Especificaciones generales para la integración de sistemas en la infraestructura de TMB

Versión 2.7

Infraestructura de Sistemas

Infraestructura Tecnològica i Operació Tecnològica de Sistemes

Direcció Executiva d'Innovació, Tecnologia i Negoci Internacional

TMB

Contenido

Control de cambios

Versión	Fecha	Autor	Cambios
1.0		Javier Jarne	
2.0	05/06/2014	Javier Jarne	Redacción en formato párrafo
2.1	07/04/2015	Javier Jarne	Inclusión de la tabla de control de cambios. Inclusión de los requisitos RA-GN-4, RA-RS-4
2.2	20/10/2018	Javier Jarne	Reflejar cambios organizativos. Incluir los nuevos requisitos de seguridad que emergen de la existencia de la Política.
2.3	14/08/2019	Javier Jarne	Introducir concepto servicio externo
2.4	08/09/2021	Juan José Del Río	Incluir requerimientos Seguridad TIC.
2.5	13/09/2021		Criterios Obligatorios vs opcionales
2.6	28/10/2021	Juan José Del Río	Repaso criterios

1 Introducción

La filosofía del diseño de la arquitectura física de los sistemas y la forma de trabajar de TMB tiene el siguiente objetivo:

Disponer de una infraestructura …

- **… adaptada a la criticidad de los diferentes entornos de TMB…**
- **… al menor coste de adquisición, operación y mantenimiento….**
- **… cumpliendo los criterios de seguridad establecidos.**

Para poder conseguirlos, hay dos grandes líneas de trabajo.

- **Consolidación**. TMB ha apostado por disponer de elementos de infraestructura comunes a todos los sistemas con el objetivo de que puedan ser utilizados para todas las soluciones. Esta reutilización permite optimizar las inversiones, disponiendo de menos equipos y, a su vez, con mayores funcionalidades.
- **Estandarización.** Se han de optimizar los recursos destinados a gestionar y mantener la infraestructura. Para ello, se ha de limitar la diversidad de elementos, sistemas operativos, software, herramientas,… ya que cada nueva tecnología introduce una mayor complejidad en los sistemas e implica un esfuerzo añadido de administración además de un gasto en formación. Por otro lado, la estandarización asegura una correcta integración con las herramientas de gestión y monitorización existentes.

Esto se traduce que las diferentes arquitecturas se apoyan en las mismas capas de HW y SW base

	Arquitectura Sistema 1		**Arquitectura Sistema 2**	**…**	**Arquitectura Sistema N**	
Aplicaciones SW						
Servidores de aplicación						
Base de datos						
Sistema Operativo						
Hardware						
Almacenamiento						
Comunicaciones						
Cableado						
CPD / Sala Tècnica						

Por tanto, los **diseños de las arquitecturas de los sistemas deben hacerse de forma integrada con la infraestructura ya existente** y con tecnologías ya existentes, descartándose soluciones que comporten la creación de silos tecnológicos.

Este documento recoge los **requisitos generales** para el diseño, adquisición y operación de una solución desde el punto de vista **del Hardware, Sistema Operativo, Almacenamiento y Base de Datos**, (aunque recoge también algún requisito diseño de otros aspectos).

Debido a que para realizar el diseño correctamente integrado es necesario el conocimiento de la infraestructura ya existente en TMB, **es necesario contar en la fase de diseño con la colaboración del personal especialista de TMB** en instalaciones físicas, cableado (departamento de Instalaciones), redes comunicaciones (departamento de Redes y Telecomunicaciones) , hardware, sistema operativo, bases de datos, middleware (departamento de Infraestructura de Sistemas) y Seguridad de la Información (Unidad de Seguridad TIC).

Además, toda la parte de **monitorización, operación y administración de los sistemas deberá consensuarse con OTS** (Operació Tecnologica de Sistemes) para garantizar que la solución es **completamente operable por TMB una vez entregada**.

2 Diseño de arquitectura

2.1 Generales

RA-GN-1	Obligatorio siempre	El diseño de las arquitecturas se ha realizado de forma que se integra con la infraestructura ya existente en TMB
RA-GN-2	Obligatorio siempre	El diseño debe contar con la participación y aceptación de los especialistas de instalaciones, redes, infraestructura, bases de datos, middleware y seguridad TIC de TMB
RA-GN-3	Obligatorio siempre	La monitorización, operación y administración de los sistemas debe ser consensuada con el personal de TMB
RA-GN-4	Obligatorio si se usa HW/Sistemas en TMB	Toda la solución debe estar correctamente licenciada a nombre de Ferrocarril Metropolità de Barcelona S.A y/o Transports de Barcelona, S.A., con licencias que permitan su reutilización posterior en caso de substitución del HW

2.2 Seguridad

RA-RS-1	Obligatorio siempre	El sistema debe cumplir con la Política de Seguridad de TMB y todas sus normativas y directrices asociadas, incluidas las de RGPD.
RA-RS-2	Obligatorio siempre	El diseño debe contemplar desde el inicio la seguridad como un factor intrínseco a su diseño y en todas sus capas.
RA-RS-3	Obligatorio siempre	El diseño debe indicar el RTO (Recovery Time Objective) y el RPO (Recovery Point Objective) que debe cumplir la solución.
RA-RS-4	Obligatorio siempre	Si el sistema se considera crítico, debe dotarse de mecanismos de alta disponibilidad y contingencia en todas sus partes fundamentales.
RA-RS-5	Obligatorio siempre	Todo equipo que deba ser accedido directamente desde Internet, deberá situarse en una DMZ.
RA-RS-6	Obligatorio siempre	Deben evitarse soluciones, arquitecturas, protocolos,… considerados inseguros o con vulnerabilidades conocidas.
RA-RS-7	Obligatorio siempre	Se prohíbe el uso de usuarios genéricos o comunes a diferentes personas. Los usuarios deben identificarse

		con el usuario de dominio personal de TMB, tanto al sistema como a las aplicaciones.
RA-RS-8	Obligatorio siempre	Tanto sistema operativo como las aplicaciones que estén instaladas en los equipos /servidores, PCs, staciones de trabajo,...) deben tener un plan de actualización para no quedar obsoletos.
RA-RS-9	Obligatorio siempre	Se debe disponer de un plan para la instalación de parches de los sistemas y aplicaciones instaladas en los equipos para evitar vulnerabilidades de seguridad.
RA-RS-10	Obligatorio siempre para equipos en TMB	Los accesos como administrador a los equipos se deberán realizar mediante la solución PAM de TMB quedando expresamente prohibido el acceso directo como administrador.

2.3 Red

RA-RD-1	Obligatorio siempre	Sólo son posibles soluciones de comunicaciones basadas en IP y soportadas por la red corporativa. No se admitirán soluciones que no utilicen esta red.
RA-RD-2	Obligatorio siempre	El diseño se adecuará a las características de la red y ha de detallar los requerimientos y necesidades de conectividad entre los equipos y el resto de sistemas de TMB (flujos de comunicación entre equipos, IPs necesarias, protocolos y puertos usados, VLANs necesarias, anchos de banda, latencias máximas, necesidad de multicast, servicios de balanceo...).
RA-RD-3	Obligatorio si hay equipo en TMB	El sistema deberá adecuarse al plan de direccionamiento IP existente en TMB.
RA-RD-4	Obligatorio si hay equipo en TMB	No se pueden extender VLANs de nivel 2 entre centros o entre segmentos de red separados por firewalls.
RA-RD-5	Obligatorio si hay equipo en TMB	La conectividad es a 1000Mbps para servidores virtuales o servidores basados en blades situados en los CPDs. Para otro tipo de servidores o ubicaciones la conexión puede estar limitada a 100 Mbps.
RA-RD-6	Obligatorio siempre	La conexión de un equipo a la red corporativa (ya sea cableada o inalámbrica) implica la aceptación y cumplimiento de los requisitos de conexión a la Red de

		TMB vigentes.
RA-RD-7	Obligatorio siempre que se use conexión LTE	Las soluciones que implican la conexión de equipos con soluciones de conexión de datos de redes de telefonía móvil (4G/5G/….) han de utilizar SIMs corporativas y APN privado.

2.4 Servidores "on premise"

RA-SR-1	Obligatorio con servidor en TMB	Todo equipo servidor debe estar situado en uno de los CPDs corporativos ubicados en el edificio de Sagrera (entornos productivos) y/o en la cochera de Triangle (entornos de productivos de contingencia, preproducción y desarrollo).
RA-SR-2	Obligatorio con servidor en TMB	Las soluciones deben estar basadas en servidores virtuales sobre VMWare. Las únicas excepciones a esta premisa son: - Equipos que requieran de software no soportado por VMWare o, que el fabricante no proporcione un soporte completo sobre VMWare o requiera de exceso de licenciamiento (como por ejemplo BD Oracle) - Equipos cuyas necesidades de recursos (I/O, tarjeta gráfica, …) impidan o desaconsejen su virtualización.
RA-SR-3	Obligatorio con servidor en TMB	En la fase de diseño se deberán dimensionar los servidores desde el punto de vista de consumo de CPU, RAM y espacio de almacenamiento (S.O. y aplicación) para reservar su espacio en la granja de VMWare
RA-SR-4	Obligatorio con servidor en TMB	Sólo se deberá suministrar HW de servidor en el caso de que justificadamente no se pueda montar la solución sobre servidores virtuales o un responsable de sistemas de TMB indique que debe ampliarse la granja de servidores virtuales.

2.5 Almacenamiento "on premise"

RA-AL-1	Obligatorio si hay base de datos en TMB	En caso de ser necesario almacenamiento adicional, se prefiere el almacenamiento centralizado a través de NAS o SAN frente a soluciones con discos locales, que están desaconsejadas.

RA-AL-2	Obligatorio con base de datos en TMB	En fase de diseño se deberá indicar los requerimientos necesarios de almacenamiento en bloque (criticidad, volumen, tiempos de acceso, necesidad de replicación entre centros, necesidad de snapshots, …), así como indicar claramente las necesidades de espacio y crecimiento futuro previsto. En función de estas necesidades, TMB indicará qué nivel de almacenamiento es el adecuado y reservará espacio en las cabinas corporativas. (All-flash Array)
RA-AL-3	Obligatorio si hay base de datos en TMB	En caso de que no se disponga de espacio en la cabina y sea necesario adquirirlo dentro del proyecto, el responsable de almacenamiento de TMB indicará, una vez entregados los requisitos, qué elementos se deben adquirir.
RA-AL-4	Obligatorio si hay base de datos en TMB	En fase de diseño se deberá indicar los requerimientos necesarios de almacenamiento de fichero (volúmenes, replicación, …) así como indicar claramente las necesidades de espacio, crecimiento y permisos necesarios referenciados a grupos de directorio activo.
RA-AL-5	Obligatorio si hay base de datos en TMB	Para todos los datos de aplicación que se utilicen se deberá presentar un plan de gestión de históricos (archivado y/o eliminación).
RA-AL-6	Obligatorio si hay datos en TMB	El acceso a los datos debe otorgarse a identificadores nominales y en función de lo que el usuario necesite saber o acceder para el desarrollo de su puesto de trabajo.
RS-AL-7	Obligatorio si hay datos en TMB	Se debe especificar claramente los datos de los que hay que hacer copia de seguridad, así como la periodicidad y retención de las mismas. Se debe entregar un procedimiento de asignación de permisos de acceso a los datos y recursos.

2.6 Bases de datos

RA-BD-1	Obligatorio si hay base de datos en TMB	En el caso de necesitar base de datos, en general se prefiere consolidar en bases de datos corporativas a una base de datos dedicada.
RA-BD-2	Obligatorio si hay base de	Las plataformas de BBDD actualmente soportadas son Oracle y SQL (siempre sobre versiones con soporte de

	datos en TMB	fabricante vigente) Otras opciones están desaconsejadas ya que no podrán ser gestionadas y/o administradas por el personal de TMB.
RA-BD-3	Obligatorio si hay base de datos en TMB	El diseño deberá proveer una descripción de los permisos necesarios y las estimaciones de espacio necesario y crecimiento anual.
RA-BD-4	Obligatorio si hay base de datos en TMB	Para todas las bases de datos que se creen o actualicen, se deberá presentar un plan de gestión de históricos (archivado y/o eliminación).
RA-BD-5	Obligatorio si hay base de datos en TMB	Toda creación de una base de datos también implicará también la presentación de una política de mantenimiento de datos, backup, y monitorización.
RA-BD-6	Obligatorio siempre	No se aconsejan mecanismos de réplicas entre diferentes bases de datos y no están permitidos entre las bases de datos corporativas existentes.
RA-BD-7	Obligatorio si hay base de datos en TMB	Se ha de contemplar en el diseño la existencia en las bases de datos corporativas de entornos de desarrollo, integración y producción y, si el sistema lo requiere, la instalación y documentación en todos los entornos.
RA-BD-8	Obligatorio si hay base de datos en TMB	En caso de que la base de datos contenga datos personales sujetos al RGPD, se debe proporcionar cifrado de estos datos y, en caso de que sea necesario la copia a desarrollo o integración se debe proporcionar la anonimización de los datos personales.
RA-BD-9	Obligatorio si hay datos en TMB	El acceso a los datos debe otorgarse a identificadores nominales y en función de lo que el usuario necesite saber o acceder para el desarrollo de su puesto de trabajo. Se debe entregar un procedimiento de asignación de permisos de acceso a los datos y recursos.
RA-BD-10	Obligatorio si hay datos personales en la BBDD	En caso de que la Base de Datos contenga datos personales que estén afectados por el RGPD se verá cifrar esta información en la Base de Datos.

2.7 PCs, estaciones de trabajo y otros sistemas distribuidos

En esta categoría se incluyen todo aquel equipamiento necesario fuera del CPD con procesador y un sistema operativo. Comúnmente son PCs, puestos de trabajo o equipos para control o gestión de otros dispositivos.

Se considera que tiene necesidades de tipo “equipo industrial” todo aquel que, por tamaño, ubicación, robustez, condiciones ambientales, consumo, características de

procesamiento en tiempo real, … requiere de soluciones específicas distintas a las de un PC estándar.

RA-SD-1	Obligatorio siempre que se use/instale un equipo en TMB	Una estación de trabajo sólo puede usarse para que un usuario interactúe con el sistema. No pueden, por tanto, utilizarse para procesos en background o tareas batch propios de equipos centrales.
RA-SD-2	Obligatorio siempre que se use/instale un equipo en TMB	En el caso de que la función de una estación de trabajo sea crítica y se tenga que garantizar su funcionamiento, se debe basar en servidores de aplicaciones o escritorios centralizados y con equipos distribuidos exclusivamente de acceso remoto (PCs corporativos, thin clients, …)
RA-SD-3	Obligatorio siempre que se use/instale un equipo en TMB	Los sistemas de backup corporativos no están diseñados ni operados para trabajar con estaciones de trabajo. Toda información que necesite ser protegida, debe almacenarse en repositorios centralizados en equipos del CPD.
RA-DS-4	Obligatorio siempre que se use/instale un equipo en TMB	Todo equipo que se instale en la red de TMB debe tener instalado un software antimalware y configurado para que se actualice automáticamente para estar al día. Preferiblemente este software será el que esté homologado en TMB.
RA-DS-5	Obligatorio siempre que se use/instale un equipo en TMB	Todo equipo que se instale en la red de TMB debe tener activados los registros de acceso y auditoría del sistema.
RA-DS-6	Obligatorio siempre que se use/instale un equipo en TMB	Todo equipo que se instale en la red de TMB debe actulizar el sistema conforme a la política de parcheado y cambio de sistema de TMB.

2.8 Gestión de la obsolescencia

RO-OB-1	Obligatorio si hay equipos en TMB	El sistema deberá indicar el fin de soporte del fabricante previsto para cada uno de sus componentes.
RO-OB-2	Obligatorio si hay equipos en TMB	En el momento de la puesta en marcha, el sistema no podrá incluir en su diseño componentes sin soporte por parte del fabricante (obsoletos) o con un fin de soporte previsto anterior al fin de la garantía.
RO-OB-3	Obligatorio si hay equipos en TMB	En caso de los componentes afectados por obsolescencia dentro de la vida útil prevista, se deberá proveer los procedimientos para sustituir/actualizar los elementos obsoletos y corregir las posibles afectaciones a otros componentes, con una estimación económica de los costes a incurrir.

3 Servidores

3.1 Requisitos Hardware

RS-HW-1	Obligatorio si el servidor está en TMB	El hardware deberá ser un modelo homologado en TMB, de última generación. Actualmente el modelo standard son servidores tipo blade HPE Synergy
RS-HW-2	Obligatorio si el servidor está en TMB	Todo servidor debe ir instalado en un rack del CPD de Sagrera o en el de Triangle.
RS-HW-3	Obligatorio si el servidor está en TMB	Al menos tres meses antes de la instalación deberán detallarse las necesidades de espacio físico en rack, alimentación eléctrica (sólo monofásica), refrigeración, puntos de red de datos y puntos de red de SAN y tipo de conectores (enchufes, latiguillos, …).
RS-HW-4	Obligatorio si el servidor está en TMB	Los procesadores han de ser Intel
RS-HW-5	Obligatorio si el servidor está en TMB	En el caso de servidores blade, siempre se incluirán 4 puertos de LAN 100/1000 y 2 de fiber channel. En caso de servidores stand-alone, incluirán un puerto de red adicional independiente para el acceso a la gestión remota. También incluirán 2 puertos fiber channel si es necesario su conexión a la SAN.
RS-HW-6	Obligatorio si el servidor está en TMB	La alimentación del equipo debe ser monofásica
RS-HW-7	Obligatorio si el servidor está en TMB	El equipo debe estar equipado con una segunda fuente de alimentación redundante.
RS-HW-8	Obligatorio si el servidor	El disco del sistema operativo debe estar en mirror

	está en TMB	
RS-HW-9	Obligatorio si el servidor está en TMB	Todo servidor físico debe llevar ILO con su correspondiente licencia para la gestión remota avanzada.
RS-HW-10	Obligatorio si el servidor está en TMB	Todos los equipos y cables deben quedar correctamente colocados, etiquetados y documentados según la normativa vigente en TMB.
RS-HW-11	Obligatorio si el servidor está en TMB	Todo el material sobrante de la instalación (cajas, embalajes, …) debe ser retirado por el propio proveedor tras la instalación.

3.2 Sistema operativo

RS-SO-1	Obligatorio si el servidor está en TMB	El sistema operativo debe estar homologado y soportado por TMB. Actualmente están soportados **Windows Server** o **Red Hat Enterprise Linux** en la última versión vigente.
RS-SO-2	Obligatorio si el servidor está en TMB	El sistema operativo se ha de suministrar actualizado a la última versión y último nivel de ServicePack y parches.
RS-SO-3	Obligatorio si el servidor está en TMB	El sistema operativo deberá venir correctamente licenciado a nombre de Ferrocarril Metropolità de Barcelona S.A y/o Transports de Barcelona, S.A., con licencias que permitan su reutilización posterior en caso de substitución del HW.

3.3 Requisitos de seguridad

RS-SG-1	Obligatorio siempre	La plataforma/S.O. deberá garantizar el acceso y almacenamiento seguro: a los datos, a los dispositivos y a los servicios que ofrece.
RS-SG-2	Obligatorio	La plataforma/S.O. deberá garantizar que solo las

	siempre	actualizaciones generadas por entidades acreditadas puedan actualizar el sistema.
RS-SG-3	Obligatorio siempre	Todo sistema debe incorporar un software antimalware o el mecanismo de control de lista blanca corporativos y el firewall local activado y configurado.
RS-SG-4	Obligatorio si el servidor está en TMB	En caso de disponer de sistemas de contingencia, su activación debe ser transparente para el resto de sistemas con los que se integre.
RS-SG-5	Obligatorio siempre	Las aplicaciones deben correr en una cuenta de usuario con el menor privilegio posible. Deben ser cuentas de servicio que no permitan hacer login desde un terminal.
RS-SG-6	Obligatorio si el servidor está en TMB	Todas las funcionalidades superfluas del sistema operativo deben venir desinstaladas o, en su defecto, deshabilitadas
RS-SG-7	Obligatorio si hay equipos en TMB	Todas las contraseñas de usuario deben poderse cambiar de forma centralizada (en el caso de equipos Windows, es automático con la pertenencia al Dominio).
RS-SG-8	Obligatorio si el servidor está en TMB	El servidor debe integrarse con los sistemas de backups corporativos, por lo cual se deberá especificar de qué directorios se ha de hacer backup y con qué periodicidad y retención. (NOTA) La integración con los sistemas corporativos puede implicar la instalación de un agente en el equipo.
RS-SG-9	Obligatorio si el equipo está en TMB	Seguir las recomendaciones de ciberseguridad de TMB para servidores.
RS-SG-10	Obligatorio si el equipo servidor está en TMB	Se deben eliminar los usuarios 'invitado', cambiar la contraseña por defecto de los usuarios que haya definidos, sobretodo el de administrador.

3.4 Otros requisitos de instalación

RS-OT-1	Obligatorio si hay	Los equipos Windows deben integrarse con uno de los dominios corporativos basados en Microsoft Active

	equipos en TMB	Directory para facilitar la gestión de usuarios y equipos.
RS-OT-2	Obligatorio si hay equipos en TMB	Los equipos Linux deben integrarse con las herramientas de gestión centralizada de configuraciones (Ansible) y parches (SuSEManager)
RS-OT-3	Obligatorio si hay equipos en TMB	Todos los equipos deben sincronizar la hora mediante protocolo NTP con los servidores de tiempos de TMB (en el caso de equipos Windows, es automático con la pertenencia al Dominio).
RS-OT-4	Obligatorio si hay equipos en TMB	El servidor ha de permitir la instalación de los agentes necesarios para su correcta integración con las herramientas de gestión (backup, monitorización, gestión de la SAN, planificador, distribución de software y parches, …)
RS-OT-5	Obligatorio si hay equipos en TMB	Los servidores se accederán únicamente mediante la herramienta PAM de TMB para su gestión y administración remota.

3.5 Software y aplicaciones

RS-SW-1	Obligatorio si hay equipos en TMB	Las aplicaciones deben hacer uso del DNS para la comunicación con otros equipos. No puede haber direcciones IP en el código o en ficheros de configuración de las aplicaciones.
RS-SW-2	Obligatorio si hay equipos en TMB	Las aplicaciones que no requieran de intervención del usuario deben correr sin necesidad de que haya una sesión iniciada
RS-SW-3	Obligatorio si hay equipos en TMB	El sistema debe estar totalmente operativo tras un reinicio sin necesidad de intervención por parte de un operador o un usuario.
RS-SW-4	Obligatorio si hay equipos en TMB	En caso de necesidad de planificación de tareas periódicas automatizadas, estas se deberán integrar con el planificador de tareas corporativo.
RS-SW-5	Recomendación	Se debe en lo posible automatizar el despliegue de las soluciones por si se han de repetir en el futuro, facilitar el mantenimiento o, sencillamente, facilitar la documentación de todo lo instalado y configurado.

4 PCs y estaciones de trabajo

4.1 Requisitos Hardware

RE-HW-1	Obligatorio si hay equipos en TMB	El HW de todos los puestos de operación necesarios se deben adecuar a los equipos homologados por TMB.

4.2 Requisitos de Sistema Operativo

RE-SO-1	Obligatorio si hay equipos en TMB	El sistema operativo para PCs y estaciones de trabajo ha de ser Windows 11 Professional OEM.
RE-SO-2	Obligatorio si hay equipos en TMB	Todos los equipos (incluyendo los monitores u otros) deberán incorporar una garantía de fabricante de 4 años.
RE-SO-3	Obligatorio si hay equipos en TMB	Es obligatorio la realización de la task sequence a través de SCCM para obtener una maqueta.
RE-SO-4	Obligatorio si hay equipos en TMB	El despliegue masivo de los equipos debe estar basado en la distribución mediante SCCM (Micorosoft System Center Configuration Manager).
RE-SO-5	Obligatorio si hay equipos en TMB	Tanto los equipos como las cuentas de usuario, así como los recursos en red necesarios deben estar integrados bajo un Active Directory (de ahora en adelante AD).
RE-SO-5	Obligatorio si hay equipos en TMB	Las políticas en el AD deben estar documentadas con detalle y describir el objetivo claramente de las mismas. La estructura de Organizational Unit deberá ser establecida mediante acuerdo con TMB.
RE-SO-6	Obligatorio si hay equipos en TMB	Todos los equipos deberán permitir las actualizaciones mensuales de Microsoft sin merma de la disponibilidad de las aplicaciones que deben correr en el equipo.
RE-SO-7	Obligatorio si hay equipos en TMB	Las aplicaciones dispondrán de las actualizaciones necesarias para su computabilidad con la actualización del sistema operativo y drivers.

RE-SO-8	Obligatorio si hay equipos en TMB	Las aplicaciones deberán ser compatibles con cualquier monitor, KVM, proyectores u otro cualquiera que tengan compatibilidad con el sistema operativo.
RE-SO-9	Obligatorio si hay equipos en TMB	La resolución de video deberá ser adaptable y compatible con cualquier dispositivo de video mientras este sea compatible con el sistema operativo, sin que se deforme el formato de salida.

4.3 Requisitos de seguridad

RE-SG-1	Obligatorio si hay equipos en TMB	Todo PC y estación de trabajo debe integrarse bajo el antivirus y software antimalware o el mecanismo de control de lista blanca corporativos
RE-SG-2	Obligatorio si hay equipos en TMB	Las cuentas de los usuarios deben estar integradas bajo la herramienta de Gestión de Identidades de TMB (siendo en este caso usuarios sólo aquellas personas que hacen login en la máquina y disponen un escritorio con acceso a las aplicaciones y datos, incluye MFA). En cualquier caso, la solución siempre debe garantizar la trazabilidad del uso que se haga desde el equipo (qué, quién, cómo, cuándo, dónde). Si la solución propone un equipo multiusuario en modo quiosco sólo mostrará la/s aplicación/es que garanticen la trazabilidad a través de las cuentas usuarios nominales. En cuanto a los usuarios utilizados para arrancar servicios (cuando sean necesarios) en los equipos deben estar integrados en el DA de TMB.
RE-SG-3	Obligatorio siempre	Las aplicaciones deben correr en una cuenta de usuario con el menor privilegio posible
RE-SG-4	Obligatorio si hay equipos en TMB	Todas las contraseñas de usuario deben poderse cambiar de forma centralizada (en el caso de equipos Windows, es automático con la pertenencia al Dominio).
RE-SG-5	Obligatorio si el equipo está en TMB	Seguir las recomendaciones de ciberseguridad de TMB para estaciones de trabajo.

4.4 Otros requisitos

RE-OT-1	Obligatorio si hay equipos en TMB	Todo PC y estación de trabajo deben integrarse con uno de los dominios corporativos basados en Microsoft Active Directory para facilitar la gestión de usuarios y equipos (si existe para estos elementos de OT) y en caso contrario debería generarse uno nuevo para su posterior federación con el existente en TMB.
RE-OT-2	Obligatorio si hay equipos en TMB	Las aplicaciones deben hacer uso del DNS para la comunicación con otros equipos. No puede haber direcciones IP en el código o en ficheros de configuración de las aplicaciones.
RE-OT-3	Obligatorio si hay equipos en TMB	Todos los PCs y estaciones de trabajo deben sincronizar la hora mediante protocolo NTP con los servidores de tiempos de TMB (en el caso de equipos Windows, es automático con la pertenencia al Dominio).
RE-OT-4	Obligatorio siempre para equipos en TMB	Para la distribución de aplicaciones en PCs, se debe seguir el siguiente modelo: • Distribución mediante Microsoft App-VDistribución de software mediante Microsoft SCCM. En todos los casos, se deberá documentar el procedimiento de generación de los paquetes e instalación.

5 Sistemas distribuidos industriales

5.1 Requisitos Hardware

RI-HW-1	Obligatorio si hay equipos en TMB	El diseño del equipo debe ser industrial, tanto desde el uso de CPUs de rango industrial (variantes industriales de CPUs con arquitectura x86 AMD, Intel o ARM), así como todos sus componentes/periféricos (tarjeta gráfica, expansión de puertos, modem, módulos de comunicaciones, I/O…) hasta el diseño del chasis que lo aloja.
RI-HW-2	Obligatorio si hay equipos en TMB	Los conectores deben ser de tipo industrial con fijaciones que soporten las normativas correspondientes en cada caso y permitan un mantenimiento sencillo. Por ejemplo, conectores resistentes a las vibraciones, desgaste, degradación por calor, etc., ….
RI-HW-3	Obligatorio si hay equipos en TMB	Los medios de almacenamiento no deben ser fácilmente accesibles desde el exterior por seguridad, pero si deben facilitar en la medida de lo posible el mantenimiento de los mismos.
RI-HW-4	Obligatorio si hay equipos en TMB	El criterio para definir si el conector hembra se coloca en la placa o en el cable es el siguiente: es más valiosa la instalación que los equipos siempre que su reparación y/o cambio suponga una larga inmovilización del vehículo/tren o una compleja sustitución de la instalación fija. En este sentido se prefiere el conector hembra en el cable en vez de en el equipo porque es más robusto y menos propenso a una intervención (sustitución y/o reparación).
RI-HW-5	Obligatorio si hay equipos en TMB	El equipo debe disponer de un fusible rápido (de acceso exterior) que lo proteja de sobre intensidades.
RI-HW-6	Obligatorio si hay equipos en TMB	El equipo debe cumplir las normativas específicas en el caso de ir embarcado en un vehículo de transporte de pasajeros o las normativas ferroviarias en el caso de ir embarcado en un tren, y además, debe venir acompañado de todas aquellas certificaciones oficiales que acrediten el cumplimiento de tales normativas. Por ejemplo, normativas: marcado E-mark, medioambientales, mecánicas, vibración, temperatura, humedad, eléctricas y electromagnéticas, inmunidad, emisiones radiadas y conducidas, compatibilidad electromagnética.

RI-HW-7	Obligatorio si hay equipos en TMB	Los medios de almacenamiento deben ser de tipo industrial para garantizar robustez, durabilidad y fiabilidad. Si el equipo industrial va a ser embarcado en vehículo/tren o susceptible de vibraciones se deben emplear medios de almacenamiento no mecánicos tales como SSD de rango industrial (discos de estado sólido) o CF industriales (Compact Flash). No se recomienda el uso de memorias flash tipo NAND (flash usb, SD, …) por su poca robustez frente a corrupciones de datos, en su lugar se prefieren memorias de tipo NOR o hibridas que aúnen lo mejor de las dos tecnologías (EFDs, ORNAND, OneNAND, mDOC…)
RI-HW-8	Obligatorio si hay equipos en TMB	Todos los conectores deben ir correctamente fijados al chasis mediante elementos de sujeción que eviten que se aflojen o se degraden al manipularlos y al recibir choques y vibraciones.
RI-HW-9	Obligatorio si hay equipos en TMB	El diseño del chasis debe favorecer la disipación de calor y la circulación de aire, así como la disposición de componentes, dispositivos y placas de expansión en el interior de la cpu.
RI-HW-10	Obligatorio si hay equipos en TMB	El slot del medio de almacenamiento, ya sea de tipo compact flash o disco duro de estado sólido debe tener un sistema de sujeción firme, robusto y duradero frente a las vibraciones, choques y manipulaciones.
RI-HW-11	Obligatorio si hay equipos en TMB	El equipo debe estar correctamente fijado preferiblemente mediante elemento standard tipo rack o carril DIN. En el caso de ir embarcado y en función de las vibraciones a las que pueda ser sometido, se recomiendan el uso de sistemas de absorción de vibraciones.
RI-HW-12	Obligatorio si hay equipos en TMB	La disposición del equipo/s y periféricos debe facilitar la disipación de calor y la circulación de aire.
RI-HW-13	Obligatorio si hay equipos en TMB	La disposición del equipo/s y periféricos debe facilitar el mantenimiento, tanto para la substitución del equipo, como para el cambio de un periférico, por ejemplo, tipo CF o disco SSD.
RI-HW-14	Obligatorio si hay equipos en TMB	El proveedor del equipo industrial debe facilitar un programa de test hardware y diagnóstico, tanto del equipo/s, periféricos, placas de I/O, así como del diagnóstico de todo el conjunto.

5.2 Requisitos de fiabilidad técnica

RI-FT-1	Obligatorio si hay equipos en TMB	Los requerimientos hardware del sistema deberán ser lo mínimo posible para cumplir todas las funcionalidades actuales y futuras. Se debe minimizar el consumo de energía y CPU, esto implica una temperatura de trabajo menor y un aumento de la fiabilidad en general.
RI-FT-2	Obligatorio si hay equipos en TMB	La arquitectura de integración debe ser lo más simple posible para favorecer la fiabilidad, el mantenimiento y el impacto en el resto del sistema donde se integre el equipo.

5.3 Requisitos del sistema operativo

RI-SO-1	Obligatorio si hay equipos en TMB	El equipo debe tener un Sistema Operativo de tipo Industrial, ya sean versiones basadas en Linux industriales o customizadas a tal efecto, o bien, soluciones comerciales para entornos embebidos o industriales tipo Windows Embedded.
RI-SO-2	Obligatorio si hay equipos en TMB	El sistema Operativo debe ser totalmente robusto frente a cortes de alimentación, reinicios continuados y corrupciones.
RI-SO-3	Obligatorio si hay equipos en TMB	El Sistema Operativo debe ser lo más eficiente posible y lo más reducido, tanto en espacio, como en consumo de recursos.
RI-SO-4	Obligatorio si hay equipos en TMB	Los sistemas de ficheros empleados y el particionado del medio de almacenamiento deben ser robustos frente a corrupciones de datos. El tipo de sistema de ficheros debe garantizar que, ante cortes de corriente o reinicios, el sistema operativo y las aplicaciones no se corrompen, y que los datos perdidos sean mínimos. Por esta razón, se recomienda el uso de particiones o incluso dispositivos de almacenamiento diferenciados para S.O/aplicaciones Vs Datos.
RI-SO-5	Obligatorio si hay equipos en TMB	El encapsulado del sistema operativo debe ser de tal forma que permita de una forma lo más simple posible su actualización completa, parcial, así como del kernel y las aplicaciones de forma desatendida.
RI-SO-6	Obligatorio si hay equipos en	El sistema debe quedar completamente operativo tras un reinicio, sin necesidad de intervención manual y arrancando en el menor tiempo posible.

	TMB	
RI-SO-7	Obligatorio si hay equipos en TMB	Los sistemas que no requieran interactuar con el usuario para su funcionamiento, no deben iniciar sesión y todo el software debe correr en modo servicio.
RI-SO-8	Obligatorio si hay equipos en TMB	La plataforma de S.O debe facilitar la integración de la forma más transparente posible de los distintos tipos de hardware, es decir, se aboga por soluciones de plataforma únicas que integren los diferentes evolutivos de hardware y no requieran el mantenimiento de diversas plataformas de S.O en función del hardware.
RI-SO-9	Obligatorio si hay equipos en TMB	La plataforma S.O debe integrar la gestión energética del HW, por ejemplo, para monitorizar los voltajes y temperatura del hardware.
RI-SO-10	Obligatorio si hay equipos en TMB	La plataforma S.O debe facilitar un mecanismo de administración remota que facilite tareas de administración, mantenimiento y configuración.
RI-SO-11	Obligatorio si hay equipos en TMB	La plataforma S.O debe ser robusta y tener mecanismos de prevención, chequeo y reparación de corrupciones lógicas y físicas de los medios de almacenamiento.

5.4 Requisitos de seguridad

RI-SG-1	Obligatorio siempre	La plataforma/S.O. deberá garantizar el acceso y almacenamiento seguro: a los datos, a los dispositivos y a los servicios que ofrece.
RI-SG-2	Obligatorio siempre	La plataforma/S.O. deberá garantizar que solo las actualizaciones generadas por entidades acreditadas puedan actualizar el sistema.
RI-SG-3	Obligatorio siempre	Todo sistema debe incorporar el software antimalware o el mecanismo de control de lista blanca corporativos
RI-SG-4	Obligatorio siempre	Todo sistema debe incorporar un sistema de firewall que habilite únicamente lo necesario y bloquee el resto.
RI-SG-5	Obligatorio siempre	En caso de disponer de sistemas de contingencia, su activación debe ser transparente para el resto de sistemas con los que se integre.
RI-SG-6	Obligatorio	Las aplicaciones deben correr en una cuenta de usuario

	siempre	con el menor privilegio posible
RI-SG-7	Obligatorio siempre	Todas las funcionalidades superfluas del sistema operativo deben venir desinstaladas o, en su defecto, deshabilitadas
RI-SG-8	Obligatorio siempre para equipos en TMB	Todas las contraseñas de usuario deben poderse cambiar de forma centralizada o por medio del sistema de actualización de forma desatendida sin necesidad de actualizar todo el S.O.
RI-SG-9	Obligatorio siempre	Los sistemas de backup corporativos no están diseñados ni operados para trabajar con equipos distribuidos. Toda información que necesite ser protegida, debe almacenarse en repositorios centralizados en equipos del CPD, o bien, la plataforma del sistema debe garantizar su propio sistema de backup y contingencia.
RI-SG-10	Obligatorio siempre para equipos en TMB	Todos los accesos a los equipos deben quedar trazados en un formato de sólo lectura que no permita su modificación posterior.

5.5 Otros requisitos

RI-OT-1	Obligatorio si hay equipos en TMB	Todos los equipos Windows deben integrarse con uno de los dominios corporativos basados en Microsft Active Directory para facilitar la gestión de usuarios y equipos. En el caso de equipos Linux deben proveerse mecanismos y herramientas para gestionar de forma centralizada los usuarios.
RI-OT-2	Obligatorio siempre	Las aplicaciones deben hacer uso del DNS para la comunicación con otros equipos. No puede haber direcciones IP en el código o en ficheros de configuración de las aplicaciones.
RI-OT-3	Obligatorio si hay equipos en TMB	Todos los equipos deben sincronizar la hora mediante protocolo NTP con los servidores de tiempos de TMB (en el caso de equipos Windows, es automático con la pertenencia al Dominio).
RI-OT-4	Obligatorio si hay equipos en TMB	En el caso de instalación mediante maqueta, se deben entregar los procedimientos para su posterior mantenimiento y actualización.

6 Operación y mantenimiento

6.1 Monitorización

RO-MO-1	Obligatorio si se necesita soporte de TMB	Todo equipo que en caso de malfuncionamiento necesite de intervención por parte de OTS (Operaciones de Tecnologías y Sistemas) o pueda afectar a un servicio del Área de Tecnología de TMB debe estar monitorizado e integrado en la consola corporativa de monitorización para los operadores de OTS.
RO-MO-2	Obligatorio si se necesita soporte de TMB	Los sistemas se han de monitorizar desde dos puntos de vista. • Visión de sistema (monitorización agregada). El objetivo es construir una visión del estado del servicio/sistema *como suma de los estados individuales de todos sus componentes*. Para ello es necesarios identificar todos los componentes tecnológicos individuales y sus relaciones. Esta información debe ser debidamente incorporada o actualizada en la CMDB corporativa. • Visión de Cliente (monitorización directa). El objetivo es construir una visión del estado del servicio/sistema *lo más parecida a lo que percibe el cliente final*.
RO-MO-3	Obligatorio si se necesita soporte de TMB	Toda la monitorización debe estar basada en una de las siguientes tecnologías: • Envío por parte de los equipos de traps SNMP basados en MIBs • Interrogación directa del estado por algún elemento de la infraestructura de monitorización a través de protocolos estándar (SSH, WMI, SNMP, Web Services, …). Si ninguno de estos protocolos habituales está disponible, no se puede garantizar la monitorización.
RO-MO-4	Obligatorio si se necesita soporte de TMB	Con la información de relaciones proporcionada anteriormente, debe suministrase además la información necesaria (pesos, dependencias) con la que se pueda implementar la Gestión de Impacto a las herramientas corporativas y que permita a operación priorizar sus actuaciones.
RO-MO-5	Obligatorio si se necesita	Con la unión de los eventos detectados o recibidos de la Visión de Sistema y la Visión de Cliente se debe construir un *Catálogo de Eventos* del servicio o

	soporte de TMB	sistema, que debe recoger todos los eventos ya sea generado por interrogación o generado por el propio sistema mediante traps SNMP
RO-MO-6	Obligatorio si se necesita soporte de TMB	Si es posible el uso de interrogación remota, para cada tipología de componente a monitorizar se debe indicar cómo supervisar y comprobar el estado de funcionamiento (lista de los parámetros a monitorizar y los umbrales de generación de alarma).
RO-MO-7	Obligatorio si se necesita soporte de TMB	Para cada tipología de componente a monitorizar se debe indicar qué eventos pueden originar y que serán enviados a la plataforma de monitorización de TMB junto con su severidad y/o criticidad que se debe mostrar.
RO-MO-8	Obligatorio si se necesita soporte de TMB	Toda alarma debe tener documentado el procedimiento de operación correspondiente para para resolver la situación de degradación o no disponibilidad del servicio/sistema.
RO-MO-9	Obligatorio si se necesita soporte de TMB	Toda alarma debe tener su correspondiente contraalarma para garantizar la integridad y coherencia de la monitorización.

6.2 Mantenimiento reactivo

RO-MR-1	Obligatorio si hay equipos en TMB	Todo elemento HW debe llevar asociado un mantenimiento de substitución o reparación de piezas de acuerdo a su criticidad.
RO-MR-2	Obligatorio si hay equipos en TMB	En el caso del equipamiento central, el HW del equipo debe tener un mantenimiento 24 x 7 in-situ con un tiempo de respuesta de como mucho 4 horas para equipos críticos y de 8 x 5 in-situ con respuesta en siguiente laborable para el resto.
RO-MR-3	Obligatorio si hay equipos en TMB	Los servidores y appliance que se adquieran deberán tener una extensión de garantía de al menos 4 años con el fabricante.
RO-MR-4	Obligatorio si hay equipos en	El sistema debe contemplar los mecanismos y procedimientos lo más automatizado posible para la

	TMB	restauración del sistema y su configuración tras una incidencia.
RO-MR-5	Obligatorio si hay equipos en TMB	En caso de ser necesaria la interacción remota con la sesión abierta para la resolución de incidencias o su mantenimiento, el sistema debe permitir la captura de sesión.
RO-MR-6	Recomendación	(RECOMENDACIÓN) Los sistemas distribuidos deberían integrarse con la herramienta de control remoto corporativa, que puede implicar la instalación de un agente en la máquina.

6.3 Mantenimiento preventivo y actualizaciones

RO-MP-1	Obligatorio si hay equipos en TMB	El sistema debe proveer de algún método o herramienta y de un procedimiento que permita el despliegue y actualización del equipo a nivel de S.O y aplicaciones de forma remota (ethernet, wireless, 3G/4G…) y desatendida
RO-MP-2	Obligatorio si hay equipos en TMB	El sistema debe proveer de algún método o herramienta que permita el despliegue y actualización del equipo a nivel de S.O y aplicaciones de forma local (tipo llave USB, …)
RO-MP-3	Recomendación	(RECOMENDACIÓN) Los sistemas distribuidos deberían integrarse con la herramienta de distribución de software corporativa, que puede implicar la instalación de un agente en la máquina.
RO-MP-4	Obligatorio si hay equipos en TMB	El sistema operativo de todos los equipos debe ser actualizado a último nivel de parches al menos dos veces cada año, sin excluir que se deba realizar una actualización por una vulnerabilidad grave.
RO-MP-5	Obligatorio si hay equipos en TMB	Los sistemas Windows se deben integrar con la herramienta de distribución de software, parches e inventario, que actualmente es Microsoft SCCM.
RO-MP-6	Obligatorio si hay equipos en TMB	La política de distribución de parches implica la distribución de todos los parches de forma gradual a todos los equipos. Si el sistema no se adapta a esta política se deben proporcionar mecanismos y recursos ad-hoc para validar qué parches se distribuyen y realizar dicha distribución.
RO-MP-7	Obligatorio si hay equipos en TMB	El sistema debe poder permitir realizar un inventario de las aplicaciones instaladas en cada equipo y su versión.

6.4 Documentación

RO-DC-1	Obligatorio	Se ha de entregar la documentación, en el formato indicado por TMB, de todo el sistema montado. La documentación incluirá al menos aspectos de: - Arquitectura física y lógica del sistema - Guías de operación (arranque y parada del sistema, consulta de estado, consulta de logs, …) - Parámetros a monitorizar, umbrales y guía de acciones correctoras a ejecutar para cada alarma o trap SNMP que el sistema envíe - Guías de administración/mantenimiento y resolución de incidencias - Listado de directorios y tipo de información de la que se debe realizar backup - Tareas planificadas - Consumos: Eléctrico, refrigeración, espacio en CPDs, …
RO-DC-2	Obligatorio	Se ha de actualizar la CMDB con la información relativa a los sistemas
RO-DC-3	Obligatorio	Si el sistema crea o modifica un Servicio o Producto de TMB (según el modelo de buenas prácticas ITIL implementadas en TMB), deberá actualizarse la documentación correspondiente
RO-DC-4	Obligatorio	Se ha de entregar la documentación original relativa a las licencias adquiridas
RO-DC-5	Obligatorio	Se ha de entregar la documentación de toda formación realizada

7 Integración de Sistemas, Servicios y Datos

7.1 Requisitos generales

REQ-INT-01	Obligatorio	De requerir **autenticación,** se debe implementar una basada en **SAML 2.0** y **OpenID Connect (OIDC)** para integrarse con los proveedores de identidad de **TMB**.
REQ-INT-02	Obligatorio	Todas las comunicaciones deben estar protegidas mediante **HTTPS** con **TLS 1.2** o superior.
REQ-INT-03	Recomendable	Implementar un sistema de **logging centralizado** para recopilar y gestionar logs de todas las aplicaciones y servicios.
REQ-INT-04	Recomendable	Utilizar **agentes de monitoreo** para supervisar el rendimiento y estado de los sistemas, asegurando un impacto mínimo en el rendimiento. Se recomienda agentes como **Filebeat, NXLog, Vector.dev** o similares. Se recomienda ofrecer endpoints de health compatibles con Prometheus para las métricas.
REQ-INT-05	Obligatorio	Los servicios deben cumplir con los **estándares de seguridad** y regulaciones aplicables del **Esquema Nacional de Seguridad (ENS)**.
REQ-INT-06	Obligatorio	Las APIs deben manejar errores de forma consistente, utilizando códigos de estado HTTP correctos y mensajes de error claros sin revelar información sensible.
REQ-INT-07	Recomendable	Se debe proveer **documentación actualizada** de las APIs utilizando **OpenAPI (Swagger)** de aquellos servicios que se ofrezcan.
REQ-INT-08	Recomendable	Implementar **control de versiones** en las APIs para facilitar la gestión de cambios y mantener compatibilidad hacia atrás.
REQ-INT-09	Obligatorio	Las integraciones internas deben realizarse a través de **APIs RESTful** seguras, siguiendo convenciones estándar y utilizando la autenticación corporativa. Recomendable vía **OIDC,** disponible también vía **APIKey.**
REQ-INT-13	Obligatorio	Cumplir con los estándares internos de seguridad y políticas de **gestión de datos** de TMB.
REQ-INT-14	Obligatorio	Para aquellas integraciones con sistemas OT. Cumplir con la **norma IEC 62443** para garantizar la seguridad. Aplicar **segmentación de redes** y principios de **mínimo privilegio.**

REQ-INT-16	Obligatorio	Las integraciones en sistemas OT internos deben realizarse a través de **protocolos seguros** y **APIs controladas**, evitando accesos directos o conexiones nativas.
REQ-INT-17	Recomendable	Realizar **evaluaciones de riesgo** y análisis de impacto regularmente en estas integraciones.
REQ-INT-18	Obligatorio	Las integraciones con sistemas externos deben realizarse a través de **APIs REST** seguras, utilizando autenticación robusta y control de acceso. Preferiblemente publicadas por **TMB API.**
REQ-INT-19	Obligatorio	Implementar **cifrado de datos en tránsito** para todas integraciones con sistemas externos. **Y en reposo** también para aquello que contenga datos sensibles.
REQ-INT-21	Obligatorio	Evitar métodos inseguros, directos o anticuados como **FTP**, **SFTP, SOAP** en integraciones con sistemas internos o externos.
REQ-INT-22	Obligatorio	Aplicar **segmentación de redes** y establecer **zonas desmilitarizadas (DMZ)** para conexiones con sistemas OT, en base a la IEC 62443,
REQ-INT-23	Obligatorio	Mantener **registros de auditoría** de todas las interacciones en los sistemas. Para para facilitar el seguimiento y la resolución de incidencias.
REQ-INT-24	Obligatorio	Las integraciones con sistemas externos deben pasar por **pasarelas de seguridad** y cumplir con las políticas de seguridad de **TMB.** En aquellos entornos segmentados por red, especialmente en el mundo OT, no deberán ser directas. Podrán hacer uso de la DMZ, y preferiblemente irán al **API de TMB**.
REQ-INT-25	Obligatorio	Implementar **validación y sanitización** de todos los datos provenientes de sistemas externos. Sobre todo en servicios de ficheros.
REQ-INT-26	Obligatorio	Utilizar el **API Gateway de TMB** para gestionar y proteger las APIs expuestas externamente, incluyendo autenticación, autorizaciones y rate limiting.
REQ-INT-27	Obligatorio	Los datos sensibles deben ser **cifrados** y cumplir con las políticas de protección de datos de la organización y regulaciones como **GDPR**.
REQ-INT-28	Recomendable	Todas aquellas integraciones de datos, que requieran de un flujo constante, deberá usar el **broker corporativo** basado en **Apache Kafka** para el streaming de datos.

REQ-INT-29	Recomendable	Para aplicaciones que requieran comunicación ligera y eficiente, considerar el uso del **protocolo MQTT** del **broker corporativo.**
REQ-INT-30	Recomendable	Los logs deben ser almacenados en un **sistema centralizado** y estar disponibles para análisis y auditoría, evitando la transferencia manual de los mismos.
REQ-INT-31	Obligatorio	Implementar **retención y eliminación segura** de logs de acuerdo con las políticas internas y regulaciones aplicables, como **ISO 27001** y el bloqueo y eliminación para aquellos afectados por **GDPR.**
REQ-INT-32	Obligatorio	Los sistemas externos deben cumplir también con las Políticas y Cuerpo Normativo de Seguridad de TMB, especialmente, los del Capítulo 15 del cuerpo normativo de TMB que fijan la relación con proveedores.
REQ-INT-33	Obligatorio	El diseño contemplará los mecanismos para que TMB pueda controlar, revisar y auditar regularmente la provisión de servicios del proveedor.
REQ-INT-34	Obligatorio	Previa a la ejecución de los servicios, todos los requisitos relacionados con la seguridad tecnológica y de la información se establecerán y acordarán con cada proveedor para delimitar y cumplir con las competencias y responsabilidades de cada una de las partes.

7.2

7.2 Aplicaciones y gestión de usuarios

RX-AU-1	Obligatorio siempre	Si la plataforma requiere de una App para su uso desde móvil, se deberá proporcionar el APK correspondiente para la distribución a los móviles corporativas desde la herramienta de MDM que utiliza TMB (actualmente VMware Workspace ONE)
RX-AU-2	Obligatorio siempre	La plataforma no debe tener gestión de usuarios desvinculada, debe integrar vía federación SAML o OIDC con la gestión de identidades corporativa de TMB. A nivel autorizaciones se permite la gestión local en base a roles que se definirán en el LDAP corporativo y se accederán a ellos a través de la federación SAML o OIDC.
RX-AU-3	Obligatorio	En el momento del registro del usuario (1r acceso) deberá presentarse un *disclaimer* legal con el texto que

	siempre	determine TMB para ser aceptado por el usuario. Sin su aceptación, se deberá impedir el acceso a la plataforma y no podrá almacenarse ningún dato personal que se dispusiera de él. Se deberá guardar constancia de dicha aceptación (fecha y texto aceptado).

7.3 Gestión del servicio

RX-GS-1	Obligatorio si se necesita soporte de TMB	El servicio deberá permitir conocerlos ANS pactados con TMB durante la fase de diseño y el valor de los mismos a lo largo del contrato
RX-GS-2	Obligatorio si se necesita soporte de TMB	Se deberán proveer de URLs para la monitorización del servicio que permitan conocer en cada momento el estado del mismo.
RX-GS-3	Obligatorio si se necesita soporte de TMB	Se deberán proveer mecanismos para el escalado de incidencias, integrado con el sistema de gestión de tickets de TMB (actualmente basado en FootPrints)
RX-GS-4	Obligatorio si se necesita soporte de TMB	Independientemente de las métricas proporcionadas por temas funcionales, se deberá generar un log de trazabilidad que guarde como mínimo el detalle de cada acceso (quién accede, cuándo y desde qué dispositivo).

7.4 Soluciones tipo IaaS o PaaS

RX-IA-1	Obligatorio si el sistema está en la nube	Las comunicaciones con servicios tipo IaaS alojados en nubes públicas o privadas sin gestión directa por parte de TMB deberán protegerse mediante el uso de túneles VPN o líneas dedicadas.
RX- IA -2	Obligatorio si el sistema está en la nube	Los sistemas ubicados en nubes públicas o privadas sin gestión directa por parte de TMB sólo podrán acceder a servicios publicados en la DMZ corporativa, nunca a servicios internos. En caso de ser necesario acceder a servicios que actualmente no se encuentran publicados, se deberá

		contemplar en el diseño del proyecto su publicación segura.
RX- IA -3	Obligatorio si el sistema está en la nube	Si la operación y mantenimiento de la solución IaaS o PaaS debe ser realizada en algún momento directamente por personal de TMB, deberá cumplir con los mismos requerimientos de las soluciones on-premise (a excepción de los relativos al HW u otras características ligadas al mismo o a los CPDs de TMB)
RX-IA-4	Obligatorio en IaaS	Si lo que se instala es Infraestructura como Servicio, ésta debe seguir las mismas condiciones de seguridad que el resto de equipos de TMB.

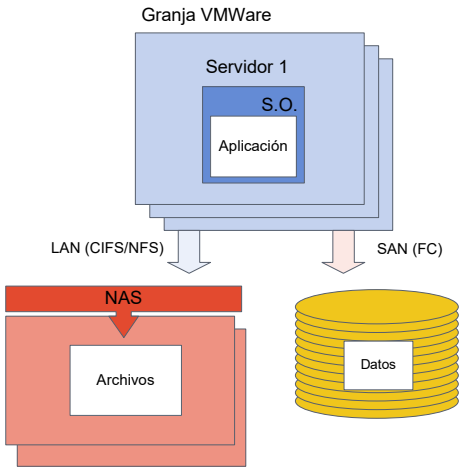
8 Anexo. Arquitecturas típicas de sistemas centrales “on premise”

A continuación, se indican arquitecturas típicas de sistemas centrales en TMB. Para facilitar la implantación y posterior mantenimiento, las soluciones se deberían adaptar a estas arquitecturas o a combinaciones de las mismas.

Los elementos comunes como la granja de VMWare, clúster de bases de datos, cajas de discos, NAS, balanceadores, infraestructura LAN/SAN, firewalls… existen ya en TMB y son comunes para toda la infraestructura.

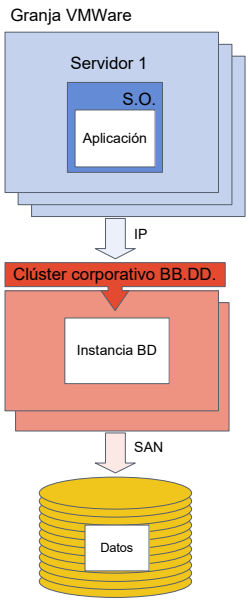
8.1 Servidor con almacenamiento externo

Descripción: Servidor(es) con S.O. Windows o Linux, ejecutándose en una granja de VMWare, con necesidad de almacenamiento externo en NAS (acceso mediante CIFS o NFS) y/o *file systems* en cabinas de disco externas (acceso mediante FC).



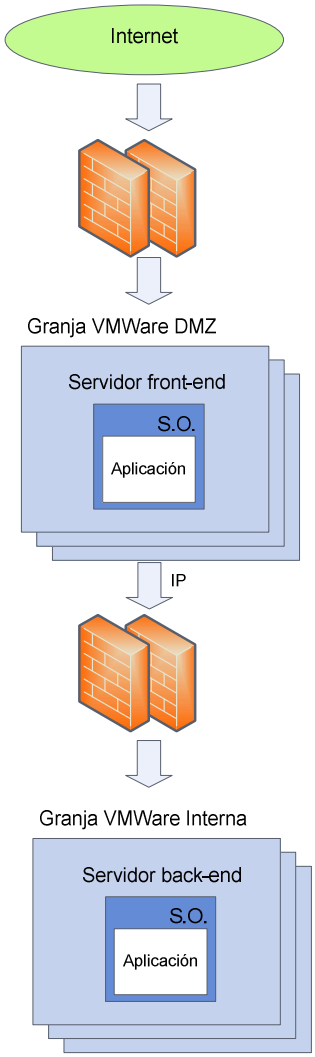
8.2 Servidor con base de datos

Descripción: Servidor(es) con S.O. Windows o Linux, ejecutándose en una granja de VMWare, accediendo a una instancia de BB.DD. en un clúster corporativo (compartido con otras instancias).



8.3 Servidor para contenidos publicados en Internet

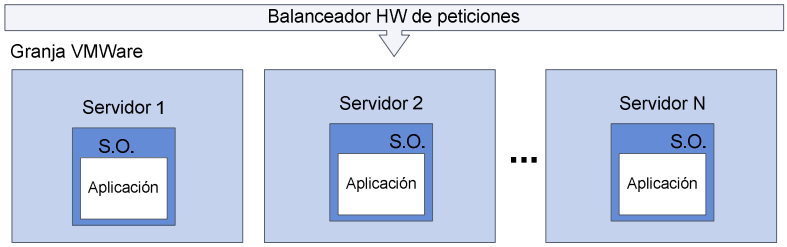
Descripción: Servidor de front-end con S.O. Windows o Linux en la granja de VMWare situada en la DMZ y un back-end sobre la granaja VMWare corporativa (interna).



8.4 Servidores de front-end balanceados

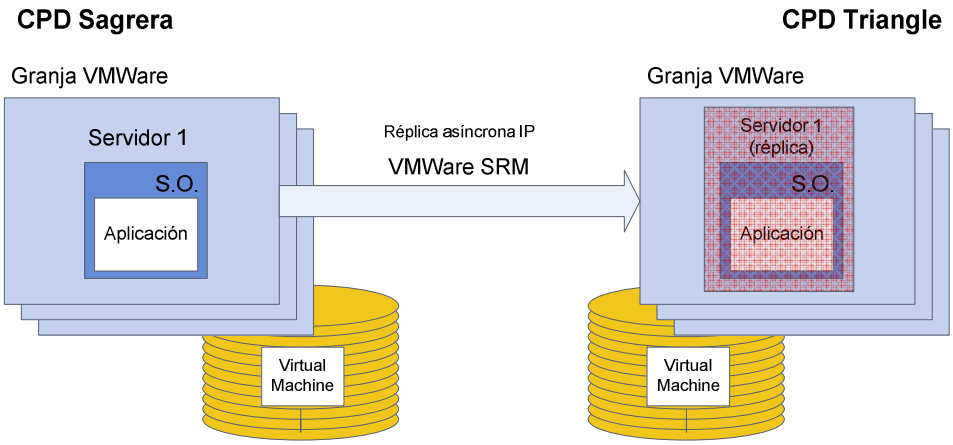
Descripción: Granja de servidores de front-end (idealmente iguales) con S.O. Windows o Linux, repartidos en distintos servidores de una granja de VMWare. Las peticiones (http, https) son balanceadas por balanceadores HW.

Esta solución está disponible tanto para servicios internos (intranet) como externos en la DMZ (internet).



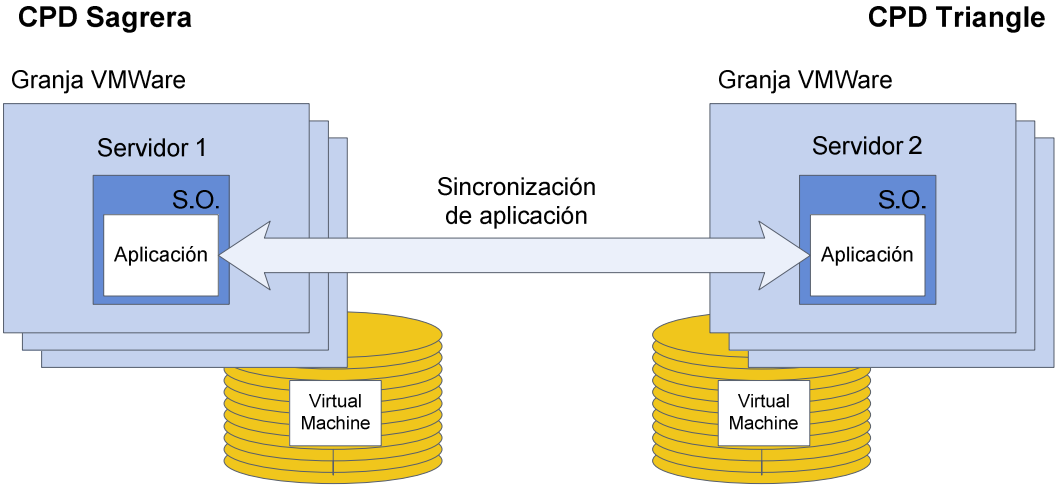
8.5 Sistemas con contingencia

Descripción: Servidor(es) con S.O. Windows o Linux, ejecutándose en una granja de VMWare en el CPD de Sagrera, con la funcionalidad de VMWare Site Recovery Manager (SRM) activada y réplica por IP.



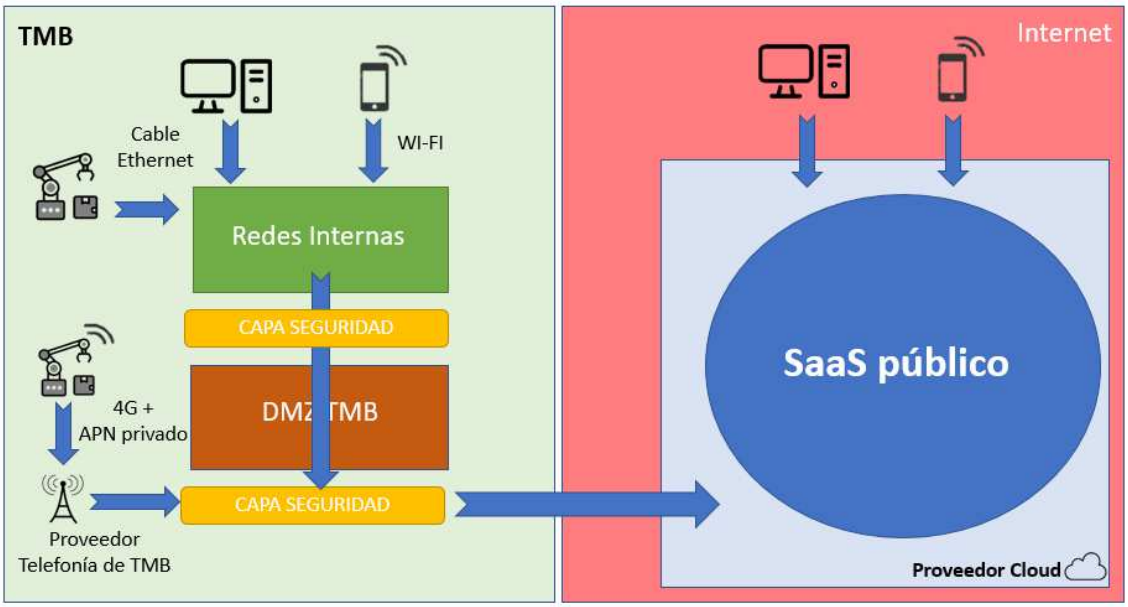
8.6 Sistemas ininterrumpidos (RTO ≈ 0)

Descripción: Servidores con S.O. Windows o Linux, ejecutándose en una granja de VMWare en el CPD de Sagrera y en el de Triangle, con la aplicación activa simultáneamente en cada uno de los centros. Qué centro ataca cada cliente y la sincronización de los datos en cada centro es gestionado por mecanismos intrínsecos a la aplicación.

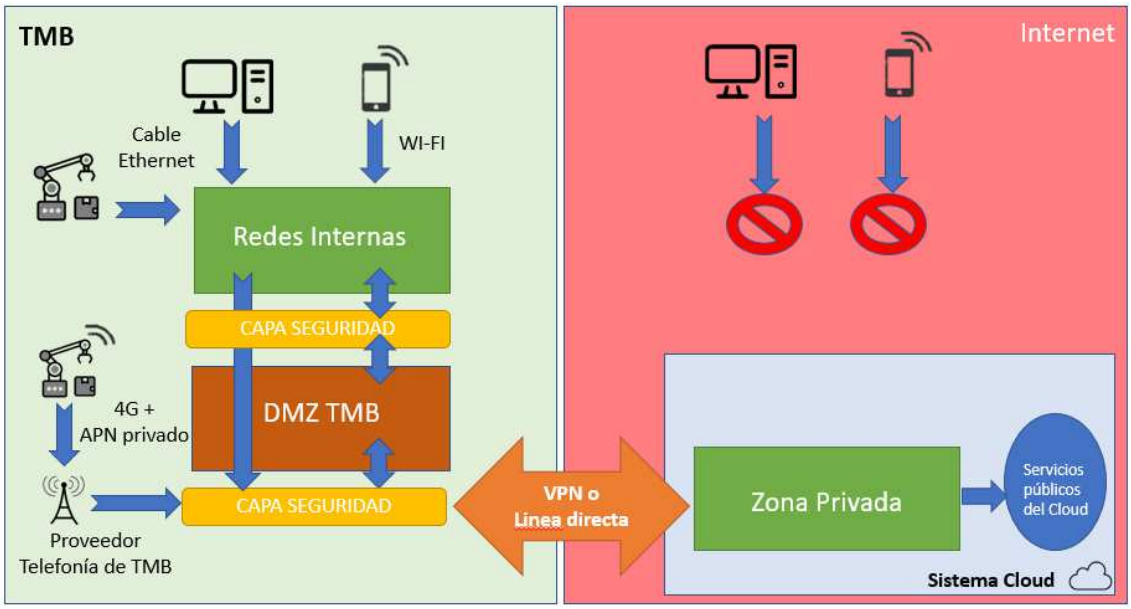


9 Anexo. Arquitecturas soportadas para sistemas “en la nube”

9.1 Sistemas públicos



9.2 Sistemas privados



9.3 Sistemas híbrido