MINISTERIO
DEL INTERIOR

SUBSECRETARÍA

DIRECCIÓN GENERAL DE
PROTECCIÓN CIVIL Y
EMERGENCIAS

DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL Y EMERGENCIAS

PLIEGO DE PRESCRIPCIONES TECNICAS PARA LA CONTRATACIÓN DEL SISTEMA DE AVISOS A LA POBLACIÓN DE LA RED DE ALERTA NACIONAL (RAN-PWS)

Julio 2021

UnidadTIC@procivil.mir.es

Quintiliano, 21
28002 MADRID
TEL 915 373 100
FAX 915 628 926

1. INTRODUCCIÓN Y ANTECEDENTES

La Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil (LSNPC) crea en su artículo 12 la Red de Alerta Nacional (RAN) de Protección Civil como mecanismo de gestión de avisos y alertas a nivel nacional, en el que participan todas las organizaciones concernidas, desde los organismos que disponen de la información que puede ser relevante en relación con emergencias actuales o posibles hasta los centros de gestión de emergencias en los distintos niveles administrativos y los servicios públicos de respuesta a incidencias (centros 112). La RAN permitirá la generación, tratamiento y difusión efectiva de los avisos y alertas de protección civil.

La RAN está gestionada por el Ministerio del Interior, a través del Centro Nacional de Seguimiento y Coordinación de Emergencias de Protección Civil (CENEM) de la Dirección General de Protección Civil y Emergencias (DGPCE). A través de esta red se transmiten los avisos desde los organismos con capacidad de detección de posibles condiciones de alerta hasta el CENEM, que comparte esta información con los centros de coordinación de emergencias de las Comunidades Autónomas. En cualquiera de estos centros, teniendo en cuenta los avisos recibidos y otra información disponible, puede tomarse la decisión de difundir un mensaje de alerta a la población para facilitar que se tomen las medidas de autoprotección que puedan ser necesarias.

La Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (el Código), establece en su artículo 110 la obligación en todos los países miembros de, donde ya estén desplegados sistemas de aviso a la población (conocidos como PWS, siglas de su nombre en inglés: Public Warning System), establecer nuevos sistemas de aviso que transmitan la información relevante a través de las redes de telefonía móvil.

España cuenta con PWS específicos y localizados para varios tipos de riesgo (instalaciones químicas o nucleares, presas, etc) normalmente basados en señales acústicas. La existencia de estos sistemas obliga a desplegar el nuevo sistema exigido por el Código, que deberá proporcionar al menos la misma cobertura que los sistemas tradicionales.

La DGPCE, en colaboración con la Dirección General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual (DGTel) del Ministerio de Asuntos Económicos y para la Transformación Digital, y en coordinación con los servicios de emergencia de las CCAA, ha valorado los requisitos para el despliegue de un sistema PWS acorde con lo estipulado en el Código, llegando a la conclusión de que el modo más rápido y efectivo de poner en marcha este servicio es a través de la contratación del despliegue, configuración y puesta en marcha de un sistema de información y comunicaciones que permita la generación de las alarmas en los centros de coordinación de emergencias, su autorización, procesado y validación, su distribución a las operadoras de telefonía móvil, y su envío a través de las redes de éstas hasta alcanzar, mediante mensajes que se mostrarán en los teléfonos móviles, a todos los ciudadanos situados en las zonas afectadas. Este sistema de información será identificado como RAN-PWS a lo largo de este documento.

La cobertura del sistema no estará limitada, como exige el Código, a las zonas que actualmente disponen de sistemas de alerta, sino que se extenderá a todo el territorio nacional, lo que permitirá la difusión de alertas para situaciones de riesgo o emergencia que actualmente carecen de esta posibilidad.

El resto del contenido de este Pliego de Prescripciones Técnicas detalla los componentes que deberán ser proporcionados y desplegados, así como su funcionamiento esperado y las condiciones de uso,

operación y mantenimiento que deberán ser cumplidas por el adjudicatario del contrato.

2. OBJETO DEL CONTRATO

El objeto de contratación es la adquisición de los elementos hardware y software (servidores, sistemas de almacenamiento, electrónica de red, así como las licencias permanentes de uso de las aplicaciones informáticas) que sean necesarios, junto con la instalación, configuración, pruebas y puesta en marcha, para el despliegue del sistema RAN-PWS en las ubicaciones y con las condiciones que se establecen en este documento.

La contratación se realizará mediante procedimiento abierto con tramitación de urgencia.

3. DESCRIPCION DEL SISTEMA

3.1 LA RED DE ALERTA NACIONAL

En la figura 1 se muestran los elementos componentes de la RAN. El sistema RAN-PWS, objeto de la presente licitación, se muestra resaltado en la parte inferior.

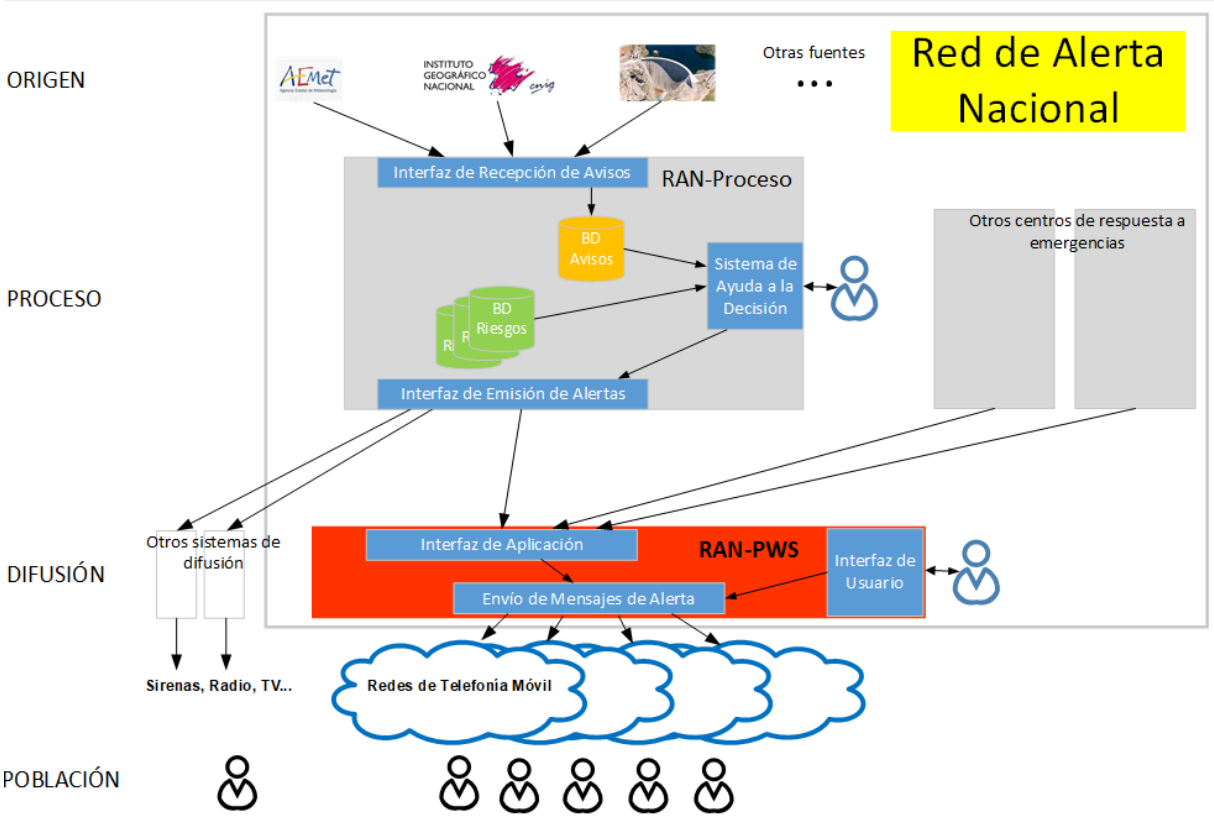

Fig 1. El Sistema de Avisos a la Población de la Red de Alerta Nacional

3.2 ARQUITECTURA DEL SISTEMA RAN-PWS

Para la distribución de mensajes masivos a través de teléfonos móviles se utilizará la tecnología Cell Broadcast (CB, o Difusión por Celdas). Este sistema permite enviar un mensaje de forma casi

instantánea a todos los teléfonos móviles que tengan una conexión establecida con las antenas de telefonía para las que se activa la emisión de la alerta. El mensaje se recibe en el móvil como un sonido acompañado de un texto con información sobre la situación de alerta.

CB ha sido definido por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI). Las Especificaciones Técnicas TS 123 041 y TS 102 900 definen los protocolos utilizados en la transmisión de datos, tanto para la recepción de los mensajes como para su distribución a través de las redes GSM, UTMS, etc de las operadoras, los tipos de datos a emplear, y los componentes básicos del sistema. Estos componentes se describen a continuación:

3.2.1 Cell Broadcast Entity (CBE)

Sistema de información que permite la definición y gestión de los mensajes de alerta. Su ubicación habitual es en las instalaciones del organismo responsable de la generación de las alertas. En el caso del RAN-PWS, dado el reparto competencial de la Protección Civil en España, no existe un único organismo competente, por lo que el CBE se ubicará en el CENEM, como centro de coordinación de alertas nacional. Aunque esté físicamente situado en esta ubicación, será posible acceder al sistema, de forma remota, desde los demás centros autorizados para su uso.

3.2.2 Cell Broadcast Center (CBC)

Sistema de información y comunicaciones, conectado directamente a las redes de un operador de telefonía móvil. El CBC recibe del CBE el mensaje a emitir junto con los parámetros necesarios para su difusión: área afectada, duración de la alerta, frecuencia de las posibles repeticiones etc. El CBC realiza el cálculo de las estaciones base de telefonía móvil que deben activarse para asegurar la entrega del mensaje a todos los terminales móviles que se encuentren dentro del área afectada.

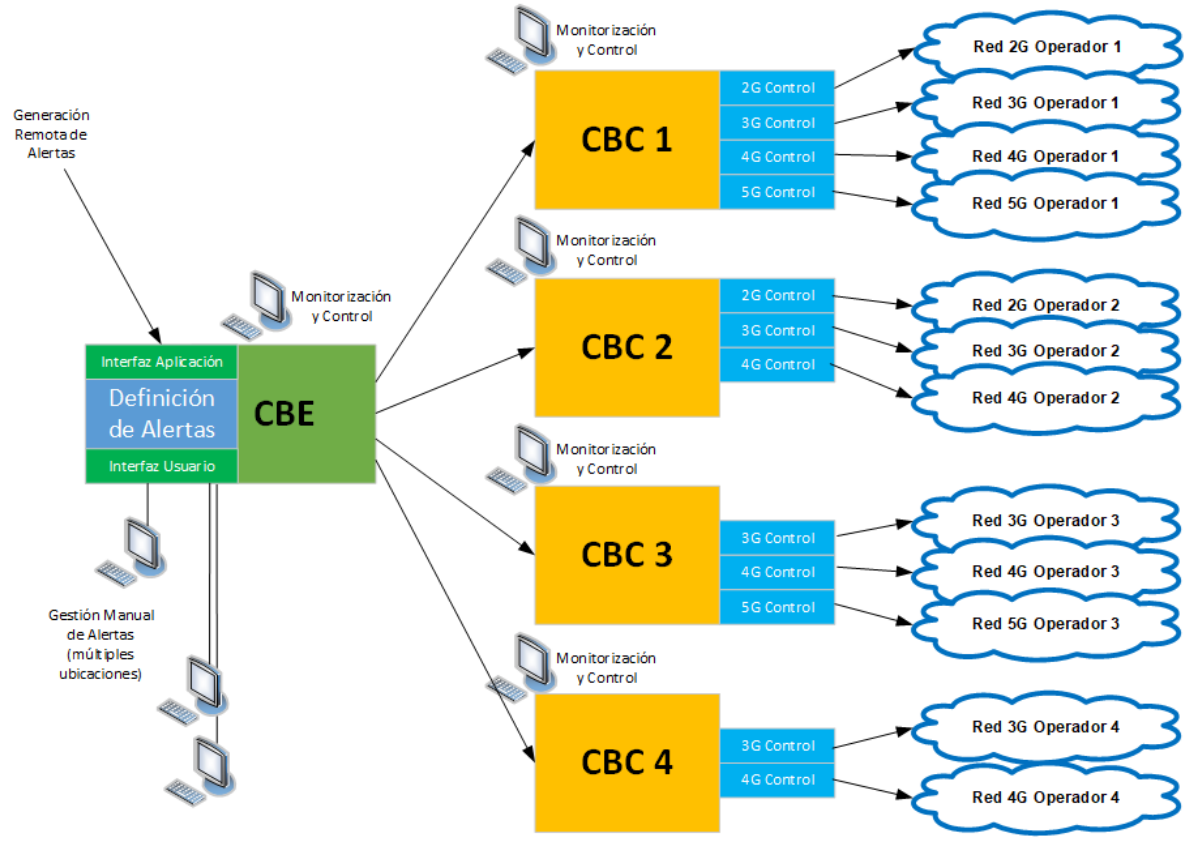

Fig 2. Arquitectura del sistema RAN-PWS

3.3 FUNCIONAMIENTO DEL SISTEMA RAN-PWS

3.3.1 Creación de alertas

Los usuarios con los permisos apropiados podrán crear alertas a través de la interfaz de usuario del sistema CBE. Será posible definir al menos los siguientes parámetros para cada alerta:

- Tipo de alerta (en función del tipo de riesgo que la causa): meteorológica, sísmica, inundación, química, radiológica, nuclear, etc
- Suceso causante (por ejemplo viento, nieve, avalancha, terremoto, accidente industrial, etc)
- Nivel de criticidad de la alerta (en función de la previsible gravedad de sus efectos): moderada (código amarillo), severa (código naranja), extrema (código rojo)
- Área afectada, definida mediante una figura geométrica (círculo o polígono). El área deberá estar comprendida dentro del territorio para el que el usuario que define o autoriza la alerta está autorizado (área de competencia)
- Tiempo de inicio: inmediato o en algún momento en el futuro
- Tiempo previsto de finalización
- Descripción del suceso y sus efectos previstos
- Mensaje a la población, con recomendaciones o instrucciones

Una vez definidos todos los parámetros necesarios se podrá ejecutar la orden de creación de la alerta, lo que generará un mensaje de aviso que será enviado a la autoridad responsable de la emisión de la alerta y al coordinador del sistema. La alerta permanecerá en el sistema pendiente de activación.

3.3.2 Activación y gestión de alertas

Los usuarios con los permisos apropiados podrán visualizar todas las alertas definidas en el CBE, dentro de su área de competencia, en sus diferentes estados: pendiente de activación, activada, en curso, y finalizada.

Las alertas en estado pendiente de activación podrán ser activadas por los usuarios autorizados. La activación provocará el envío inmediato de la alerta a los CBC para su difusión. Posteriormente y en función de los mensajes de confirmación recibidos de los CBC la alerta pasará a los estados en curso y finalizada.

3.3.3 Cancelación de alertas

En cualquiera de los estados: pendiente de activación, activada, y en curso, será posible lanzar la orden de cancelación de la alerta. En este caso, si la alerta ya estaba activada o en curso se enviará orden de cancelación a los CBC para que interrumpan la difusión de la alerta y notifiquen su cancelación. La alerta se mantendrá registrada en el sistema en estado cancelada.

3.3.4 Publicación de alertas en página web

Existirá una página web de acceso público en el que permanentemente se mostrarán las alertas en curso, de modo que sea posible obtener, a través de ella, información adicional cuando los ciudadanos reciben una alerta en su terminal móvil.

Para facilitar el acceso a esta página será posible incluir un enlace a ella dentro del texto de los mensajes de alerta.

La página deberá estar dimensionada para soportar accesos masivos en momentos muy puntuales.

3.3.5 Acceso a las alertas desde aplicación móvil

Opcionalmente, el adjudicatario podrá proporcionar una aplicación móvil, disponible sin coste en los principales mercados de aplicaciones, que permitirá a los ciudadanos que la tengan descargada:

- Recibir, si la aplicación está configurada para recibirlos, los mensajes de alerta en el momento que éstas sean activadas en el CBE
- Configurar la aplicación para recibir las alertas que cumplan una o varias de las siguientes condiciones:
    - Alertas que afectan a ciertas ubicaciones predefinidas por el usuario (incluida su posición actual)
    - Alertas de ciertos tipos preseleccionados
- Acceder en cualquier momento al estado de todas las alertas que hayan sido activadas en las últimas horas

La aplicación móvil, incluyendo su código fuente y las librerías necesarias para su compilación, quedarán en poder de la Administración como parte de los entregables del proyecto.

3.3.6 Seguimiento y Control

Los usuarios autorizados dispondrán, a través del Centro de Control del CBE, de un menú de visualización del estado de las alertas del sistema, dentro de su área de competencia.
Los CBC dispondrán también de los menús necesarios para el seguimiento de las alertas que hayan sido recibidas en su sistema.

4. DESCRIPCIÓN DE LOS TRABAJOS OBJETO DEL CONTRATO

4.1 OBJETIVO

El adjudicatario deberá proveer y desplegar los sistemas informáticos que permitan el funcionamiento descrito en el punto anterior en las ubicaciones que se indican a continuación. El despliegue incluirá:

- instalación de los sistemas informáticos y de comunicaciones necesarios
- provisión, instalación y activación de licencias perpetuas para el uso de los sistemas
- configuración de los componentes del sistema y realización de las pruebas que demuestren su correcto funcionamiento en todos los escenarios que se describen en este documento

4.2 TAREAS

Las tareas a realizar por el adjudicatario para asegurar el cumplimiento de las funciones descritas, se agrupan en los siguientes apartados:

4.2.1 Suministro e instalación

1. El CBE se desplegará en las instalaciones que designe la Dirección General de Protección Civil

y Emergencias.

2. Se desplegarán cuatro instancias de CBC, una en cada una de las ubicaciones que designen las operadoras de telefonía móvil que disponen red de acceso radio propia en España, en cuyas redes se integrarán estos sistemas.
3. Se configurarán los protocolos y canales de comunicación entre CBE y CBCs para asegurar la transmisión inmediata de los mensajes de alerta del primero a los segundos, y el retorno de información de control de los segundos al primero.
4. Se proporcionará la información y el soporte necesarios para permitir a las operadoras realizar la integración de los CBCs con sus redes de comunicaciones.

4.2.2 Pruebas y puesta en funcionamiento

5. Una vez en marcha las tareas de instalación, siguiendo la planificación se llevarán a cabo los protocolos de pruebas (unitarias, de carga, de integración) necesarios para asegurar el correcto funcionamiento de todos los componentes.
6. Previamente a la aceptación del sistema se realizará una demostración de su funcionamiento completo, desde la definición de la alerta a su distribución a teléfonos móviles situados en la zona definida en la alerta. La demostración podrá hacer uso de entornos de simulación y pruebas que eviten la necesidad de probar el funcionamiento en un entorno real.

4.2.3 Gestión del proyecto de despliegue y puesta en marcha

7. En el momento de la firma del contrato el adjudicatario pondrá en marcha una Oficina de Gestión del Proyecto (OGP) que se responsabilizará de coordinar todas las actividades de despliegue de los distintos componentes en las ubicaciones que designen la Administración y las operadoras, la interconexión de esos componentes, su configuración, y la definición y ejecución del plan de pruebas. Además, la OGP generará informes periódicos de seguimiento del proyecto y será el interlocutor del adjudicatario con la DGPCE.
   La OGP se mantendrá activa tras la entrega del sistema RAN-PWS, durante la primera fase del periodo de operación y mantenimiento del sistema, al menos hasta la fecha de entrada en vigor de la obligación del artículo 110 del Código (Junio de 2022).

4.3 REQUISITOS DEL SISTEMA

El sistema RAN-PWS cuya puesta en marcha es el objeto de este contrato deberá cumplir los siguientes requisitos:

4.3.1 Arquitectura del sistema

RA1. Arquitectura del sistema RAN-PWS
El sistema desplegado se ajustará a la arquitectura de alto nivel descrita en el apartado 3.2.

RA2. Arquitectura del CBC

La solución de CBC deberá adaptarse a la arquitectura que se muestra con algo más de detalle en la Figura 3: el CBC se organizará con una arquitectura de tres capas que garantice una separación entre las capas de acceso (conexiones internas a la red de acceso del operador, por un lado, y conexión con el CBE externo por otro lado), la capa de la lógica de servicio, y la capa de datos.

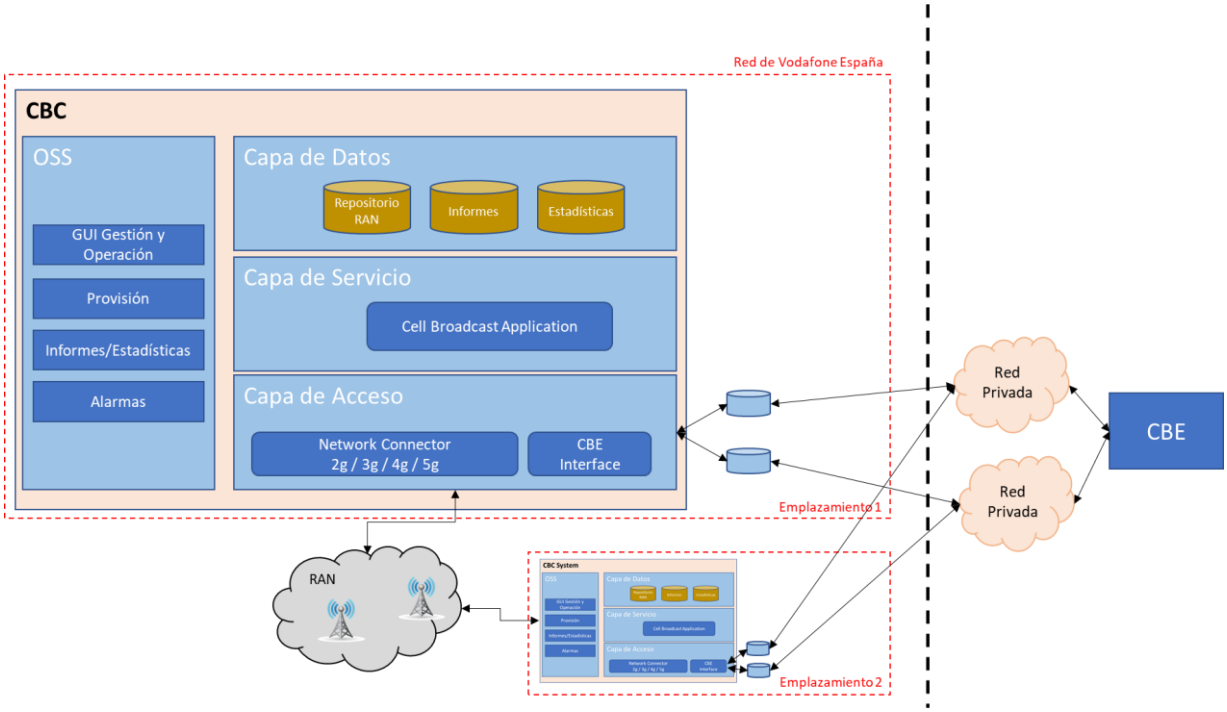

Fig 3. Arquitectura del CBC

4.3.2 Requisitos funcionales

4.3.2.1 Funcionamiento del CBE:

RF1. Creación de la alerta
El sistema dispondrá de dos interfaces para la introducción de los datos de las alertas a publicar:

a. Interfaz de usuario: permitirá la definición, a través de opciones de menú, de una nueva alerta, o la modificación de una alerta definida previamente. Una vez completada la introducción de los datos será posible guardar la alerta (en estado inactivo) para su revisión posterior, o bien activar la alerta, o eliminarla del sistema
b. Interfaz de aplicación: mediante un mecanismo *web service* o equivalente será posible la creación de una nueva alerta a partir de los datos recibidos desde un sistema remoto. El interfaz de aplicación implementará el protocolo CAP 1.2 de OASIS.
Las alertas definidas por esta vía se activarán automáticamente

RF2. Opciones del interfaz de usuario

El interfaz de usuario se ejecutará sobre un navegador estándar, sin necesidad de instalación de módulos adicionales. El acceso se realizará usando protocolos seguros para la autenticación y autorización.

El interfaz permitirá la introducción, a través de formulario o similar, de los parámetros de la alerta descritos en el apartado 3.3.1. Para facilitar la tarea de introducción de los datos este interfaz deberá permitir:

- Selección de la criticidad de la alerta entre los niveles disponibles en el sistema
- Selección de la zona afectada a partir de una librería de zonas. Esta librería incluirá por defecto, como zonas predefinidas, todos los límites administrativos de España (Comunidades

Autónomas, Provincias, Ayuntamientos). Será posible añadir nuevos conjuntos de zonas predefinidas (conocidas como *geocodes*) a través de opciones de administración del sistema
- Alternativamente, se podrá definir la zona de afectación, desde cero o a partir de una zona predefinida, haciendo uso de una herramienta de edición de zonas que permita su visualización y modificación sobre un mapa
- Los mapas mostrados para la definición de la zona afectada podrán ser complementados, a elección del usuario, con capas adicionales de información geográfica, que deberán estar accesibles a través de servicios WMS externos y/o ficheros GIS (raster o vectoriales) existentes en el sistema
- Selección del mensaje de alerta a partir de una librería de mensajes predefinidos
- Los mensajes predefinidos deberán disponer de versiones en, al menos, todas las lenguas oficiales de España y en Inglés
- Al seleccionar uno de los mensajes predefinidos existirá la opción de incluir hasta tres versiones del mensaje (por ejemplo, en catalán, castellano e inglés) en el texto de la alerta
- Alternativamente, se podrá definir el mensaje de alerta, desde cero o editando uno de los mensajes predefinidos
- Selección de los canales por los que se debe difundir la alerta. Inicialmente estarán disponibles y activados por defecto los canales: CBC, página web y, si está disponible, aplicación móvil

RF3. Activación de la alerta
El sistema permitirá la activación manual de una alerta que haya sido definida a través del interfaz de usuario (las alertas generadas a través del interfaz de aplicación se activarán automáticamente). La activación, manual o automática, generará un mensaje que se enviará a los usuarios supervisores que hayan sido definidos en el sistema para el ámbito del organismo que ha definido la alerta, y al administrador del sistema RAN-PWS. La alerta quedará en estado Activada.

RF4. Confirmación de alerta
El sistema permitirá a los usuarios con permisos de supervisor confirmar las alertas que se encuentren activadas en el ámbito de su competencia. Existirá un perfil de administración de alertas que podrá confirmar cualquier alerta activada en el sistema.

Una vez recibido el número de confirmaciones requeridas, se producirá el envío de la información de la alerta a los CBC y a los demás mecanismos que hayan sido definidos en el sistema para su difusión.

Será posible configurar, para cada ámbito definido en el sistema, el número mínimo de confirmaciones a recibir para que la alerta pueda ser enviada.

RF5. Publicación de alertas
El CBE enviará las alertas, en el momento de su confirmación, a una página web de acceso público en la que se mostrarán todas las alertas en vigor. Será posible incluir, dentro del texto del mensaje de alerta, un enlace a esta página web para facilitar el acceso a esta información.

Si la oferta incluía una aplicación móvil, las alertas se publicarán también a través de este medio.
La página web y, en su caso, la aplicación móvil, se considerarán como un mecanismo adicional de difusión de alertas a la población.

Las interfaces entre el CBE y los sistemas de publicación de alertas (página web y aplicación móvil en su caso) usarán protocolos estándar de modo que puedan ser utilizados por herramientas de terceros con autorización de la Administración.

RF6. Seguimiento de alertas
El sistema permitirá, a través de una Consola de Control, hacer un seguimiento del estado y evolución de las alertas a partir de su activación: quién y cuándo las definió, las activó y las confirmó.

Una vez confirmadas se podrá acceder a la información disponible en el sistema (procedente de los CBC o de otros sistemas de difusión de alertas) relativa al estado de la difusión de la alerta.

RF7. Consola de operación del CBE
La consola de operación del CBE permitirá, además de las acciones descritas en los requisitos RF2 y RF6, las necesarias para acceder a toda la información relevante sobre el funcionamiento del sistema:
- monitorización de todos los módulos de la aplicación, incluyendo la conexión con los CBC
- acceso al estado y evolución de los indicadores claves de rendimiento (KPI) del sistema
- acceso a los registros del sistema

RF8. Consola de administración del CBE
La consola de administración del CBE permitirá realizar, además de las opciones disponibles en la consola de operación:
- gestión de usuarios del sistema
- acceso, con capacidad de modificación, a todas las opciones de configuración del sistema

RF9. Registro de actividad del CBE
Todos los sucesos y actividades relevantes realizados sobre el sistema CBE se registrarán en un archivo especial (Registro del Sistema) que almacenará información suficiente (fecha y hora, usuario, actividad, etc) que permita verificar a posteriori los detalles de cualquier acción realizada sobre el sistema.

Los siguientes aspectos del registro deberán ser configurables:
- contenido: qué acciones y sucesos se registran, y cuáles no
- formato: qué campos deben registrarse, y en qué orden deben mostrarse
- retención: periodo de tiempo para el que se deben conservar los datos, y tratamiento a realizar sobre los datos antiguos

4.3.2.2 Funcionamiento de los CBC:

RF10. Comunicaciones CBE - CBC
La comunicación entre el CBE y los CBC, en lo que respecta al envío de alertas, se ajustará también al protocolo CAP 1.2. En particular se tendrá en cuenta la especificación ATIS-0700008 - CELL BROADCAST ENTITY (CBE) TO CELL BROADCAST CENTER (CBC) INTERFACE SPECIFICATION.

Existirá además un flujo de información desde los CBC al CBE para dar visibilidad, en el CBE, sobre el estado de los CBC y la situación de las alertas recibidas en ellos.

RF11. Conexión del CBC a las redes de telefonía móvil
Para difundir los mensajes de alerta recibidos desde el CBE, el CBC deberá integrarse con todos los módulos controladores de red de las distintas tecnologías, BSC (2G), RNC (3G), MME (4G) y AMF (5G), de los que disponga el operador independientemente del número, fabricante, modelo y versión de cada uno de ellos.

Para asegurar la integración con estos elementos de la red de acceso del operador, el CBC deberá soportar los siguientes protocolos en la medida en que sean de aplicación:
- 3GPP TS 48.049, "Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface

specification"
- 3GPP TS 23.041, "Technical realization of Cell Broadcast Service (CBS)"
- 3GPP TS 25.324, "Broadcast/Multicast Control (BMC)"
- 3GPP TS 29.168, "Cell Broadcast Centre interfaces with the Evolved Packet Core; Stage 3"
- 3GPP TS 44.012, "Short Message Service Cell Broadcast (SMSCB) Support on the Mobile Radio Interface"
- 3GPP TS 22.268, "Public Warning System (PWS) requirements"
- 3GPP TS 23.038, “Alphabets and language-specific information”
- 3GPP TS 27.005, "Use of Data Terminal Equipment - Data Circuit terminating Equipment (DTE-DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS)"
- ETSI TS 102.900, “EU-ALERT using the Cell Broadcast Service”

RF12. Soporte de “RAN Sharing”
El CBC deberá soportar arquitecturas de redes "RAN Sharing" de modo que los nodos de red compartidos entre varios operadores se comporten, en cuanto a la difusión de los mensajes de alerta, igual que lo harían si hubiera nodos independientes para cada operadora.

Los interfaces CBC-BSC (Cb) y CBC-RNC (Iu-BC) serán comunes para los nodos BSCs y RNCs que se comparten en el modelo de RAN Sharing.

RF13. Soporte de IP/SCTP para MME
La conectividad del CBC con los nodos MME deberá ser IP/SCTP utilizando el interfaz SBc, y deberá soportar la característica multi-homing de SCTP.

El CBC deberá soportar la arquitectura de agrupación de MME (varios controladores MMEs que gestionan la misma lista de eCellids).

RF14. Tipo y tamaño de los mensajes
El sistema CBC deberá soportar de manera nativa el envío de los tipos (texto o binario) y longitudes de mensaje (hasta 15 páginas de 93 caracteres) definidos en los estándares y protocolos de aplicación.

RF15. Mapa de coberturas
Para ser capaz de determinar los elementos de red que deben ser activados para que el mensaje recibido se difunda por toda el área indicada en el mensaje de alerta, el sistema CBC deberá mantener un mapa de coberturas de todas las celdas de la red de acceso del operador en sus diferentes tecnologías.

Deberá existir un mecanismo de actualización periódica (diariamente si no se indica otro) de esta información de cobertura a través de la recepción de ficheros generados por el operador. Los ficheros estarán preferiblemente en formato texto o CSV y se recibirán mediante el protocolo de intercambio de ficheros SFTP.

El formato de los ficheros y el protocolo de comunicaciones serán comunes para todos los CBC y se acordarán entre el proveedor y todos los operadores antes de comenzar el despliegue del sistema.

RF16. Lógica de selección de celdas
El CBC implementará una lógica de selección de celdas que asegure que se minimiza el número de terminales situados dentro del área de afectación que no reciben el mensaje de alerta ("falsos negativos").

Simultáneamente se intentará minimizar también el número de terminales situados fuera del área de afectación que sí reciben el mensaje ("falsos positivos").

En los casos en los que no sea factible reducir ambos números simultáneamente (por ejemplo en las zonas limítrofes del área afectada) prevalecerá el criterio de minimizar los falsos negativos.

RF17. Tamaño de las áreas de alerta
El CBC deberá ser capaz de definir un área geográfica tan pequeña como la que pueda ser definida por una única celda de la red del operador.

El CBC deberá ser capaz de definir un área geográfica tan grande como la que defina la red completa del operador en territorio español.

RF18. Terminales receptores de la alerta
El CBC deberá enviar los mensajes de alerta recibidos desde el CBE hacia todos los dispositivos móviles que se encuentren en el área de afectación indicada en el mensaje y que estén registrados en la red del operador, incluyendo los siguientes:

- los que se encuentren en situación de itinerancia ("roamers")
- todos los que, perteneciendo a otro operador, se encuentren compartiendo la red de acceso del operador en modo "RAN sharing"
- todos los pertenecientes a operadores móviles virtuales que se conecten a la red de acceso del operador.

Todos ellos en cualquiera de las tecnologías de red desplegadas en la red del operador.

RF19. Funcionamiento autónomo de los CBC
Los CBC funcionarán de forma totalmente integrada con la red de cada operador, de modo que no será necesaria ninguna intervención manual para la difusión de la alerta una vez recibida en el CBC.

RF20. Proceso de alertas en paralelo
Los CBC serán capaces de procesar y gestionar múltiples alertas en paralelo, con o sin solapamiento en sus áreas de afectación.

RF21. Información sobre el estado de la difusión
Los CBC mantendrán, durante el tiempo en que se mantenga activa la alerta, toda la información relativa a su estado de difusión: relación de celdas ya activadas, y de las pendientes de activar, número de repeticiones enviadas, tiempo previsto de finalización, etc. Esta información será transmitida al CBE para facilitar el control de la difusión de la alerta.

RF22. Consola de operación del CBC
La consola de operación del CBC permitirá el acceso a toda la información relevante sobre el funcionamiento del sistema:

- monitorización de todos los módulos de la aplicación, incluyendo la conexión con el CBE y con los elementos de la red de acceso del operador, hasta nivel de celda
- acceso al estado y evolución de los indicadores claves de rendimiento (KPI) del sistema
- acceso a los registros del sistema

RF23. Consola de administración del CBC
La consola de administración del CBC permitirá realizar, además de las opciones disponibles en la consola de operación:

- gestión de usuarios del sistema

- acceso, con capacidad de modificación, a todas las opciones de configuración del sistema

RF24. Registro de actividad del CBC
Todos los sucesos y actividades relevantes realizados sobre el sistema CBC se registrarán en un archivo especial (Registro del Sistema) que almacenará infomación suficiente (fecha y hora, usuario, actividad, etc) que permita verificar a posteriori los detalles de cualquier acción realizada sobre el sistema.

Los siguientes aspectos del registro deberán ser configurables:
- contenido: qué acciones y sucesos se registran, y cuáles no
- formato: qué campos deben registrarse, y en qué orden deben mostrarse
- retención: periodo de tiempo para el que se deben conservar los datos, y tratamiento a realizar sobre los datos antiguos

4.3.2.3 Requisitos de los sistemas de publicación de alertas

RF25. Accesibilidad
El adjudicatario se compromete a cumplir las obligaciones relativas a accesibilidad que se derivan del Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

En concreto, la página web y la aplicación móvil opcional que se describen en el requisito RF5 deberán ser desplegadas de acuerdo a las especificaciones del Real Decreto citado, y las acciones de seguimiento y control del cumplimiento de los requisitos que se detallan en el mismo deberán ser realizadas como parte de la operación y mantenimiento del sistema durante el periodo en que este mantenimiento esté vigente.

Adicionalmente, la empresa adjudicataria hará uso de la herramienta gratuita puesta a disposición por el Observatorio de Accesibilidad Web (OAW) para evaluación automática de los criterios básicos de accesibilidad. De esta forma, la empresa adjudicataria se cerciorará del cumplimiento mínimo de dichos criterios, debiendo presentar los resultados de dicha evaluación a la DGPCE.

4.3.3 Requisitos de instalación

RI1. Plazos
El sistema completo, formado por el CBE y los cuatro CBC, deberá estar instalado y funcionando de acuerdo con las especificaciones indicadas en los puntos 4.3.1 y 4.3.2 en un plazo de 4 meses desde la firma del presente contrato.

RI2. Ubicaciones
El CBE se instalará en un Centro de Proceso de Datos (CPD) designado por la DGPCE en Madrid. Se desplegará una instalación de respaldo, con capacidad de suplir el funcionamiento de la instalación principal, en otro de los CPD del Ministerio del Interior.

Los CBC se instalarán en los CPD que designen las Operadoras de Telefonía Móvil, contando cada uno de ellos con una ubicación alternativa, que deberá estar situada en un edificio distinto y a una distancia de al menos 5km de la ubicación principal.

Todas las ubicaciones estarán en territorio español.

RI3. Equipamiento e Infraestructuras

El adjudicatario proveerá el equipamiento hardware y software básico para que los sistemas de información desplegados puedan funcionar de manera autónoma, con la mínima dependencia posible de otros sistemas y servicios ajenos al RAN-PWS. En concreto, el adjudicatario proveerá e instalará en las ubicaciones indicadas arriba:

- Servidores redundantes para el alojamiento de los servicios (que se ejecutarán, salvo excepciones, sobre máquinas virtuales) con el software mínimo requerido para su funcionamiento (hipervisor, sistema operativo, etc)
- Almacenamiento redundante (cabinas de discos en configuración RAID-5 o alternativa equivalente)
- Conectividad de red a nivel 2, con conmutadores redundantes
- Elementos de bastionado (firewalls) para proteger la conexión con los sistemas externos

Las infraestructuras que se pondrán a disposición del sistema RAN-PWS por parte de los titulares de los CPD en los que se aloje son:

- Servicios básicos: alimentación eléctrica, aire acondicionado, protección contra incendios, control de accesos
- Espacio físico: para, como máximo, un nuevo rack en cada CPD
- Conectividad a nivel 3, para el acceso a otras redes según sea necesario

RI4. Características de los equipos hardware del sistema RAN-PWS

Los equipos provisionados como parte del sistema RAN-PWS quedarán como propiedad de la Administración General del Estado, que podrá ceder su uso a los operadores de telefonía, según sea necesario para asegurar la prestación del servicio de avisos a la población.

RI5. Características del software del sistema RAN-PWS

Tras la instalación del sistema RAN-PWS, la Administración General del Estado quedará en posesión de licencias perpetuas para el uso de todo el software que haya sido instalado como parte del sistema, incluyendo software de virtualización, sistemas operativos, sistemas de gestión de bases de datos y los distintos componentes software de CBE y CBC.

Las licencias de uso del software podrán ser cedidas para su uso por los operadores según sea necesario para asegurar la prestación del servicio de avisos a la población.

RI6. Acceso a redes de comunicaciones

La provisión del acceso de los componentes del sistema RAN-PWS (específicamente, el CBE y los CBC) a las redes de comunicaciones que sean necesarias para su operación corresponderá al titular de la ubicación en la que se instalen estos componentes. En particular, se proporcionará el acceso a:

- redes administrativas, utilizadas para el acceso al CBE a través del interfaz de usuario o de aplicación
- red de interconexión que se defina para el enlace entre CBE y CBC
- redes de acceso de los operadores en las que se integrarán los CBC

El adjudicatario configurará los módulos del sistema RAN-PWS para hacer uso de los accesos proporcionados y demostrará su correcto funcionamiento por los medios que considere oportunos, pero no tendrá la obligación de asegurar el funcionamiento de sistemas de terceros (por ejemplo, sistemas de gestión de emergencias que envíen alertas al CBE a través del interfaz de aplicación, o módulos de comunicaciones usados por las operadoras para la difusión de las alertas a través de sus redes).

RI7. Requisitos específicos relativos a la instalación de CBE y CBC

Debido a las características especiales de criticidad y alta disponibilidad de los servicios que se prestan en las ubicaciones en las que se desplegarán el CBE y los CBC, además del cumplimiento de los requisitos de instalación reflejados en este apartado será preceptivo el cumplimiento de los requisitos específicos de instalación que se detallan en el Anexo I de este PPT.

4.3.4 Requisitos de seguridad

RS1. Seguridad desde el diseño
La arquitectura del sistema y sus mecanismos de operación cumplirán los requisitos de seguridad requeridos en función de la criticidad de la información gestionada por el sistema. En este punto se seguirán las directrices del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).

RS2. Bastionado y seguridad de entornos
Con independencia de los posibles sistemas de seguridad perimetral pre-existentes en los CPD en los que se instalen los componentes del RAN-PWS, el adjudicatario incluirá en su oferta, configurará e instalará los elementos de bastionado (separación de entornos, firewalls a nivel de red y de aplicación, etc) y de seguridad interna (actualizaciones de seguridad, antivirus, etc) que sean necesarios para garantizar que el sistema permanece protegido en todo momento contra amenazas informáticas de cualquier procedencia.

RS3. Copias de seguridad
El sistema contará con un mecanismo para la realización de copias periódicas de la información contenida en él, asegurando que éstas se conservan en una ubicación diferente al CPD principal en el que se aloja el sistema. Las copias de seguridad deberán servir tanto para recuperar información del sistema que se pierda o se corrompa por cualquier motivo, como para volver a poner en funcionamiento el sistema tras un fallo catastrófico.

RS4. Comunicaciones seguras
Las comunicaciones de entrada al CBE (interfaz de usuario e interfaz de aplicación) estarán protegidas en cuanto a autenticación, integridad de los mensajes y confidencialidad mediante protocolos SSL/TLS y certificados X.509 o equivalentes. Lo mismo aplica a las comunicaciones entre CBE y CBCs.

La definición, generación y activación de los certificados necesarios estarán incluidas en las tareas del adjudicatario como parte del proceso de instalación y puesta en marcha del sistema.

RS5. Control de acceso al sistema
El control del acceso físico a los sistemas será responsabilidad del titular de la ubicación en la que se instalen éstos. El control de acceso lógico será definido e implantado por el adjudicatario.

El control de acceso lógico deberá utilizar mecanismos seguros de autenticación, preferiblemente basados en el sistema Cl@ve 2 de la Administración General del Estado.

El control de acceso a través de la interfaz de aplicación estará basado en certificados, de modo que solo se autorice el acceso a las aplicaciones cliente que presenten un certificado reconocido.

RS6. Autorización y Permisos
Una vez comprobada la identidad del usuario y otorgado acceso al sistema, este tendrá los permisos asignados por el administrador del sistema.

La gestión de permisos será independiente para cada componente: el CBE y cada uno de los CBCs tendrá su propio administrador del sistema responsable de la gestión de los permisos en su ámbito, para lo que dispondrá de una consola de administración con interfaz gráfico que facilite la gestión tanto de los usuarios como de sus permisos.

Dentro del CBE los permisos tendrán dos componentes:

- Nivel de privilegio, que definirá el nivel de criticidad de las tareas que el usuario puede realizar: consulta de datos, creación de alertas, activación y cancelación de alertas
- Área de competencia, que definirá el territorio para el que el usuario puede realizar las tareas permitidas por su nivel de privilegio. Por ejemplo, un usuario que tenga asignada como área de competencia el territorio de una comunidad autónoma no podrá definir o autorizar alertas que afecten a una zona que se extienda más allá de los límites de dicha Comunidad

RS7. Trazabilidad
Las acciones realizadas por cada usuario del sistema, y los eventos críticos de comunicaciones relativos a la recepción y envío de los mensajes de alerta, quedarán recogidos en un registro de actividades del sistema que deberá contar con medidas especiales de salvaguarda y control de accesos. El acceso a este registro requerirá de permisos especiales, también otorgados por el administrador.

RS9. Requisitos específicos relativos a la seguridad de los CBC
Debido a las características especiales de criticidad y exposición a riesgos de ciberseguridad de los servicios que se prestan por las operadoras de telefonía, que se verán afectados por el despliegue de los CBC en sus redes de comunicaciones, además del cumplimiento de los requisitos de seguridad reflejados en este apartado será preceptivo el cumplimiento de los requisitos específicos de seguridad que se detallan en el Anexo II de este PPT.

4.3.5 Requisitos de garantía de funcionamiento

RG1. Garantía de equipos hardware
Los equipos desplegados como parte del sistema estarán cubiertos por una garantía de sus fabricantes que garantice la sustitución o reparación de cualquier componente que deje de funcionar de acuerdo a sus especificaciones. Esta garantía del fabricante deberá permanecer en vigor durante todo el plazo de garantía ofertado por el adjudicatario para el sistema RAN-PWS.

RG2. Vida útil de equipos hardware
Los equipos instalados deberán tener un plazo de fin de soporte publicado por el fabricante superior al periodo de garantía ofertado para el sistema, y en todo caso igual o superior a cuatro años.

Los equipos que por cualquier circunstancia sobrevenida queden sin soporte del fabricante antes de finalizar el periodo mencionado deberán ser sustituidos por el adjudicatario del contrato como parte de la garantía del sistema, sin ningún coste para el titular de la instalación de CBE o CBC afectada.

RG3. Garantía del software
La garantía ofertada por los licitadores deberá incluir todas las actualizaciones de software necesarias para garantizar el correcto funcionamiento del sistema. Estas actualizaciones incluirán al menos los parches de seguridad y la corrección de los errores detectados en cualquiera de sus componentes.

RG4. Tiempos de respuesta
Los valores máximos admisibles, en cómputo mensual, de los tiempos de respuesta que se definen en el apartado 6.1.1 serán los siguientes:

	Atención	Intervención	Recuperación	Resolución
Incidencia Crítica	30 min	1 h	4 h	24 h
Incidencia No Crítica	4 h	12 h	24 h	96 h

El adjudicatario deberá calcular mensualmente el valor real de cada uno de estos parámetros a partir del registro de incidencias, verificando el cumplimiento de este requisito.

RG5. Número de incidencias
Los valores máximos admisibles, en cómputo anual, del número de incidencias que se reportan en el funcionamiento de cada componente del sistema (CBE y CBC) son los siguientes:

	CBE	CBC
Incidencia Crítica	1	1
Incidencia No Crítica	12	12

RG6. Requisitos para intervenciones sobre el sistema
Todas las tareas de reparación o actualización que sea necesario realizar para asegurar el correcto funcionamiento del sistema RAN-PWS, y que puedan afectar a la operación de las redes del titular de la instalación, deberán ser aprobadas por éste, y deberán solicitarse con antelación suficiente para evitar que interfieran con otras actividades o trabajos en la red.

Todas las tareas que puedan afectar a la operación de las redes del titular deberán validarse previamente en el entorno de pruebas del CBE/CBC.

RG7. Apoyo a la gestión de cambios en el alojamiento del sistema RAN-PWS
El adjudicatario valorará, a petición del titular de la instalación, el posible impacto sobre el funcionamiento del sistema RAN-PWS de cualquier cambio previsto en la infraestructura sobre la que se aloja el sistema o en los sistemas con los que se comunica.

Si alguno de estos cambios resultara en la necesidad de realizar adaptaciones menores en el sistema RAN-PWS, el adjudicatario deberá proporcionar el soporte necesario para su realización.

5. CONDICIONES DE LA EJECUCIÓN Y ENTREGA DEL SISTEMA

5.1 Interlocución

Como interlocutor del adjudicatario ante la Administración, con responsabilidad sobre la totalidad del proyecto, el adjudicatario nombrará a un Supervisor del Programa (SP) para la implantación del sistema RAN-PWS. Todas las comunicaciones relativas a aspectos de coordinación y gestión del proyecto se realizarán entre el SP y el Director Técnico (DT) del Proyecto designado por la DGPCE.

Las comunicaciones entre la DGPCE y el Adjudicatario para informar sobre la evolución de la ejecución del proyecto o sobre actuaciones concretas, solicitar intervenciones, notificar incidencias, etc se realizarán, cuando no se requiera una respuesta inmediata, preferentemente por medios que permitan dejar constancia de la comunicación, como el correo electrónico. Se limitará el uso del teléfono a las comunicaciones de carácter urgente.

5.2 Oficina de Gestión del Proyecto

El adjudicatario pondrá a disposición del proyecto una oficina de gestión del proyecto (OGP), encargada de la definición y mantenimiento del plan general de proyecto y de sus planes parciales, del seguimiento de todas las actividades, y la generación de informes de progreso. La OGP será además responsable de la coordinación con los participantes en todas las tareas que requieran su participación, incluyendo la definición de los detalles de operación de los sistemas, la coordinación para el acceso a las instalaciones, la realización de pruebas, etc.

Las comunicaciones de la OGP irán dirigidas al DT y al SP, de modo que cualquier acción que sea necesario tomar pueda discutirse entre éstos de manera ágil.

La DGPCE tendrá la potestad de decidir las actuaciones a acometer en respuesta a los problemas detectados, que serán ejecutadas por el adjudicatario.

5.3 Hitos y Entregables

En el momento de la formalización del contrato, el adjudicatario proporcionará todos los datos de contacto para asegurar la interlocución y el acceso a la información sobre el estado del proyecto.

Como máximo dos semanas después de la formalización, el adjudicatario presentará un plan de proyecto con los principales hitos que permitan su seguimiento durante la fase de despliegue del sistema. Estos hitos deberán incluir al menos los que se indican a continuación.

En un plazo no superior a tres meses tras la formalización del contrato, el adjudicatario deberá haber completado la instalación básica, en sus ubicaciones definitivas, del CBE y de los cuatro CBC. En este momento será posible realizar las pruebas unitarias de cada uno de estos sistemas, aunque no se exigirá que en este punto se puedan probar las comunicaciones entre ellos, o con sistemas externos. Tampoco será exigible en este punto la existencia de sistemas redundantes para asegurar la alta disponibilidad de los sistemas.

Al final del cuarto mes de ejecución del contrato se habrán probado los interfaces (de usuario y de aplicación) de entrada de datos del CBE, así como las comunicaciones entre CBE y CBC.

A la finalización del plazo fijado para la entrega del sistema el adjudicatario habrá completado la conexión entre todos los sistemas que componen el RAN-PWS, incluyendo las pruebas de integración, y habrá demostrado el correcto funcionamiento de las comunicaciones con los sistemas externos. En particular, se habrá verificado el funcionamiento completo del sistema en conexión con todas las tecnologías de red (2G, 3G, 4G y 5G) en uso por las operadoras.

En este punto se deberán haber completado también las instalaciones de los sistemas redundantes que aseguren la alta disponibilidad de la solución.

El Adjudicatario facilitará en el momento de la entrega del sistema toda la documentación relativa a:

- La arquitectura del sistema, con todos los componentes desplegados en cada ubicación, sus parámetros básicos, y las funciones que realizan
- El esquema de red y comunicaciones del sistema, incluyendo el detalle de los protocolos utilizados para cada intercambio de información
- Manuales de usuario del sistema
- Manuales de operación del sistema

- Manuales de mantenimiento básico del sistema

Esta documentación se entregará en castellano y se mantendrá actualizada, incluyendo todos los cambios y actualizaciones que se vayan incorporando al sistema, durante todo el plazo de garantía que se acuerde como parte del presente contrato.

5.4 Documentación

El adjudicatario del contrato deberá preparar y entregar en el momento de la entrega del sistema al menos la siguiente documentación relativa a la instalación:

- Arquitectura del Sistema y de sus componentes CBE y CBC
- Listado de todas las plataformas/nodos que lo componen y los modelos y versiones utilizados (p.e. hardware, sistema operativo, middleware, aplicaciones, bases de datos, etc)
- Detalle de todos los interfaces y protocolos utilizados con otros sistemas o apliaciones
- Diagrama detallado de toda la infraestructura de red
- Matriz de comunicaciones que describa toda la conectividad del sistema
- Esquema de todas las bases de datos usadas por el sistema
- Detalle de los interfaces, de usuario o de aplicacion, usados por el sistema en sus comunicaciones con elementos externos
- Listado de ficheros de configuración, con explicación detallada de cada parámetro (uso, valores válidos y valor por defecto, mecanismos de modificación, etc)

El adjudicatario del contrato deberá preparar y entregar en el momento de la entrega del sistema al menos la siguiente documentación relativa a la operación del sistema:

- Descripción del funcionamiento de todos los módulos que componen el sistema, la interacción de cada módulo con los demás, y con elementos externos
- Flujo básico de información para cada caso de uso típico del sistema
- Acceso a parámetros del sistema, PKI, y alarmas
- Detección básica de errores y procedimientos básicos de recuperación

El adjudicatario del contrato deberá preparar y entregar en el momento de la entrega del sistema al menos la siguiente documentación relativa a la administración del sistema:

- Procedimiento de consulta y modificación de los parámetros del sistema
- Procedimientos de gestión de usuarios
- Procedimientos y buenas prácticas para la monitorización del estado del sistema, y para su actualización en caso necesario
- Procedimientos de apagado, reinicio, restauración, etc
- Listado de todas las alarmas definidas en el sistema, su significado y posibles acciones a tomar en caso de que ocurran

El adjudicatario del contrato deberá preparar y entregar en el momento de la entrega del sistema al menos la siguiente documentación relativa a la seguridad del sistema:

- Descripción de las medidas y mecanismos de seguridad disponibles en las diferentes capas o niveles del sistema (aplicación, red y base de datos)
- Detalle sobre cómo se protege la información sensible cuando se transmite internamente entre los componentes del sistema
- Descripción de las medidas y mecanismos de seguridad que se aplican para proteger las conexiones entre el CBE/CBC y los sistemas o redes externas

El adjudicatario del contrato deberá preparar y entregar en el momento de la entrega del sistema al menos la siguiente documentación relativa a los perfiles de usuario:

- Procesos de gestión de cuentas de usuario (creación, borrado, modificación de permisos, etc.)
- Detalle sobre el repositiorio de cuentas de usuario
- Descripción de los diferentes perfiles de usuario utilizados y su correspondiente caso de uso para el que se requieren
- Detalle de las cuentas no personales necesarias (p.e. 'root' o 'admin')
- Detalle de los mecanismos de autenticación y autorización disponibles (p.e. single-sign-on, 2-factor-Authentication - 2FA, certificados, etc.)

Se entregarán manuales de uso de los procedimientos de instalación del sistema (desde cero o desde copia de seguridad), actualización y vuelta atrás de nuevas versiones o parches de software.

Se entregarán manuales de operación y mantenimiento básico del sistema. Estos manuales incluirán información sobre buenas prácticas y procedimientos habituales derivados de la experiencia del proveedor con el uso de su sistema en distintos entornos y con diversos elementos de red de distintos fabricantes (problemas habituales, procedimientos de reinicio de equipos, etc).

La documentación del sistema proporcionada se mantendrá permanentemente actualizada (mediante liberación de nuevas versiones y notas de actualización de la documentación) durante todo el periodo de garantía del sistema.

5.5 Formación

El adjudicatario de esta licitación deberá organizar un curso de capacitación inicial para el personal del Ministerio del Interior y de cada una de las operadoras en las que se instarán los CBC (se contemplarán como mínimo 12 asistentes por curso). La formación deberá incluir:

- Explicación completa de todas las características y posibilidades de configuración del sistema ajustándose a la arquitectura y particularidades de la implantación realizada
- Flujo de servicios (incluido el aprovisionamiento)
- Procesos y procedimientos en la operación y mantenimiento (incluida monitorización y alarmados)

Los cursos de formación deben ofrecerse en español. Las sesiones de formación se realizarán preferiblemente en las instalaciones designadas por cada titular.

Durante los seis primeros meses tras la puesta en funcionamiento del sistema, el proveedor pondrá a disposición de cada titular un servicio de acompañamiento ("babysitting") para la realización de las tareas de operación del sistema y formación adicional en el puesto de trabajo.

6. GARANTÍA DEL SISTEMA

Se fija un plazo de garantía del sistema desplegado de dos años a partir de la fecha de recepción. Los licitadores podrán ofertar la ampliación de este periodo en hasta dos años más, hasta un máximo de cuatro años. Durante este periodo de tiempo el adjudicatario del contrato será responsable del correcto funcionamiento del sistema, según las especificaciones detalladas en este documento.

6.1 Características de la garantía

Durante todo el plazo de garantía la DGPCE y los usuarios que esta designe deberán poder establecer contacto con el adjudicatario para reportar cualquier problema que se detecte en el funcionamiento del sistema. Para ello el adjudicatario proporcionará los datos de contacto (teléfono, correo electrónico y, si está disponible, página web) para el registro de incidencias y peticiones relativas al funcionamiento del sistema RAN-PWS.

El acceso a este sistema de reporte de incidencias/peticiones estará abierto a personal autorizado de la Administración (para el CBE) y de cada uno de los operadores (para los CBC). La DGPCE tendrá acceso que le permita visualizar el estado de todas las incidencias del sistema.

El adjudicatario proporcionará también una matriz de escalado de las incidencias para dar visibilidad a su tratamiento desde el momento en que son reportadas.

Además de este sistema informático de registro y seguimiento de incidencias, el adjudicatario nombrará a un responsable de atención al sistema con el que la DGPCE podrá ponerse en contacto en cualquier momento.

Para asegurar la respuesta ágil a las incidencias que se produzcan, el adjudicatario deberá disponer de los medios técnicos, materiales y humanos que considere necesarios para asegurar el funcionamiento continuado de los sistemas entregados, y garantizar que el personal encargado de la operación del sistema dispone de toda la información necesaria de mando y control.

La respuesta a las incidencias se prestará en idioma español.

Para minimizar los tiempos de resolución, los medios necesarios de respuesta deberán encontrarse suficientemente próximos a las ubicaciones en las que se instalarán el CBE y los CBC de modo que, cuando sea necesario, sea posible el acceso a ellas con retrasos mínimos. En concreto se deberá asegurar que el tiempo de traslado a cualquiera de las ubicaciones del sistema no excede de los límites de tiempo indicados para la Intervención en respuesta a incidentes (requisito RG4).

Para facilitar la resolución de ciertas incidencias se podrán desplegar, siempre con autorización de los titulares de las ubicaciones en las que se aloja el sistema, mecanismos de acceso remoto entre la sede del adjudicatario y las ubicaciones del CBE y los CBC.

Periódicamente, y cuando se considere necesario por haberse producido alguna incidencia relevante, se mantendrán reuniones de seguimiento de las incidencias, para el análisis de las causas de los problemas detectados de modo que se minimice la probabilidad de que vuelvan a ocurrir.

6.2 Parámetros de calidad de funcionamiento del sistema

Durante el plazo de garantía del sistema RAN-PWS el adjudicatario, en cumplimiento de sus responsabilidades sobre la calidad del funcionamiento del sistema RAN-PWS, se compromete a responder a todas las incidencias que se reporten sobre este funcionamiento. Este compromiso, para ser efectivo, debe poder ser medido de una forma objetiva. Para ello se definen dos tipos de parámetros: por un lado los tiempos de respuesta a las incidencias (que deben ser lo más bajos posibles para minimizar posibles pérdidas de servicio del sistema), y por otro lado el número total de incidencias que se produzcan (que también deben minimizarse).

Los requisitos relativos a las características y funcionamiento de la garantía, que se detallan en el

apartado 4.3.5 de este documento, incluyen los valores máximos aceptables para ambos tipos de parámetro, distinguiendo entre dos tipos de incidencia según su afecto sobre el funcionamiento del sistema:

- Incidencia crítica: la que afecta al funcionamiento básico del sistema, de modo que su finalidad (el envío de mensajes de alerta a la población) no puede ser cumplida. Las incidencias críticas pueden ser totales (por ejemplo, el CBE no permite generar alertas) o parciales (por ejemplo, uno de los CBC no responde)
- Incidencia no crítica: cualquiera que no afecte al funcionamiento básico del sistema (por ejemplo, si no es posible dar de alta a nuevos usuarios)

6.2.1 Tiempos de respuesta:

Se consideran cuatro tiempos diferentes en la respuesta a las incidencias:

- Tiempo de atención: el transcurrido entre la notificación de la incidencia y la recepción de la primera respuesta
- Tiempo de intervención: el transcurrido desde la notificación de la incidencia hasta el momento en que un técnico es asignado y comienza a trabajar para su resolución
- Tiempo de recuperación del servicio: el transcurrido desde la notificación de la incidencia hasta el momento en que el servicio de difusión de alertas vuelve a estar operativo (posiblemente en modo degradado, o con menores garantías de resistencia ante nuevos fallos)
- Tiempo de resolución: el transcurrido desde la notificación de la incidencia hasta el momento en que el sistema vuelve a su estado previo, con plena operatividad

El requisito RG4 especifica los valores máximos permisibles para cada uno de estos tiempos, según la criticidad de la incidencia.

6.2.2 Número de incidencias:

El requisito RG5 especifica el número máximo de incidencias reportadas anualmente, también en función de su criticidad.

6.3 Alcance de la garantía

Las actividades y obligaciones del adjudicatario descritas en este apartado se limitarán exclusivamente a asegurar que el sistema suministrado funciona correctamente, de acuerdo con las especificaciones de este documento, durante el plazo fijado de garantía. El adjudicatario no está obligado a realizar otras tareas propias del mantenimiento del sistema como revisiones periódicas, seguimiento de los parámetros de funcionamiento, o actualizaciones que no sean requeridas por razones de seguridad o fallos de funcionamiento.

Aunque el servicio de mantenimiento no está incluido en la presente contratación, los licitadores presentarán una propuesta de mantenimiento del sistema con la descripción de los servicios incluidos y su coste anual estimado. Esta propuesta servirá como referencia para la posible futura contratación de este tipo de servicio.

7. DERECHOS Y OBLIGACIONES DE LAS PARTES

7.1 Transferencia de tecnología

El contratista estará obligado a facilitar a las personas designadas por la DGPCE la información y documentación necesarias para disponer de un pleno conocimiento técnico de las circunstancias en que se desarrollarán los trabajos de despliegue y puesta en marcha, de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

El adjudicatario estará obligado a ofrecer toda la ayuda necesaria en la transferencia de conocimiento a la DGPCE o a las partes que ésta designe con el fin de asegurar la continuidad del funcionamiento del sistema tras su puesta en funcionamiento. El adjudicatario deberá aportar un plan en el que se incluirán la documentación y formación que se describen en el apartado 5 de este pliego como parte integrante de esta transferencia.

El conocimiento a transferir contemplará entre otros: información de la situación actual del sistema, explicación de la documentación entregada, infraestructura hardware y software, instalación del entorno para el funcionamiento, credenciales de acceso, relación de incidencias conocidas y medidas adoptadas para su resolución, riesgos identificados y procedimientos operativos asociados.

7.2 Propiedad Intelectual

La Administración obtendrá mediante la ejecución de este contrato licencias permanentes de uso del sistema, en las condiciones que se detallan en el requisito RI5 del apartado 4.3.3 de este PPT.

La propiedad intelectual de los sistemas informáticos desplegados como consecuencia de la ejecución del presente contrato permanecerá en poder del adjudicatario.

No obstante lo anterior, el adjudicatario depositará el código fuente, las librerías necesarias para la compilación del sistema, y todos los scripts y herramientas necesarias para su instalación y puesta en marcha bajo la custodia de un tercero, en el lugar y a través del acuerdo que le parezca más oportuno. El acuerdo de custodia deberá permitir a la Administración obtener acceso a esta información exclusivamente en el caso de que, en una futura licitación del servicio de mantenimiento del sistema, el adjudicatario no quiera o no pueda proporcionar este servicio en condiciones de precio y prestaciones similares a las de la propuesta de mantenimiento incluida en la oferta.

Si se diera esta situación la Administración adquiriría el derecho de modificar, adaptar y actualizar, por sí o por un tercero, dicho código para asegurar la continuidad del servicio que proporciona el sistema RAN-PWS.

En Madrid, a 1 de Julio de 2021

Fernando Prieto Fernández
Vocal Asesor

ANEXO I. REQUISITOS ESPECIALES DE INSTALACIÓN

0. Generalidades

0.1 Todo proveedor que tome parte en este proceso de licitación deberá incluir en el proyecto de implantación presentado como parte de su oferta técnica el grado de cumplimiento (Total, Parcial, Ninguno) de su propuesta para cada uno de los requisitos que se incluyen en este documento.
Se podrá incorporar una breve explicación, además del grado de cumplimiento, cuando sea necesaria para aclarar o delimitar alguna característica del sistema.

0.2 Los licitadores que requieran cualquier tipo de información relativa a las instalaciones y redes sobre las que deberá realizarse la instalación del sistema, o sobre los procedimientos de acceso y gestión de dichas instalaciones, podrán dirigirse por escrito al órgano de contratación a través de los medios de contacto disponibles en la Plataforma.
El órgano de contratación hará llegar la consulta a las entidades titulares de las instalaciones ("los titulares") sobre las que se solicita información, y tomará las medidas necesarias para asegurar que la respuesta pertinente se proporciona en un plazo razonable.
En este proceso, para el acceso a ciertos tipos de información se requerirá a las empresas la firma de un acuerdo de confidencialidad.

0.3 A partir de la firma del contrato, el adjudicatario se compromete a tratar de forma confidencial toda la información sobre los titulares y sus instalaciones a la que tenga acceso como consecuencia de la realización de las tareas del contrato.

1. Arquitectura

1.2. Elementos HW y SW

1.2.1 Todo proveedor que tome parte en este proceso de licitación deberá incluir una descripción detallada de todos los componentes hardware que componen su solución y su configuración recomendada

1.2.2 Los sistemas CBE y CBC se instalarán preferiblemente sobre infraestructura virtualizada. Si el proveedor lo justifica, y esto no tiene impacto en la disponibilidad del sistema, el sistema podrá ser instalado sobre infraestructura hardware dedicada (*bare metal*)

1.2.3 El adjudicatario del contrato proveerá todos los componentes hardware de la solución de CBE y CBC, sea virtualizada o no. Estos componentes deberán ser desplegados como una entidad física autocontenida que se conectará a la red del titular a través de una interfaz bien definida.

1.2.4 Si la solución hardware estuviera basada en infraestructura virtualizada, el proveedor deberá proporcionar el detalle completo del software de virtualización utilizado así como un inventario detallado de todas las máquinas virtuales necesarias y los recursos requeridos por cada una de ellas.

1.2.5 En caso de despliegue sobre infraestructura virtualizada, a elección del titular los componentes de la instalación del CBE/CBC se podrán desplegar integrados dentro de su infraestructura de virtualización, o en una infraestructura separada.
En cualquiera de los dos casos el proveedor deberá facilitar todo el hardware y las licencias de software de virtualización necesarios para el funcionamiento del sistema.

1.2.6 El proveedor deberá describir todos los componentes software de la solución (Hipervisor de Virtualización, Sistema Operativo, Base de Datos, Servidor de Aplicaciones y cualquier otro componente software) y los correspondientes requisitos para su correcto funcionamiento

1.2.7 Los proveedores proporcionarán la descripción de la interfaz de conexión de los sistemas instalados con la red del titular en la forma de una matriz de comunicación que defina las conexiones necesarias que deben configurarse entre el sistema desplegado y los elementos / entidades de la red.

1.2.8 La conectividad de los CBC con la red del operador, incluyendo las conexiones con los nodos de la red de acceso (BSC/RNC/MME/AMF), estará basada en interfaces IP

1.2.9 La solución deberá utilizar la pila IPv4 para las comunicaciones. Deberá existir también la opción de usar IPv6, que será activada si el titular lo indica antes del comienzo del despliegue.

1.2.10 La solución ofertada no incluirá ninguna restricción técnica o limitación de capacidad que no sean sus límites de HW. Los sistemas CBE y CBC no verán limitada su capacidad de proceso de mensajes de alerta en ningún momento por alguna licencia de software u otras limitaciones que no sean de HW.

1.2.11 La solución implementada será escalable en recursos hardware, de modo que cualquier incremento en la capacidad requerida del sistema pueda quedar cubierto añadiendo elementos hardware (servidores, memoria, disco) a la instalación existente, sin necesidad de reemplazar ningún componente del sistema.

1.2.12 Todos los componentes hardware incluidos en la solución ofertada tendrán garantía del fabricante que incluya soporte 24x7 durante un periodo de al menos 2 años.

1.3. Alta Disponibilidad

1.3.1 El CBE y cada uno de los CBC deberán desplegarse en dos localizaciones geográficas diferentes designadas por cada titular. Las dos instancias, o nodos, de CBE/CBC resultantes estarán debidamente sincronizadas y serán completamente independientes una de la otra, de manera que un fallo en una de ellas no impactará en el funcionamiento y operación de la otra.

1.3.2 La arquitectura del nodo principal del CBE/CBC no podrá contar con puntos únicos de fallo, a nivel de equipamiento hardware, alimentación eléctrica, refrigeración, interfaces de red, y módulos software.

1.3.3 El almacenamiento de la información del sistema contará con sistemas de replicación de información y tolerancia a fallos tanto en los discos como en las conexiones a ellos.

1.3.4 En caso de cualquier incidencia software o hardware, el segundo emplazamiento debe ser capaz de operar el servicio con todas las garantías de rendimiento y capacidad. Los proveedores deberán describir la solución ofertada de alta disponibilidad y redundancia geográfica, indicando los tiempos estimados de recuperación del servicio en el emplazamiento de respaldo ante un fallo del emplazamiento primario.

1.3.5 Se deberá garantizar que no se requiera intervención manual para conmutar el servicio en caso de fallo. Los proveedores deberán describir los procedimientos de conmutación y recuperación automática del servicio aplicado a varios escenarios de fallo posibles.

1.3.6 La propuesta deberá incluir una solución técnica para el caso de los elementos de la red de acceso del operador que no soporten múltiples conexiones con el nodo CBC.

1.4. Tolerancia a fallos

1.4.1 Todos los componentes del CBE/CBC susceptibles de ello (fuentes de alimentación, ventiladores, interfaces de red, unidades de almacenamiento, etc) deberán estar redundados y configurados para la activación automática en caso de fallo en uno de los componentes.

1.4.2 El CBC deberá ser capaz de mostrar información del estado de todos los controladores de radio de la red del operador y de sus celdas.

1.4.3 El CBC deberá mantener una continua comunicación con los controladores de la red BSC/RNC/MME/AMF. Los fallos de conexión que se detecten deberán reportarse como alarmas del sistema.

1.4.4 Ante fallos de conexión con los elementos de red, el sistema deberá realizar intentos automáticos de reconexión.

1.4.5 El CBC debe contar con una herramienta o mecanismo que permita comprobar manualmente la disponibilidad de las conexiones con los elementos de la red del operador, incluidas las estaciones de radio (mínimo), y con los dispositivos móviles (deseable)

1.5. Entornos

1.5.1 Tanto la solución CBE como los CBC desplegados deberán incluir entornos separados para Pruebas y Producción.

1.5.2 Los entornos de pruebas deberán permitir ensayos, verificaciones y validaciones del funcionamiento de los componentes del sistema sin que ello impacte en el rendimiento del sistema en producción. Las pruebas deberán contemplar al menos los siguientes escenarios:
- Probar actualizaciones, parches o nuevas funcionalidades en software o hardware
- Probar actualizaciones, parches o nuevas funcionalidades de sistemas remotos (CBE o CBC), cuando afecten al interfaz de comunicaciones CBE - CBC
- Probar actualizaciones, parches o nuevas funcionalidades en nodos de red: BSC, RNC, MME o AMF
- Realizar pruebas de carga y rendimiento del sistema
- Probar el funcionamiento de los mecanismos de alta disponibilidad, tanto en el propio nodo (balanceo de servicios, en modo local y con el centro de respaldo remoto) como por cambios que se produzcan por balanceo en sistemas remotos (CBC, CBE o nodos de la red del operador)

1.5.3 Además de las capacidades ofrecidas por el entorno de pruebas, el sistema deberá permitir la realización de ensayos y simulacros de envío de mensajes, con o sin difusión real a terminales particulares, en el entorno de producción. Estos simulacros harán uso de los componentes de los sistemas de producción y de los elementos de red utilizados para dar el servicio.

2. Instalación y Puesta en Servicio

2.1. Compromiso de actuación

2.1.1 Todo proveedor que tome parte de este proceso de licitación debe garantizar que tanto el proceso de instalación y despliegue del CBE/CBC como su operativa una vez entre en servicio, no comprometerá la estabilidad de las redes del titular, y que no se producirá ningún impacto negativo en el servicio por estos motivos.

2.1.2 Todo proveedor que tome parte en este proceso de licitación deberá proponer un plan de despliegue y un procedimiento de aceptación del sistema para cada una de las instalaciones de CBE/CBC previstas. Tras la adjudicación del contrato, estos procedimientos deberán ser revisados y acordados entre el adjudicatario y cada uno de los titulares.

2.1.3 En los procedimientos concretos de colaboración entre proveedor y titulares que se definirán al comienzo del proceso de despliegue se seguirán los siguientes principios básicos:
a. Serán a cargo del proveedor todas las actividades de suministro, instalación y pruebas unitarias de todos los componentes del sistema CBE/CBC
b. Serán a cargo del titular de las instalaciones en la que se realiza el despliegue las tareas de incorporación a su infraestructura de los nuevos elementos instalados (por ejemplo, instalación de nuevos cuadros eléctricos, actualización del sistema de gestión de inventario, incorporación de alarmas al sistema de monitorización, archivado y gestión de copias de respaldo, etc)
c. En todos los puntos de conexión entre la nueva infraestructura desplegada y la instalación pre-existente (por ejemplo, alimentación eléctrica, conexión a la red de datos, envío de alarmas, etc) proveedor y titular deberán cooperar activamente para asegurar la rápida resolución de cualquier discrepancia
La DGPCE, como Directora del Proyecto de despliegue del RAN-PWS, actuará de árbitro en cualquier conflicto que aparezca en relación a este requisito.

2.1.4 Todo proveedor que tome parte en este proceso de licitación se comprometerá a colaborar estrechamente con los proveedores de los nodos de las redes de acceso de los operadores para realizar las pruebas de conectividad que sean necesarias, trabajando con dichos proveedores para la corrección de los problemas que pudieran aparecer y generando los correspondientes informes de las pruebas de interoperabilidad realizadas.

2.1.5 El estudio de la compatibilidad de los terminales móviles con los protocolos y mensajes de Cell Broadcast está fuera del alcance de este proyecto.

2.2. Tareas de Instalación

2.2.1 El adjudicatario de este contrato será responsable de la instalación de todos los componentes hardware de su solución, debiendo coordinar con el titular de cada alojamiento los detalles de ubicación física, conexión a alimentación eléctrica, necesidades de refrigeración y demás aspectos que deban ser aplicados. Para ello el adjudicatario deberá generar una propuesta inicial de replanteo que especifique los componentes, características y necesidades previstas de la instalación que servirá de base para la coordinación entre las partes.

2.2.2 La necesidad o no de provisión de un bastidor para instalar los componentes del CBE/CBC, y sus características, incluyendo las posibles fuentes de alimentación (PDU), deberá ser acordada con el titular del alojamiento del sistema.

2.2.3 El adjudicatario de este contrato será responsable de establecer la conexión a la red de datos del titular de todos los componentes del CBE/CBC, usando cableado propio o proporcionado por el titular, a elección de éste. Los interfaces de conexión (tipo de conector y de cable) y parámetros de red (velocidad de transmisión de datos, direcciones, rutas, etc) deberán ser acordados con el titular del alojamiento.

2.2.4 Todos los nodos que formen parte del sistema del CBE/CBC deberán contar con al menos tres interfaces IP diferenciados para su conexión a las siguientes redes:
- Red de Servicios (para gestión del tráfico propio del servicio), que se podrá desdoblar en varias:
  . Red de conexión con la Administración, para la conexión CBE - CBC
  . Red de acceso, para la conexión del CBC con los elementos de red del operador
  . Red de operación, para la conexión a los interfaces de consola de administración y operación
- Red de Gestión (para la operación y mantenimiento del nodo, incluyendo copias de seguridad)
- Red de Consola (conexión al puerto serie para tareas de administración del nodo)

2.2.5 El direccionamiento IP de todos los componentes de la solución será asignado por el titular.

2.2.6 Las conexiones del CBE/CBC a la red del titular se realizarán, a elección de este, por uno de los mecanismos siguientes:
- conexión directa desde los interfaces de red de los servidores desplegados a los conmutadores/enrutadores de la red del titular
- conexión desde conmutadores que estarán incluidos en el sistema desplegado. Las características y la configuración de estos conmutadores serán revisadas y aprobadas por el titular para garantizar la ausencia de riesgos sobre la operación de su red

2.2.7 Todos los servidores desplegados como parte del CBE/CBC deberán contar con puerto de red de consola (conexión para tareas de administración del nodo, incluyendo encendido/apagado, consulta de estado y acceso al registro de logs)

2.2.8 Todas las tareas de instalación se tendrán que planificar dentro de ventanas de mantenimiento. El proveedor necesitará la aprobación del titular para realizar estas actividades, que deberán solicitarse con antelación suficiente para no interferir con otras actividades o trabajos en la red.

2.2.9 El adjudicatario deberá encargarse de la limpieza y correspondiente traslado para su posterior eliminación como corresponda de todos los residuos y materiales desechables que se hayan producido como consecuencia del proceso de instalación.

3. Entrega del Sistema

3.1. Pruebas de aceptación

3.1.1 El proveedor deberá facilitar un documento con la descripción de todos los casos de prueba que se ejecutarán para el proceso de aceptación de los sistemas CBE y CBC. Para cada caso de prueba, se detallarán todos los pasos a ejecutar y los resultados esperados. El titular revisará el plan y podrá modificar algún aspecto de las pruebas propuestas y agregar pruebas específicas.

3.1.2 Cuando la infraestructura hardware se encuentre desplegada se procederá, de manera conjunta con el equipo técnico del titular, a validar el correcto funcionamiento de los equipos y a realizar la aceptación física de la instalación.

3.1.3 Una vez que el sistema CBC haya sido configurado y ajustado para dar servicio se realizarán las pruebas de conexión del sistema con los elementos de la red de acceso del operador. Para este fin el proveedor usará el entorno de pruebas del CBC y el operador pondrá a disposición del proyecto los equipos y entornos de prueba necesarios, incluyendo elementos de red, celdas y terminales cliente.

3.1.4 Una vez superadas las pruebas de conexión en el entorno de pruebas, se realizarán pruebas equivalentes en el entorno de producción.

3.1.5 Una vez completadas las pruebas de conexión de los CBC con los elementos de las redes de acceso, se procederá a realizar las pruebas de integración del sistema, en el que deberá demostrarse el funcionamiento conjunto del CBC con el CBE, y con elementos reales de la red de acceso del operador.

3.1.6 Se realizarán pruebas de carga del sistema, en principio usando el entorno de pruebas y, si es asumible por los operadores, en el entorno de producción.
Para cada caso de prueba previsto se detallará previamente la tipología de tráfico a generar y la carga máxima que está previsto alcanzar.

3.1.7 El conjunto de las pruebas realizadas deberá asegurar que se verifican al menos los siguientes aspectos de la instalación:
- funcionalidad de CBE y CBC acorde con las especificaciones
- intercambio de datos CBE - CBC
- comunicaciones con los elementos de la red de acceso del operador
- rendimiento del sistema (número de mensajes, cobertura territorial, tiempos de respuesta) adecuados al funcionamiento previsto del sistema
- no afectación a otros servicios de los titulares, y en particular a los servicios de la red de acceso del operador
- generación de eventos y alarmas del sistema cuando se dan las condiciones para ello
- generación y visualización de los KPI
- verificación del funcionamiento de todos los mecanismos de redundancia del sistema
- restauración parcial y total del sistema desde copia de seguridad

4. Operativa de Funcionamiento del Sistema

4.1. Procedimientos de actualización y restauración

4.1.1 Los procedimientos de actualización del CBE y del CBC deberán ser validados previamente en los entornos de pruebas, y no deben requerir una parada perceptible del servicio (mayor de unos pocos minutos). La duración de los trabajos de actualización no será superior a 6h en total.

4.1.2 El procedimiento de restauración del CBE y CBC, en caso de ser necesario, estará sujeto a las mismas restricciones, respecto a la parada del servicio y al tiempo total necesario, que el procedimiento de actualización.

4.1.3 Los procedimientos de instalación y de restauración del CBE y CBC se realizarán con un usuario del sistema dedicado. Este usuario debe ser diferente de "root" para los sistemas UNIX y de "Administrador" para los sistemas de Microsoft.

4.1.4 Los procedimientos de instalación y de restauración deben probarse paso a paso en los entornos de pruebas antes de su ejecución en el entorno de producción.

4.2. Monitorización y medida del rendimiento

4.2.1 Los sistemas CBE y CBC deberán proporcionar un conjunto de indicadores o KPIs claramente definidos y medibles para supervisar la disponibilidad, el rendimiento, la capacidad, la congestión, la calidad del servicio, las condiciones de carga, etc.
Los KPIs y eventos deben tener, para el CBC, granularidad mínima a nivel de celda.

4.2.2 El proveedor debe proporcionar pautas sobre el rango de valores que deben cubrir los KPIs para asegurarse de que el sistema esté en buen estado.

4.2.3 La tasa o frecuencia con la que deben calcularse estos KPI debe ser configurable (como mínimo cada 5 minutos)

4.2.4 Las consolas de operación de CBE y CBC tendrán la capacidad de mostrar de forma permanente los valores de los KPIs recogidos o calculados en las últimas horas, con su evolución, y con una comparación con los valores de referencia.

4.2.5 Igualmente los valores de los KPIs se archivarán en un fichero que será accesible desde la red del titular para su uso, si este lo considera necesario, en sus sistemas de monitorización. El proveedor debe proporcionar la sintaxis del fichero o interfaz a través del cual se harán disponibles los datos de KPIs.

4.3. Alarmas del Sistema

4.3.1 Los sistemas CBE y CBC en producción deberán generar alarmas de funcionamiento (distintas de los mensajes de alerta cuya transmisión a la población es el objeto del sistema), con diferentes niveles de criticidad, que se mostrarán en la consola de operación del sistema, y se enviarán, a través de traps SNMP/syslog, al servicio que determine el titular.

4.3.2 La plataforma debe proporcionar un conjunto de alarmas de funcionamiento del sistema sobre:
- Indisponibilidad de cualquier elemento de la aplicación
- Conectividad a otras aplicaciones y / o elementos de red
- Porcentaje de ocupación de discos por encima del umbral que se defina
- Problemas de replicación de la base de datos (si la plataforma tiene una capa de base de datos con un modo de replicación para el procedimiento de recuperación)
- Problemas en el mecanismo de replicación de clústeres

Será posible además definir alarmas del sistema relacionadas con umbrales de contadores específicos. El Proveedor proporcionará una lista de contadores y el umbral asociado sugerido para la monitorización del sistema con el fin de garantizar un nivel de calidad de servicio adecuado.

4.3.3 Cuando se produzca la condición de disparo de una alarma:
- se mostrará un mensaje de alarma claramente identificable en la consola de operación
- se registrarán los datos de la alarma en un archivo de registro del historial de alarmas
- se enviará uno o más traps SNMP/syslog con información sobre la alarma

4.3.4 Las alarmas se podrán configurar, incluyendo su activación/desactivación, nivel de criticidad y texto asociado, a través de parámetros de configuración del sistema.

4.3.5 Las alarmas activas se podrán reconocer y desactivar a través de la consola de operación.

4.3.6 Debe ser posible visualizar las alarmas actualmente activas y las alarmas históricas a través de consultas personalizables en la consola de operación.

4.3.7 Las alarmas (tanto activas como históricas) se deberán poder exportar en formato CSV.

4.4. Sincronización de tiempo

4.4.1 El Protocolo NTP (*Network Time Protocol*) para sincronización horaria de los equipos debe estar activado en el CBC con la configuración que defina el titular de la instalación.

4.4.2 En caso de que el servidor NTP envíe un valor de reloj incorrecto (es decir, con una diferencia de tiempo de la muestra anterior mayor a un umbral acordado), la plataforma debe desconectarse automáticamente del servidor NTP y continuar con el reloj local. Se debe dar una alarma en esta situación.

ANEXO II. REQUISITOS ESPECIALES DE SEGURIDAD

1. Características del Sistema

1.1. Diseño del Sistema

1.1.1 El CBC deberá aportar un diseño de la solución compatible con una arquitectura de 3 zonas básicas de seguridad y las correspondientes medidas de seguridad de acceso y privilegios.

1.1.2 El sistema deberá adaptarse, en la medida de lo posible, a todos los estándares que a nivel de seguridad se encuentren vigentes en las instalaciones del titular. Estos estándares se comunicarán al proveedor tras la adjudicación, previamente al comienzo de la implantación del sistema.

1.2. Robustecimiento de Protocolos

1.2.1 Todos los componentes del CBC, tales como Servidores Web, Sistemas Operativos, Bases de Datos, etc. deberán robustecerse de acuerdo a las mejores prácticas de seguridad.

1.2.2 La información de autenticación a los sistemas se transmitirá a través de un protocolo cifrado. No se permite la autenticación utilizando texto en "claro" sin cifrar.

1.2.3 El sistema o servicio del CBC debe proporcionar un número mínimo de servicios abiertos necesarios para la prestación del servicio.
Se podrá permitir el acceso por algún protocolo adicional (por ejemplo, ping) si su activación facilita la monitorización del sistema.

1.2.4 El CBC deberá utilizar protocolos encriptados para el intercambio de mensajes con sistemas o servicios remotos (por ejemplo: SSH y TLS).

1.2.5 El CBC deberá utilizar protocolos encriptados para la gestión y transferencia de archivos (por ejemplo: SSH y SFTP). En el caso de utilizar SFTP, se deberá usar un puerto diferente al que se usa para SSH.

2. Protección de Accesos

2.1. Autenticación y Autorización de accesos

2.1.1 El acceso de los usuarios del sistema CBC se realizará únicamente desde redes corporativas, nunca desde redes públicas.

2.1.2 Los usuarios no administrativos sólo podrán acceder a los servicios frontales del sistema (consolas de administración y de operación) y no deben tener acceso directo a ningún otro servicio.

2.1.3 Se mostrará un "banner" o aviso legal en todas las interfaces de usuario que permitan inicio de sesión interactivo (sistema operativo y aplicación) antes de la validación del usuario. El aviso deberá indicar que sólo los usuarios autorizados pueden acceder al sistema de acuerdo con las obligaciones legales. Se deberá considerar el idioma local (castellano - Español/España) y aquellas consideraciones legales aplicables en España.
La redacción no contendrá información sobre el propósito, la ubicación o el propietario del sistema/dispositivo o cualquier otra información de identificación

2.1.4 En el proceso de autenticación para acceder al sistema CBC se aplicará lo siguiente:
- Las contraseñas no se muestran mientras se ingresan en el sistema y no se transmiten en texto claro a través de la red.
- La información de inicio de sesión se valida sólo al completar todos los datos de entrada. Si surge una condición de error, el sistema no indicará qué parte de los datos es correcta o incorrecta.

2.1.5 Después de un máximo de 3 intentos de inicio de sesión fallidos secuenciales, la cuenta de usuario se bloqueará automáticamente durante un período definido (al menos 20 minutos). La acción generará una alarma SNMP y quedará reflejada en el Registro del sistema como evento crítico.

2.1.6 Después de iniciar sesión correctamente, la aplicación presentará la fecha, la hora y el resultado (es decir, éxito o fracaso) del último intento de inicio de sesión del usuario de una manera claramente visible.

2.1.7 El acceso a las consolas de operación y administración debe incluir un tiempo de expiración de la sesión tras superarse una cantidad configurable de minutos de inactividad (por ejemplo, 15 minutos).

2.1.8 A cada usuario con acceso al Sistema se le asignará un identificador de usuario único. Este valor no cambiará durante todo el ciclo de vida de la aplicación.

2.1.9 Cada cuenta de usuario estará protegida con una contraseña (u otra información secreta conocida solo por el usuario).

2.1.10 Los usuarios deberán cambiar su contraseña en el primer intento de inicio de sesión exitoso después de la creación de la cuenta o el restablecimiento de la contraseña.

2.1.11 Las contraseñas y contraseñas encriptadas no se escribirán en ninguna ubicación que sea accesible para usuarios no administrativos.

2.1.12 Los administradores no podrán leer las contraseñas de usuario en texto sin cifrar.

2.1.13 El sistema aplicará controles de seguridad de las contraseñas en línea con las buenas prácticas habituales respecto a longitud mínima, combinación de distintos grupos de caracteres (minúsculas, mayúsculas, números, etc), no repetición, caducidad, etc.
Los controles de seguridad serán configurables de manera sencilla por el administrador del sistema.

2.1.14 El sistema proporcionará un procedimiento de confirmación de cambio de contraseña para evitar errores de escritura del usuario

2.1.15 El sistema obligará al usuario a ingresar su contraseña actual así como su nueva contraseña al realizar un cambio de contraseña.

2.1.16 El CBC utilizará un modelo de acceso basado en roles o perfiles para administrar los permisos de los usuarios. Deben existir al menos los siguientes:
a) Administrador del sistema (puede modificar los parámetros del sistema)
b) Usuario del sistema (puede realizar operaciones funcionales)
c) Auditor (usuario con permiso de lectura únicamente)

2.1.17 El CBC no podrá hacer uso de contraseñas predefinidas o codificadas (por ejemplo, en el código fuente).

2.1.18 Las contraseñas se almacenarán de forma segura (p.e. en un formato hash). Sólo se utilizarán algoritmos diseñados específicamente para el almacenamiento de contraseñas (por ejemplo, bcrypt o PBKDF2).

2.1.19 El sistema deberá proporcionará al administrador la capacidad de desactivar o suspender cuentas de forma manual o automática, de forma que permita que se pueda cumplir con los criterios de seguridad más frecuentes, como haber excecido el período de inactividad, el abandono de la empresa o un cambio de función del usuario, etc.

2.1.20 El sistema proporcionará al usuario administrador la capacidad de mostrar todos los privilegios de acceso específicos del usuario.

2.1.21 Siempre que sea apropiado, el sistema deberá permitir restringir a los usuarios a establecer una sola sesión a la vez.

2.1.22 Si fuera necesario el uso de cuentas funcionales (cuentas utilizadas por scripts y procesos) se deben utilizar métodos de autenticación seguros, incluyendo el uso de contraseñas muy seguras (un mínimo de 15 caracteres aleatorios).

2.2. Seguridad del Interfaz de Aplicación

2.2.1 Las interfaces de aplicación a las que se pueda acceder desde redes externas, o desde zonas de la red interna con un nivel de seguridad inferior, se proporcionarán a través de un canal de comunicación seguro.

2.2.2 El acceso de aplicaciones cliente a través de los interfaces de aplicación requerirá un certificado SSL cliente con al menos la siguiente configuración:
a) emitido por una autoridad de certificación de confianza
b) X509 versión 3
c) la fuerza de la clave pública debe ser al menos de 2048 bits
e) Los certificados deben reemplazarse al menos cada 2 años a menos que superen los 4096 bits

2.2.3 Como protocolo de transporte se usará TLS 1.2 o superior.

2.2.4 Como protocolos de cifrado se usarán AES o Camelia.

2.2.5 Como algoritmo de hash se usará SHA-2 (se recomienda SHA-256)

2.2.6 El protocolo de intercambio de claves implementado deberá:
a) Generalmente usar intercambios de claves DH efímeros
b) Utilizarse al menos el parámetro Diffie-Hellmann de 2048 bits
c) Utilizarse el intercambio de claves RSA solo para clientes incompatibles con DHE o en caso de DHE por motivos de rendimiento
d) Desactivarse todos los demás intercambios de claves (por ejemplo, DH y ADH, ECDH)

2.2.7 Al implementar el canal SSL / TLS, se deben tomar las siguientes consideraciones:
a) Desactivar la compresión.
b) Habilitar la renegociación segura.
c) Desactivar la renegociación iniciada por el cliente.
d) Habilitar la reanudación de la sesión.
e) Seleccionar el cifrado compatible más seguro según las preferencias del servidor.

2.2.8 Los servicios web críticos se protegerán con firewalls de aplicaciones web.

2.2.9 Todas las aplicaciones e interfaces web deberán cumplir con la última versión de la "Guía de OWASP para la creación de aplicaciones web seguras" publicada por OWASP - "Open Web Application Security Project" (www.owasp.org).

2.2.10 Antes de la puesta en funcionamiento, las aplicaciones web podrán ser revisadas por el equipo de seguridad de los titulares de las instalaciones, que deberá contar con la colaboración del proveedor para la realización de las pruebas necesarias.

2.2.11 Se pondrán en marcha mecanismos para detectar y combatir ataques de denegación de servicio (DoS / DDoS).

2.2.12 El sistema estará protegido mediante mecanismos de detección de tráfico anómalo (por ejemplo, IDS, sondas IPS, etc.).

2.2.13 Todas las interfaces externas de aplicación deberán, directamente o mediante firewall de aplicación, controlar las solicitudes entrantes sintáctica y semánticamente antes de que sean procesadas por la aplicación. Esto incluye la comparación con las opciones permitidas y prohibidas esperadas, los tipos de campo, la longitud / tamaño, las estructuras y los estándares.

2.2.14 El interfaz de aplicación implementará un controlador de errores.
Los seguimientos de pila y otra información interna, como fragmentos de código, nombres de archivos o direcciones IP internas, no se revelarán a la entidad que llame al cliente del interfaz.

2.2.15 Cuando las interfaces estén expuestas a redes no confiables, deben restringir el acceso a direcciones IP especificadas y aprobadas mediante listas de control de acceso o similar.

3. Protección de Datos

3.1. Integridad de la Información

3.1.1 Los datos críticos del sistema se transmitirán junto con sumas de verificación (checksum) utilizando funciones "hash" potentes para garantizar la integridad de los datos durante la transmisión.

3.1.2 Todas las operaciones que modifiquen datos (por ejemplo, actualizar, eliminar, insertar) deben garantizar que no haya una etapa intermedia en la operación que pueda dar lugar a problemas de integridad de los datos. La operación debe de estar totalmente completada o totalmente incompleta.

3.1.3 Todos los procesos que reciban una entrada de datos (tanto manuales como automatizados) deberán controlar y validar los datos de entrada en términos de formato, longitud y sintaxis.

3.2. Copias de seguridad

3.2.1 Debe ser posible hacer una copia de seguridad de cada componente de la plataforma de forma manual o automatizada y sin necesidad de parada del sistema.

3.2.2 La frecuencia de las copias de seguridad automatizadas dependerá de la importancia de los datos:
- Para datos críticos, la copia de seguridad debe ser diaria.
- Para datos no críticos o estáticos, la copia de seguridad puede ser semanal o mensual.

3.2.3 El período de retención de las copias de seguridad será configurable.

3.2.4 El sistema de copias de seguridad aplicado al CBC aceptará conexiones SFTP desde un servidor externo de modo que sea posible, si el titular así lo indica, transferir las copias de seguridad a un sistema centralizado de gestión de copias de respaldo.

3.2.5 El sistema de copias de seguridad aplicado al CBC realizará, directamente o a través del sistema de copias de respaldo del titular copias remotas de la información de respaldo del sistema, que deberán ser accesibles desde las dos ubicaciones en las que esté desplegado el CBC.

3.2.6 Debe ser posible recuperar el sistema completo, en condiciones de ser puesto en producción inmediatamente, en caso de pérdida de datos o configuraciones a partir de la copia de seguridad local o remota.

3.3. Protección de Datos de Carácter Personal

3.3.1 Está prohibido procesar, transferir o almacenar datos de los entornos de producción en los entornos de pruebas. Si los datos de producción se van a utilizar en entornos no productivos, éstos se anonimizarán para enmascarar los datos confidenciales y personales. El proceso de anonimización utilizado se acordará con el departamento de Seguridad del titular.