Servicio de "PLATAFORMA HÍBRIDA PARA RTVE.ES"

Expediente S/01421/2021

Evaluación técnica

Índice	Página

1 Objetivo del documento

El presente documento evalúa las propuestas técnicas presentadas para el expediente S/01421/2021, "Plataforma Híbrida para RTVE.es". Para esta evaluación se han recibido dos propuestas técnicas, las de las empresas EVOLUTIO CLOUD ENABLER S.A.U. y la de NEXTRET, S.L.

Para la valoración técnica de las propuestas se tendrá en cuenta lo establecido en el Pliego de Condiciones Técnicas (PCT, en adelante) y en el Pliego de Condiciones Generales (PCG, en adelante). Las propuestas técnicas podrán obtener un máximo de 50 puntos, y de ellas se valorará *el detalle, la pertinencia y la precisión de la información aportada (PCG, pag.22)* en cada uno de los puntos siguientes que deben aparecer en dichas propuestas (PCG, pág. 22 y 23):

- *Plan de transformación: se otorgará 5 puntos al plan más robusto, viable, y que permita hacer la transformación en el menor tiempo posible, y la* ***idoneidad del equipo*** *propuesto al plan.*

- *La solución al almacenamiento y distribución de la media será valorada, otorgándose 15 puntos a la mejor propuesta. Es necesario incluir una estimación del tiempo estimado que se un video va a requerir para ser segmentado y distribuido. Este valor será luego exigido una vez instalado y en operación, y el adjudicatario estará obligado a, como mínimo igualarlo.*

- *Plan de adquisición del servicio: se otorgará 10 puntos al mejor plan de adquisición en términos de solidez, riesgo y pertinencia para el sector media.*

- *Modelo de aislamiento de tenants y DMZ: se otorgará 5 puntos a la arquitectura multi tenant, y, especialmente, a las capas de acceso, seguridad y aislamiento de la DMZ. El licitador tendrá que presentar el modelo de gestión de los tenants, así como los mecanismos de acceso y seguridad de la DMZ, y cómo se implementa el cierre perimetral y el acceso del personal propio de RTVE, así como los mecanismos de seguridad que protegen los activos digitales.*

- *Arquitectura general del servicio: se valorará con hasta 5 puntos a la mejor solución arquitectural. Para poder valorarla los licitadores han de entregar un esquema general de la arquitectura mostrando donde se ubica cada subservicio, así como las principales ventajas que a su juicio aportan sus diferentes soluciones arquitecturales, tratando de estar centradas en la casuística específica de RTVE y de sus prioridades para con la plataforma descritas como parte de este pliego.*

- *Propuesta arquitectura de Kubernetes: se valorará con 10 puntos la mejor propuesta de implementación del cluster Kubernetes, poniéndose especial énfasis en la implementación propuesta del modelo de integración continua multitenant y multi cloud, así como el conocimiento del equipo que lo gestionará. Igualmente, para la arquitectura de Kubernetes, se enumerarán las principales ventajas que a su juicio aporta su solución arquitectural, tratando de estar centrada en la casuística específica de RTVE y de sus prioridades para con la plataforma de Kubernetes descritas como parte de este pliego.*

Como se establece en el PCG, página 22, *se penalizará la falta de concreción, de información específica y de detalle. Además, se penalizará especialmente la falta de coherencia de la propuesta, incluso, la incoherencia entre cada uno de los criterios*.

Adicionalmente, y a efectos de evaluar la idoneidad del equipo propuesto, se utilizará únicamente la información presente en los currículos aportados por los licitadores dentro de las propuestas técnicas. Cualquier información que no haya sido aportada no será objeto de

valoración, y, en cualquier caso, y como se establece en el PCG, podrá ser objeto de penalización.

En lo que sigue, se analizará cada una de las propuestas entregadas. Para una mejor comprensión, y para poder hacer un análisis comparativo entre ofertas, para cada propuesta analizaremos el plan de transformación, la solución del almacenamiento, el plan de adquisición, el modelo de aislamiento, la arquitectura general y la propuesta de arquitectura de Kubernetes.

Para llevar a cabo la valoración las propuestas serán valoradas por:

- Personal de RTVE, formado por D. Juan Francisco Arévalo López Reina, Jefe de Unidad de Operaciones Digitales, y D. Israel Sánchez López, Responsable de Sistemas de la Unidad de Operaciones Digitales.
- Personal de la empresa INECO, que, en virtud del encargo para la Asistencia técnica de proyectos de RTVE Digital, en materia, entre otros, de Cloudificación, que cuenta con la asignación de D. Francisco Javier Polo Gómez, Consultor TIC con más de cuarenta años de experiencia en el sector media, y D. Rafael Hernández Núñez, Consultor TIC con más de treinta años de experiencia en proyectos de implantación de plataformas TIC.

2 EVOLUTIO CLOUD ENABLER S.A.U.

Tras el estudio de la propuesta técnica presentada por la empresa EVOLUTIO CLOUD ENABLER S.A.U. (Evolutio, en adelante) se procede a evaluar cada uno de los puntos.

1. Plan de transformación

El objeto del plan de transformación está delimitado por lo establecido en el PCT en el punto 3.2. que establece dos estadios: la migración de la media, y la migración del resto de servicios a microservicios. Es por ello que el plan ha de contemplar ambos escenarios, así como las restricciones, alcances y limitaciones para cada uno de ellos.

De hecho, en la pregunta 17 de los licitadores se incide en este aspecto (enviada el 13 de septiembre):

> *En PCP Anexo II Criterios técnicos de valoración subjetiva (Pag22) Se valora con 5 puntos el "Plan de Transformación": se otorgará 5 puntos al plan más robusto, viable, y que permita hacer la transformación en el menor tiempo posible, y la idoneidad del equipo propuesto al plan. El Plan de Transformación se refiere a la transformación de la media (1 dic 2021,* posteriormente modificado a tres meses tras la firma del contrato*) o a la transformación de servicios con fecha máxima de conclusión en 1-diciembre-2024?*

Contestación, el 16 de septiembre:

> *El alcance de la transformación de la plataforma se indica en el punto 3.2 del PCT, Evolución técnica de la plataforma. En él se indican dos estadios: la solución de la media, y el resto de servicios. La valoración técnica se hará teniendo en cuenta las dos transformaciones.*

La transformación de todas las aplicaciones de RTVE en microservicios servidos desde la nueva plataforma supone uno de los principales retos del proyecto. RTVE adjuntó el anexo técnico con el listado de las aplicaciones actuales susceptibles de ser transformadas. RTVE para el plan requiere que el adjudicatario sea responsable de todo el proceso de transformación, incluyendo todos los trabajos necesarios, desde el estudio de las aplicaciones a migrar, su parcelación en procesos, e incluso, la escritura o reescritura de todo el código necesario para transformar estas aplicaciones en módulos susceptibles de ser ejecutados en el cluster Kubernetes, teniendo en cuenta lo expuesto en el punto 3.2 del PCT:

- *Antes del 1 de diciembre de 2024 todos los servicios de RTVE tienen que ser microservicios. RTVE tiene que certificar cada uno de los microservicios, y, en ningún caso, es admisible una pérdida de funcionalidad, ni una degradación de los tiempos de respuesta. En caso de incumplimiento habrá unas penalizaciones de acuerdo a los ANS.*

- *Todos los trabajos que permitan convertir un servicio en microservicio han de ser ejecutados por el adjudicatario por sus propios medios. RTVE ha de colaborar dando documentación, y en la realización de planes de pruebas. En cualquier caso, es responsabilidad del adjudicatario la validación previa a la puesta a producción.*

- *En la propuesta del servicio de migración, los licitadores han de incluir:*
    - *Equipo técnico (con todos los currículos detallados, certificaciones, etc.)*
    - *Jefe de proyecto*
    - *Cronograma detallado de migración completo*
    - *Grado de concurrencia de trabajos*

  Toda esta información será valorada.

Tras la lectura de la propuesta destacamos:

- El licitador en su propuesta técnica plantea un proceso de transformación de las aplicaciones a microservicios en cinco etapas.

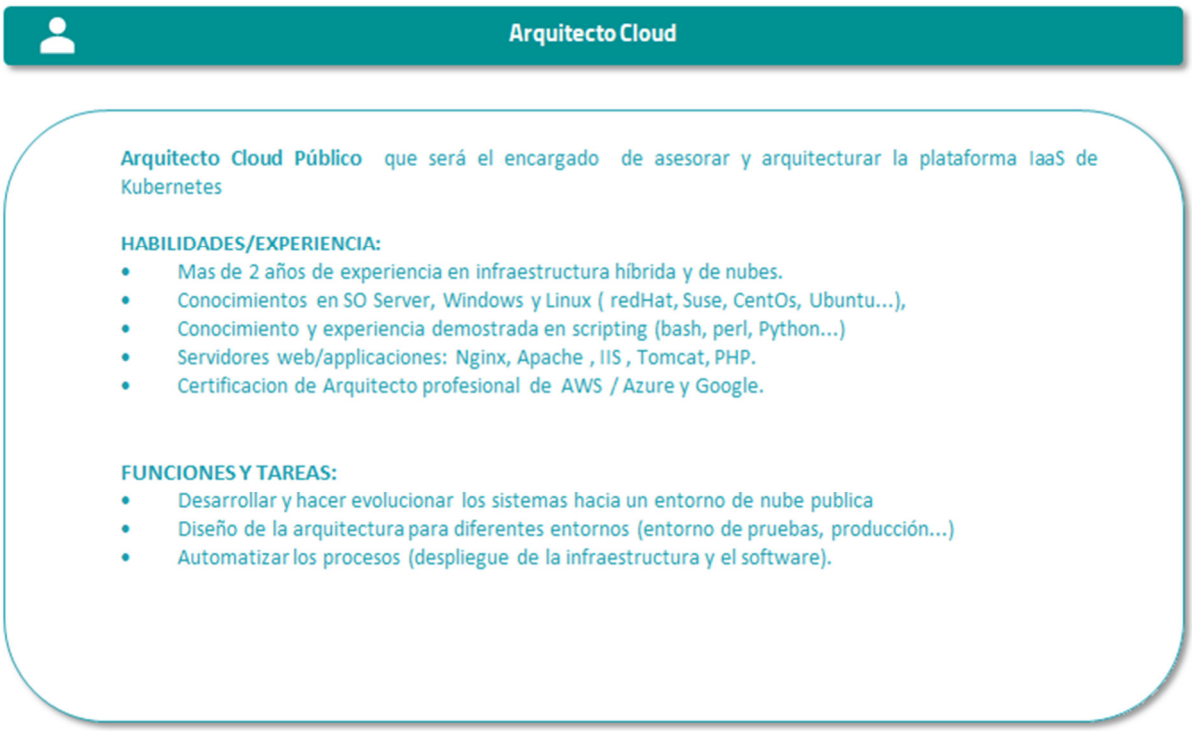
- Para agilizar y garantizar la migración a microservicios frente a problemas logísticos de entrega de material, el licitador indica en su propuesta que q*ueremos que una posible demora no previsible en el proyecto de transición genere una demora en la transformación (ver más detalle en apartado 2.7.1.6 Gestión de Riesgos de Transformación a Microservicios). Para esto en Evolutio hemos pensado en un plan de contingencia a llevar a cabo como parte del mismo proyecto desde el día 0, consistente en la preparación de un entorno de trabajo en laboratorio configurado dentro de la instancia Cloud de Evolutio, donde será posible ir avanzando tareas y sprints de transformación a microservicios de los servicios RTVE, a la espera de poder volcar todo lo trabajado en el entorno de desarrollo de la plataforma IaaS de RTVE*

- Respecto al equipo del Proyecto de transformación, Evolutio refiere que "*pondremos a disposición de RTVE un equipo multidisciplinario y orientado a las necesidades del cliente, formado por profesionales competentes tanto en las familias de tecnologías involucradas (nube, Kubernetes, microservicios, etc…), como en las habilidades directivas y de coordinación necesarias para llevar una transformación de este nivel"*.

Analizando con más detalle la propuesta, llama la atención que, aunque RTVE ha marcado lo crítico de la transformación y juzgando la información aportada, **ninguno** de los perfiles añadidos por el licitador **demuestra tener suficiente experiencia en infraestructura**

virtualizada y **ninguno menciona explícitamente experiencia alguna en entorno Kubernetes**.

Como ejemplo, el Arquitecto Cloud, cuyo detalle se muestra en el punto B.3.4 de la pág. 163 y cuya responsabilidad la describe Evolutio como "encargado de asesorar y arquitecturar IaaS de Kubernetes", **no presenta en su currículum experiencia o conocimiento alguno en esta tecnología, sino que muestra listados genéricos sin indicación de proyectos, años de experiencia, rol en cada proyecto, etc**. Esta forma de entregar y documentar los currículos lleva a una ausencia de información que, según establece el PCG, en la página 22, ha de ser penalizada.



El resto de perfiles aportados muestra una carencia similar.

Ante la posible falta de experiencia, el licitador indica que se apoyará en los servicios de un tercero con el que hará una subcontratación, tal y como expone en la página 4 de su oferta cuando dice que "*utilizará los servicios partner especializado en el desarrollo de aplicaciones en microservicios*". Pero, tampoco en este caso se da información que permita validar experiencia específica, en contra de lo exigido en el PCT. El hecho de utilizar a un tercero para unos trabajos técnicos **no exime al licitador** de tener que aportar detalles suficientes sobre la experiencia empresarial y el perfil de los técnicos que dicho partner haya acordado incorporar al acuerdo de servicio.

Respecto al plan de migración de la media presentado por el licitador, destaca el hecho de que éste no cumple con lo especificado en el PCT sobre las entregas. En concreto, el licitador indica que en un plazo de tres meses será capaz de tener disponible la instalación y puesta en funcionamiento de los elementos que conforman la solución de la media, pero, en este punto, el licitador confunde el alcance exigido: en tres meses se exige tener la solución de la media completa, no sólo el hardware, sino también toda la información migrada, sus backups, etc., y este hito, según lo establecido en la planificación entregada, el licitador lo ha previsto a los seis meses que es cuando plantea se haya movido todos los datos a la nueva infraestructura.

Sobre la solución de la media hay que tener en cuenta que:

1. *A efectos de esta licitación, la media que se va a segmentar ha de estar almacenada en la plataforma (p*ág. 7 del PCT*).*

2. *La solución tiene que estar operativa tres meses después de la firma del contrato (ACLARACIÓN 20S-01421-2021).*

3. *El licitador ha de prestar el servicio desde la nueva plataforma a los tres meses de la firma del contrato (ACLARACIÓN 20S-01421-2021).*

4. *En ningún caso será admisible que la solución para la distribución de media se provea utilizando las cabinas EMC que forman parte de la infraestructura actual de RTVE. Toda la distribución de media tiene que hacerse por medios del adjudicatario (pág. 18 del PCT).*

Por todo lo anterior, la planificación entregada por el licitador es inadmisible. Aceptar el planteamiento implica incumplir todos los hitos marcados en el PCT.

En el siguiente punto desarrollamos este aspecto de forma más amplia.

2. La solución al almacenamiento y distribución de la media:

La importancia de la toma de control, **urgente migración** y gestión de la Media se deja bien explícita desde los primeros puntos del PCT. En él se detalla lo siguiente:

- PCT, Punto 2 - Pag 5.- El servicio requerido debe… *proveer una solución de almacenamiento en los términos que se indican en este pliego, escalable y disponible de manera inmediata para RTVE.es*

- PCT, Punto 3.2 - Pag 14.- *Solución de la media: dados los problemas con el almacenamiento, y dado lo crítico que es la distribución de la media, se ha determinado una partida específica para toda la transformación de la media. La solución tiene que estar operativa el 1 de diciembre de 2021*.

  Respecto a la última frase de este último punto sobre la fecha de entrega de toda la transformación de la media, en nota aclaratoria publicada por RTVE con fecha 1 de octubre de 2021 se dice lo siguiente:

  > *"Ante la imposibilidad de adjudicar el contrato en la fecha inicialmente prevista, se comunica los siguientes cambios en las fechas de los siguientes puntos establecidos en el PCT:*
  >
  > *1.-Se modifica en la sección 3.2 página 14 el siguiente párrafo:*
  >
  > *Solución de la media: dados los problemas con el almacenamiento, y dado lo crítico que es la distribución de la media, se ha determinado una partida específica para toda la transformación de la media. La solución tiene que estar operativa el 1 de diciembre de 2021.*
  >
  > *Por esta otra redacción:*
  >
  > *Solución de la media: dados los problemas con el almacenamiento, y dado lo crítico que es la distribución de la media, se ha determinado una partida específica para toda la transformación de la media. La solución tiene que estar operativa tres meses después de la firma del contrato."*

Es decir, dado que la licitación se ha pospuesto sobre la fecha inicialmente prevista, en realidad el segundo de los puntos establece que **la Media debe servirse desde la nueva infraestructura como muy tarde tres meses después de la firma del contrato para este nuevo servicio**.

- PCT, Punto 4.2 – Pág. 18.- "*En ningún caso será admisible que la solución para la distribución de media se provea utilizando las cabinas EMC que forman parte de la infraestructura actual de RTVE. Toda la distribución de media tiene que hacerse por medios del adjudicatario*."

Incidiendo en este punto, en la respuesta dada el 16 de septiembre a la pregunta número 9, realizada tras la publicación del pliego por los potenciales licitadores, se dice:

> *"Pregunta 9: En el PPT Punto 4.2 Plataforma Legacy Propiedad RTVE (pag18), se comenta: En ningún caso será admisible que la solución para la distribución de media se provea utilizando las cabinas EMC que forman parte de la infraestructura actual de RTVE. Toda la distribución de media tiene que hacerse por medios del adjudicatario*
>
> *Querríamos confirmar si Se podrán utilizar las cabinas EMC durante el primer año del contrato?*
>
> *Enviada*
>
> *13/sep/2021*
>
> *Contestada*
>
> *16/sep/2021*
>
> *En el punto 4.2 del PCT, página 18 se establecen las condiciones de uso de la plataforma Legacy de RTVE. En ese epígrafe se establecen las restricciones al uso del hardware de RTVE, limitándose especialmente los casos en los que no será admisible el uso de la cabina EMC. El licitador podrá plantear una solución que use las cabinas siempre y cuando no incumpla lo indicado en el PCT."*

En otra respuesta dada el día 17 de septiembre a la pregunta número 10 se recalca que no podrá utilizarse el CPD de Prado del Rey en ningún caso:

> *"Pregunta 10: En el PPT Punto 4.2 Plataforma Legacy Propiedad RTVE (pag18) "Aunque el licitador tiene la obligación de ejecutar el contrato con su propio material, y como medida para facilitar la adquisición del servicio, y mitigar el riesgo para la continuidad del servicio de RTVE.es, RTVE posibilita el uso de hardware adquirido en el expediente 2015/10021 "Plataforma de Cloud Híbrida" y listado en el anexo técnico" Se podrá utilizar el CPD de RTVE (Prado del Rey) como CPD-A durante el primer año de contrato??*
>
> *Enviada*
>
> *13/sep/2021*
>
> *Contestada*
>
> *17/sep/2021*
>
> *la utilización del CPD de RTVE de Prado del Rey va en contra de lo que se establece en el PCT y no está permitido"*

El hecho de disponer de tres meses para la toma de control y migración de la media supone dar al proveedor del servicio el tiempo necesario para preparar el entorno y realizar la migración adecuadamente en tiempo y forma.

Frente a estos requerimientos, Evolutio plantea lo siguiente:

Pág. 11 – punto 2.2.:

> *"3.- En cada nueva zona de disponibilidad se proporcionará una cabina de almacenamiento para alojar en modo activo-activo un almacenamiento inicial vivo que cubra las necesidades para la migración de los volúmenes actuales a los nuevos emplazamientos, dimensionado para satisfacer los requisitos del pliego. Dichas cabinas de almacenamiento proporcionarán:*
>
> - *Almacenamiento SAN que estará conectado a los hipervisores de vCloud y a las máquinas Oracle.*
> - *Almacenamiento NAS dedicado a servir contenido de media."*

Además, en el apartado 2.2.4 de su OT, Evolutio declara buscar, con la nueva solución de almacenamiento mencionada, y entre otros beneficios para RTVE, "S*atisfacer el hito declarado en PCT acerca de la transformación de la media como máximo en tres meses tras la firma del contrato*".

Evolutio concreta esto unos párrafos más adelante (OT Evolutio, pág. 31) cuando pone que:

> "*Con el objetivo de garantizar el hito de la transformación de la media como máximo tres meses tras la firma del contrato, Evolutio movilizará inmediatamente la disposición de la nueva solución de almacenamiento y efectuará la migración incorporando los servicios profesionales del actual prestatario Equinix con objeto de abordar un plan razonable y factible técnicamente en donde se aceleren los tiempos al evitarse las tareas de análisis de la configuración existente de almacenamiento*"

A continuación, respecto de la implantación antes comentada de la media, el licitador añade las siguientes informaciones:

- En el Cronograma general de la figura 44 puede verse como la entrega de la nueva NAS que ha de servir la media, más la migración de la media en si a esta nueva infraestructura, **finaliza en junio de 2022, algo que, según la planificación, corresponde con el sexto mes desde el inicio de la prestación**.

  Esta fecha de finalización de los trabajos de la implantación de la NAS y migración de la media se ve reforzada por la información que aparece en la figura 46, epígrafe WS2, punto 2.3, donde **se puede observar la misma fecha antes enunciada**.

  Justo tras esta figura se explicita que:

  > "*El plan de adquisición del servicio gestionado se detalla en el apartado 2.6.2 Migración a Nueva Infraestructura IaaS. … Seguidamente se describen las actividades necesarias para el despliegue del almacenamiento NAS. Además del despliegue de la solución IaaS, se contempla la preparación de entornos PRE y PRO, así como la simulación de una migración de servicio para preparar la migración real de los dos entornos*."

- Buscando el apartado referido anteriormente en el punto 2.3 de su OT, en el apartado "2.6.2 Migración a Nueva Infraestructura IaaS", y más concretamente en el subapartado "2.6.2.3 Despliegue Almacenamiento NAS", la "Figura 60: Cronograma del Despliegue Almacenamiento NAS" detalla todo el proceso de migración propuesto

aclarando que, mientras que el nuevo hardware puede estar disponible en 3 meses desde el comienzo del servicio, la migración de la media en producción a esta nueva infraestructura no se llevará a cabo en su totalidad hasta el 15 de junio de 2022. Esto, trasladado a fechas reales marcadas por la firma del contrato, **implica esperar casi seis meses después de la firma para poder empezar a servir la media desde la nueva infraestructura**.

Por todo lo anterior, hay una discrepancia entre lo suscrito en un principio en la OT de Evolutio, acerca de los tiempos de entrega de la nueva solución de servicio de la media y los plazos explícitos que aparecen en los cronogramas. Si analizamos con más detenimiento la propuesta, el licitador confunde la implantación del hardware con la prestación del servicio de la media.

En este sentido, en el PCT se indica cuál es el alcance de la solución de la media, que involucra no sólo el almacenamiento con su solución de HA –Alta Disponibilidad- (pág. 7 PCT) sino también backups (págs. 7 y 19 PCT), migración finalizada completamente (pág. 7 PCT), instanciación de sistemas de segmentado (pág. 7 PCT), aplicación de DRM (pág. 7 PCT) y pruebas. Es por ello que la prestación del servicio de la media que plantea el licitador sólo puede llevarse a cabo, como pronto, tras el proceso de migración, esto es, a partir del sexto mes desde el inicio del servicio, ya que es en esa fecha cuando el licitador plantea haber migrado los datos, ya que, sin los datos, es imposible prestar el servicio de distribución de la Media. El cumplimiento de estos plazos no resuelve la prestación del servicio actual de RTVE.es, ya que, tras el tercer mes, como se indicó en la corrección del día 1 de octubre de 2021, el adjudicatario ha de prestar el servicio de la media desde la nueva infraestructura.

Si a lo anterior añadimos que, durante los tres primeros meses, el licitador no indica ningún proceso de movimiento de discos, cabinas, hardware desde Prado del Rey, a ninguna ubicación, sólo puede concluirse que:

1. El licitador durante los seis primeros meses piensa proveer el servicio utilizando los recursos actuales (y es por ello por lo que llega a un acuerdo con Equinix, actual prestador de la Cloud de RTVE.es) utilizando la infraestructura actual, implicando el uso de las líneas con Prado del Rey, las cabinas de Prado y el hardware de Prado, cosa explícitamente prohibida en la licitación, **tal y como puede verse en la respuesta dada el día 17 de septiembre a la pregunta número 10 de los licitadores** (ver más arriba)

2. El licitador plantea el uso de **las dos cabinas EMC, tanto la del CPD de Prado del Rey como la que se hospeda en el CPD de Equinix, que forman parte actualmente de la infraestructura de RTVE en servicio durante un plazo aproximado de seis meses, lo cual también está explícitamente prohibido en el PCT, Punto 4.2 – Pág. 18**.

Por todo lo anterior, la solución de la media no es aceptable, ya que incumple, al menos durante tres meses, los términos establecidos en la licitación.

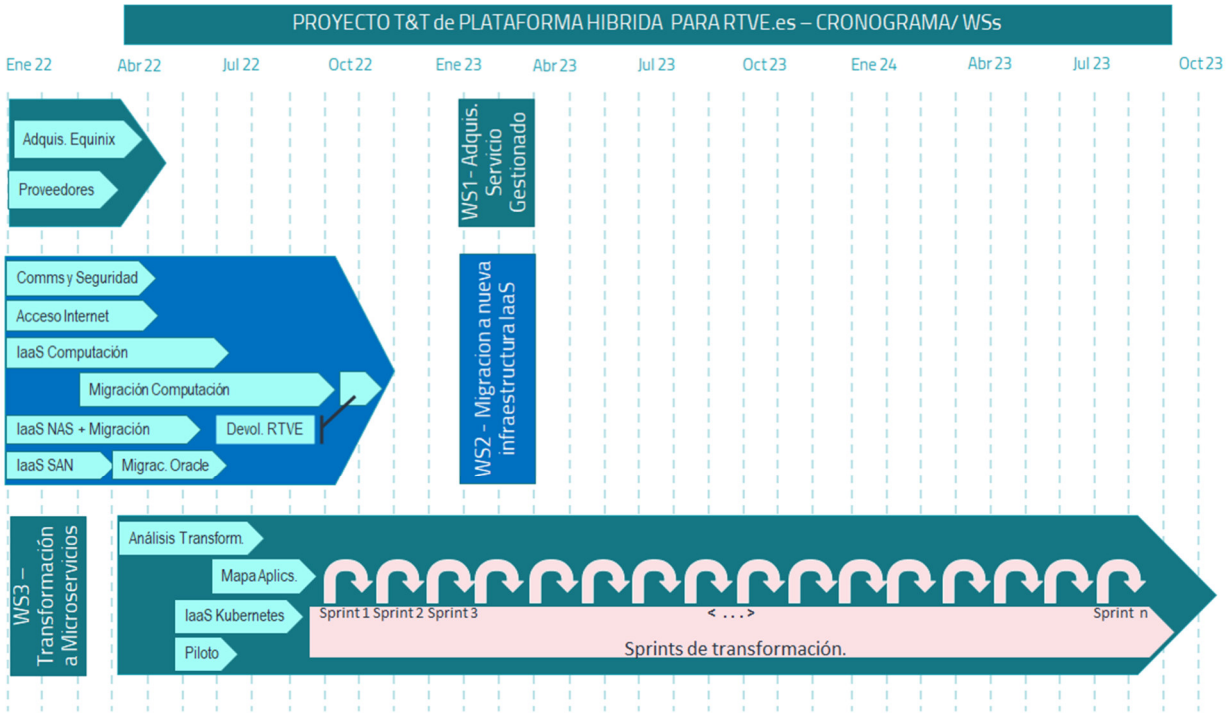
Adicionalmente, y ya en lo que respecta a la solución en sí, hemos detectado los siguientes elementos:

1. La solución de almacenamiento centralizado que propone el licitador usando la misma cabina, supone un alto riesgo para la continuidad del servicio. A juicio de RTVE e INECO, esta arquitectura es de alto riesgo y dados los patrones de exigencia de cómputo y tráfico de RTVE.es, no funcionará bien con Oracle ni en momentos de alta carga.

2. Si bien la conectividad interna de la solución cumple con lo establecido en el PCT, hemos detectado que el modelo de conectividad con CDN es insuficiente.

3. No se ha incluido el dimensionamiento exacto de máquinas que va a utilizar como servidores de origen para el tráfico segmentado, ni tampoco las configuraciones del producto *Unified Streaming* para dicha segmentación.

3. Plan de adquisición del servicio



Respecto al Plan de adquisición del servicio, el licitador indica:

> "*El plan de adquisición … tiene una duración estimada de 4 meses y se ha diseñado para asegurar una transición suave, que minimice los riesgos de afectar a los niveles del servicio actuales, a la vez que trabaja en la transformación del servicio hacia el nuevo modelo orientado a la gestión de microservicios sobre IaaS Docker/ Kubernetes*.
>
> *Un pilar fundamental de esta transición suave es el acuerdo que Evolutio ha alcanzado con Equinix, actual proveedor de RTVE del servicio IaaS del anterior pliego, para que extienda el servicio que presta hoy en día a RTVE durante los cuatro primeros meses del nuevo contrato…*"

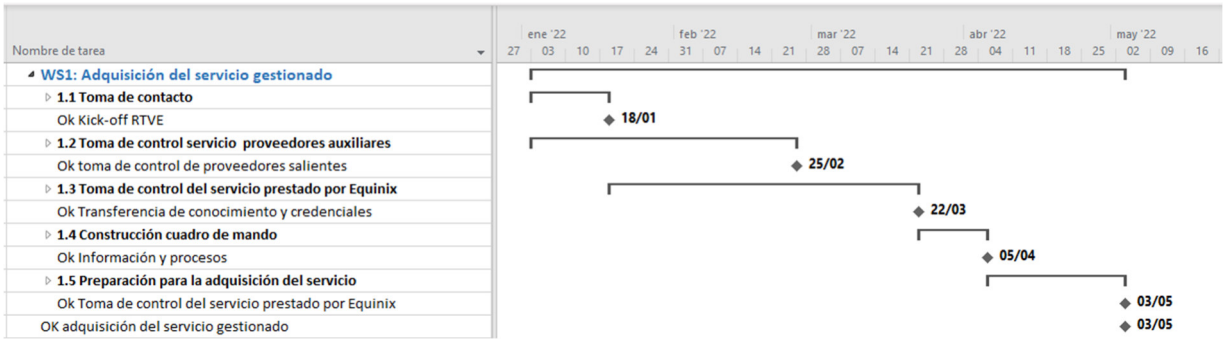
Llama la atención que el plazo de 4 meses que declara Evolutio para terminar el proceso de adquisición del servicio **excede en un mes** del requerido explícitamente en el PCT Pág. 31. donde pone lo siguiente:

> *"Plan de adquisición del proyecto, y, especialmente:*
>
> - *Cronograma general del servicio.*
> - *Planificación detallada (incluyendo recursos, personal, etc.) para el cumplimiento del hito del 1 de diciembre (*cambiado a **tres meses** desde el

inicio del servicio según se ha detallado en el punto 1 en el que ha sido valorado el plan de transformación*)*

- *Si es el caso, uso del material de RTVE y fechas de devolución.*
- *Evaluación de riesgos, y, especialmente, la evaluación del riesgo de no adquirir el servicio con fecha 6 de diciembre de 2021 (*ídem comentario segundo punto*) ".*

Por otra parte, en cuanto al cronograma de adquisición del servicio, el licitador establece un período de 2 meses para la Toma de Control del servicio prestado por Equinix, proceso que empieza 18 días después del comienzo del servicio. Esto puede verse en la figura 45 de la pág. 90 de su OT que se reproduce a continuación:



A este respecto, RTVE valora negativamente dos cuestiones.

La primera es que, pudiendo empezar la toma de control de los proveedores externos desde el primer día del servicio, tal y como puede verse reflejado en la figura anterior, Evolutio espere 18 días para comenzar este mismo proceso con Equinix, máxime cuando esta empresa empieza y se mantiene como **partner** de Evolutio durante todo el servicio. Esto puede observarse claramente en la figura 34 de su OT que se reproduce a continuación.

Figura 34: Esquema Adquisición del Servicio Gestionado

La segunda cuestión que RTVE no valora positivamente es que Evolutio tenga que dedicar 2 meses a la toma de control del servicio prestado por Equinix dada la especial relación de partner que para este proyecto mantiene con esta empresa.

Esto incide negativamente de forma clara en el tiempo total requerido para la toma de control y, por tanto, en el desfase respecto al tiempo de adquisición del servicio solicitado en el PCT.

Siendo el hecho de excederse en un mes en si negativo, en el caso de la oferta de Evolutio, RTVE no considera penalizable este hecho dada la continuidad garantizada del servicio al integrar a Equinix en su oferta.

RTVE tampoco valora positivamente el que Evolutio plantee que "*La propuesta de Evolutio es continuar prestando el servicio y su gestión desde el primer día de adjudicación del contrato, de la misma forma en que se viene prestando hoy en día*" cuando lo que RTVE requiere en el PCT es un cambio en el servicio de plataforma.

4. Modelo de aislamiento de tenants y DMZ

Respecto al modelo de aislamiento de tenants y DMZ, es llamativo que el licitador tan **sólo menciona una vez la palabra DMZ** en su oferta técnica (pág. 6) y no es para explicar nada al respecto de su posible puesta en marcha o configuración. Sólo se menciona en un índice de temas.

Respecto al aislamiento de los tenants, el licitador propone, por un lado, la creación de dos zonas de disponibilidad configuradas en Alta Disponibilidad con componentes redundantes y seguridad anti DDOS. En esta parte de la propuesta, la única frase que dedica al aislamiento de los tenants aparece en el punto 2.2.5 (pág. 11) cuando dice:

> "*Con respecto a la redundancia de la solución:*
> • *Lógica y físicamente las zonas de disponibilidad están separadas, pero se muestra un portal de vCloud de acceso unificado para ambas. También existe una réplica síncrona de la cabina para el almacenamiento NFS.*
> • *En esta infraestructura se podrán desplegar Tenants y vDC (Virtual Datacenters) de manera separada en ambas zonas de disponibilidad, aplicando una lógica de balanceo externa.*"

Es decir, se habla de desplegar tenants de manera separada en cada zona de disponibilidad, pero no de aislar tenants entre sí dentro de la misma zona de disponibilidad. Y esta estrategia de aislamiento es lo que requiere RTVE en un escenario de multi-tenants (grupos de usuarios) para unos mismos recursos.

Sólo en las páginas 28/29 de la OT (Oferta Técnica), dentro del apartado de la solución anti-malware, Evolutio menciona que el Administrador Deep Security de Trend Micro propuesto en la arquitectura de esta solución permite el aislamiento de directivas de Tenants individuales y la delegación de la administración de seguridad a administradores de cada Tenant. No menciona, sin embargo, como se integra este administrador con el panel de control de Openshift.

EL PCG en la pág. 22 del Anexo II deja bien claro:

- Modelo de aislamiento de tenants y DMZ: se otorgará 5 puntos a la arquitectura multi tenant, y, especialmente, a las capas de acceso, seguridad y aislamiento de la DMZ. El licitador tendrá que presentar el modelo de gestión de los tenants, así como los mecanismos de acceso y seguridad de la DMZ, y cómo se implementa el cierre perimetral y el acceso del personal propio de RTVE, así como los mecanismos de seguridad que protegen los activos digitales.

RTVE valora muy negativamente el hecho de que Evolutio no exponga ningún criterio ni diseño técnico al respecto de la DMZ, así como la falta de información técnica detallada al respecto de la solución planteada para el aislamiento de los Tenants en un entorno Multi-tenant.

El diagrama presentado no contempla más que la conexión a muy alto nivel de los elementos entre sí, pudiéndose considerar como un diagrama de nivel físico de bajo detalle. La descripción de los elementos que lo conforman no deja de ser una simple enumeración de características del producto sin la explicación técnica detallada exigida por RTVE.

RTVE considera que, como mínimo, el licitador tendría que haber entregado diagramas de red de capa dos, con el detalle de la segmentación necesaria para diferenciar las distintas redes de servicio que la solución debe abarcar, gestión, NFS, backends, frontales, etc., donde debería dejarse clara la primera línea de aislamiento de la DMZ, así como el diagrama de capa tres que permita entender cómo se interconectan las distintas redes de la plataforma a nivel lógico con los diferentes elementos de red que encaminan y filtran el tráfico. En definitiva, una definición mínima de la arquitectura de red que permitiera a RTVE ver que el proveedor ha ideado la solución tal y como se estipulaba en el pliego, y de la que la propuesta de Evolutio adolece.

Adicionalmente, se evalúa negativamente también la falta de un escenario de Disaster Recovery que contemple el paradigma multicloud y multitenant que se solicita en este pliego.

Por otro lado, RTVE echa en falta en esta propuesta un plan de seguridad que identifique los riesgos de la plataforma y establezca los hitos para la planificación, implementación, monitorización y evaluación del mismo durante la migración y resto de la vida del contrato; ni siquiera se describen las políticas de seguridad básicas que se implantarían de forma inicial.

Fruto de esta falta de definición, tampoco aparece en ningún punto de la propuesta los SLAs que permitan la evaluación de la ejecución de dicho plan durante el contrato. RTVE estableció como una prioridad de este pliego la necesidad de este plan de seguridad, y la propuesta de Evolutio, más allá de especificar productos que podrían utilizar y enumerar características de los mismos, no ha definido tampoco el mínimo para permitir a RTVE una evaluación positiva de este punto.

Una vez evidenciada la falta en la propuesta de lo fundamental, si se han evaluado algunos puntos positivos de la solución, como son la propuesta de la inclusión del sistema AntiDDoS basado en Cloud e independiente del propio servicio de los proveedores de las conexiones y el añadido de los servicios Antimalware de Trendmicro DeepSecurity para servidores y contenedores.

5. Arquitectura general del servicio

Respecto a la arquitectura general del servicio, Evolutio presenta su oferta diciendo "*Nuestra propuesta de valor consiste en un ejercicio de renovación tecnológica y de consolidación de los entornos anteriores en un entorno homogéneo basado en* ***vCloud****. El nuevo entorno de virtualización propuesto se utilizará como base para desplegar la infraestructura de contenedores solicitada.... lo que se propone es desplegar un cluster distribuido entre* ***dos zonas de disponibilidad****, basado en vCloud, con capacidades SDN y con* ***funcionamiento activo-activo*** *… permitirá conexiones a los proveedores de cloud pública, en los que se podrán desplegar igualmente los contenedores, orquestados desde el mismo interface centralizado e integrado en el ciclo DevOps mediante Jenkins*"

Esta arquitectura se apoya en una serie de elementos que se describen de forma poco precisa en los seis puntos que presenta en el epígrafe 2.2 (pág. 8 OT). De estos elementos, RTVE quiere hacer hincapié en algunos que resultan llamativos. Por un lado, Evolutio propone:

> "*3.- En cada nueva zona de disponibilidad se proporcionará una cabina de almacenamiento para alojar en modo activo-activo un almacenamiento inicial vivo que cubra las necesidades para la migración de los volúmenes actuales a los nuevos emplazamientos, dimensionado para satisfacer los requisitos del pliego. Dichas cabinas de almacenamiento proporcionarán:*
> - *Almacenamiento SAN que estará conectado a los hipervisores de vCloud y a las máquinas Oracle.*
> - *Almacenamiento NAS dedicado a servir contenido de media.*"

Es decir, Evolutio propone la utilización de una misma cabina para servir SAN, NAS y NFS, así como la réplica activo-activo y los backups. Siendo todos estos elementos grandes demandantes de recursos IO, sobre todo el servicio de la Media que implica el movimiento de una gran cantidad de pequeños paquetes en momentos críticos, RTVE considera muy arriesgado apostar por una sola cabina, por muy redundantes que sean sus elementos, para tener éxito en esta tarea.

El segundo punto sobre el que RTVE quiere centrar su análisis es el que hace referencia a la transición desde una arquitectura basada en máquinas virtuales desplegadas a partir de plantillas creadas en Puppet a otra, tipo agent-less, integrada con Jenkins. Evolutio plantea:

> "6.- *Con respecto al despliegue de artefactos y máquinas virtuales durante las fases de transformación, la necesidad de urgencia y de minimizar el riesgo para migrar el entorno antiguo de computación desde los antiguos emplazamientos hasta el nuevo, nos obliga a adoptar un esquema conservador de despliegue en dos fases:*
> - *Existirá una primera fase en la que se reconfigurarán y moverán las máquinas virtuales desde la plataforma antigua a la nueva. Para este despliegue se utilizará Satellite y se reinstanciarán las máquinas virtuales con nuevas plantillas que incluirán* ***optimizaciones en Puppet****, así como la inclusión del agente antivirus en la configuración base de las mismas. ...*"

RTVE, sin embargo, no plantea en ningún punto del PCT que el licitador pueda dedicar sus recursos humanos y de tiempo limitados a la optimización de plantillas Puppet durante la toma de control y migración a la nueva plataforma, sino que requiere de una rápida toma de control de los actuales servicios para un inicio lo más inmediato y en paralelo de su transformación en microservicios.

En la página 5 del PCT, RTVE indica claramente que:

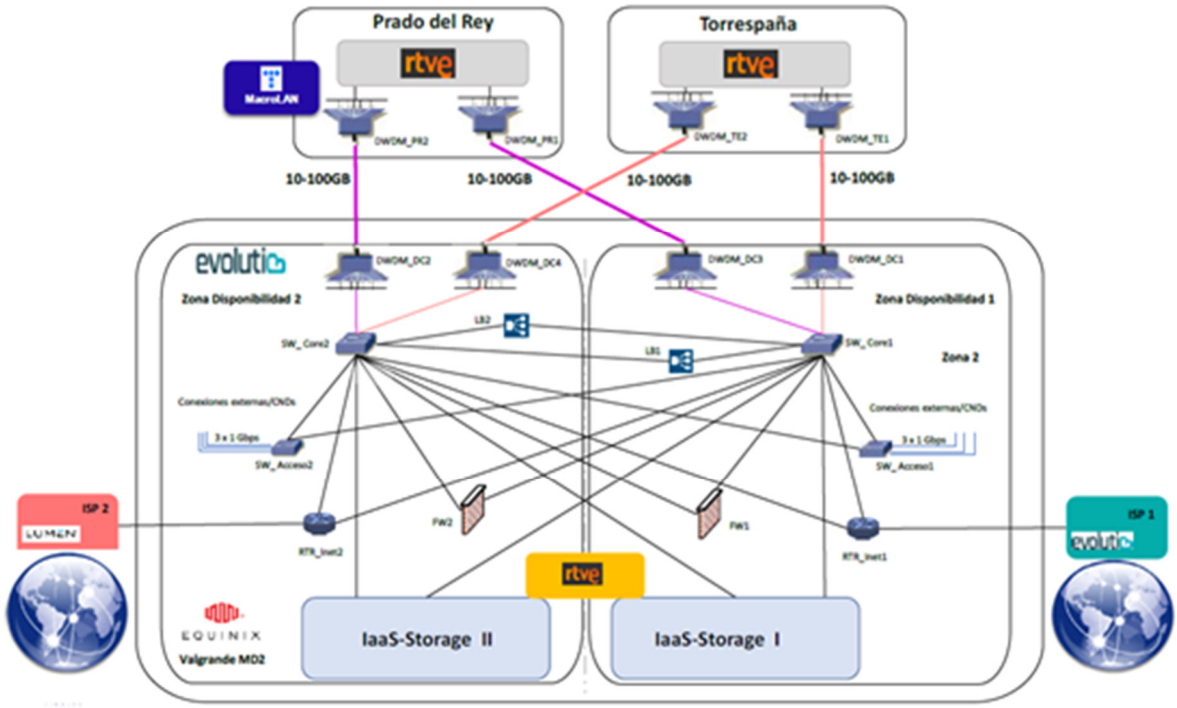
> "*El adjudicatario también será responsable de migrar del modelo actual de RTVE.es basado en Puppet a un sistema basado en Docker/Kubernetes con un modelo orientado a microservicios*".

Es decir, RTVE solicita una migración de las máquinas virtuales "sin mejoras/modificaciones" a la nueva infraestructura para la toma rápida de control del servicio en su nueva ubicación, y el inicio lo antes posible de la migración de los servicios en ellas hospedados a microservicios.

Finalmente, en la pág. 23, Anexo II del PCG de RTVE se indica claramente lo siguiente:

> "... *los licitadores han de entregar un esquema general de la arquitectura mostrando donde se ubica cada subservicio, así como las principales ventajas que a su juicio aportan sus diferentes soluciones arquitecturales ...*".

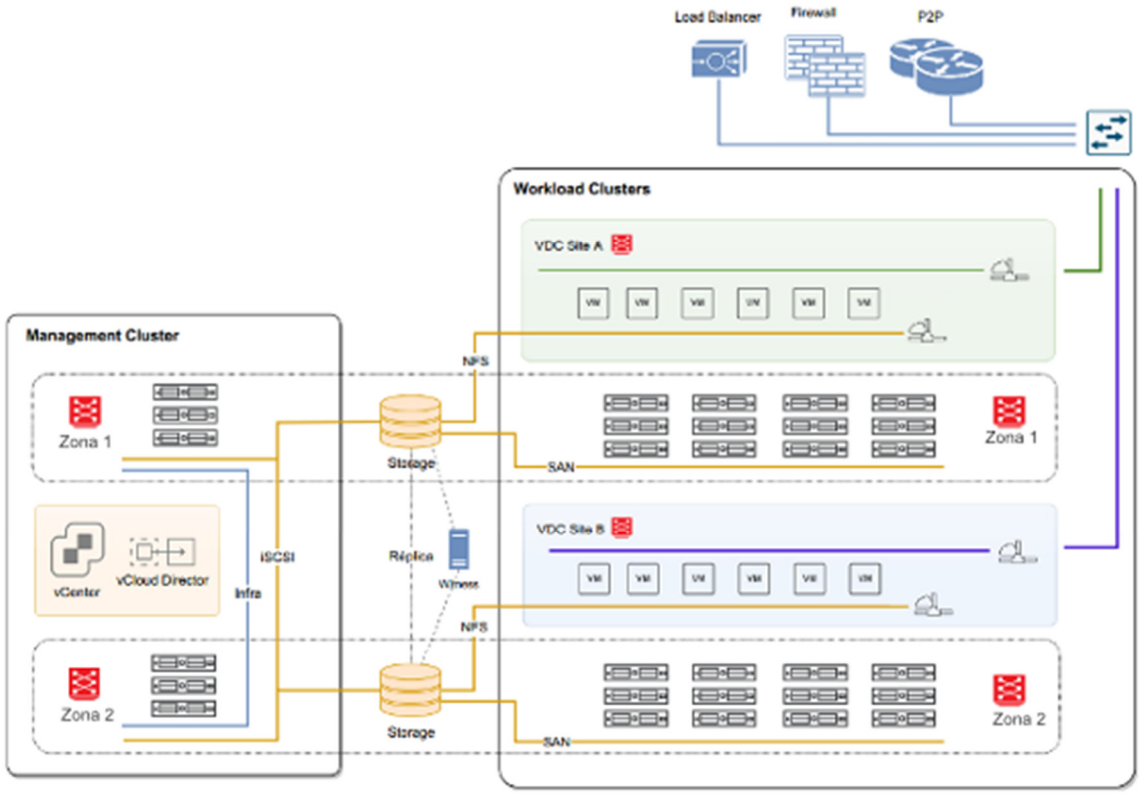
A este respecto, Evolutio muestra el siguiente esquema y lo presenta en la pág. 2 de su OT como "Arquitectura a Alto Nivel de la Solución":



A RTVE le parece totalmente insuficiente este esquema para explicar donde se ubica claramente cada sub-servicio. Como ejemplo, se hace notar la presencia de dos bloques representativos de IaaS-Storage para mostrar la existencia de dos cabinas de almacenamiento. Debido a que estas cabinas sirven tanto NAS como SAN y NFS, el dibujo presentado adolece del necesario detalle.

Esta complejidad, a juicio de RTVE, no debiera ser óbice para presentar un esquema más detallado que localizara debidamente cada tipo de almacenamiento y sus correspondientes vínculos físicos/lógicos. Aunque el vínculo directo entre el almacenamiento y el switch core se podría entender como una interconexión lógica para servicio de la media, esta relación no se entiende para el servicio SAN ni NFS, servicio que debiera aparecer detrás de los VDC que sirven las máquinas virtuales.

Esto queda reflejado en otro esquema que aparece en la figura 6 de la página 10 de la OT:



Aquí puede verse como las cabinas que sirven el almacenamiento cuelgan de los VDCs que sirven la virtualización. Lo que RTVE entiende es que esto debiera haber quedado reflejado de algún modo en el esquema de la "Arquitectura a Alto Nivel de la Solución".

6. Propuesta arquitectura de Kubernetes

Además de lo expuesto en el PCG sobre los criterios de valoración a tener en cuenta en las ofertas presentadas, ya mencionados al inicio de esta evaluación, aparece lo siguiente en el PCT con respecto a la propuesta requerida de Arquitectura Kubernetes:

> *"Arquitectura técnica completa de la solución, incluyendo todo el detalle para que RTVE pueda valorarla. Se valorará negativamente la ausencia de detalle."*

Y concretamente menciona sobre el modelo de microservicios:

> *"Modelo de microservicios: arquitectura global con todos los elementos (monitorización, deployment, control de instancias, etc)."*

A tenor de lo anterior, en este apartado la valoración se centrará en los siguientes aspectos:

- Arquitectura de Kubernetes completa
  - En la que se prestará especial atención a la propuesta del modelo de integración continua multi-tenant y multi cloud
  - el conocimiento del equipo que lo gestionará

En el punto "*2.Oferta Técnica*" de la OT (pág. 6) Evolutio inicializa la presentación de su propuesta de Arquitectura de Kubernetes. Para ello hace referencia al apartado 2.2.3 de la

OT. En dicho apartado, cuyo enunciado es "*Servicios de Seguridad y Balanceo de Carga*", no hay referencia alguna a la arquitectura de Kubernetes más que en lo que esta pueda hacer uso y disfrute del entorno de seguridad mencionado.

No es hasta el apartado 2.2.5, pág. 37 de su OT, donde podemos encontrar las primeras referencias a la arquitectura Kubernetes. Aquí Evolutio dice que:

> "*pondrá a disposición de RTVE una plataforma hybrid – multicloud capaz de provisionar cargas de trabajo basadas en clusters Kubernetes … es básico que la solución elegida esté lo más desacoplada posible de la solución de infraestructura … proponemos abordar las primeras fases de la transformación utilizando al principio Openshift como solución principal … Dado el listado proporcionado, hemos entendido que la mayor parte de las aplicaciones no son aplicaciones pesadas y que lo que prima es la modularidad y disponibilidad, por lo que nuestra propuesta consiste en establecer un despliegue equilibrado entre recursos de coordinación y gestión vs recursos útiles de trabajo en nuestra plataforma, siendo en cualquier caso preferible un tamaño pequeño de los clusters.*"

Desde la pág. 38 hasta la pág. 44 se justifica la elección del producto, Openshift Container Platform 4, en base a las ventajas y funcionalidades redactadas por el propio creador del producto, así como de la infraestructura propuesta, basada en 4 clusters, a partir de la estimación de recursos de cómputo inicial que precisarán las aplicaciones a migrar a microservicios.

Aunque el dimensionamiento inicial de la infraestructura parece, a priori, válido y la elección de Openshift puede resultar adecuada para las necesidades de RTVE, un correcto diseño de arquitectura debería mostrar mayor detalle técnico de cada uno de los componentes, así como dar solución a aspectos importantes que la propuesta de Evolutio no contempla o detalla:

- No se especifica ningún sistema para la gestión de identidades. Se desconoce si el producto seleccionado para la propuesta permite, de base, integración con sistemas de gestión de identidades o si es necesario alguna herramienta tercera
- No se detalla cómo se realizará el control de acceso a partir de esta identificación de identidad remarcada en el punto anterior, de forma que en función de los roles o permisos asociados al usuario pueda operar de una u otra forma la plataforma.
- No aparece detallado ningún sistema de monitorización para la plataforma de Kubernetes, con el que velar por el estado de los microservicios, así como de la propia infraestructura. En la pág. 50 de la OT aparece mencionado el concepto monitorización como tarea a realizar en el momento que una aplicación esté dando servicio: *"En la fase OPERATE tenemos la aplicación publicada, expuesta a Internet, por lo que la seguridad puede estar comprometida en cualquier momento, por eso llevamos a cabo Monitorización y Logging"*. No se detalla si será necesario integrar soluciones como Prometheus y Grafana o si, por el contrario, Openshift ya presenta estas funcionalidades de base.
- Del mismo modo, la única referencia y detalle sobre una de las partes más importantes de la arquitectura, como es el sistema de logging de los contenedores o microservicios, es la mencionada en el punto anterior. Es indispensable conocer cómo se podrá acceder, visualizar y filtrar el log de las aplicaciones. Soluciones, por ejemplo, como el stack completo de ELK (ElasticSearch, Logstash, Kibana) o similares deberían aparecer detalladas en toda propuesta de arquitectura de Kubernetes.
- A nivel de almacenamiento tampoco se detalla cual será la integración entre los clusters de Openshift y el sistema de almacenamiento propuesto. Preguntas como, el tipo de almacenamiento que se podrá consumir (bloque, NFS, Object Storage,

etc.), o si será necesario trabajar con dynamic storage para los volúmenes, no son respondidas y se desconoce si será Openshift el que ya dispone de las herramientas adecuadas para cubrir estas necesidades o si será necesario realizar integraciones adhoc.

- Tampoco aparece detalle sobre ningún Service Mesh, como Istio, ni monitorización del mismo, como Kiali. Tampoco se da detalle sobre si estos aspectos quedan cubiertos o no por Openshift.
- No se menciona como se realizará la gestión de secrets y si será necesario disponer de soluciones como Vault.
- No se detalla ninguna solución de backup para la arquitectura de Kubernetes ni cómo se dispondrá de un disaster recovery en caso de no existir.
- Tampoco se especifica ni menciona ninguna integración con los sistemas de balanceo y seguridad a nivel de red.

En cuanto a la integración continua (CI/CD) en la propuesta de Evolutio aparece en la pág. 39:

> *"Jenkins y Openshift 4.0 están plenamente integrados para hacer productivo y automático mediante CI/CD el despliegue de aplicaciones en pods openshift, evitando así que los desarrolladores tengan que preocuparse de la infraestructura y permitiendo que se centren en las aplicaciones, mientras que en otro tipo de soluciones hay que hacer adaptaciones para esta integración".*

También se hace referencia a conceptos muy interesantes, como GitOps o la infraestructura como código, pero de nuevo de forma muy general y sin mucho detalle:

> *"La gestión del repositorio y su estructura es importante para dar un enfoque moderno a nuestros despliegues, teniendo como objetivo GitOps para conseguir una integración lo más alta posible entre desarrollo y arquitectura, incluyendo en esta parte la infraestructura como código".*

De esta propuesta se hubiera esperado un detalle más pormenorizado y que aparecieran mencionadas soluciones para aspectos como:

- **Templating** empleado para los manifests de k8s
- **GitOps:** Propuesta de soluciones a nivel de GitOps o, de ser el caso, cómo Openshift permite alcanzar este objetivo.
- **Infraestructura como código.** Aparece mencionado Terraform, pero como parte de la metodología de desarrollo de Scripts (pág. 50 de la OT)
- **Generación de imágenes**. ¿Soluciones como Kaliko para la generación de imágenes serán necesarias, u Openshift cubre este aspecto?
- **Sistemas para la gestión de Rollouts**. No se detalla si Openshift permite establecer políticas de rollout, si estas se gestionan también como código o es necesario especificarlas a nivel de interfaz.
- **Gestión de Workflows o eventos**.
- **Gestión de Backups**

De la implementación propuesta del modelo de integración continua multi-tenant y multi cloud, en el punto 4 de este documento ya se ha reflejado la poca información aportada al respecto de los entornos multi-tenant.

En la pág. 39 de la OT, Evolutio indica lo siguiente:

- *Frente a lo que sería una herramienta simple de despliegue Kubernetes, Openshift ofrece de forma integrada múltiples facilidades adicionales para construir un entorno multicloud orientado al desarrollo de las aplicaciones (facilidades serverless, brokers de mensajes, gestión de colas y eventos, gestión multicluster) y de seguridad."*

Pero una vez más no da ningún tipo de detalle sobre el mismo, no se sabe si la integración que permite Openshift a nivel multi-cloud es equivalente a soluciones como Crossplane, que permiten la integración con terceros mediante CRD de k8s. Así mismo, para la gestión de sistemas multi-tenant tampoco se entra en detalle para valorar ventajas y desventajas de Openshift frente a soluciones y/o herramientas cada vez más extendidas como Capsule o vCluster

3 NEXTRET, S.L.

Tras el estudio de la propuesta técnica presentada por la empresa NEXTRET, S.L. (NexTReT, en adelante) se procede a dejar constancia de los razonamientos necesarios utilizados para la valoración de esta oferta.

1. Plan de transformación:

En el Gantt 3.9.3 "*Planificación detallada para el hito de la transformación* de la media*"* en la pág. 79 se echa en falta lo siguiente:

1.- Preparación de la infraestructura para la recepción de las líneas con los CDN
2.- Prueba de esta conectividad
3.- Instalación, configuración y prueba de la infraestructura de almacenamiento CEPH

En la pág. 7 de su OT hablan del almacenamiento para cada recurso (separan el almacenamiento de ORACLE del de las máquinas virtuales y la media):

1.4.2 Solución de almacenamiento y distribución media

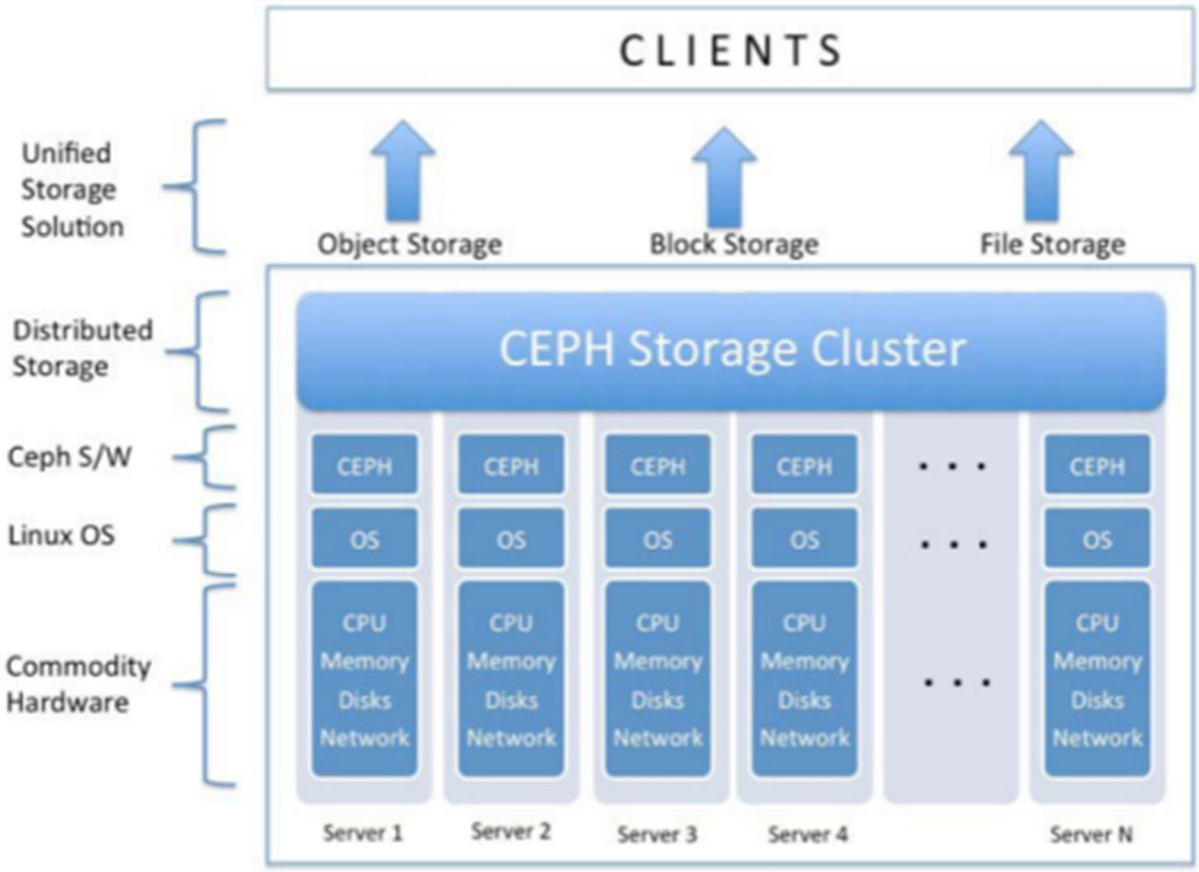
Solución de almacenamiento multicapa de alto rendimiento y óptimo coste

La solución de almacenamiento prevista permite disponer de cualquier tipo de almacenamiento adecuado a cada caso de uso:

- *Almacenamiento local NVMe para casos de componentes que ya proporcionan replicación por sí mismos (MongoDB, Elasticsearch, etc) y, se benefician de una latencia ultrabaja (<1ms)*
- *Almacenamiento basado en el uso de una cabina para almacenamiento compartido de baja latencia (Oracle)*
- *Almacenamiento distribuido (CEPH) que permite una provisión dinámica de volúmenes en entornos de microservicios, así como almacenamiento de bloque para máquinas virtuales, sistema de archivos escalable horizontalmente por ejemplo para la media y basado en objetos (tipo Amazon S3) para casos de uso futuros.*

La cabina de discos Huawei Ocean Store Dorado 3000 NVMe, ofertada en el epígrafe 2.3.3 Solución de almacenamiento, se propone sólo para el servicio de almacenamiento del cluster de ORACLE

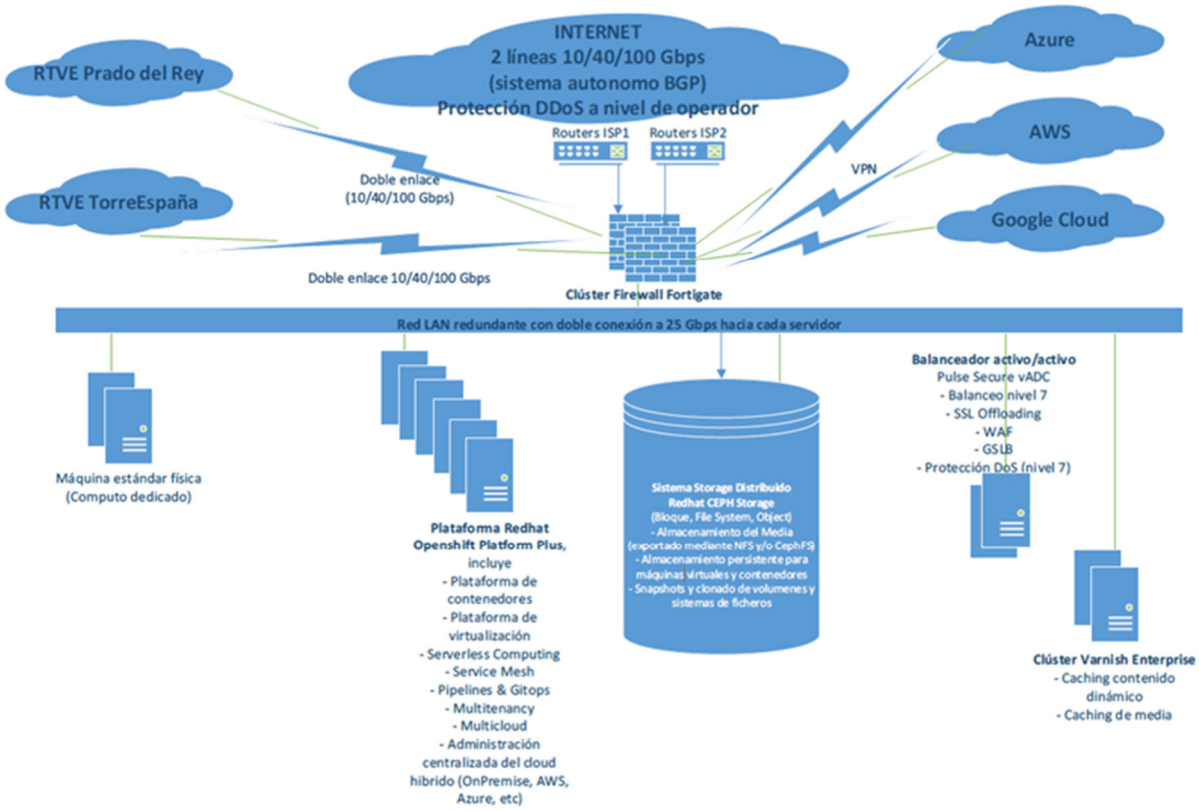
Según Julio Lozano Bahilo, del Instituto de Física Corpuscular de la UAM (Madrid) (url - https://indico.ific.uv.es/event/2837/contributions/3987/attachments/2943/3280/CEPH.pdf), el almacenamiento CEPH tiene una representación gráfica y unos requerimientos como se expone a continuación:



CEPH requiere de:

- *– Monitor: mantiene un mapa de la estructura del cluster en cada momento*
- *– Nodos OSD: albergan los Object Storage Daemons que almacenan los datos, efectúan su réplica, su recuperación y el balanceo de carga entre OSDs, etc … Se ejecutan en los servidores de almacenamiento.*
- *– MDS: MetaData Server que se ocupa de los metadatos para el CEPH Filesystem.*
- *– RADOSGW: Gateway que facilita conexiones externas a la red local*

De este esclarecedor detalle, que no ha sido incluido en la OT de NexTReT, puede derivarse que el almacenamiento CEPH propuesto por esta empresa, se va a instanciar en máquinas físicas con almacenamiento tanto NVME como discos SATA de 18TB. El problema es que NexTReT no da ningún detalle acerca de esta configuración ni del planteamiento que va a utilizar para montar el cluster de discos que se necesita para el servicio de la Media. No es lo mismo crear un cluster independiente de servidores físicos que montar dicho cluster sobre maquinas virtualizadas en el entorno de Kubernetes. El rendimiento de la plataforma Kubernetes puede verse afectado de forma considerable en el segundo caso.



Esclarecido este punto, de la representación gráfica de la arquitectura general del servicio podría derivarse que el cluster de servidores que va a hospedar el almacenamiento CEPH se va a instanciar sobre máquinas físicas independientes del entorno Kubernetes. El problema es que nos falta detalle de la instalación y configuración de dicho cluster:

- ¿Cuándo se va a instalar la infraestructura de servidores físicos que soporta el almacenamiento?
- ¿Cuántas máquinas físicas se van a instalar?
- ¿Cuál es la configuración de estas máquinas físicas?
- ¿Cuántos discos SATA de 18TB se van a poner en cada servidor físico?
- ¿Cuántas de dichas máquinas físicas van a realizar la función de controladores y/o monitores?

Si se quiere ofrecer el mínimo de 5PB, que RTVE requiere para empezar, serían necesarios un mínimo de 12 servidores con 24 discos SATA de 18TB cada uno. Pero bien podría ser otro el diseño ya que un determinado modelo de procesador o de chipset puede ser insuficiente para manejar todo el IOPS requerido. La diferencia en rendimiento entre una configuración y otra puede llegar a ser importante. Y NexTReT no da información alguna en este sentido.

Respecto a la política de Backup, en la página 25 de su OT, epígrafe 2.3.4., NexTReT no plantea backup alguno del almacenamiento a largo plazo (probablemente refiriéndose al almacenamiento de la media del archivo profundo (media que no está en uso durante un período de tiempo determinado)). Es decir, si se estropea el almacenamiento CEPH barato donde se guarda esta media (pool basado en EC (Erasure Coding) en vez del sistema de replicación estándar (3 por defecto)), se pierde esta para siempre.

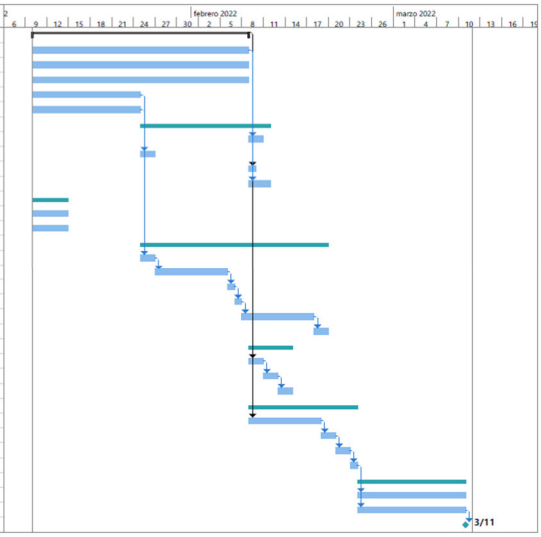
En cualquier caso, servir las máquinas virtuales, cualesquiera que estas sean y en el entorno en que estén montadas, y la media desde el mismo repositorio parece arriesgado en momentos pico.

Respecto al plan de transformación de aplicaciones a microservicios, NexTReT incluye explicaciones y comentarios acerca del proceso y la seguridad del entorno Kubernetes que demuestran un buen conocimiento de la plataforma de contenedores a crear. También incluye un detalle de los pasos a seguir para su adecuada implementación y la migración de aplicaciones a microservicios. En particular, encontramos un "*Análisis de la situación de partida y plan de acción*" en el punto 3.10.3. de la pág. 80 que refleja cierta experiencia en el proceso, aunque **no entra en todo el detalle que podría** dada la información aportada en el pliego y su anexo.

2. La solución al almacenamiento y distribución de la media:

Respecto a la solución al almacenamiento y distribución de la media, ya se ha comentado en el punto anterior que, aunque se definen los recursos para servir la media, en el Gantt de detalle que se aporta bajo el epígrafe 3.9.3 *Planificación detallada para el hito de la transformación de la media* en la pág. 79 de la OT falta detalle sobre el proceso de adquisición, montaje y configuración de la infraestructura necesaria para dar el servicio de almacenamiento CEPH referenciado, así como para la preparación de la infraestructura al objeto de permitir la conectividad de las líneas procedentes de los CDNs.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Aprovisionamiento infraestructura**	**30 días**	**lun 1/10/22**	**mar 2/8/22**
2	Enlaces a Internet	30 días	lun 1/10/22	mar 2/8/22
3	Enlaces a TorreEspaña y Prado del Rey	30 días	lun 1/10/22	mar 2/8/22
4	Servidores para infraestructura hibrida	30 días	lun 1/10/22	mar 2/8/22
5	Firewalls	15 días	lun 1/10/22	lun 1/24/22
6	Switching y routing	15 días	lun 1/10/22	lun 1/24/22
7	Despliegue de comunicaciones			
8	Configuración de routers y sistema autónomo BGP	2 días	mié 2/9/22	jue 2/10/22
9	Configuración de switching	2 días	mar 1/25/22	mié 1/26/22
10	Pruebas de comunicaciones y rendimiento de los enlaces	1 día	mié 2/9/22	mié 2/9/22
11	Configuración de la conectividad con los distintos clouds (Azure, AWS, Google Cloud) mediante VPN	3 días	mié 2/9/22	vie 2/11/22
12	Puesta en marcha de herramientas de tiquet y call center			
13	Alta de locuciones y flujos de llamadas	5 días	lun 1/10/22	vie 1/14/22
14	Definición de usuarios y perfiles en herramienta de tiqueting	5 días	lun 1/10/22	vie 1/14/22
15	Migración de firewalls y balanceadores			
16	Configuración del clúster de firewalls en alta disponibilidad	2 días	mar 1/25/22	mié 1/26/22
17	Migración de reglas des de los firewalls actuales	10 días	jue 1/27/22	sáb 2/5/22
18	Despliegue de los balanceadores	1 día	dom 2/6/22	dom 2/6/22
19	Configuración del clúster de balanceadores en alta disponibilidad	1 día	lun 2/7/22	lun 2/7/22
20	Migración de las VIPs de servicio y reglas de F5 y A10 de forma progressiva	10 días	mar 2/8/22	jue 2/17/22
21	Traslado de los rangos de IPS públicas de RTVE al nuevo sistema autónomo	2 días	vie 2/18/22	sáb 2/19/22
22	Despliegue de servidores de infraestructura			
23	DNS	2 días	mié 2/9/22	jue 2/10/22
24	LDAP, integración de la validación de usuarios en Openshift	2 días	vie 2/11/22	sáb 2/12/22
25	DHCP	2 días	dom 2/13/22	lun 2/14/22
26	Despliegue de la infraestructura hibrida			
27	Despliegue de los servidores y la plataforma para la nube hibrida (Openshift)	10 días	mié 2/9/22	vie 2/18/22
28	Creación de las diversas zonas	2 días	sáb 2/19/22	dom 2/20/22
29	Prueba de conceptoi con un despliegue en Kubernetes y una maquina virtual	2 días	lun 2/21/22	mar 2/22/22
30	Tests y control de calidad	1 día	mié 2/23/22	mié 2/23/22
31	Migración de servicios al nuevo CPD			
32	Traslado de máquinas virtuales al nuevo entorno	15 días	jue 2/24/22	jue 3/10/22
33	Despliegue de nuevas cargas de trabajo en contenedores	15 días	jue 2/24/22	jue 3/10/22
34	Todas las cargas de trabajo operativas en la nueva infraestructura	0 días	vie 3/11/22	vie 3/11/22



Por otro lado, el almacenamiento descrito en su OT, aunque muestra un rendimiento sobresaliente, adolece del mismo problema de concepto que el de la oferta de Evolutio.

Esto puede verse reflejado en el siguiente párrafo copiado de la página 7 de su OT, epígrafe 1.4.2 *Solución de almacenamiento y distribución media:*

> *La solución de almacenamiento prevista permite disponer de cualquier tipo de almacenamiento adecuado a cada caso de uso:*
>
> - *Almacenamiento local NVMe para casos de componentes que ya proporcionan replicación por sí mismos (MongoDB, Elasticsearch, etc) y, se benefician de una latencia ultrabaja (<1ms)*

- *Almacenamiento basado en el uso de una cabina para almacenamiento compartido de baja latencia (Oracle)*
- *Almacenamiento distribuido (CEPH) que permite una provisión dinámica de volúmenes en entornos de microservicios así como almacenamiento de bloque para máquinas virtuales, sistema de archivos escalable horizontalmente por ejemplo para la media y basado en objetos (tipo Amazon S3) para casos de uso futuros.*

Como puede verse en el tercer punto, NexTReT ofrece servir tanto la Media como el almacenamiento de la Virtualización y NFS desde el Almacenamiento CEPH. La idea de servir las máquinas virtuales y la media desde el mismo repositorio parece arriesgada en momentos pico.

Respecto al servicio en sí de la media, NextTreT sí que aporta información útil cuando en la página 34 epígrafe 2.3.8. Arquitectura distribución para la Media refiere con detalle toda la arquitectura propuesta, con la salvedad mencionada del necesario detalle de la infraestructura sobre la que se va a dar el servicio de almacenamiento distribuido CEPH, mostrando, incluso, algunos beneficios extraordinarios de su oferta a este respecto. En página 35 dice lo siguiente:

> *"A lo largo del servicio y especialmente cuando se amplíen las línea de Internet a anchos de banda de 40 y 100 Gbps se propondrá mediante la configuración adecuada del balanceo dinámico de peticiones por GSLB* ***la posibilidad de utilizar las líneas a Internet propias para el servicio directo a los usuarios sin pasar por la CDN*** *(para una parte del tráfico y en momentos de actividad baja/media en los que esto sea posible) con el consiguiente ahorro de costes en cuanto al ancho de banda consumido por los usuarios hacia las CDNs"*

Es decir, se plantea incluso la posibilidad de liberar parcialmente a RTVE de su dependencia respecto a los CDN para servir la Media.

3. Plan de adquisición del servicio

El PCT, en su pág. 31, resume claramente lo que se requiere de un Plan de Adquisición del Servicio:

La oferta debe contener al menos los siguientes apartados:

…

- *Plan de adquisición del proyecto, y, especialmente:*
  - *Cronograma general del servicio.*
  - *Planificación detallada (incluyendo recursos, personal, etc.) para el cumplimiento del hito del 1 de diciembre*
  - *Si es el caso, uso del material de RTVE y fechas de devolución.*
  - *Evaluación de riesgos, y, especialmente, la evaluación del riesgo de no adquirir el servicio con fecha 6 de diciembre de 2021.*

Como consecuencia de los retrasos sufridos en la publicación del Pliego y la entrega de ofertas por parte de los potenciales suministradores del servicio, la fecha tope del 6 de diciembre para la adquisición del servicio se transformó en un **plazo móvil de tres meses** desde la puesta en marcha del servicio tras la firma del contrato.

Como puede verse en la OT en su página 77, epígrafe 3.9 *Plan de Adquisición del Servicio*, sub-epígrafe 3.9.1 *Cronograma General del Servicio*, NexTReT muestra la siguiente figura:

De este cronograma parece derivarse que el proceso **total** de Transición e Implantación -o adquisición del servicio- tiene una duración de **un mes**. Sin embargo, en el detalle de este proceso que puede verse en el epígrafe posterior 3.9.2 *Metodología*, sub-epigrafe 3.9.2.1 *Transición / Implantación del Servicio*, NexTReT detalla dicho proceso quedando bien claro que este **no incluye creación de infraestructura nueva alguna y traslado / adquisición de servicios a dicha infraestructura**. El listado de acciones incluidas por NexTReT en este proceso es suficientemente preciso:

- *Recopilación de información de la plataforma y reuniones con las partes implicadas.*
- *Revisión del modelo de relación.*
- *Comprobación y actualización del inventario.*
- *Redacción de la documentación de explotación del servicio.*
- *Redacción de los procedimientos de operación del servicio.*
- *Preparación de la formación interna del equipo de NexTReT*
- *Elaboración de documentación, procedimientos y workflows de comunicación y escalado entre NexTReT y Línea de negocio*
- *Implantación de las herramientas de gestión:*
    - *Configuración de la herramienta de monitorización*

Buscando el debido proceso, incluyendo algún tipo de cronograma, de creación, configuración y migración / traslado / adquisición de los servicios actuales a la nueva plataforma, se ha encontrado un Gantt, ya mostrado en el punto anterior, donde se detalla parcialmente este proceso con sus plazos estimados de ejecución. Es decir, **el Gantt que incluye una parte esencial del proceso de adquisición del servicio se encuentra en el epígrafe 3.9.3 *Planificación detallada para el hito de la transformación de la media*, donde, sin embargo, no puede encontrarse nada al respecto de dicha transformación de la media**.

Si juntamos este proceso de creación, configuración y migración / traslado / adquisición de los servicios actuales a la nueva plataforma (que puede verse en el Gantt referido) con el mes inicial que NexTReT llama de Transición e Implantación, **esta OT cumpliría con el plazo de tres meses exigido en el PCT para este caso**.

Aclarado esto, el Gantt que muestra el detalle del proceso de creación y traslado de los servicios prestados por RTVE a la nueva infraestructura, parece adecuado a lo que se requiere de un complejo proceso como este.

4. Modelo de aislamiento de tenants y DMZ

Con referencia al modelo de aislamiento, NexTReT indica en la pág. 47 punto 2.4.1 que:

> *"Mediante las capacidades de seguridad que proporciona la plataforma se permitirá un aislamiento de los diversos tenants definidos en la plataforma gracias al uso de NetworkPolicies y de Redhat Openshift Service Mesh (que usa istio para controlar los accesos entre servicios*).

En pág. 50 puede también leerse:

> *"Aislamiento entre entornos y aplicaciones y seguridad para el Service Mesh: OpenShift Container Platform le permite segmentar el tráfico de red en un solo clúster para crear clústeres de múltiples tenants que aíslan a los usuarios, equipos, aplicaciones y entornos de los recursos no globales."*

La enumeración de las herramientas a utilizar es útil pero quizá algo insuficiente dada la falta del detalle que se esperaba en una oferta donde el modelo de microservicios se plantea como el eje de toda una transformación del servicio.

Sobre el modelo de DMZ, NexTReT señala en pág. 47, epígrafe "2.4.2 *Modelo de DMZ"* y sub-epígrafe 2.4.2.1 que, *"Para poder acceder de forma remota a la plataforma y las diversas redes se definirá la correspondiente VPN integrada con el directorio LDAP de RTVE que presentará las siguientes características de seguridad:*

- *Autenticación de doble factor: ……..*
- *Perfiles de usuarios: ……..*
- *Auditoria de accesos con generación de alertas: ……."*

En relación a la Seguridad de accesos y cierre perimetral, NexTReT en la pág. 47 punto 2.4.2.2 que:

> *"Usando una política de mínimos accesos necesarios se limitará a nivel de firewall el tráfico entre servidores a los accesos requeridos para el correcto funcionamiento de las aplicaciones y la monitorización de la infraestructura.*
>
> *A nivel de perímetro todo acceso desde Internet a los servicios publicados, así como los accesos vía VPN, será auditado de manera que se permitirá obtener una trazabilidad ante cualquier circunstancia o incidente de seguridad."*

Esta no es la explicación que se espera de la creación y configuración de una zona desmilitarizada abierta a internet. Sólo trata modelos de aislamiento de comunicaciones entre RTVE y la nueva plataforma.

Si bien en esta propuesta aparecen diagramas con la arquitectura por capas de la red para algunos de los servicios principales, se considera insuficiente como para evaluarlo dado que faltarían, al menos, diagramas físicos y lógicos de capa dos, con la segmentación que separe los distintos tipos de redes, y de capa tres, con los encaminamientos entre dichas redes.

En cualquier caso, aparecen identificadas dos redes, Backend y DMZ, y se habla de la separación de las mismas mediante firewall, con balanceadores en DMZ, backends con

políticas en firewall físico y zonas en contenedores vía Service Mesh. Se echan en falta más redes identificadas, como redes de servicios, de gestión, de NFS, etc. y la propuesta de segmentación de las mismas.

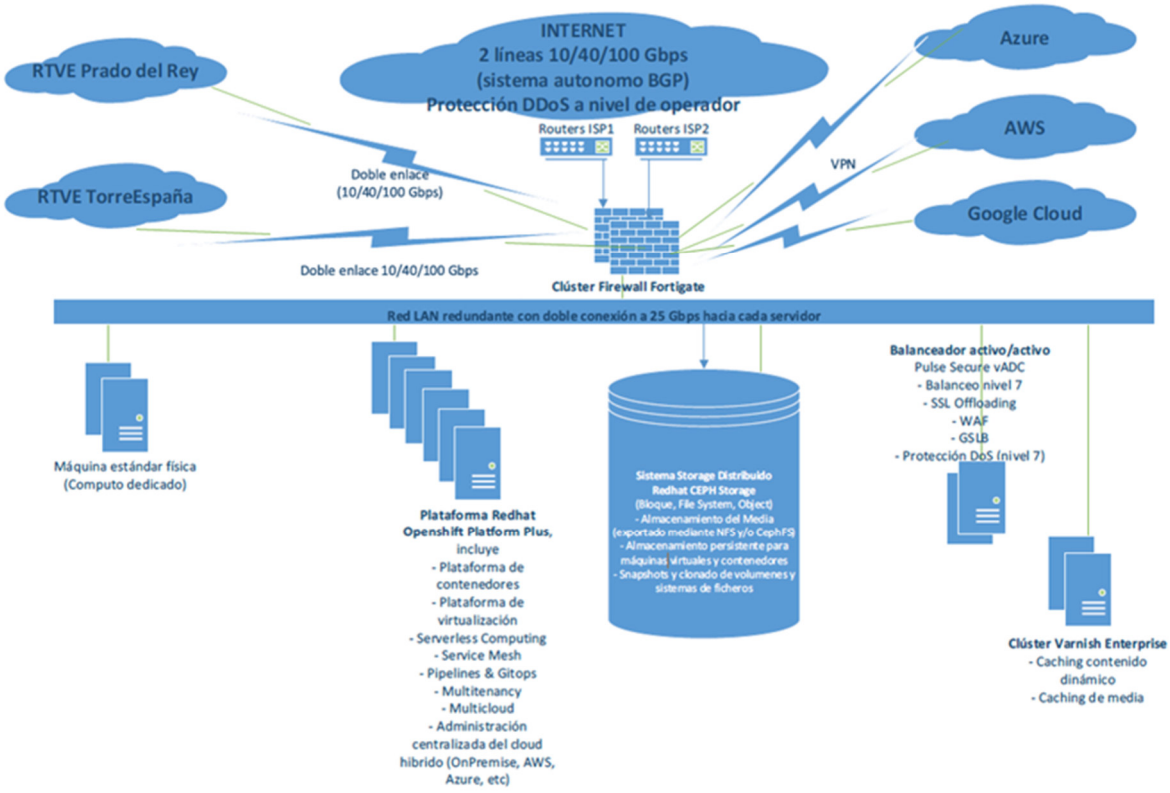
En este aspecto, por el lado positivo, si se ha evaluado la propuesta de Disaster Recovery que se ha planteado y que, aun no estando descrita con detalle, contiene dos emplazamientos físicos separados que hacen uso de las características multicloud del servicio solicitado, así como la predisposición de la solución a proporcionar, en cuanto sea necesaria, la ampliación de las conectividades, planteando de base hardware con capacidades para ello y un plan de actualización de las mismas.

Por otro lado, tampoco aparece descrito ningún plan de seguridad ni, por ende, políticas de seguridad, análisis de riesgos de la plataforma, plan de monitorización, implantación, ni SLAs asociados a dicho plan, aunque se especifica, de nuevo vagamente, que los niveles 2 harán mantenimiento preventivo y proactivo, con pruebas de intrusión, así como el nivel 3 programará políticas de actualización y garantizará la disponibilidad de los recursos.

Tras la enumeración de lo principal, también cabe destacar que echamos en falta una solución antimalware a nivel de nodos servidores y contenedores.

5. Arquitectura general del servicio

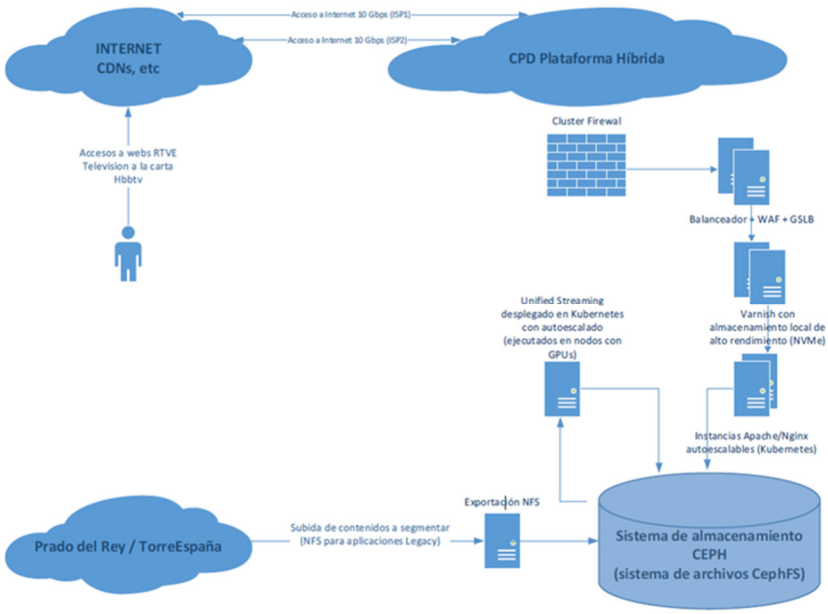
La arquitectura que plantea NexTReT se **centra en el uso de la nueva infraestructura de Kubernetes** para soportar todo el cómputo posible. Esto puede verse en el esquema de la arquitectura general del servicio incluido en la pág. 12 de la OT, epígrafe 2.2. Arquitectura técnica completa de la solución, sub-epígrafe 2.2.1 Arquitectura general del servicio:



Queda patente que la infraestructura dedicada a servir Redhat Openshift Platform Plus está más que dimensionada si se compara con la poca infraestructura dedicada a las máquinas físicas de cómputo dedicado.

Como aspecto negativo de este esquema presentado, puede verse como el balanceador no parece estar ubicado en el lugar adecuado para ejercer su función. Lo mismo sucede con el cluster de Varnish enterprise.

Estos recursos, sin embargo, sí que aparecen bien ubicados en el gráfico que aparece en la pág. 34 de la OT, epígrafe 2.3.8 *Arquitectura distribución para la media:*



Por último, el gráfico general muestra claramente cómo el almacenamiento CEPH se presenta centralizado en una sola infraestructura. Esto, a la vista del dibujo presentado, hay que imaginarse que está replicado por zona de disponibilidad, ya que no aparecen estas reflejadas con ningún recurso gráfico o textual. Además, ya se comentó antes que este almacenamiento CEPH es único para servir tanto la Media como el almacenamiento de las máquinas virtuales y la replicación entre zonas, y ello resulta muy arriesgado en momentos pico.

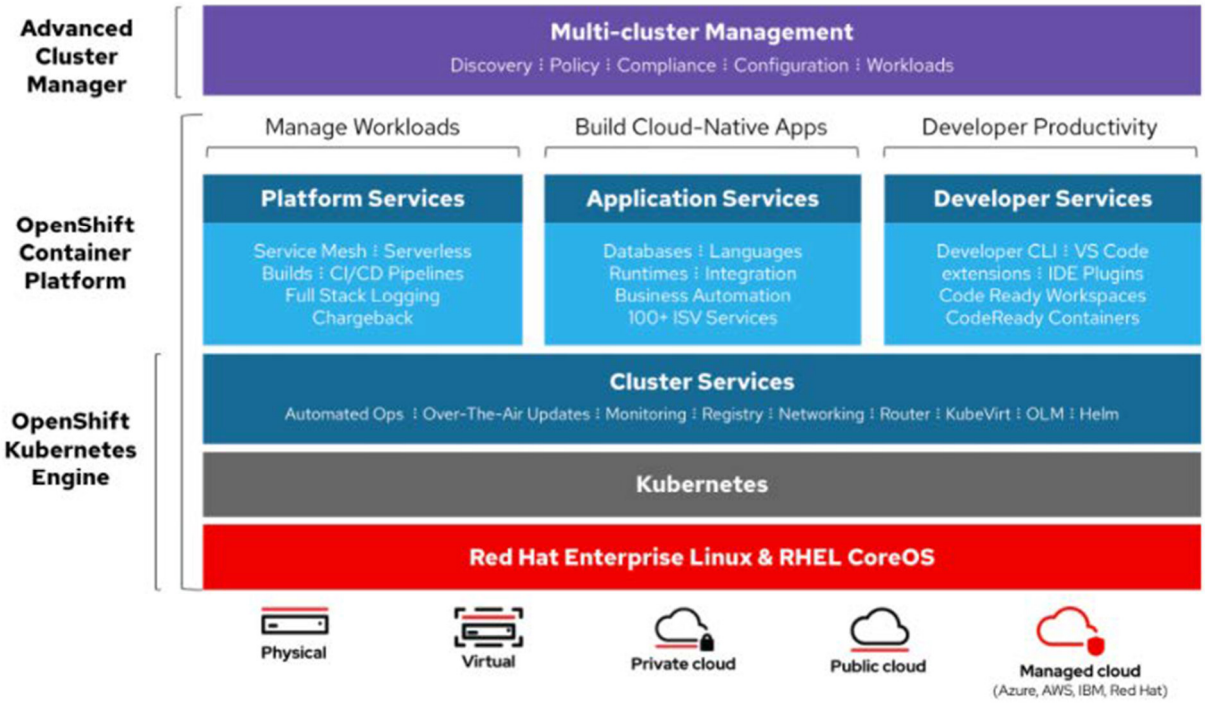
Es verdad que, tal y como puede verse reflejado en los comentarios del punto 2 que trata sobre la solución de almacenamiento, esta oferta de NexTReT saca el servicio del almacenamiento del cluster de ORACLE de esta cabina común, algo que parece importante desde el punto de vista de conseguir un mayor rendimiento tanto para el cluster de ORACLE como para el resto de servicios, incluyendo la Media.

6. Propuesta arquitectura de Kubernetes

Como puede verse en la OT en su página 8, epígrafe 1.4.6 Arquitectura de Kubernetes, NexTReT indica que su solución se basa en dos pilares:

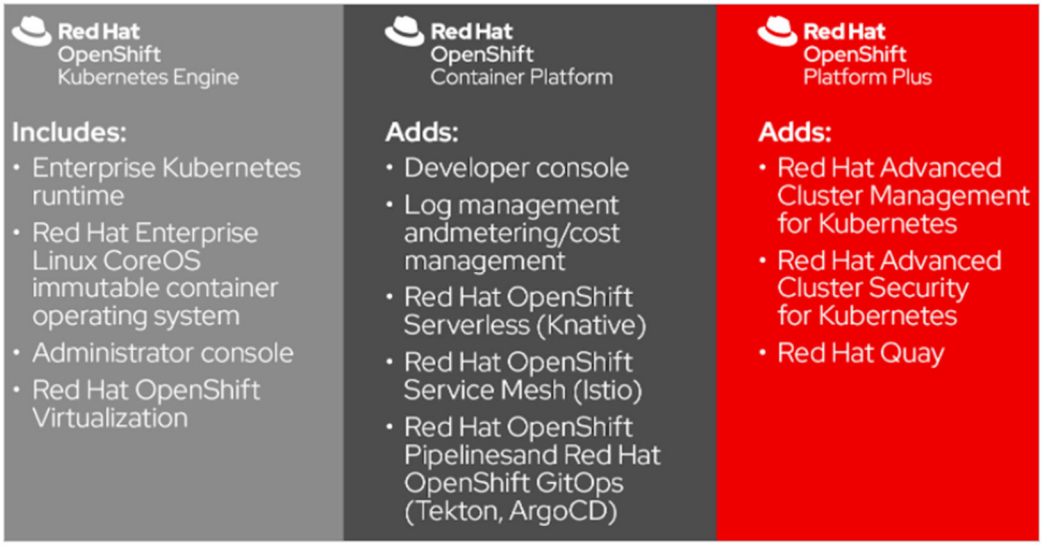
1.- *Estándares abiertos de mercado, Red Hat Openshift*
2.- *Experiencia en el desarrollo y transformación de microservicios Node JS*.

En la pág. 48 de su OT, epígrafe 2.5 *Propuesta de arquitectura de Kubernetes*, sub-epígrafe 2.5.5, NexTReT ofrece Openshift Plus, que ofrece dos capas de servicio extra sobre la versión Openshift Container Platform 4 que ofrece Evolutio:



Con Red Hat OpenShift Platform Plus, las organizaciones pueden implementar funciones de seguridad y administrar aplicaciones de manera más consistente donde sea que vivan en la nube híbrida abierta y en cualquier punto del ciclo de vida del software. Entre las ventajas hay que señalar el hecho de que la versión Plus incluye **Red Hat Advanced Cluster**

Security, recurso que permite gestionar desde Openshift la seguridad de los clusters de forma eficiente, algo que no viene incluido con la versión OCP (Openshift Container Platform) que ofrece Evolutio.



Dicho esto, **NexTReT**, en este epígrafe concreto, donde debería explicar este punto en detalle, **no presenta una propuesta de arquitectura de servicios sobre Kubernetes como tal adaptada al planteamiento que RTVE refleja en el PCT**. Tal y como ocurría con la propuesta de Evolutio se echan en falta definición y detalle de cómo se va a dar solución a determinados aspectos esenciales en este tipo de arquitecturas:

- A nivel de almacenamiento tampoco se detalla cual será la integración entre los clusters de Openshift y el sistema de almacenamiento propuesto. Si es cierto que en la pág. 7, sección 1.4.2, se menciona que:

    - *"Almacenamiento Distribuido (CEPH) que permite una provisión dinámica de volúmenes en entornos de microservicios"*.

  Pero no se especifica ningún detalle más.

- No se menciona como se realizará la gestión de secrets y si será necesario disponer de soluciones externas como Vault.

A diferencia de Evolutio, si hace mención expresa de los siguientes aspectos:

- En cuanto a la gestión de identidades y la securización en base a ésta, mencionan que la versión de Openshift Platform Plus permite **integración directa con LDAP y con otros muchos sistemas de terceros** (pág. 50, apartado 2.5):

    Seguridad integrada con LDAP y otros múltiples sistemas de autenticación: Se soporta de forma nativa la integración con directorios LDAP, así como otros muchos sistemas (Keystone, Github, GitLab, Google, OpenID, etc).

Así mismo, en la pág. 37, apartado 2.3.11.1 mencionan que esta solución podría ampliarse con Api Gateway o integraciones con terceros, como KeyCloak o soluciones con integraciones en OAuth o OIDS.

- Sobre el sistema de monitorización la propuesta de NexTReT hace mención expresa en la pág. 42, apartado 2.3.11.4 *Monitorización*, al uso de **Openshift Service Mesh** junto con **Jaeger** y **Kiali** como solución para la monitorización de la arquitectura Kubernetes. Añaden, además, como realizarán la monitorización de la propia infraestructura de forma externa a las integraciones o soluciones que ofrece la versión Openshift, en la pág. 44, sección 2.3.13 Modelo de Monitorización. Harán uso de **Grafana y Prometheus**.

- Sobre la gestión de logs, en la misma pág. 44, sección 2.3.13, mencionan como solución, aunque sin mucho detalle, el **uso de Fluentd/Elasticsearch/Kibana**, que es una de las soluciones más extendidas en este tipo de infraestructuras.

- En cuanto a la solución de backup para la arquitectura de Kubernetes, en la sección 2.3.4 Backups, pág. 25, se detalla una solución completa para casi todos los aspectos:

  Se realizarán copias de seguridad periódicas (consensuando con RTVE una periodicidad razonable para cada tipo de datos) a un sistema de almacenamiento externo basado en NFS de todo el contenido almacenado en CEPH, que incluye entre otros:
  - *Volúmenes utilizados como almacenamiento persistente en pods (block storage y file storage)*
  - *Backup completo del sistema etcd que contiene toda la configuración de Kubernetes en Openshift*
  - *Backup granular de artefactos en Openshift (Deployments, Secrets, ConfigMaps, ReplicaSets, etc) que permita recuperar un servicio determinado a un estado pasado (realizado mediante la solución Velero).*

- Con respecto a la integración con los sistemas de balanceo y seguridad a nivel de red. Se menciona en la pág. 37 de la sección 2.3.11.1, y así aparece detallado en la figura, el uso de un **API Gateway**:

  El API Gateway es un componente opcional pero altamente recomendable en cuanto organiza, autentica/autoriza, monitorea, etc. la publicación de los microservicios. En una analogía totalmente abierta a debate, cumple una función similar a los Enterprise Service Bus de los tiempos de los servicios web SOAP/XML.

El siguiente punto a tener en cuenta en la validación de la arquitectura Kubernetes requerida es la propuesta de integración continua (CI/CD), sobre la que, en la pág. 23, sección 2.3.2 Solución para realizar la integración continua, se menciona:

OpenShift proporciona un contenedor Jenkins certificado para construir canalizaciones de entrega continua y también escala la ejecución de la canalización mediante el aprovisionamiento bajo demanda de esclavos Jenkins en contenedores

Además, proponen posteriormente una migración a Openshift Pipelines, basado en Tekton:

- *OpenShift Pipelines permite a los equipos crear, probar e implementar sus aplicaciones utilizando pipelines nativos de la nube y tomar el control del ciclo de vida de sus aplicaciones.*
- *Canalizaciones al estilo de Kubernetes: cree canalizaciones utilizando CRD de Kubernetes estándar que son portátiles en las distribuciones de Kubernetes.*
- *Funciona sin servidor: crea y ejecuta canalizaciones, punto. Sin servidor de CI / CD para administrar y mantener.*
- *Implementar en múltiples plataformas: sus canalizaciones se ejecutan en Kubernetes, pero puede implementar en muchas Kubernetes, VM y plataformas sin servidor desde la canalización.*
- *Cree imágenes con las herramientas de Kubernetes: puede utilizar la herramienta de creación de su elección para crear imágenes. Source-to-Image (S2I), Buildah y Dockerfiles, Jib, Kaniko y más.*
- *Herramientas de desarrollo: herramienta de línea de comandos para interactuar con las canalizaciones además de integraciones con la consola de desarrollador de OpenShift y complementos IDE.*

Aunque hacen referencia a conceptos importantes dentro de la solución Openshift Pipelines, como el uso de CRDs o soluciones para la generación de imágenes como Kalico o Jib, se echa en falta detalle sobre otros aspectos:

- Templating empleado para los manifests de k8s
- GitOps: Propuesta de soluciones a nivel de GitOps o, de ser el caso, cómo Openshift permite alcanzar este objetivo. ¿Soluciones como ArgoCD serían necesarias?
- Sistemas para la gestión de Rollouts. No se detalla si Openshift permite establecer políticas de rollout, si estas se gestionan también como código o es necesario especificarlas a nivel de interfaz.
- Gestión de Workflows o eventos.

Es verdad, sin embargo, que en los distintos epígrafes de su OT puede verse como NexTReT apunta al uso intensivo de recursos containerizados en Kubernetes para migrar o evolucionar varios servicios esenciales (incluyendo la mayoría de las máquinas virtuales) de la plataforma.

Respecto a los perfiles del equipo técnico propuesto por NexTReT, se aprecia un mayor detalle en las experiencias descritas y en las referencias laborales de todos ellos, a pesar de que experiencia pasada concreta en arquitectura Kubernetes no aparece explícitamente en ninguno de estos perfiles.

En referencia a la cualificación de los responsables del proyecto, esta parece de un nivel superior al de Evolutio, especialmente la del responsable del proyecto y la del Administrador Linux que parece se hará cargo de la administración de Kubernetes. Este perfil, aunque es el de una persona joven, muestra especialización en dicha área en particular. (5.4 Administrador Linux – OLA – Experiencia Profesional actual en Kubernetes).

4 Valoración

Tras la revisión de las propuestas de ambos proveedores, y tras el análisis comparativo del detalle técnico, el personal dedicado a la valoración de las propuestas acuerda la siguiente valoración:

Epígrafe	Puntos mejor valorada	Evolutio	NexTRet
1. Plan de transformación	5	0	5
2. Solución de almacenamiento y distribución media	15	0	15
3. Plan adquisición del servicio	10	10	7
4. Modelo aislamiento y Tenants	5	3	5
5. Arquitectura General del servicio	5	2	5
6. Propuesta arquitectura Kubernetes	10	6	10
	50	**21**	**47**