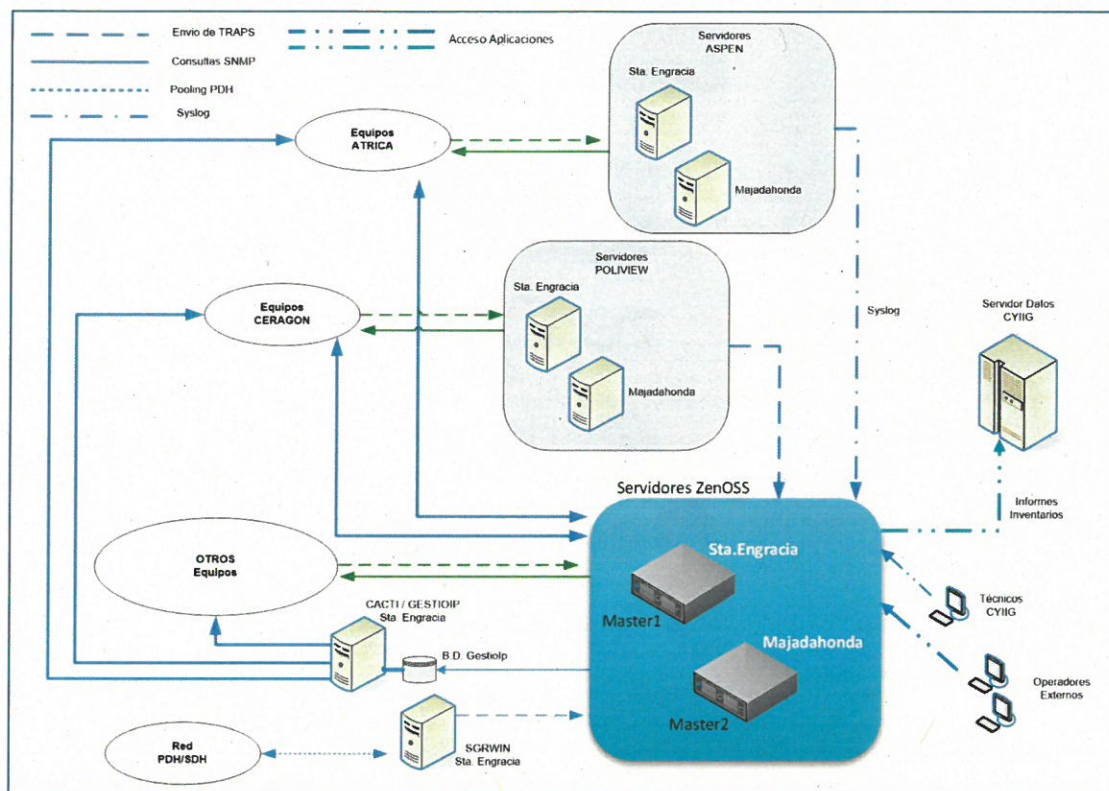


Se describe con más detalle cada una de las arquitecturas según la capa lógica

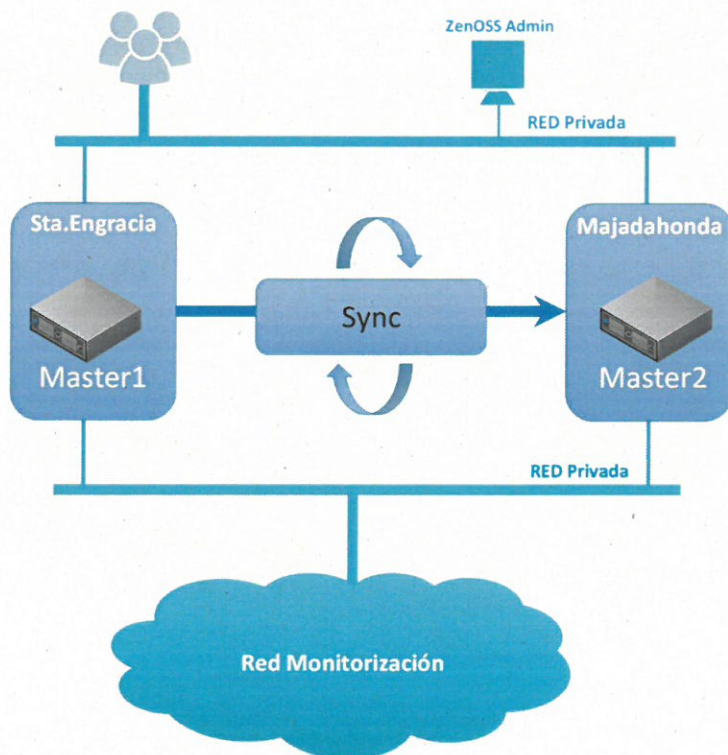
## 2.4.2 Arquitectura ZenOSS

La solución de máxima disponibilidad consiste en un ZenOSS Master standalone en una ubicación principal y un segundo servidor Master en otra ubicación distinta para mayor disponibilidad geográfica a la solución, que cuentan con un sistema de sincronización de configuraciones entre ambos así como un procedimiento de contingencia que permita un backup y restore de la aplicación.

La arquitectura lógica es la siguiente:



Y la arquitectura lógica a nivel de aplicación Zenoss es la siguiente:

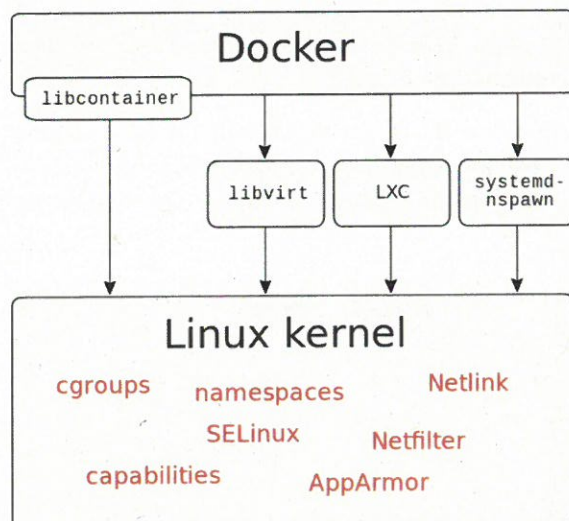




### 2.4.3 Arquitectura lógica Docker

La versión existente de ZenOSS apuesta por una arquitectura opensource denominada Docker. Esta plataforma permite gestionar aplicaciones distribuidas dando una capa de virtualización en su despliegue. Así ZenOSS puede desplegarse de forma distribuida y extenderse rápidamente para entornos donde la demanda de dispositivos monitorizados crece muy rápidamente.

Dentro de la filosofía Docker, ZenOSS es una aplicación que se despliega a través de lo que denominan una "imagen", que está preparada para comenzar a funcionar. Cuando Docker lanza la imagen crea lo que se denomina un "contenedor", que aloja y ofrece recursos para que el entorno software funcione. Usa una filosofía parecida a VMWare, pero Docker es una virtualización de entornos a través de contenedores software y con la ventaja de que no contienen un OS anfitrión por cada contenedor. Esto hace que se puedan desplegar aplicaciones cada una en un contenedor y estén aisladas entre ellas evitando conflictos de software. Para conseguirlo, Docker a través de diferentes interfaces, utiliza los recursos del Kernel como se ilustra en la siguiente Figura:

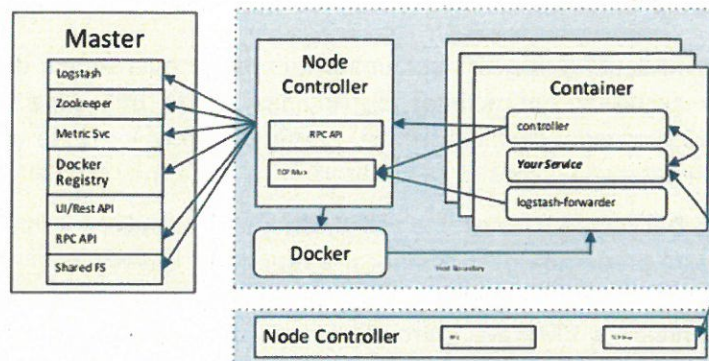


Los entornos que despliega permiten interconectividad entre ellos a través de interfaces lógicas. Esto da la característica de poder gestionar aplicaciones distribuidas.

### 2.4.4 Arquitectura Control Center

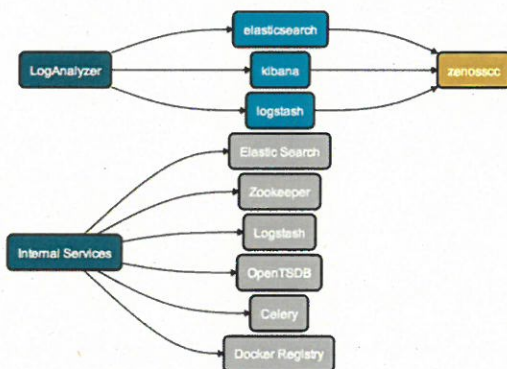
La lógica de funcionamiento del Control Center es la siguiente





ZenOSS usa el Application Programming Interface (API) de Docker para hacer las funciones de orquestación a través de un entorno denominado "Control Center" (CC). Es un desarrollo opensource propio de ZenOSS, que permite gestionar las funciones de Docker a través de una interface Web sencilla y que está disponible desde la primera instalación de la solución. El CC soporta distribución de carga entre los denominados CC nodes, servidores que reparten la carga de recursos (CPU, Memoria, Disco) para el despliegue de los contenedores Docker.

La siguiente figura muestra ejemplos de la información proporcionada por un CC desde su interface Web. A la izquierda se muestra un grafo con información de servicios desplegados en contenedores Docker, y a la derecha una imagen con el consumo de recursos generado por un contenedor de ZenOSS.



## 2.4.5 Funcionalidades de ZenOSS

La versión instalada de ZenOSS Core 5, tiene numerosas ventajas respecto a versión anteriores como las siguientes:

- Nuevo Zenoss Control Center
  - Gestión de estado de todos los servicios de ZenOSS.
  - Permite consolidar las configuraciones a través de plantillas de servicios.
  - Despliegue de ZenOSS de forma rápida en cualquier servidor con control center vía Docker.
  - Snapshot y rollbacks de forma nativa para backup/restore.



- Soporte de los nuevos ZenPack y ZenDMD para versión 5.
- Nuevo Backup y Restore online.
- Nuevo despliegue Multi-host.
- Nuevo despliegue Multi-resource pools distribución de los recursos hardware.
- Nuevas funcionalidades de rendimiento mediante Big Data
  - OpenTSDB/HBase es la arquitectura base.
  - Gráficos en HTML5 con exportado a CSV
  - Mejora la barra superior de display – Permite quitar el display para maximizar la consola de eventos en entornos de operación NOC.
  - Menos pérdida en el intervalo de retención de KPI's. Ahora OpenTSDB permite granular el intervalo, que era una limitación trabajando con RRD's.
  - Nueva recolección y visualización de KPI's asimétrica.
  - Soporte de Timezone.
  - Disponible nueva API de KPI, etiquetado y guardado de KPI MOM – Para integraciones externas.
- Mejoras UX
  - Nuevos gráficos agregados - Consolidar varios gráficos de componentes en una sola tabla para diagnosticar mejor la causa raíz y un análisis de la causa / efecto.
  - "Event Classes" y "Transform's UI" con resaltado de sintaxis
  - Nuevo interface para gestión y mantenimiento de los dispositivos.
- Dashboards dinámicos
  - HTML Portlet
  - Network Map Portlet
  - Site Window Portlet
  - Daemon Processes Down Portlet
  - Device Chart Portlet
  - Device Issues Portlet

- Event View Portlet
- Google Map Portlet
- Open Events Chart Portlet
- Production States Portlet
- Watch List Portlet

#### 2.4.6 Configuración de eventos

Las características más relevantes de la configuración de eventos actual es:

- Tratamiento de eventos de monitorización generados por la propia aplicación
  - Tratamiento de mensajes syslog, y más concretamente de los mensajes syslog enviados por el gestor ASPEN. La configuración actual contempla el tratamiento de varios tipos de mensajes, considerando la extracción de varbinds específicos a partir de la información contenida en los mismos:
  - Tratamiento de traps SNMP: basado en la compilación de las MIBs de los fabricantes identificados en el apartado 2.2,
  - Customización de la configuración (categoría, severidad, mensaje...) de los eventos recibidos.
  - Realización de acciones automáticas que se definen por medio de shell scripts.
- La siguiente tabla describe de forma orientativa, las acciones ejecutadas por los shell scripts.

**Tabla descriptiva de los scripts implementados:**

| Script                                    | Descripción  |
|---|--|
| Lanzar_Ping.ksh                           | Hacer un ping al equipo  |
| xnmtelnetcyii.ksh xterm                   | Conexión Telnet  |
| Lanzar_ParametrosInfo.ksh                 | Solicita los parámetros según el tipo de equipo del que se trate                                       |
| GUI_BasesDatos.sh                         | Solicitar las estadísticas e información de Aspen, OpenView y GestioIp                                 |
| Lanzar_Pedir_estadisticas_radios_menu.ksh | Solicitar las estadísticas de errores de los últimos 15 min y ultimas 24 h de todas las radios Ceragon |



|                             |  |
|-----------------------------|--|
| Lanzar_www.ksh              | Lanzar Navegador Web sobre dispositivo seleccionado  |
| Lanzar_Grafica.ksh          | Ver las graficas del CACTI de equipo   |
| LanzarConfigDispositivo.ksh | Entra la configuración de dispositivo. Diferente segun dispositivo seleccionado            |
| Lanzar_Reset_equipos.ksh    | Reset de 4RF, Enertel y Wimax EB exclusivamente  |
| ovmibBrwEvent               | Bring up the SNMP MIB browser, on the first source defined by the list of indicated events |
| Lanzar_Gestion_Eventos.ksh  | Gestion de eventos de radio Ceragon. Activación y desactivación                            |

## Acciones automáticas:

| Script  | Descripción  |
|---|--|
| /opt/OV/bin/local/statusAlarm.ksh \$r \$ar \$G \$S \$1 \$10                         | Asigna los Node Up/Down en cada categoría según el tipo de quipo   |
| AtricaAlarmasExternas.ksh \$1 \$2 \$3   | Traduce el texto de la alarma externa en los equipos Atrica, distingue según el equipo fuente.                             |
| /opt/OV/bin/local/cyii/acciones/HirschmannAlarmasExternas.ksh \$r "\$1" "\$2" "\$3" | Genera las alarmas de activación y clear de las alarmas externas de los switch Hirschmann mediante una consulta del estado |
| /opt/OV/bin/local/cyii/acciones/Temperaturas_Altas_Log.ksh \$r ON/OFF               | Logea las alarmas de temperatura cuando se activan y desactivan  |
| /opt/OV/bin/local/Energia_received_xc.ksh \$r "Tension Baja" \$1 \$N \$S \$**       | Genera los eventos de activación o clear dependiendo de una variable   |
| /opt/OV/bin/local/Dycec_received.ksh \$r \$R \$e \$G \$S \$*                        | Genera los eventos de activación o clear dependiendo de una variable también cambia la criticidad                          |
| /opt/OV/bin/local/cyii/acciones/ArubaEventos.ksh "\$2"                              | Según la MAC que viene en la alarma la traduce al nombre del equipo  |
| /opt/OV/bin/local/cyii/acciones/Delta_NuevosEventos.ksh \$r \$4 \$3 \$S \$5 \$6 \$7 | Genera los eventos de activación o clear dependiendo de una variable   |



|  |  |
|--|--|
| <pre>echo `date` - \$r &gt;&gt; /export/home/compartida/Documentacion/Telefono_LineaCaliente.txt DISPLAY Caída de FAX Residencia Valmayor (\$r). !!! Avisar a CYII !!!</pre> | <p>Muestra un Popup cuando se caen unas extensiones especialmente criticas y se logea las caídas</p>                     |
| <pre>/opt/OV/bin/local/cyii/Herramientas/Aruba/ConmutacionBackup/ArubaPortEnable_AlcalaO.ksh # principal NODES AlcalaO-Edar-WMX</pre>  | <p>Sistema automático para proteger un radioenlace ante una caída.</p>   |
| <pre>/opt/OV/bin/local/cyii/acciones/KorenixAlarmasExternas.ksh \$r "\$2" SDESC</pre>  | <p>Genera los eventos de activación o clear dependiendo de una variable y añade el texto correspondiente a la alarma</p> |

#### 2.4.7 Correlaciones

Adicionalmente a la configuración específica de los eventos considerada en el apartado anterior se encuentran activas las siguientes correlaciones:

Se estima que la cantidad total de correlaciones es de 260 aprox, incluyendo correlaciones de tipo PairWise (Problema / Resolución) que pueden proceder de syslog

Adicionalmente a las correlaciones de tipo pairwise se encuentran activas y personalizadas (ej. intervalo temporal) diversas correlaciones de tipo "Rate" y "Enhance".

#### 2.4.8 Tools (scripts)

La definición de tools específica, a ejecutar desde el interfaz gráfico que permiten obtener información adicional sobre el entorno gestionado. Estas tools se basan en la definición de scripts.

Se estima que la cantidad total de scripts a migrar de la plataforma antigua a la nueva consola unificada de eventos es de 200 aproximadamente y 25 de telnet.

En la tabla adjunta (ejemplos):



| Resumen de Scripts                             |  |   |   |
|--|--|---|---|
| Herramientas lanzadas manualmente              |  |   |   |
| Denominación                                   | Script   | Función   | Hace uso de   |
| Pedir estadísticas Radios                      | cyii/acciones/Pedir_estadisticas/Pedir_estadisticas_radios.ksh   | Extrae las estadísticas de las radios (IP-MAX e IP-10) sobre calidad del enlace   | /opt/OV/bin/mibtable  |
| Control Acceso a Servidores                    | cyii/Herramientas/Control_Acceso_Servidores/Control_Acceso.sh  | Habilita el usuario que utilizan empresas externas para el mantenimiento de los servidores permite dar un fecha de finalización.<br>También se hace un loggeo de todos los comandos lanzados por el usuario                 | utiliza ssh para lanzar otro script que esta situado en otro servidor (el del cacti).                                   |
| Parametros Equipos                             | cyii/parametros/Lanzar_ParametrosInfo.ksh<br>Conjunto de scripts por tecnologia  | comprueba que el equipo hace ping con el comando ovfiltertest detecta de que tecnologia se trata y lanza el script correspondiente a esa tecnologia.<br>Comunmente se usa comando snmp para sacar la informacion del equipo | /opt/OV/bin/ovfiltertest<br>/usr/sfw/bin/snmpget<br>/opt/OV/bin/snmpwalk<br>/opt/OV/bin/mibform<br>/opt/OV/bin/mibtable |
| Resetear Dispositivo                           | cyii/acciones/Reset_equipos.ksh<br>Conjunto de scripts por tecnologia  | comprueba que el equipo hace ping con el comando ovfiltertest detecta de que tecnologia se trata y lanza el script correspondiente a esa tecnologia.<br>Reinicia el equipo normalmente mediante un script hecho en telnet   | /opt/OV/bin/ovfiltertest<br>/usr/local/bin/expect   |
| Restaurar Conexion TETRA                       | cyii/Herramientas/Atrica/Cambio_buffer_E1_automatico.ksh   | realiza un cambio en un parametro snmp. Para reconocer sobre que equipos debe realizarlo existe unos ficheros con unas tablas.  | /usr/bin/zenity<br>/usr/sfw/bin/snmpset<br>/usr/sfw/bin/snmpget   |
| Habilitar/Deshabilitar traps de radios Ceragon | cyii/acciones/Gestion_Eventos/Gestion_Eventos.ksh  | Deshabilita traps de las radios Ceragon   |   |
| Alarmas SGRWIN                                 | cyii/acciones/SGRWIN_alarmas.ksh   | Solicita las alarmas de la tecnologia PDH a otro servidor a traves de snmp y las muestra en forma de tabla  | /opt/OV/bin/snmpwalk  |
| Poner Alias Atrica                             | cyii/atrica_alias/ponerAlias_GUI.ksh   | Fija los alias a los puertos en los equipos Atrica  | /usr/sfw/bin/snmpset<br>/usr/bin/zenity<br>/usr/sfw/bin/snmpwalk  |
| Herramientas lanzadas automaticamente (cron)   |  |   |   |
| resetear videocamaras                          | cyii/Tareas/Videocamaras_reset.ksh<br>cyii/Expect/Videocamaras/Videocamaras_reset.tcl  | Diariamente resetea las videocamaras  | /usr/local/bin/expect   |
| reseto servicio PowCom                         | cyii/Enertel/Reset_servicio/Enertel_reinicio_servicio_PowCom_por_fichero_lista.sh  | Diariamente por grupos resetea un servicio en los equipos enertel   | /usr/local/bin/expect   |
| recoger Alias                                  | cyii/atrica_alias/recolectaTodosAliasAtrica.ksh<br>cyii/cisco_alias/recolectaTodosAliasCisco.ksh   | Diariamente se recolectan todos los alias   | /usr/sfw/bin/snmpget<br>/opt/OV/bin/snmpwalk  |
| comprobacion servidores                        | /opt/OV/bin/local/cyii/Tareas/mon_estadoDNS.ksh<br>/opt/OV/bin/local/cyii/Tareas/mon_Aspen_log_parte-1.ksh<br>/opt/OV/bin/local/cyii/Tareas/mon_Polyview.ksh | Cada hora se comprueban todos los servidores lanzando un trap simulado a cada uno y se comprueba (10 minutos mas tarde) que nos lo retorna.   | /opt/OV/bin/ovevent<br>/usr/sfw/bin/snmptrap  |
| Actualizar hora Enertel                        | cyii/acciones/Enertel_actualizar_hora.ksh  | pone en hora los enertel  |   |
| Tratamiento de eventos                         |  |   |   |
| equipos Delta                                  | cyii/acciones/Delta_NuevosEventos.ksh  | convierte los traps de los equipos delta en dos traps clear y activacion  | /usr/sfw/bin/snmptrap   |
| Textos Alarmas externas Atrica                 | cyii/acciones/AtricaAlarmasExternas.ksh  | introduce un texto descriptivo en la alarma externa (Dry Contact), los textos pueden variar según la fuente   | /opt/OV/bin/ovevent   |
| alarmas externas de switch Korenix             | cyii/acciones/KorenixAlarmasExternas.ksh   |   |   |
| alarmas externas de switch Hirschmann          | cyii/acciones/HirschmannAlarmasExternas.ksh  |   |   |
| Inventario                                     |  |   |   |
| Inventario Atrica                              | cyii/Inventario/AtricaDatosInventarioTodo.ksh  | Saca un inventari de equipos atrica   | /opt/OV/bin/snmpwalk<br>/opt/OV/bin/ovfiltertest<br>/usr/sfw/bin/snmpget  |
| Parametros Equipos                             |  |   |   |
| Parametros Enertel                             | cyii/acciones/EnertelInfo.ksh  |   |   |

## 2.4.9 Tratamiento de eventos

### Tratamiento de eventos – Fuentes de eventos



- Eventos de monitorización de la propia solución de supervisión (Node up/down, interface up/down)
- Notificaciones enviadas por los equipos de red en forma de traps SNMP
- Notificaciones enviadas por los gestores de red – en forma de traps SNMP y/o mensajes syslog, con especial atención a los mensajes syslog del gestor ASPEN.

#### Tratamiento de eventos - correlaciones básicas

- Deduplicación de eventos: identificación de sucesivas ocurrencias de un mismo evento
- Correlaciones de eventos de tipo problema / resolución:
  - Parejas de eventos problema / resolución
  - Eventos individuales que cuentan con un campo que permite identificarlos como problema / resolución
  - Inventario básico para los equipos.

#### 2.4.10 Inventario detallado

El modelado de los equipos y ciertas consultas sobre el inventario incluyen el enriquecimiento del inventario básico de los equipos con información proveniente de fuentes externas a los equipos (BD, tablas excel, ficheros,...).

#### 2.4.11 Gráficas

Se realiza polling SNMP y monitorización de rendimiento en tiempo real sobre los equipos para la representación de gráficas de datos de distinta índole, para la generación de alarmas en caso de superación de ciertos umbrales predefinidos y para tener gráficas con la evolución histórica de diversos contadores.



### 3. ALCANCE

Conforme a lo estipulado en sucesivos apartados del presente Pliego de Prescripciones Técnicas, en adelante PPT, el alcance de este contrato comprende los siguientes elementos fundamentales:

- Mantenimiento correctivo-preventivo y soporte de la solución de supervisión descrita en el presente pliego, en los horarios y con los SLAs definidos posteriormente.
- Actualizaciones de software.
- Una bolsa de 350 horas para asistencias técnicas por parte de personal experto en los componentes instalados durante el periodo del contrato.
- Impartición de cursos al personal de Canal sobre la solución de monitorización Zenoss.
- Revisión y actualización de los procedimientos de operación y mantenimiento de la infraestructura actual.

El alcance del contrato será de 4 años desde la firma del mismo.

#### 3.1 Mantenimiento preventivo y correctivo

El adjudicatario realizará el mantenimiento correctivo-preventivo y dará soporte de la solución de supervisión descrita en el presente pliego, en los horarios y con los SLAs definidos posteriormente, así como realizará una auditoría periódica del sistema.

El adjudicatario dispondrá de un centro de soporte al usuario 24x7 para la recepción de incidencias, con el que se podrá contactar por teléfono móvil y correo electrónico.

El seguimiento de las incidencias se llevará a cabo haciendo uso de la aplicación que determine el Canal de Isabel Segunda, el adjudicatario también podrá proponer una aplicación propia de gestión de incidencias en la que se puedan acometer las siguientes tareas:

Realizar un registro de incidencias con la información: fecha y hora de apertura/cierre de la incidencia, sistemas afectados, estado de la incidencia, criticidad, descripción de los efectos que produce la incidencia, acciones realizadas, equipo de trabajo, etc.

- Realizar un control de tiempos, de manera que se pueda verificar el cumplimiento de los niveles de servicio asociados a cada tipología de incidencia.
- Realizar la asignación y escalado de tareas entre las diferentes partes involucradas en la resolución de la incidencia.
- Publicación de actas o informes de intervención con la descripción de las actuaciones realizadas.
- Generación de notificaciones a los interesados: escalado de incidencias, publicación de informes, etc.



En la medida que sea técnicamente posible, el adjudicatario tendrá acceso a la herramienta de ticketing que indique Canal de Isabel Segunda y documentará los detalles de todas las incidencias y registros que se le asignen.

### 3.1.1 Regímenes de servicio

Con objeto de garantizar la prestación del servicio con la calidad requerida, es necesario categorizar las incidencias en función de su afectación al servicio y definir los tiempos requeridos de atención, respuesta, atención, transporte y seguimiento para cada una de ellas. La categorización de las incidencias será realizada por Canal de Isabel Segunda cuando se comunique la apertura de la misma y en función de los criterios que se indican a continuación.

Clasificación de las incidencias:

1. **Criticidad Muy Grave:** aquellas que implican la pérdida total de los servicios de supervisión de ambos servidores Zenoss.
2. **Criticidad Grave:** aquellas que implican la pérdida total de los servicios de supervisión de uno de los servidores Zenoss.
3. **Criticidad Media:** aquellas que no tienen una afectación directa en el servicio, pero implican una degradación en la operación o la gestión de uno de los servidores Zenoss.
4. **Criticidad Leve:** resto de incidencias sin afectación al servicio.

Una incidencia puede ver rebajada su criticidad cuando se hayan aplicado soluciones paliativas temporales que reduzcan su afectación al servicio, aunque no se haya resuelto completamente la misma. De igual modo, una incidencia también puede subir de criticidad si durante su análisis o resolución aumentase el grado de afectación al servicio.

Definición de los parámetros de servicio:

**Horario de atención (HA):** Franja horaria de disponibilidad del servicio asociado.

**Tiempo de respuesta (TR):** Tiempo desde que Canal de Isabel II notifica la incidencia hasta que recibe confirmación de recepción de la misma por parte del adjudicatario.

**Tiempo de transporte (TT):** Tiempo transcurrido desde la notificación de la incidencia hasta el inicio de las actividades encaminadas a su resolución. La confirmación de inicio de actividades se podrá realizar telefónicamente o por correo electrónico dirigido al punto de contacto para la incidencia por parte de Canal de Isabel II.

**Tiempo de actividad (TA):** Tiempo que transcurre desde el inicio de realización de actividades (TT) hasta que se reporta información sobre el primer diagnóstico y avance de la resolución de la incidencia o consulta.

**Tiempo de seguimiento (TS):** Tiempo máximo periódico de actualización del avance de la resolución de la incidencia o consulta, hasta su resolución.

Tabla de Parámetros de Servicio:

En la siguiente tabla se especifican los valores aplicables a los parámetros de servicio descritos anteriormente para cada clase de incidencia, también descritas anteriormente. Los tiempos indicados



son máximos y son la referencia para posibles aplicaciones de penalizaciones por incumplimiento de parámetros de servicio.

| Clase de incidencia | HA  | TR         | TT        | TA         | TS       |
|---------------------|---|------------|-----------|------------|----------|
| Muy Grave           | 24x7  | 10 minutos | 1.5 horas | 30 minutos | 1 hora   |
| Grave               | 8x5: L-V de 8:00 a 20:00<br>Excluidos festivos nacionales | 15 minutos | 3 horas   | 1 hora     | 2 horas  |
| Media               | 8x5: L-V de 8:00 a 20:00<br>Excluidos festivos nacionales | 1 hora     | 24 horas  | 2 horas    | 1 día    |
| Leve                | 8x5: L-V de 8:00 a 20:00<br>Excluidos festivos nacionales | 1 hora     | 48 horas  | 2 horas    | 1 semana |

El reporte de avance de las incidencias de criticidad baja y de las consultas, según el parámetro de servicio TS de 1 semana, se podrá concentrar para todas las incidencias de estas clases que estén abiertas simultáneamente en un mismo día de la semana.

Para todas las clases de incidencia, la información de avance reportada tras cada periodo de TS debe de añadir siempre datos o información nuevos que justifiquen la existencia de actividad y/o seguimiento de la incidencia.

A título informativo, se indica en la siguiente tabla el número de incidencias registradas en el anterior contrato de mantenimiento de la solución actual, desde Julio de 2017 a Marzo de 2019:

- 2017
  - Muy Grave 0
  - Grave 2
  - Media 4
  - Leve 0
- 2018
  - Muy Grave 0
  - Grave 7
  - Media 9
  - Leve 0
- 2019
  - Muy Grave 0
  - Grave 1
  - Media 3
  - Leve 0
- Total general: 26

Como consecuencia del incumplimiento de los parámetros de servicio indicados, Canal de Isabel II podrá proponer la aplicación de las correspondientes penalizaciones, de conformidad con lo establecido en el Pliego de Cláusulas Administrativas Particulares.



### 3.1.2 Generación de informes semanales y mensuales

El adjudicatario realizará y entregará a Canal informes de incidencias mensuales según los formatos y modelos definidos al efecto, en el inicio del contrato.

Estos informes deben presentar los datos de las incidencias de forma ordenada y agrupada de manera que se pueda identificar claramente el número de incidencias abiertas/cerradas en el período de interés, la criticidad de estas incidencias, los emplazamientos o sistemas afectados y las actuaciones más destacadas llevadas a cabo o pendientes de realizar.

Todas las incidencias quedaran registradas en la aplicación descrita en el apartado anterior.

### 3.1.3 Gestión del servicio

Los trabajos asociados con el seguimiento y control son imprescindibles para garantizar la consecución de los niveles de servicio solicitados. En esta línea, se llevarán a cabo reuniones mensuales de seguimiento de la actividad, de tipo presencial o remota, para realizar un análisis de los principales indicadores, identificación de planes de acción e identificación de problemas que requieran un escalado a niveles superiores. Como soporte para estas reuniones de seguimiento, se dispondrá de los informes técnicos de resolución y seguimiento de incidencias, informes mensuales o cualquier otra documentación técnica de interés.

En un plazo máximo de 48 horas el adjudicatario elaborará y entregará a Canal de Isabel II la correspondiente acta de reunión. El acta de reunión debe contener un resumen de los temas tratados en la misma, destacando las decisiones acordadas y los puntos de acción, para los que deberá especificar un responsable y una fecha objetivo de ejecución. En un plazo máximo de una semana a partir de la recepción del acta de reunión, se deberá firmar por las partes implicadas para dar conformidad a su contenido.

## 3.2 Actualizaciones de software

### 3.2.1 Acceso a correcciones de software

Hasta la finalización del contrato, se puede generar correcciones a una versión de software existente o bien una nueva versión estándar de software de manera que se corrijan posibles disfunciones o defectos detectados durante el funcionamiento de las distintas versiones. En caso de que Canal considerara oportuna la introducción de la corrección de una versión de software, se instalará la misma mediante una intervención "in-situ".

Tras la actualización el adjudicatario llevará a cabo un período de observación de tres días durante el cual el estará disponible 24x7, pudiendo ser requerido su acceso al sistema e incluso la intervención local en él en un plazo inferior a 4 horas desde la activación de la alarma.

Mediante este servicio se deberán poner a disposición del Canal de Isabel Segunda todas las modificaciones de la versión del software que se esté utilizando. Las correcciones podrán entregarse de forma individual o bien agrupar varias modificaciones de software en un único paquete.

La adquisición e instalación de las correcciones de software no supondrán ningún coste al Canal y correrán a cargo del adjudicatario.



### 3.2.2 Acceso a nuevas versiones de software

Hasta la finalización del contrato desde el adjudicatario comunicará a Canal de Isabel Segunda, la disponibilidad de nuevas versiones de software tan pronto como disponga de la información proporcionada por el fabricante sobre el contenido y la fecha de aparición de las mismas.

Para cada nueva versión de software el adjudicatario proporcionará al Canal un análisis de la idoneidad de la implantación sobre la solución existente en ese momento en el Canal, destacando las nuevas funcionales, correcciones y posibles riesgos que pueda llevar a cabo la implantación de dicha versión, en dicho análisis vendrá detallado el coste de su implantación, valorándola en horas de trabajo.

La instalación de cualquier nueva versión de software será acordada entre Canal y el adjudicatario, y el coste de la misma se imputará a la bolsa de horas existente en el presente contrato.

Cualquier actualización se realizará siempre mediante una actuación "in-situ" por parte del personal del adjudicatario.

Tras la actualización el adjudicatario llevará a cabo un período de observación de tres días durante el cual el estará disponible 24x7, pudiendo ser requerido su acceso al sistema e incluso la intervención local en él en un plazo inferior a 4 horas desde la activación de la alarma.

La edición tanto de una corrección de software como de una nueva versión de software incluirá la producción, la realización de pruebas por parte del adjudicatario junto con el Canal de Isabel Segunda y el suministro de un paquete de software maestro en soporte digital de la corrección o de la nueva versión de software.

Todas las modificaciones software que se introduzcan en el sistema deberán ser compatibles con los elementos existentes en la actualidad. En ningún momento la introducción de una corrección software o nueva versión supondrá la pérdida de prestaciones existentes o la obligación de cambiar el modo de funcionamiento del sistema.

Será responsabilidad del adjudicatario informar periódicamente y con la antelación suficiente a Canal de Isabel Segunda la posible obsolescencia de los equipos hardware que componen la red con indicación de aquellos que los sustituirán.

### 3.2.3 Realización de pruebas

El adjudicatario estará obligado a llevar a cabo pruebas previas de compatibilidad de las nuevas versiones de software antes de proceder a instalar las mismas en la red de Canal. Para ello, el adjudicatario deberá disponer de una maqueta o entorno de pruebas, donde probar y validar las nuevas correcciones o versiones de software, previamente a la implantación de las mismas en el sistema de supervisión de red de Canal, siguiendo un protocolo que recogerá las medidas y comprobaciones sugerido por el adjudicatario a Canal, así como aquellas otras que se acuerden entre el contratista y Canal.

El personal técnico de Canal validará las nuevas versiones y su compatibilidad con la que se encuentre en uso y si el proceso de validación es positivo se dará el visto bueno al comienzo de la instalación en la red de Canal según el calendario y los requisitos que se acuerden posteriormente.

### 3.3 Bolsa de horas

Se incluirá una bolsa de 350 horas anuales de técnico especialista de soporte del sistema de supervisión para la realización de desarrollos adicionales y evolutivos del sistema.



La prestación del servicio de bolsa de horas de técnico especialista se realizará tras una solicitud específica de los servicios técnicos de Canal de Isabel Segunda en la que se detallarán los desarrollos o funcionalidades adicionales a implementar sobre la herramienta de supervisión. El adjudicatario contestará a cada solicitud realizada con una estimación de horas para cada uno de los trabajos a realizar y confirmando la viabilidad de los mismos, una vez conocido la previsión de imputación de horas de cada trabajo será Canal de Isabel Segunda el que determine si esos trabajos se llevarán a cabo y la priorización de los mismos.

Los servicios de soporte a cargo de la bolsa de horas se podrán realizar de forma remota (telefónicamente, correo electrónico, acceso por VPN a los sistemas...), aunque Canal de Isabel Segunda podrá requerir, si lo considera necesario que dichos trabajos se desarrollen en dependencias de Canal.

### 3.4 Formación

Será objeto del presente concurso la impartición de formación tanto para personal de Canal como personal subcontratado, se darán cursos para 3 perfiles de usuarios (administradores, operadores y supervisores) el temario se definirá con el Canal de Isabel II Gestión.

- CURSOS: Administrador, operador y supervisor de Zenoss
- TURNOS: 2 (Cada uno de los tres cursos se impartirá 2 veces, para permitir la asistencia de todo el personal necesario.)
- OBJETIVOS:
  - Capacitación para el mantenimiento de la herramienta Zenoss como administrador.
  - Capacitación para el uso de la herramienta Zenoss como operador.
  - Capacitación para el uso de la herramienta Zenoss como supervisor.
- DURACIÓN DE CADA CURSO Y TURNO: 20, 20 y 20 horas respectivamente (cada turno).
- ASISTENTES APROXIMADOS A CADA CURSO: De 15 a 20 personas repartidos en dos turnos
- MEDIOS Y SALA: aportados por el Canal de Isabel II Gestión
- FECHA: A determinar según necesidad del Canal de Isabel II Gestión

Todos los equipos de red suministrados deberán soportar el protocolo SNMP v1, v2 y v3 de gestión y disponer de las MIBs correspondientes para facilitar la integración de funciones de gestión en una plataforma central externa y abierta.

Será objeto de contrato la integración de todos los sistemas incluidos en proyecto, resultante de la reingeniería necesaria, en el sistema de supervisión (basado en SNMP) de CANAL, así como la provisión del sistema de gestión y supervisión propietario de los equipos suministrados que permitan todos los aspectos de operación y mantenimiento, así como de las plataformas necesarias para contenerlos.

Los trabajos de integración en el sistema serán los siguientes:

- Integración y categorización de traps.
- Formateo de alarmas según indicaciones de CANAL.



- Análisis de todas las alarmas que genera el equipo y, de acuerdo con CANAL, elección de aquellas más importante.
- Inclusión en los mapas de tecnologías.

#### 4. ACCESO REMOTO

El adjudicatario estará obligado a proveer un acceso mediante VPN u otro método que defina Canal a los servicios de información de Canal. El coste de los mismos, correrán a cargo del adjudicatario.



## 5. FORMATO DE LAS OFERTAS

En este apartado se establecen las condiciones de presentación de las ofertas.

En general, se establece que las empresas licitadoras describirán del mejor modo posible su solución para las necesidades descritas e informar a canal gestión con mayor detalle posible de las ventajas, prestaciones y funcionalidades de su solución ofrece.

Las empresas licitadoras se ajustarán a las siguientes normas relativas a la presentación de sus ofertas. Se presentará una única oferta por lote la cual se describe a continuación:

La oferta técnica que describa la solución ofertada se presentará, preferiblemente, en carpetas de anillas, papel DIN A4, con interlineado a doble espacio y letra no inferior a 12 puntos, con membrete del licitador, identificación del documento, página y total de páginas. El número de copias de la misma será de DOS (2).

Adicionalmente, se entregará una copia electrónica (preferentemente CD-ROM) de los documentos generados, en formato compatible con MS-Office XP. Los planos, esquemas, folletos u otros documentos no compatibles se entregarán solamente en papel y en formato PDF.

El contenido y organización de las ofertas se ajustará a los apartados descriptivos detallados en el presente Pliego de Prescripciones Técnicas y contendrá la estructura definida en el PCAP

En relación al Resumen Ejecutivo, éste incluirá de manera específica y, como mínimo, los siguientes aspectos:

Breve descripción de la persona natural o entidad licitadora. En este punto, si el licitador dispone de la Certificación ISO 9001 deberá adjuntar una copia de la misma.

Resumen de la propuesta de detalle.

Capacidad para acometer los trabajos y suministrar los servicios objeto de esta asistencia, indicando si para el desarrollo del proyecto contará con el concurso de otras entidades y en que ámbitos.

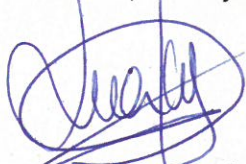
Estrategias propias del licitador en relación al desarrollo del servicio propuesto y planificación temporal del mismo.

Experiencia real y demostrable en relación a los trabajos y suministros objeto de este concurso.

Descripción general de las mejoras que se proponen en relación a las prestaciones, sistemas y servicios requeridos y que impliquen una mejora sustancial en la prestación del servicio por parte de Canal Gestión.

Compromiso expreso de cumplimiento de los requisitos definidos en este Pliego de Prescripciones Técnicas y en la oferta.

En Madrid, 25 de julio de 2019



Juan Sánchez García  
Director de Innovación e Ingeniería