**ARQUITECTURA DE TECNOLOGIA Y SEGURIDAD**

**Modelo para el Desarrollo y Gobierno de Nuevo Core de Pensiones**

**EVOL**

para AFP Integra y Prima AFP



Índice

[1 Propósito 4](#_Toc522839152)

[2 Glosario de Términos 5](#_Toc522839153)

[3 Stakeholders 6](#_Toc522839154)

[4 Objetivos y Restricciones 7](#_Toc522839155)

[4.1 Objetivos de Negocio 7](#_Toc522839156)

[4.2 Objetivos de TI 7](#_Toc522839157)

[5 Restricciones 8](#_Toc522839158)

[6 Cumplimiento 9](#_Toc522839159)

[6.1 Principios Estratégicos 9](#_Toc522839160)

[6.2 Principios de Negocio 9](#_Toc522839161)

[6.3 Principios de Tecnología y Seguridad 12](#_Toc522839162)

[6.4 Estándares 13](#_Toc522839163)

[7 Arquitectura de Tecnológica TO-BE 14](#_Toc522839164)

[7.1 Infraestructura tecnológica 14](#_Toc522839165)

[7.1.1 Capacidades 14](#_Toc522839166)

[7.1.2 Arquitectura de Referencia 22](#_Toc522839167)

[7.1.3 Arquitectura de Referencia en el DRP 26](#_Toc522839168)

[7.1.4 Diagrama de Servidores 27](#_Toc522839169)

[7.1.5 Modelo Tecnológico de Asociación 28](#_Toc522839170)

[7.1.6 Lineamientos 30](#_Toc522839171)

[7.2 Seguridad 31](#_Toc522839172)

[7.2.1 Capacidades 31](#_Toc522839173)

[7.2.2 Arquitectura de Referencia 35](#_Toc522839174)

[7.2.3 Patrones 36](#_Toc522839175)

[7.2.4 Componentes 37](#_Toc522839176)

[7.2.5 Vista de Seguridad de Datos 38](#_Toc522839177)

[7.2.6 Vista de Seguridad Perimetral 39](#_Toc522839178)

[7.2.7 Caso de Uso 40](#_Toc522839179)

[7.2.8 Lineamientos 41](#_Toc522839180)

Información de Documento

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre de Proyecto:** | Proyecto Kadabra | | |
| **Preparado Por:** | Nestor Cayllahua | **Número Versión:** | 1.0 |
| **Título:** | Arquitectura de Tecnología y Seguridad | **Fecha:** | 21/08/2018 |
| **Revisado Por:** | José Luis Rentería | **Fecha de Revisión:** | 22/08/2018 |

Lista de Distribución

| **Desde** | **Fecha** | **Teléfono/Correo Electrónico** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

| **Para** | **Acción\*** | **Fecha Fin** | **Teléfono/Correo Electrónico** |
| --- | --- | --- | --- |
|  |  |  |  |

\* Tipos de Acción: Aprobar, Revisar, Informar, Archivo, Otros (por favor, especificar)

Historial de Versiones

| **Número Versión** | **Fecha** | **Revisado Por** | **Descripción** | **Nombre de Archivo** |
| --- | --- | --- | --- | --- |
| 1.0 | 22/08/2018 | José Luis Rentería | Creación | KADABRA - D\_Arquitectura\_Tecnologica y Seguridad\_V1\_0.docx |
| 1.1 | 26/08/2018 | José Luis Rentería | Creación | KADABRA - D\_Arquitectura\_Tecnologica y Seguridad\_V1\_1.docx |
| 1.2 | 27/08/2018 | José Luis Rentería | Creación | KADABRA - D\_Arquitectura\_Tecnologica y Seguridad\_V1\_2.docx |
| 1.3 | 27/08/2018 | José Luis Rentería | Creación | KADABRA - D\_Arquitectura\_Tecnologica y Seguridad\_V1\_3.docx |

# Propósito

Este documento muestra la arquitectura de tecnología y seguridad para el Proyecto Kadabra. Contiene los artefactos de arquitectura creados durante el proyecto. Provee una vista cualitativa de la solución y apuntan a comunicar la intención de los arquitectos.

# Glosario de Términos

|  |  |
| --- | --- |
| **Nombre** | **Significado** |
| IaaS | Infrastructure as a Services |
| PaaS | Platform as a Services |
| CaaS | Container as a Services |
| SAN | Storage área network |
| NAS | Network Attached Storage |
| DAS | Direct Access Storage |
| Infiniband | Bus de comunicaciones de alta velocidad |
| LAN | Local Area Network |
| WAN | Wide Area Network |
| MPLS | Multiprotocol Level Switching |
| VPN | Virtual Private Network |
| IAM | Identity Access Management |
| DMZ | Demilitarized zone |
| VLAN | Virtual Local Atrea network |

# Stakeholders

Esta sección muestra las responsabilidades de los stakeholders para la arquitectura de Tecnología y Seguridad. Los stakeholders son personas que participan activamente en el proyecto, o cuyos intereses pueden verse afectados positiva o negativamente por la ejecución o la finalización del proyecto.

|  |  |
| --- | --- |
| Rol/Grupo | Nombres |
| Arquitecto Empresarial/EVOL | José Luis Rentería |
| Arquitecto de Aplicaciones/EVOL | Juan Pablo Gonzales |
| Arquitecto de Datos/EVOL | Nestor Cayllahua |
| Arquitecto de Datos/EVOL | Jorge Guerreros |
| Arquitecto de Infraestructura/EVOL | Nestor Cayllahua |
| Arquitecto de Seguridad/EVOL | Jose Luis Renteria |
| Analista Funcional/EVOL | Maura Cieza |
| Arquitecto TI/Integra | Pedro Tapia |
| Arquitecto TI/Prima | Rayner Huamantumba |
| Líder Técnico/Integra | Marcelo Meza |
| Líder Técnico/Prima | Nancy Bohorquez |
| Analista Senior Desarrollo/Integra | William Ccucho |
| Analista Senior Desarrollo/Integra | Luis Polo |
| Arquitecto TI/Prima | Marco Begazo |
| Arquitecto TI/Prima | Mauricio Soto |
| Arquitecto TI/Prima | Oscar Macedo |

# Objetivos y Restricciones

En esta sección describe los objetivos, tanto de negocio como de TI, las restricciones y las capacidades que la arquitectura To-Be debe cumplir.

## Objetivos de Negocio

|  |  |
| --- | --- |
|  | Objetivo de Negocio |
| Desafíos del SPP | Mejorar la imagen del Sistema Privado de Pensiones |
| Dar mejor soporte a la centralización de procesos del SPP |
| Reducir costos de administración de fondos de pensiones |
| Necesidades del Negocio de AFP’s | Fidelización y diferenciación |
| Diversificar oferta de productos |
| Simplificar procesos |
| Mejorar servicios |
| Reducir el riesgo operativo automatizando procesos manuales |

## Objetivos de TI

|  |
| --- |
| Objetivo de TI |
| Reducir obsolescencia tecnológica. |
| Disminuir los costos de desarrollo, mantenimiento y operación del Core de pensiones. |
| Mejorar Time-To-Market para implementación de cambios. |
| Aprovechar sinergias tecnológicas entre AFP’s. |
| Incrementar la calidad y servicio al cliente interno y externo. |
| Contar con un sistema seguro y confiable. |
| Definir políticas y procedimientos de TI. |
| Facilitar la implementación futura de un modelo BPO basado en el nuevo Core de pensiones |

# Restricciones

Esta sección describe las restricciones que se deben tomar en cuenta en cualquier trabajo de arquitectura.

* 1. **Escalas**

|  |  |  |
| --- | --- | --- |
| Tipo | Valor | Descripción |
| Severidad | Bajo | Impacto Menor. Se pueden tomar acciones rápidas para resolverlas. |
| Moderado | Impacto Medio. Si no se realiza acción podría causar traer consecuencias a corto plazo. |
| Grave | Impacto ­alto. Se requiere acción urgente. |
| Crítico | Impacto muy alto. Se requiere acción urgente. |
| Probabilidad | Raro | Podría ocurrir sólo en circunstancias excepcionales. |
| Improbable | Probabilidad baja de ocurrencia. |
| Posible | Probabilidad media de ocurrencia. |
| Probable | Probabilidad alta de ocurrencia. |
| Casi seguro | Probabilidad muy alta de ocurrencia. |

* 1. **Restricciones de Financieras y Presupuesto**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Restricción | Severidad | Probabilidad | Actividades de Mitigación |
| C1 | Presupuesto del Proyecto | Grave | Probable | Revisar políticas y procedimientos de compra del proyecto o de ambas AFP’s para que el presupuesto pueda ser utilizado con control. |

* 1. **Restricciones Externas y Negocio**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Restricción | Severidad | Probabilidad | Actividades de Mitigación |
| C2 | Cambios deben ser realizados teniendo en cuenta la normativa y regulación de la SBS. | Crítico | Probable | Revisar normativa y regulación para asegurar su cumplimiento. |

* 1. **Otras Restricciones**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Restricción | Severidad | Probabilidad | Actividades de Mitigación |
| C3 | Estándares de seguridad y protección de datos | Crítico | Probable | Tomar en cuenta Ley de Protección de Datos Personales, Circular G-140-2009, Circular G-193-2017 |

# Cumplimiento

Esta sección muestra los principios a los que se adhiere la Arquitectura Empresarial, así como las políticas y otros estándares que ésta debe seguir.

## Principios Estratégicos

|  |  |
| --- | --- |
| **Nombre** | **La arquitectura KADABRA debe soportar un esquema de multiempresa.** |
| **Código** | PAS01 |
| **Declaración** | La arquitectura KADABRA debe soportar un esquema de asociación entre varias AFP’s. |
| **Justificación** | Este principio está asociado a la estrategia de negocio definida por KADABRA que deja abierta la posibilidad de incluir a otras AFP’s. |
| **Implicancias** | Implementar una arquitectura que soporte Multiempresa.  Asegurar una arquitectura que permita el desarrollo, mantenimiento y operación común del Core de Pensiones de KADABRA  Alinear las definiciones propias de cada empresa con las definidas para KADABRA. |

## Principios de Negocio

|  |  |
| --- | --- |
| **Nombre** | **Continuidad del negocio** |
| **Código** | PAN01 |
| **Declaración** | Las operaciones de KADABRA se mantienen a pesar de las interrupciones del sistema. |
| **Justificación** | KADABRA debe contar con la capacidad de continuar la operativa, independientemente de los eventos externos (desde caídas de sistema hasta todo tipo de desastres). |
| **Implicancias** | Evaluar la criticidad e impacto de las aplicaciones a fin de determinar qué nivel de continuidad se requiere y qué plan de recuperación es necesario.  Implementar revisiones periódicas, pruebas de vulnerabilidad y exposición o, el diseño de servicios de misión crítica para garantizar la continuidad del funcionamiento del negocio, a través de capacidades redundantes o alternativas.  Implementar procesos de continuidad de negocio.  Asegurar la ejecución de los procesos, incluyendo la gestión de riesgos en situaciones en donde se vea afectada la operación de KADABRA. |

|  |  |
| --- | --- |
| **Nombre** | **Orientación a servicios** |
| **Código** | PAN02 |
| **Declaración** | La arquitectura KADABRA se basa en un diseño orientado a servicios que refleje las actividades de los procesos de negocio. |
| **Justificación** | La orientación de servicio ofrece agilidad y asegura el flujo de información entre procesos. |
| **Implicancias** | Implementar un gobierno que permita catalogar los servicios y medir impacto de los cambios a realizar en los mismos. |

|  |  |
| --- | --- |
| **Nombre** | **Responsabilidad de TI** |
| **Código** | PAN03 |
| **Declaración** | El área de TI es responsable de implementar procesos e infraestructura que permitan que las soluciones construidas cumplan con los requerimientos definidos por el usuario en términos de funcionalidad, niveles de servicio, costo y tiempo de entrega. |
| **Justificación** | La definición de estos procesos permitirá cumplir con las expectativas del negocio y con las capacidades que se implementarán para KADABRA. |
| **Implicancias** | Crear procedimientos que gestionen la demanda de KADABRA, cumpliendo los estándares y mejores prácticas de gobierno, desarrollando KPI’s que permitan medir el cumplimiento de este principio. |

|  |  |
| --- | --- |
| **Nombre** | **Implementación de un lenguaje común** |
| **Código** | PAN04 |
| **Declaración** | Se debe promover la elaboración de documentación y modelamiento de los procesos de KADABRA mediante un lenguaje común que facilite su entendimiento y comunicación. |
| **Justificación** | Una mejor comunicación entre las distintas áreas (negocio y TI) permite agilizar la interacción entre las mismas. |
| **Implicancias** | Implementar el uso de plantillas y modelamiento de procesos con notación BPMN. |

|  |  |
| --- | --- |
| **Nombre** | **Gobernabilidad de procesos** |
| **Código** | PAN05 |
| **Declaración** | KADABRA adopta el concepto de gobernabilidad de procesos de punta a punta (E2E), incluyendo la información que fluye a través de estos. |
| **Justificación** | La gobernabilidad de procesos permite la generación de valor asociada a la identificación de responsabilidades, gestión y control integral de los procesos. |
| **Implicancias** | Definir los responsables de los procesos (Process Owner).  Gestionar los procesos a través de indicadores y programas de mejoramiento continuo.  Identificar y definir controles de mitigación de riesgos de proceso. |

|  |  |
| --- | --- |
| **Nombre** | **La gestión de requerimientos de negocio es un asunto de todos** |
| **Código** | PAN06 |
| **Declaración** | La alta dirección, representantes de arquitectura y Stakeholders participan en las decisiones de gestión de requerimientos de negocio para lograr los objetivos de KADABRA. |
| **Justificación** | Este principio garantiza que la gestión de requerimientos de negocio esté alineada con la visión de KADABRA. |
| **Implicancias** | Implementar roles y responsabilidades para abordar los requerimientos.  Formar grupos de trabajo entre expertos de negocio y personal TI para definir las metas y objetivos de KADABRA |

|  |  |
| --- | --- |
| **Nombre** | **Aplicaciones de uso común** |
| **Código** | PAN07 |
| **Declaración** | Se desarrollan aplicaciones de uso común para todo el entorno de KADABRA y no aplicaciones aisladas a la funcionalidad, capacidad y expectativa de ésta. |
| **Justificación** | El permitir y mantener capacidades o funciones duplicadas es costosa, y alienta la aparición de datos contradictorios e inconsistentes. |
| **Implicancias** | Crear una política de gobierno que norme el uso de aplicaciones comunes que asegure su alineamiento a las expectativas funcionales de KADABRA. |

|  |  |
| --- | --- |
| **Nombre** | **Cambios basados en requerimientos de negocio** |
| **Código** | PAN08 |
| **Declaración** | Se realizan cambios en las aplicaciones y datos en respuesta a las necesidades de negocio. |
| **Justificación** | La base de cualquier cambio propuesto es principalmente dar soporte a los objetivos estratégicos y operacionales del negocio de KADABRA. |
| **Implicancias** | Alinear los procesos de gestión de cambio a este principio.  Implementar mejoras o cambios en los sistemas de información basados en una necesidad de negocio documentada. |

## 

## Principios de Tecnología y Seguridad

|  |  |
| --- | --- |
| **Nombre** | **Uso de estándares de TI** |
| **Código** | PAT01 |
| **Declaración** | Las decisiones e iniciativas de TI son evaluadas en base a estándares previamente definidos. |
| **Justificación** | Las decisiones de cambio de los recursos de TI se evaluarán con los estándares de TI definidos, para asegurar la vigencia tecnológica del sistema KADABRA. |
| **Implicancias** | Implementar políticas, normas y procedimientos que rijan la adquisición de tecnología.  Publicar estándares tecnológicos de las herramientas utilizadas en KADABRA.  Mantener una hoja de ruta de actualización tecnológica. |

|  |  |
| --- | --- |
| **Nombre** | **Interoperabilidad** |
| **Código** | PAT02 |
| **Declaración** | El software y el hardware deben cumplir con estándares definidos que promuevan la interoperabilidad de datos, aplicaciones y tecnología. |
| **Justificación** | Los estándares ayudan a mejorar la capacidad de administrar sistemas, mejorar la satisfacción del usuario y proteger las inversiones de TI existentes, maximizando el retorno de la inversión y reduciendo los costos. |
| **Implicancias** | Implementar procedimientos para establecer estándares de interoperabilidad, revisarlos periódicamente y mantenerlos actualizados. |

|  |  |
| --- | --- |
| **Nombre** | **Infraestructura escalable** |
| **Código** | PAT03 |
| **Declaración** | La infraestructura debe ser escalable de acuerdo a la necesidad del negocio. |
| **Justificación** | Permite que el sistema pueda operar de manera óptima según cambios en la carga operativa. |
| **Implicancias** | Monitorear el rendimiento de la infraestructura para asegurar la atención óptima de la operación diaria. |

|  |  |
| --- | --- |
| **Nombre** | **Seguimiento de auditoría** |
| **Código** | PAT04 |
| **Declaración** | Todas las acciones del usuario y del sistema deben dejar un rastro de auditoría. |
| **Justificación** | Este principio permite tener un seguimiento de las acciones de los usuarios a fin de detectar algún comportamiento que pueda afectar la confiabilidad de la información. |
| **Implicancias** | Implementar un servicio de auditoria centralizado. |

## Estándares

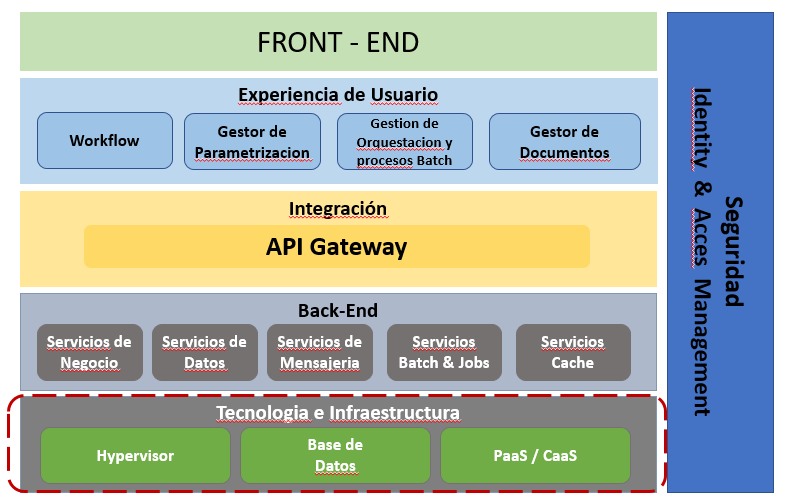
Se utilizarán los siguientes estándares en el presente entregable:

* ARCHIMATE un es lenguaje de notación unificado utilizado para modelamiento de arquitectura empresarial de alto nivel, el cual permite visualizar e identificar las aplicaciones negocio, sub-aplicaciones, componentes, bases de datos, Infraestructura, seguridad y servicios con sus respectivas interacciones.

## 

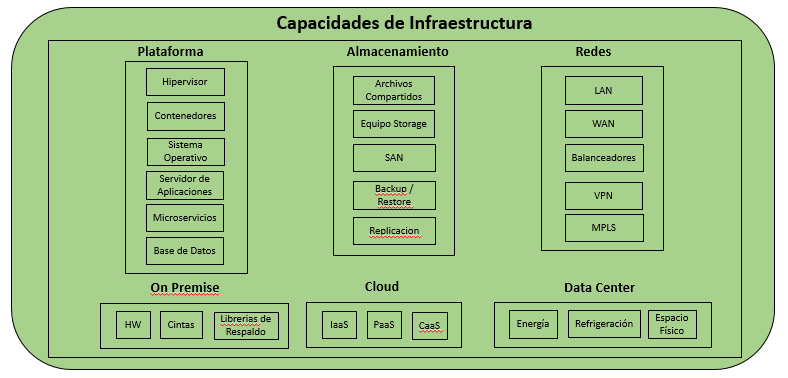
# Arquitectura de Tecnológica TO-BE

Esta sección contiene los esquemas y gráficos que representan la arquitectura de tecnología TO-BE.



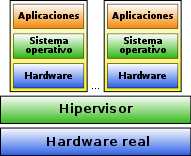
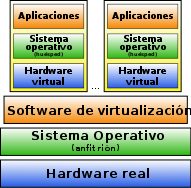
## Infraestructura tecnológica

### Capacidades



#### Plataforma

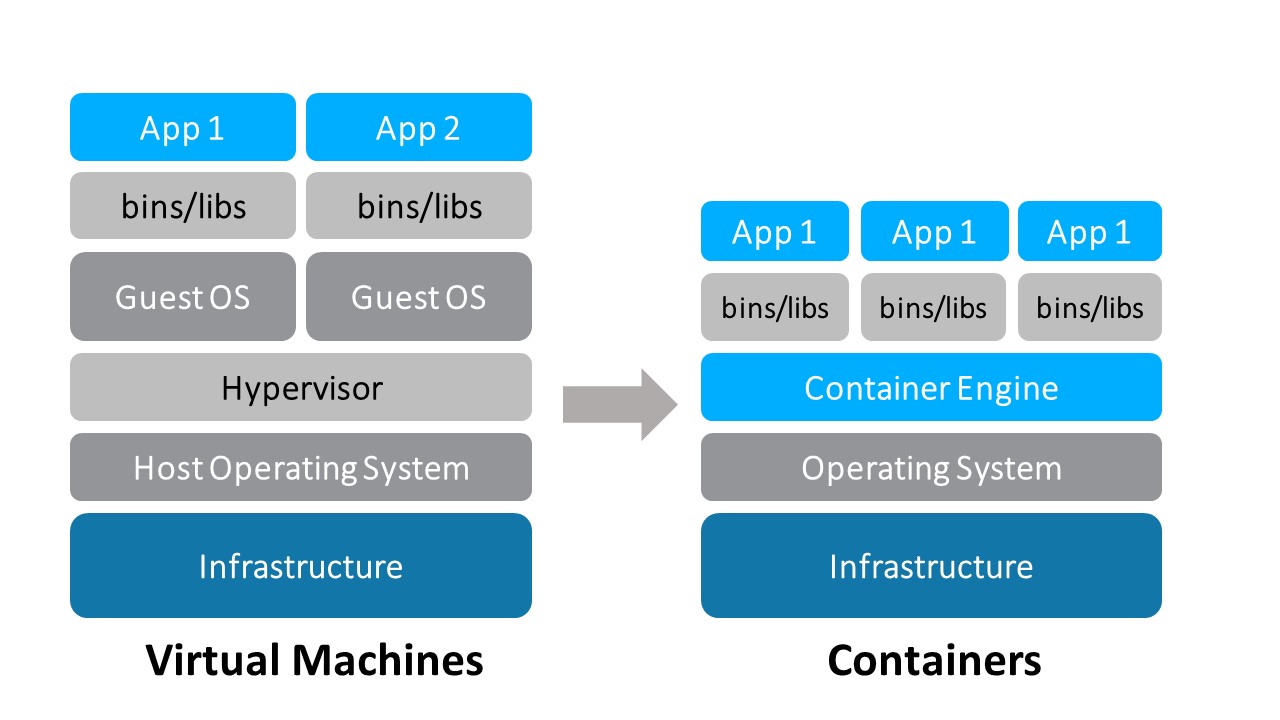
**Hypervisor**.- Es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos.

Bare Metal Hyp 1 Hyp tipo 2

En la arquitectura Kadabra se ha definido la utilización de hipervisores para virtualizar y exponer VMs que serán utilizadas en las aplicaciones monolíticas y para la parte batch.

**Contenedores**. - Los contenedores comparten recursos con el sistema operativo sobre el que se ejecutan, de esta manera podemos arrancar o parar el contenedor rápidamente, mientras que las máquinas virtuales se aíslan del sistema operativo y se comunican a través de un hipervisor. Los contenedores nos permiten encapsular la aplicación y sus dependencias. La portabilidad de los contenedores hace que los problemas causados por cambiar el entorno donde está corriendo la aplicación se reduzca a la mínima expresión. Por lo tanto, trabajar con contenedores se hace más productivo el desarrollo y el despliegue de aplicaciones.



En la Arquitectura kadabra se ha definido la utilización de contenedores para la parte de microservicios.

**Sistema Operativo**. – Es un software que se encarga de gestionar todos los recursos del Sistema informático, imprescindible para el funcionamiento de máquinas físicas o virtuales que sirven de intermediario entre los recursos materiales, el usuario y las diferentes aplicaciones.

Algunas cosas más concretas que puede realizar un Sistema Operativo son:

- Múltiples programas se pueden ejecutar al mismo tiempo, el sistema operativo determina qué

aplicaciones se deben ejecutar en qué orden y cuánto tiempo.

- Gestiona el intercambio de memoria interna entre múltiples aplicaciones.

- Se ocupa de entrada y salida desde y hacia los dispositivos de hardware conectados, tales como discos, puertos y periféricos.

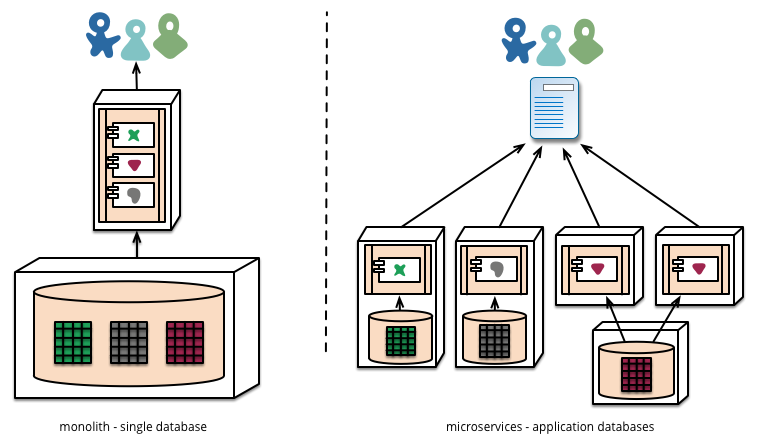
- En los equipos que pueden proporcionar procesamiento en paralelo, un sistema operativo puede

manejar la forma de dividir el programa para que se ejecute en más de un procesador a la vez

En la Arquitectura Kadabra se ha definido utilizar Linux o Unix por su versatilidad, compatibilidad y facilidad de uso para el core tecnológico y Windows para el AD.

**Servidores de Aplicaciones. -** se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negociación y de acceso a los datos de las aplicaciones. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.

**Microservicios. -** Los microservicios son una arquitectura y un enfoque sobre la escritura de software en el que las aplicaciones se dividen en componentes más pequeños e independientes entre sí. A diferencia de un enfoque tradicional y monolítico sobre las aplicaciones, en el que todo se crea en una única pieza, los microservicios están separados y funcionan conjuntamente para llevar a cabo las mismas tareas. Cada uno de estos componentes, o procesos, son los microservicios. Este enfoque sobre el desarrollo de software valora la granularidad por ser liviana y la capacidad de compartir un proceso similar en varias aplicaciones.

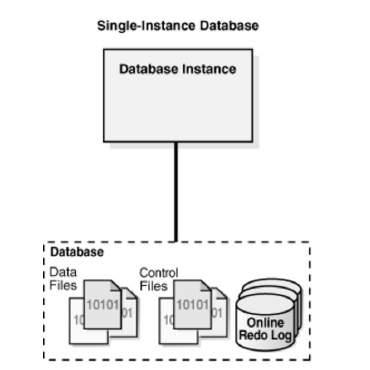


En la arquitectura kadabra el objetivo es entregar software de calidad más rápido. Aunque los microservicios son un medio para tal fin, se deben considerar otras cuestiones al dividir las aplicaciones en microservicios como administrarlos, orquestarlos y gestionar los datos.

**Base de datos**. - Una base de datos es una colección de información organizada de forma que pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos. Los usuarios pueden acceder a la información usando herramientas específicas de consulta y de generación de informes. Estos sistemas también proporcionan métodos para mantener la integridad de los datos, para administrar el acceso de usuarios a los datos.

Para el almacenamiento de los datos puede contar con sistemas de disco propio o [almacenamiento de conexión directa](https://es.wikipedia.org/wiki/Almacenamiento_de_conexi%C3%B3n_directa) ([DAS](https://es.wikipedia.org/wiki/Direct_Attached_Storage)), puede conectarse a una [red de almacenamiento](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento) ([SAN](https://es.wikipedia.org/wiki/Storage_Area_Network)) o conectarse a un sistema de [almacenamiento en red](https://es.wikipedia.org/wiki/Almacenamiento_conectado_en_red) ([NAS](https://es.wikipedia.org/wiki/Network_Attached_Storage)).

Una base de datos comprende tres elementos para formar un sistema de gestión de bases de datos (DMBS). La base de datos física es el repositorio, el motor de base de datos es el software que permite el acceso a los datos, y el esquema de base de datos es la estructura especificada de los datos. Las bases de datos pueden almacenar la mayoría de los tipos de archivos, incluyendo numéricos, de texto y multimedia, y tienen una estructura de datos para organizar la información almacenada.



En la Arquitectura kadabra se está considerando una base de datos de réplica en el DRP en modo de lectura para ser utilizadas por las herramientas de explotación de datos de cada una de las AFP’s

#### Almacenamiento

**Archivos Compartidos**. - Un archivo compartido es una propiedad de un archivo informático que tiene la característica de poder ser accedido o manipulado por múltiples personas, computadoras, sesiones o programas. Generalmente utilizado en sistema de alta disponibilidad

**Equipo Storage**. - El almacenamiento es un mecanismo que permite a una computadora retener datos, de forma temporal o permanente. El almacenamiento también puede denominarse almacenamiento de datos informáticos o almacenamiento de datos electrónicos.

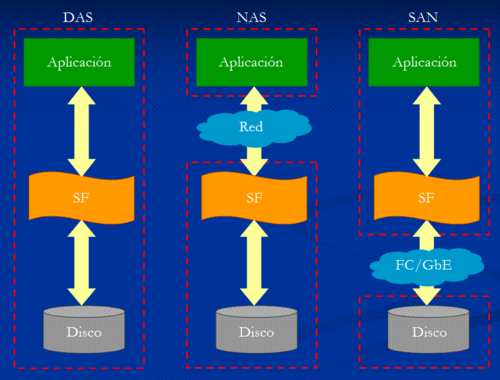
En la arquitectura kadabra se busca contar con una infraestructura de Storage que brinde disponibilidad y una alta performance de acceso a disco. Recomendamos utilizar un equipo Storage cuyos discos sean SSD en raid 10 y con un nivel mayor a 800,000 IOPs.

**Redes de Acceso a disco**. – Entre las redes de acceso disco tenemos NAS (Network Attached Storage), DAS (Direct attached storage), SAN (Storage Area Network) e Infiniband.

DAS es el método tradicional de almacenamiento y el más sencillo. Consiste en conectar el dispositivo de almacenamiento directamente al [servidor](https://es.wikipedia.org/wiki/Servidor), es decir, físicamente conectado al dispositivo que hace uso de él.

NAS es la tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de servidores a través de una red (normalmente [TCP/IP](https://es.wikipedia.org/wiki/TCP/IP)), haciendo uso de un [sistema operativo](https://es.wikipedia.org/wiki/Sistema_operativo) optimizado para dar acceso con los protocolos [CIFS](https://es.wikipedia.org/wiki/CIFS), [NFS](https://es.wikipedia.org/wiki/NFS), [FTP](https://es.wikipedia.org/wiki/File_Transfer_Protocol) o [TFTP](https://es.wikipedia.org/wiki/TFTP).

SAN es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos. Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN está totalmente separado del tráfico de usuario. Es una red de almacenamiento dedicada que proporciona acceso de nivel de bloque a varios (LUN).

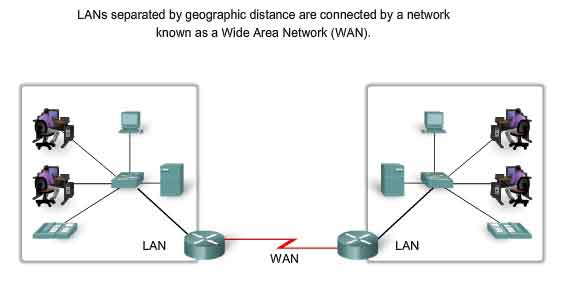


**Respaldos**. - una copia de los datos se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque.

#### Redes

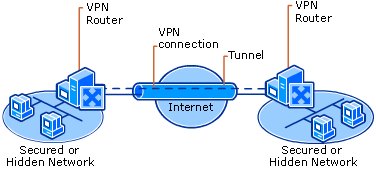
**LAN. -** Una red de área local (Local Area Network, o LAN) es un grupo de equipos de cómputo y dispositivos asociados que comparten una línea de comunicación común o un enlace inalámbrico con un servidor. Normalmente, una LAN abarca computadoras y periféricos conectados a un servidor dentro de un área geográfica distinta, como una oficina o un establecimiento comercial. Las computadoras y otros dispositivos móviles utilizan una conexión LAN para compartir recursos o un almacenamiento en red.

**WAN. -** El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial. Un ejemplo de red **WAN** es la propia Internet.

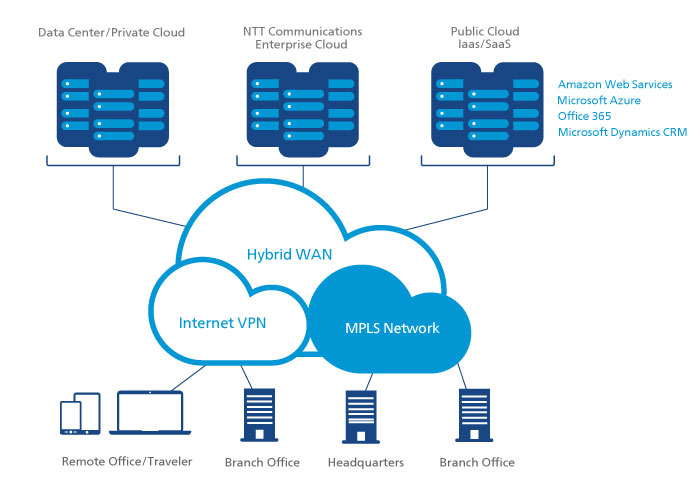


**Balanceadores de Carga.-** Un Balanceador de carga fundamentalmente es un dispositivo de [hardware](https://es.wikipedia.org/wiki/Hardware) o [software](https://es.wikipedia.org/wiki/Software) que se pone al frente de un conjunto de servidores que atienden una [aplicación](https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica) y, tal como su nombre lo indica, asigna o balancea las solicitudes que llegan de los clientes a los servidores usando [algoritmo](https://es.wikipedia.org/wiki/Algoritmo)s.

**VPN**.- es una tecnología de [red de computadoras](https://es.wikipedia.org/wiki/Red_de_computadoras) que permite una extensión segura de la [red de área local](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local)([LAN](https://es.wikipedia.org/wiki/Local_Area_Network)) sobre una red pública o no controlada como [Internet](https://es.wikipedia.org/wiki/Internet). Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.[1](https://es.wikipedia.org/wiki/Red_privada_virtual#cite_note-1)​ Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.



**MPLS.-** Opera entre la [capa de enlace de datos](https://es.wikipedia.org/wiki/Capa_de_enlace_de_datos) y la [capa de red](https://es.wikipedia.org/wiki/Capa_de_red) del modelo [OSI](https://es.wikipedia.org/wiki/Modelo_OSI). Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en [paquetes](https://es.wikipedia.org/wiki/Paquete). Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP. MPLS reemplazó a [Frame Relay](https://es.wikipedia.org/wiki/Frame_Relay" \o "Frame Relay) y ATM como la tecnología preferida para llevar datos de alta velocidad y voz digital en una sola conexión. MPLS no solo proporciona una mayor fiabilidad y un mayor rendimiento, sino que a menudo puede reducir los costes de transporte mediante una mayor eficiencia de la red.



#### On - Premise

**Hardware**.- se refiere a las partes físicas tangibles de un [sistema informático](https://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico); sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.[1](https://es.wikipedia.org/wiki/Hardware#cite_note-AAFA-1)​ Los cables, así como los gabinetes o cajas, los [periféricos](https://es.wikipedia.org/wiki/Perif%C3%A9rico_(inform%C3%A1tica)), y cualquier otro elemento físico involucrado, componen el hardware o soporte físico.

**Tape.-** es el tipo de [dispositivo de almacenamiento de datos](https://es.wikipedia.org/wiki/Dispositivo_de_almacenamiento_de_datos) que lee o graba en el [soporte de almacenamiento de datos](https://es.wikipedia.org/wiki/Soporte_de_almacenamiento_de_datos) de tipo [cinta magnética](https://es.wikipedia.org/wiki/Cinta_magn%C3%A9tica_de_almacenamiento_de_datos).

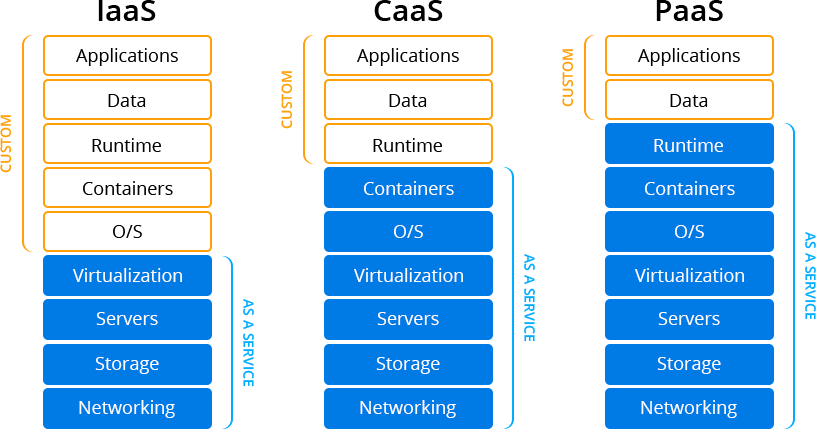
**Librerías**. - Es el equipo que opera los tapes, es un dispositivo de almacenamiento que contiene una o más unidades de cinta, varias ranuras para sostener cartuchos de cinta, un lector de código de barras para identificar cartuchos de cinta y un método automatizado para cargar cintas (un robot).

#### Cloud

**IaaS**. - IaaS proporciona acceso a recursos informáticos situados en un entorno virtualizado, la"nube" (cloud), a través de una conexión pública, que suele ser internet. En el caso de IaaS, los recursos informáticos ofrecidos consisten, en particular, en hardware virtualizado, o, en otras palabras, infraestructura de procesamiento. La definición de IaaS abarca aspectos como el espacio en servidores virtuales, conexiones de red, ancho de banda, direcciones IP y balanceadores de carga. Físicamente, el repertorio de recursos de hardware disponibles procede de multitud de servidores y redes, generalmente distribuidos entre numerosos centros de datos, de cuyo mantenimiento se encarga el proveedor del servicio cloud.

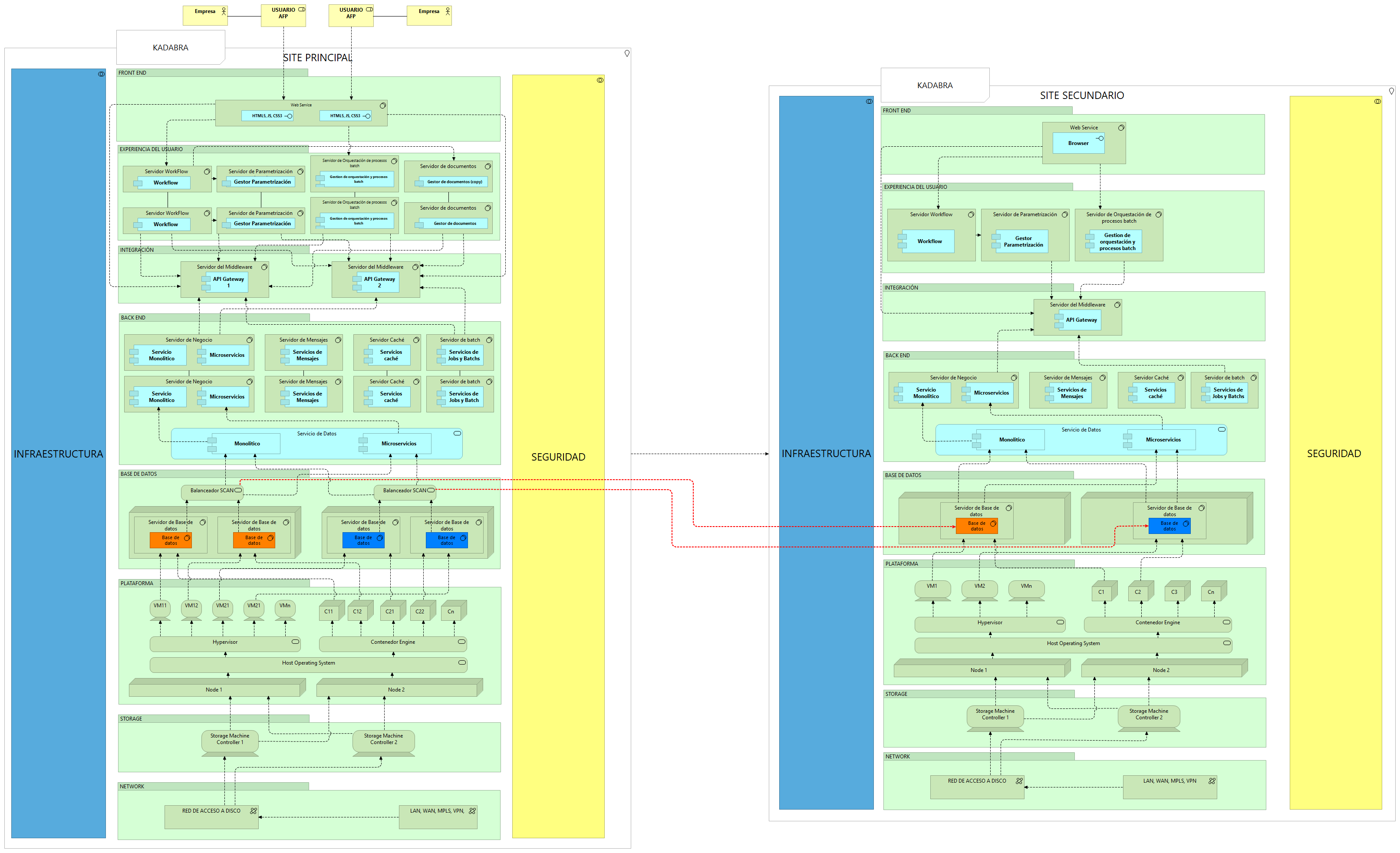
**PaaS. -** El concepto de Plataforma como Servicio (**PaaS**, Platform as a Service) es una categoría de servicios **cloud** que proporciona una plataforma y un entorno que permiten a los desarrolladores crear aplicaciones y servicios que funcionen a través de internet.

**CaaS. -** es uno de los conceptos más modernos, y frecuentes, de computación en la nube. CaaS se encuentra en un punto intermedio entre el IaaS y el PaaS. CaaS es un nuevo concepto por el cual podemos disponer de contenedores a demanda. Por ello, con el CaaS podemos cumplir con las necesidades del IaaS (ya que no necesitamos un hardware virtualizado) y nos acercamos también al PaaS, ya que los contenedores se utilizan para implementar el producto final.

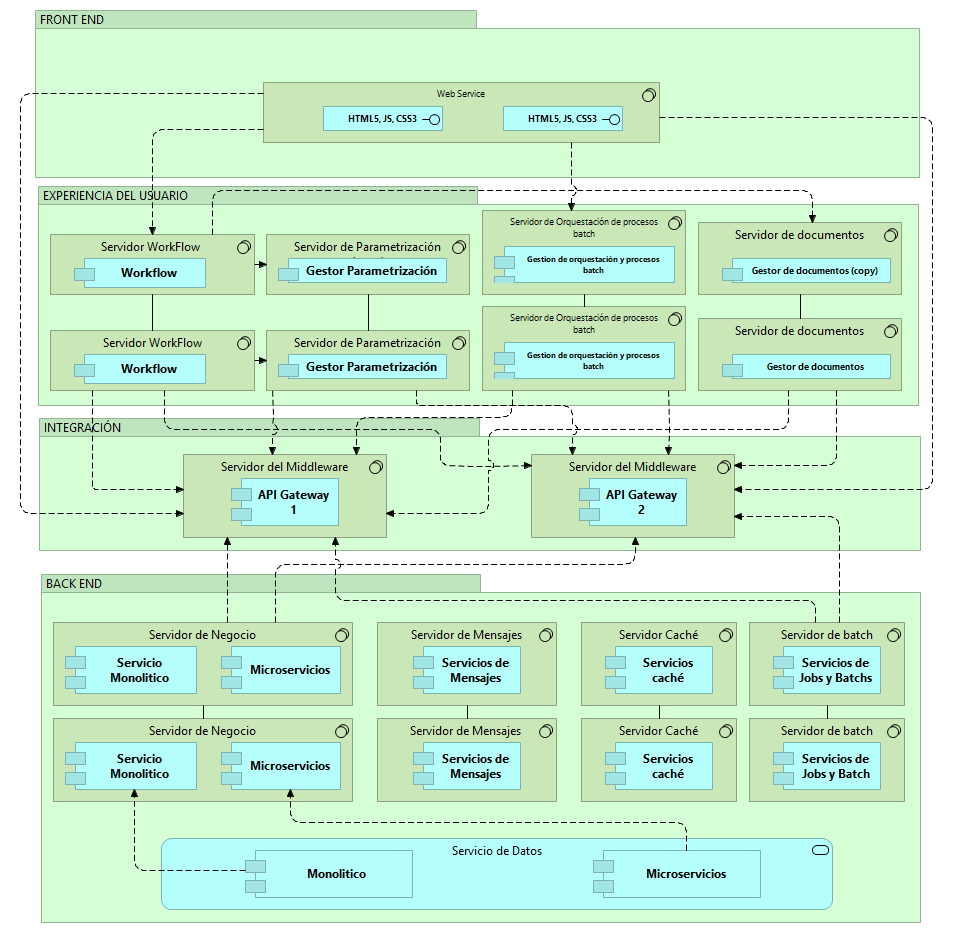


### Arquitectura de Referencia

A continuación, se describe la arquitectura referencial de infraestructura en la que se expone las capas de redes, storage, plataforma, Base de datos, backend, integración, experiencia de usuario y front end desde la perspectiva tecnológica.

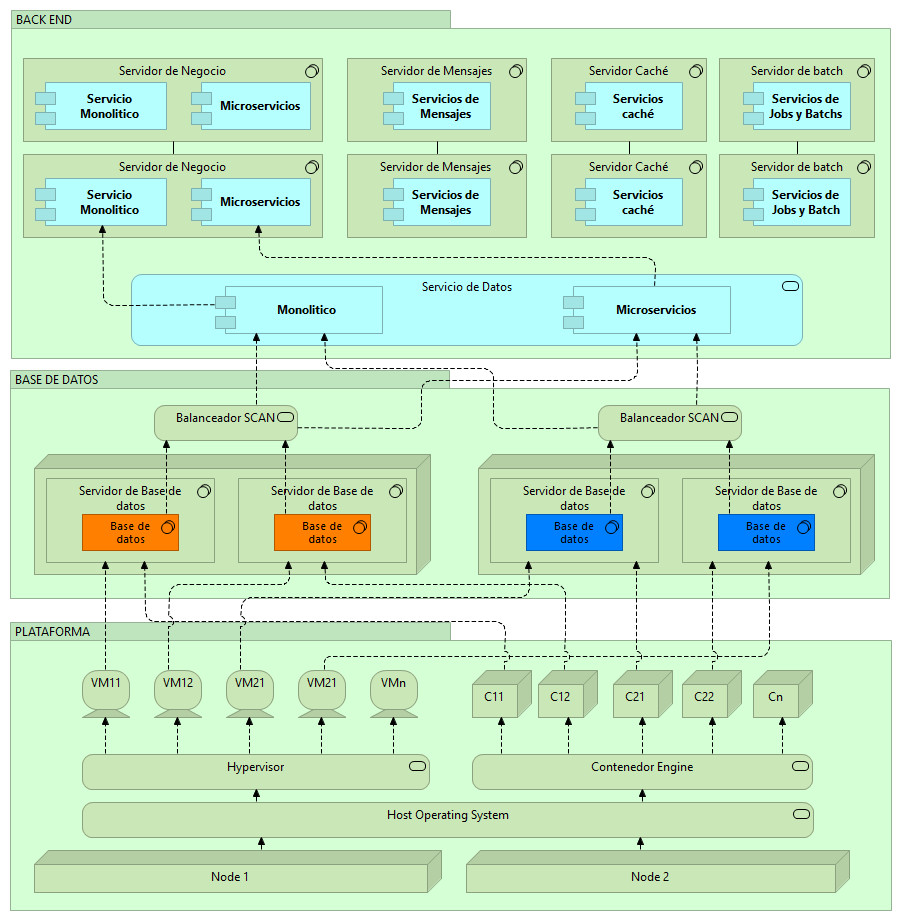


A continuación, se hará una descripción de las Capas de front end, experiencia de usuario, integración y backend a nivel de infraestructura y tecnología.



Se está considerando **alta disponibilidad para todas las capas de las arquitectura kadabra**

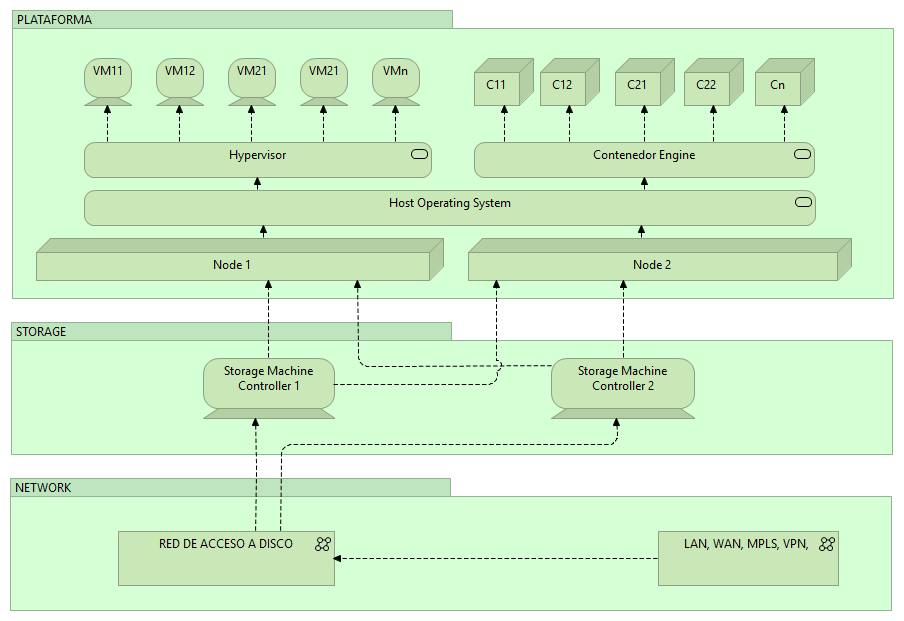
A continuación, se hará una descripción de las capas de Base de datos y plataforma a nivel de infraestructura y tecnología.



En la capa de Base de datos se ha definido que se mantengan 2 instancias completamente separadas, independientemente en cada instancia podrá utilizarse o no el tema de multitenant. En la arquitectura se ha considerado alta disponibilidad para la base de datos que se exponen a los servicios de negocios de microservicios y para los servicios monolíticos base de datos standalone. Además de considerar una base de datos de Standby Activo en el DRP como base de datos de réplica para que sea utilizados por cada AFP para su explotación de datos.

En la capa de plataforma se está considerando una misma infraestructura que maneje 2 nodos en alta disponibilidad, y la utilización de un hipervisor para la virtualización y exposición de máquinas virtuales y también un motor de contenedores para la exposición de conteiner, en las cuales estarán mapeados los microservicios.

A continuación, se hará una descripción de las capas de Storage y Network.

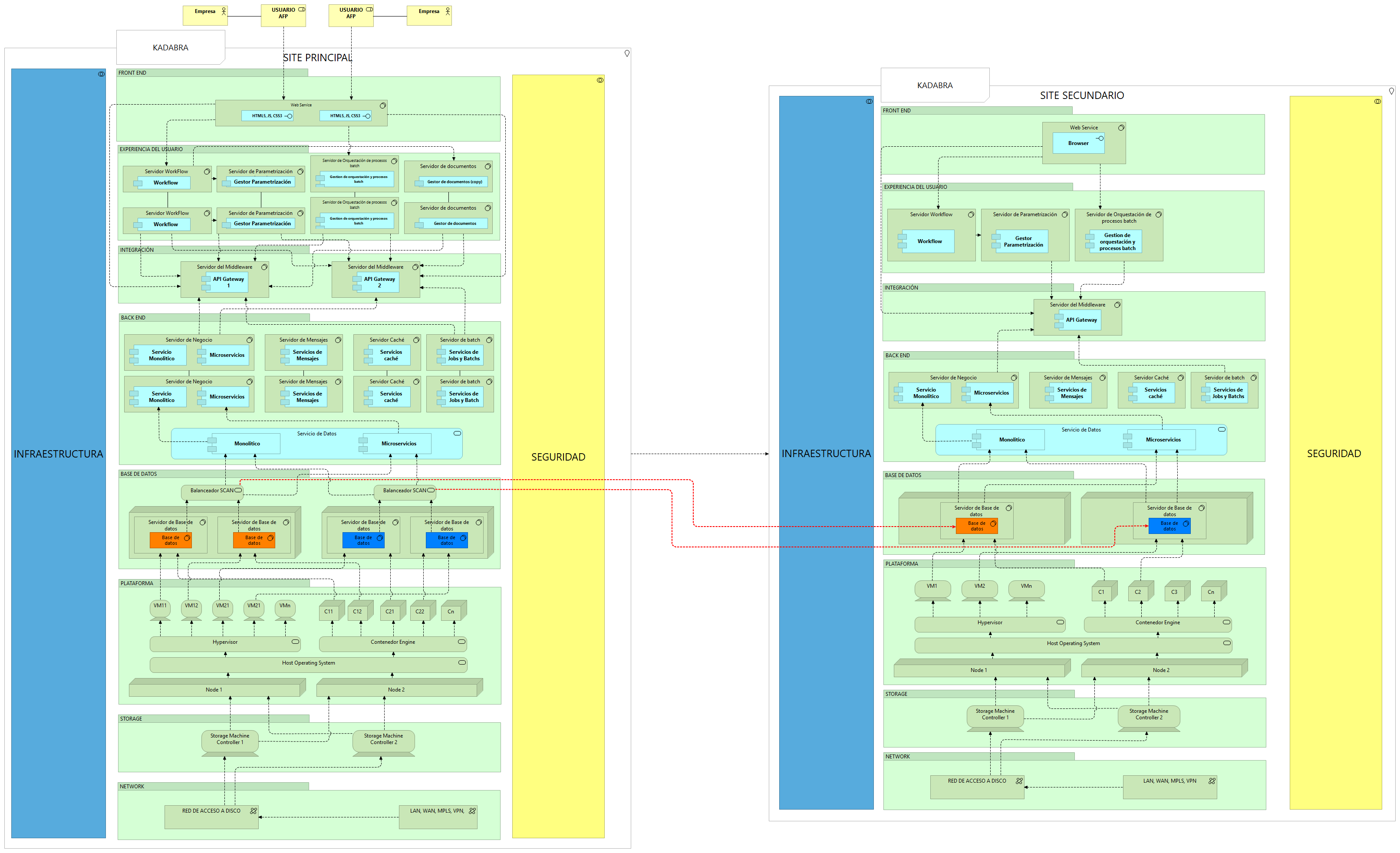


En la capa de storage se está considerando un equipo que tenga alta redundancia a nivel de controladores y que pueda asignar las capacidades a las Máquinas virtuales y/o a los contenedores, con un nivel de IOPs que satisfagan las necesidades de lectura y escritura en disco.

En la capa de Network tenemos 2 tipos: las redes de acceso a disco que para la infraestructura propuesta se ha considerado la red SAN o Infiniband por su alto desempeño. Las redes de acceso LAN, VLANs, MPLS y/o VPN.

### Arquitectura de Referencia en el DRP

A continuación, se describe la arquitectura referencial de infraestructura para el DRP en la que se expone las capas de redes, storage, plataforma, Base de datos, backend, integración, experiencia de usuario y front end.

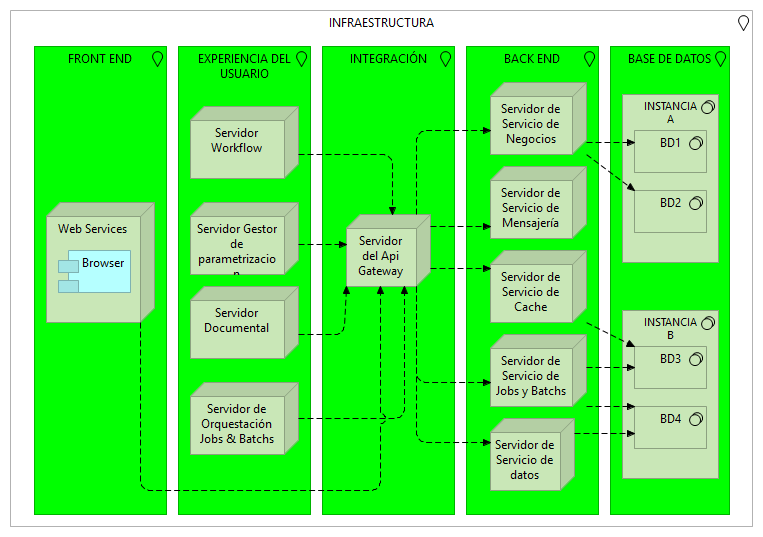


En la arquitectura del DRP se ha considerado que la capacidad a nivel de recursos sea máxima un 70% de la capacidad de producción, adicionalmente NO se dispondrá de alta disponibilidad para ninguna de las capas, y finalmente se prescindirá de algunos servicios de documentos en el DRP. Además, no se dispondrán de todas las capacidades de seguridad, como: Auditoria y bloqueo de sentecias sql. Para la arquitectura Kadabra se va a considerar un RTO de 2 horas y un RPO de 15 min.

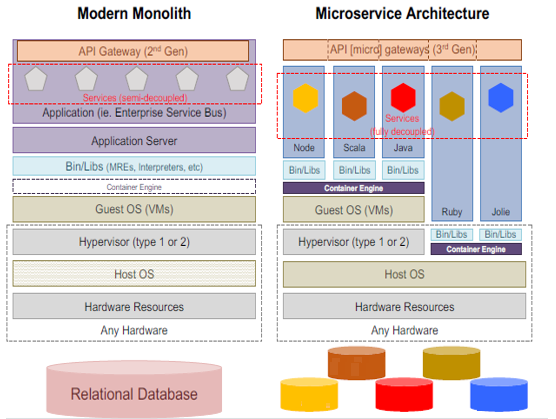
En lo referente al Tema del HA se está sugiriendo utilizar en la arquitectura de referencia con la estrategia de Activo – Activo, con el propósito de conseguir una máxima disponibilidad sin descartar la opción de Activo – Pasivo, cuya elección se definirá en la etapa de implementación.

### Diagrama de Servidores

A continuación, se describe la infraestructura a nivel de servidores por capas de manera general



A continuación, se describe la arquitectura para una aplicación monolítica y de microservicios



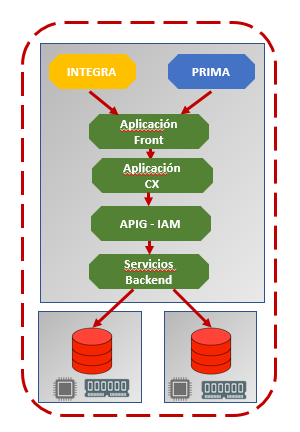
### Modelo Tecnológico de Asociación

A continuación, se describe el modelo tecnológico de asociación para el ambiente productivo y el ambiente de certificación en el que se comparte los servicios del front end, experiencia de usuario, integración y back end. Para la capa de base de datos se trabajará un esquema separados a nivel de instancias, motor y VMs.

Para el versionado de servicios se tendrá que implementar estándares de desarrollo respecto al versiona miento de la URI(Uniform Resource Identified), que tiene componentes que permiten manejar el versionado de servicios, a través de un esquema, una autoridad, ruta, consulta y un fragmento. Esto nos va a permitir manejar un estrategia de versionado manteniendo 2 uris distintas para un mismo servicio.

Ejem: http(s)://www.kadabra.com/<proceso de negocio>/**v1**/aplicación/capacidad/método1

http(s)://www.kadabra.com/<proceso de negocio>/**v2**/aplicación/capacidad/método1



Ventajas

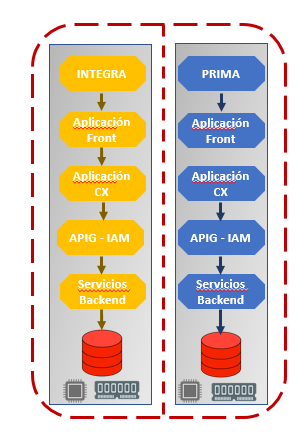
* Optimización de recursos de computo.
* Como consecuencia del punto anterior menores costos de inversión.
* Menor complejidad en los procesos de gobierno como el despliegue de aplicaciones y servicios, como también del mantenimiento y las operaciones del Core KADABRA.

Desventajas

* Mayor cantidad de configuraciones a nivel de los componentes, aplicaciones y servicios para lograr el procesamiento de las transacciones de forma independiente por cada AFP asociada.
* Mayor riesgo de afectación en los servicios de KADABRA ante posibles errores en los despliegues de las aplicaciones y servicios.
* Mayor complejidad para lograr customizaciones o personalizaciones por cada AFP asociada, manteniendo la premisa de desarrollar mas lógica de negocio en los servicios del backend y configuraciones en las apis de integración.

Mayor riesgos ante posibles eventos de seguridad.

Se describe el modelo tecnológico de asociación para el ambiente de Desarrollo en el que se mantienen separadas todas las capas.



VENTAJAS

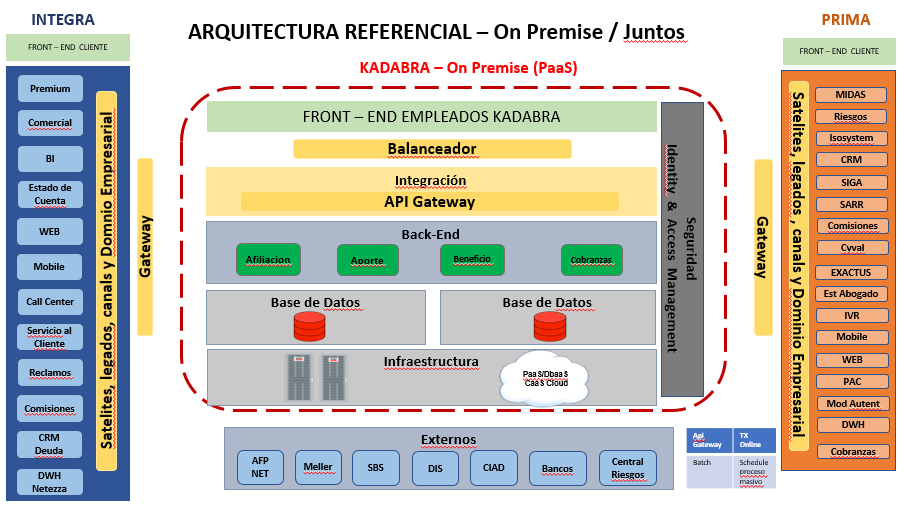
* Mayor facilidad de personalización y customización de los servicios y aplicaciones para cada AFP asociada.
* Despliegues independientes por cada AFP, menor es la dependencia en la gestión de los mantenimientos, sin que estos afecten a cada AFP
* Minimiza el riesgo de afectación del servicio debido a la saturación de componentes compartidos y errores producto de los procesos de despliegue.
* Separación del trafico red por cada AFP asociada, producto de ello reduce el riesgo de cualquier incidente de seguridad para ambas AFP asociadas.
* Menor riesgo ante posibles eventos de seguridad debido a que se tienen todos los componentes separados.

DESVENTAJAS

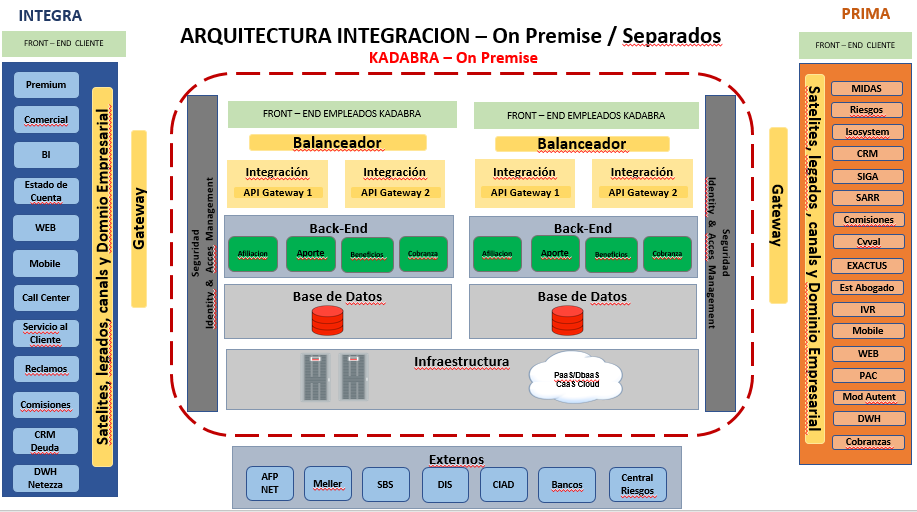
* Mayor cantidad de recursos de computo a utilizar, por ende mayores costos de inversión.
* Mayor cantidad de licencias a utilizar, aumenta el costo de inversión.
* Mayor gobierno en los procesos de despliegues de aplicaciones y servicios por cada uno de los componentes que conforma la arquitectura de KADABRA.
* Mayor gobierno en los procesos de mantenimiento de los componentes tecnológicos de KADABRA.
* Como consecuencia de los puntos anteriores también se evidencia mayor cantidad de recursos humanos para el gobierno y operatividad de KADABRA.

En la arquitectura Kadabra se está proponiendo un modelo (Dedicated On Premise Cloud) que vendría hacer On premise PaaS, el HW es proporcionado por la marca y el servicio es cloud del tipo IaaS o PaaS. Es un paso intermedio antes de pensar migrar por completo a la nube pública.

Esquema de Asociación para el ambiente Productivo y Certificación



Esquema de asociación para Desarrollo



### Lineamientos

HA Alta disponibilidad. En la arquitectura propuesta se ha definido que todas las capas manejaran un esquema del HA salvo la capa de front end y la capa de experiencia de usuario.

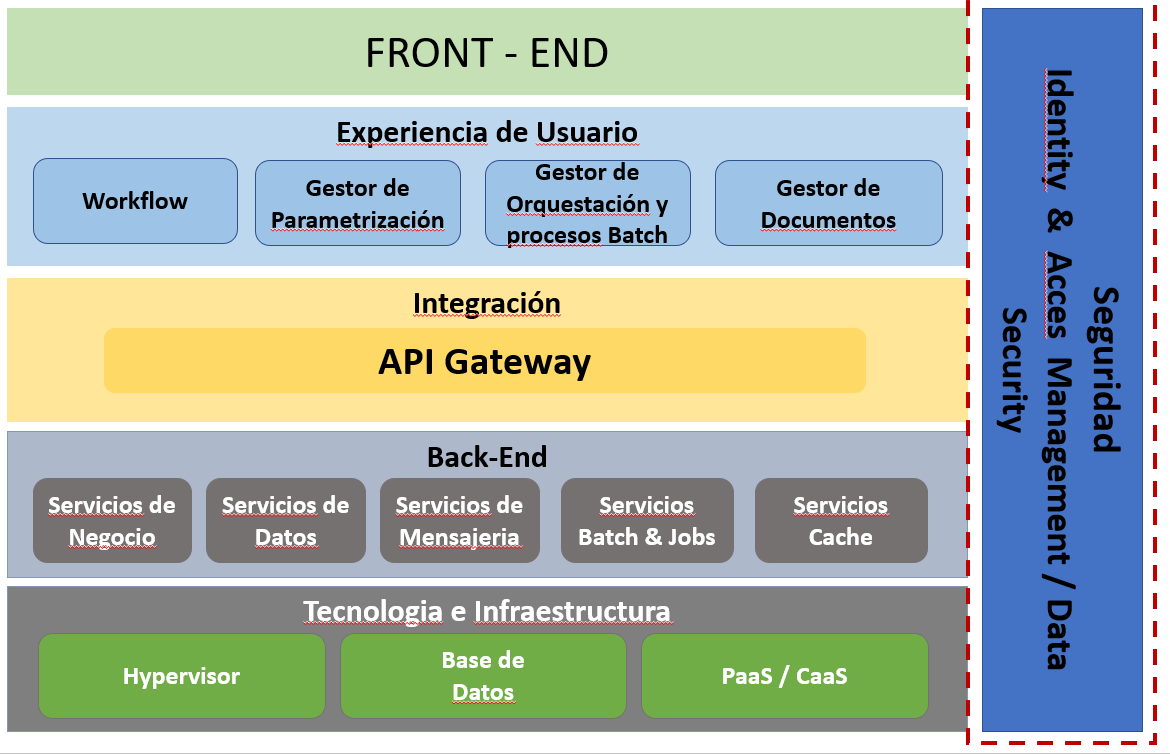
DRP Disaster Recovery. En la arquitectura se está considerando un site de contingencia con una arquitectura similar a la de producción (On premise PaaS) con una capacidad a nivel de recursos del 70% y sin considerar HA en el DRP.

Mutitenant de base de datos. - Se ha definido en la arquitectura que las bases de datos manejaran instancias separadas y cada instancia es libre de utilizar multitenant o no.

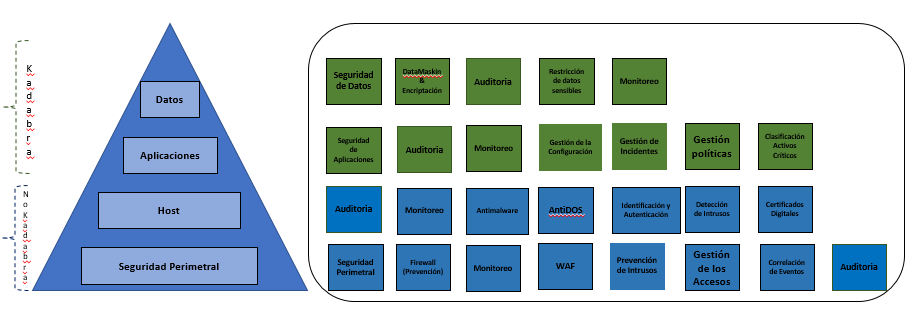
Modelo de Asociación. - Se ha definido en la arquitectura es juntos para las capas de aplicación y separados para la parte de datos tanto para el ambiente productivo como de certificación. Para el caso del ambiente de desarrollo el modelo de asociación será separados en todas sus capas.

## Seguridad

Esta sección contiene los esquemas y gráficos que representan la arquitectura de Seguridad TO-BE



### Capacidades



#### Gestión de los Accesos

Esta capacidad gestionara los ingresos debidamente controlados desde los canales de cada AFP hacia los recursos ubicados en la capa de Integración, Backend e Infraestructura de KADABRA; el encardado de canalizar esta capacidad es el componente de integración API Gateway con el de seguridad IAM.

**Capacidad fuera de KADABRA.**

#### Identificación y Autenticación

Esta capacidad se encargará de la identificación de usuarios (Clientes y/o Empleados) común un único punto de acceso, utilizando como semilla el usuario y password para generar el token de sesión y autorización para acceder a los recursos del backend, los componentes encargados de generar esta capacidad son el API Gateway, IAM y el LDAP (replica de cada AFP).

**Capacidad fuera de KADABRA.**

#### Seguridad de Datos

Esta capacidad será cubierta por el motor de base de datos escogido y manejará la granularidad de la seguridad de los datos, este se ayudará del componente IAM y el servicio de datos.

**Capacidad dentro de KADABRA.**

#### Seguridad de Aplicaciones

Esta capacidad será manejada en la capa de integración con el componente API Gateway y el componente de seguridad IAM para llegar a los servicios del Backend e Infraestructura de forma transparente.

**Capacidad dentro de KADABRA.**

#### Detección de Intrusos

Capacidad queda cubierta con el componente de red y seguridad Firewall (Contra Fuego) y permitirá detectar accesos no autorizados en la red analizando el tráfico y reportando el evento a la oficina de seguridad y centro de monitoreo de KADABRA.

**Capacidad fuera de KADABRA.**

#### Prevención de Intrusos

Al contrario de la capacidad de Detección de Intrusos esta corta el tráfico y rechaza las tramas a nivel de red, esta capacidad será manejada por el Firewall.

**Capacidad fuera de KADABRA.**

#### Seguridad Perimetral

Capacidad a nivel de diseño de red para mitigar el acceso indebido a las capas de KABABRA, esta contara con una DMZ de presentación para exposición de APIs a los canales de cada AFP , una VLAN protegida para la capa de Front-End, Integración y Experiencia de Usuario y otra VLAN para la persistencia de los datos mediante el componentes de base de datos.

**Capacidad fuera de KADABRA.**

#### Datamasking / Encriptación

Capacidad que permitirá la ejecución de políticas y reglas para convertir y transformar mediante algoritmos la salida de data no relacionada para ser utilizada para ambientes de Pruebas e Integración y encriptación de datos para ambientes productivos, esta capacidad será ejecutada en un componente tecnológico independiente del motor de base de datos.

**Capacidad dentro de KADABRA.**

#### Gestión de la Configuración

Capacidad que será expuesta por los componentes de integración API Gateway y seguridad IAM para la configuración de políticas de los usuarios.

Se considerará un componente de la gestión de la configuración para gobernar la infraestructura y la seguridad.

**Capacidad dentro de KADABRA.**

#### Gestión de Incidentes

Será manejada por un componente de gestión de incidentes que tendrá las capacidades de:

1. Analizar los componentes de tecnológicos que forman KADABRA.
2. Registro manual y automático de incidentes relacionados con KADABRA.
3. Visualizar incidentes relacionados a los componentes de KADABRA.
4. Manejar un historial de incidentes.

Se generarán reportes de incidentes o vulnerabilidades para ser analizadas por los oficiales de seguridad de KADABRA para tomar las acciones preventivas y correctivas según sea el caso.

Se utilizara un componente de mesa de ayuda orientado a gestionar los incidentes de kadabra manteniendo SLAs, tiempo de respuesta y comunicaciones que definirán en conjunto con las AFPs asociadas.

**Capacidad dentro de KADABRA.**

#### Gestión de Políticas

Esta capacidad será manejada por el componente **Policy Server** el cual se conectará con el IAM para ejecutar las políticas de accesos y autorización de cada AFP hacia KADABRA.

**Capacidad dentro de KADABRA.**

#### Clasificación de Activos Críticos

Esta capacidad está orientada a identificar los componentes críticos dentro de KADABRA que ante un evento controlado y no controlado pueda afectar el funcionamiento de los servicios externos e internos de las AFPs asociadas. La salida de esta capacidad será una matriz de clasificación de activos versus criticidad.

**Capacidad dentro de KADABRA.**

#### Restricción de Datos Sensibles

Capacidad que permitirá la ejecución de políticas y reglas para restringir el acceso a datos clasificados como sensibles, esta capacidad será ejecutada en un componente tecnológico independiente del motor de base de datos.

La encriptación permitirá que algunos datos sensibles se vuelvan ilegibles gracias a un algoritmo que desordena sus componentes. Por lo tanto cualquier servicio que no disponga de las llaves no podrá acceder a la información y solo podrá visualizar datos cifrados.

**Capacidad dentro de KADABRA.**

#### Auditoria

Capacidad de auditoria centralizada el cual permitirá registrar en tiempo real los cambios que se realicen en el LDAP, sistemas de archivos, servicios, base de datos.

El IAM Ofrece funcionalidades para la administración de roles e identidades, la administración de aprobaciones y pedidos, la administración de derechos basados en políticas, la integración de tecnología y la automatización para el cumplimiento y las auditorias

Para la auditoria de Base de datos se dispondrá de un componente que permita una primera línea de defensa para las base de datos y consolidación de la data de auditoria, ofreciendo reportes de regulación como SOX, PCI, DSS y HIPPA

**Capacidad dentro de KADABRA.**

#### Certificados Digitales

Capacidad que manejara el intercambio de llaves asimétricas para la encriptación del medio de transporte TLS 1.2, los certificados generados serán de tipo WILDCARD para la generación de sub-dominios, estos certificados se guardaran en el balanceador de la DMZ de presentación y serán solo utilizados por las APIs que se expondrán hacia los canales de cada AFP.

**Capacidad fuera de KADABRA.**

#### Correlación de Eventos

Capacidad que manejara las diferentes bitácoras de las aplicaciones, servicios y componentes de la arquitectura KADABRA para luego analizar datos e identificar las relaciones entre estas con el fin de correlacionar eventos para realizar acciones, enviar alertas basadas en las reglas definidas en KADABRA.

**Capacidad fuera de KADABRA.**

#### Monitoreo

Capacidad que tendrá que ser gestiona con una herramienta que permita mostrar la trazabilidad de las transacciones de negocio end2end de todas las componentes de KADABRA.

**Capacidad fuera de KADABRA.**

#### Antimalware

Capacidad ejecutada dentro de la capa de seguridad de KADABRA con la finalidad de prevenir, detectar y remediar software malicioso en los servidores KADABRA.

**Capacidad fuera de KADABRA.**

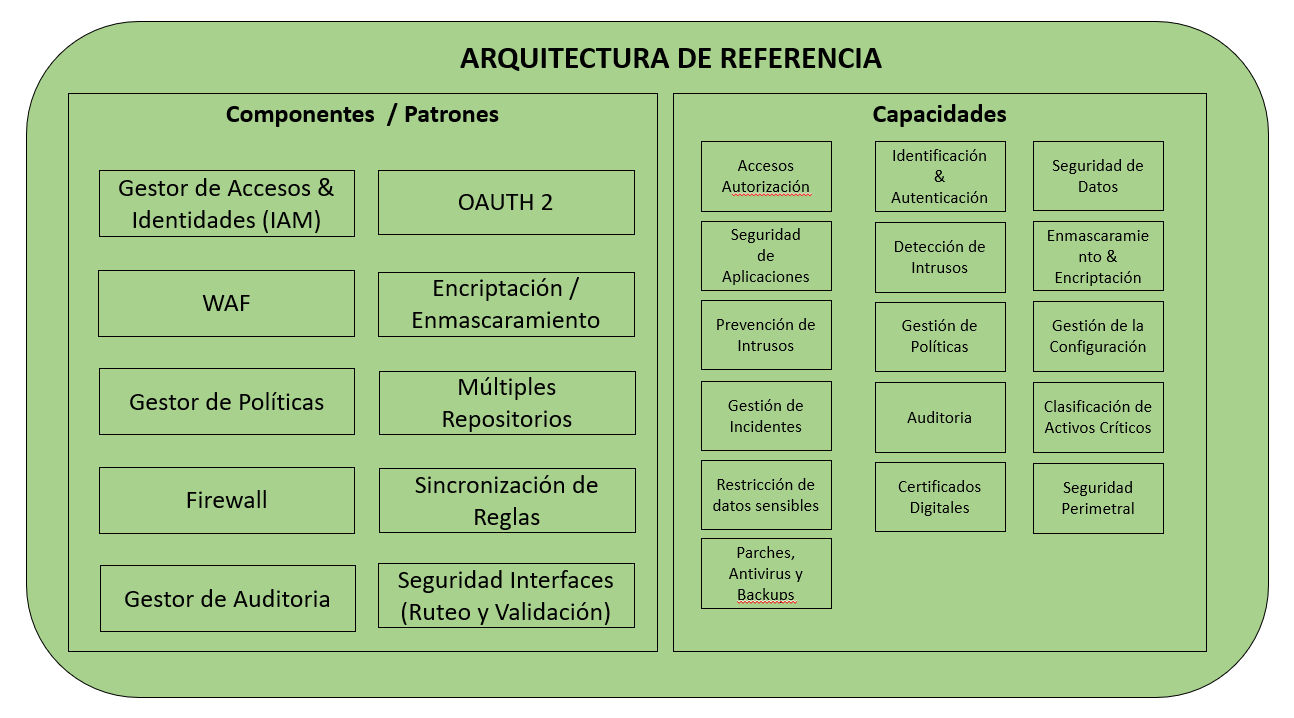
#### AntiDoS

Capacidad que se encargara de proteger los servicios de la capa Front-End e Integración ante ataques de servicio que puedan afectar los SLAs de KADABRA, este componente se encargara de Analizar en tiempo real y a alta velocidad todos los paquetes y mitigar los riesgos dejando pasar sola las IPs legitimas.

**Capacidad fuera de KADABRA.**

### Arquitectura de Referencia

A continuación, se muestra la arquitectura de referencia de seguridad planteada para KADABRA.



Compuesta por componentes tecnológicos, patrones, estándares y capacidades.

### Patrones

#### OAUTH 2

Es un patrón basado en el estándar de la industria para implementar las capacidades de autorización, la implementación de dicho patrón será responsabilidad del API Gateway y el IAM, el cual se utilizará para brindar acceso a los recursos de KADABRA.

Para el funcionamiento de este patrón se implementarán los siguientes recursos:

1. Un servidor de autorización y generación de TOKENS.
2. Base de datos con la METADATA de los accesos y TOKENS generados.

#### Encriptación / Enmascaramiento

Este patrón utilizara algoritmos de sustitución, intercambio, variación de cifras y fechas, cifrado de datos y eliminación de datos según se desarrollen los requerimientos para las pruebas y exposición de datos.

#### Múltiples Repositorios

Este patrón permitirá manejar de forma independiente los diferentes repositorios de cada AFP como directorio activo, LDAP, base de datos y file system; también gestionará en forma independiente las políticas y reglas de acceso por cada AFP.

#### Sincronización de Reglas Acceso

Este patrón permitirá refrescar en tiempo real los cambios que se realicen desde los repositorios LDAP o Active Directory de cada AFP; este patrón podría dejar de utilizarse si solo si el IAM se conecte directamente a cada repositorio de cada AFP sin ninguna restricción técnica.

#### Seguridad de Interfaces (Ruteo y Validación)

Este patrón sera gestionada básicamente en la capa de integración con el componente API Gateway el cual se integrará con el IAM para ejecutar las políticas de acceso a los servicios del backend.

#### Estándares y normativas de Seguridad de Información

El estándar y/o norma **ISO/IEC 27001** es la norma que se utilizara para implementar las siguientes capacidades:

* Garantizar los controles para salvaguardar y proteger la información.
* Confiabilidad.
* Integridad.
* Disponibilidad de información.
* Seguridad perimetral

**ISO 27003**, guía de buenas prácticas cuyo objetivo es la implementación de estándares sobre Sistemas de Gestión de la Seguridad de la Información (SGSI), gestión de roles y responsabilidades, auditoria, políticas claves de seguridad, y seguimiento y monitoreo que serán configuradas para KADABRA.

**ISO 27004**, Implementación de métricas y técnicas asociada a controles en la implementación del SGSI, para el caso de KADABRA servirá para la sustentación de los controles SOX enviados desde las áreas de negocio y seguridad hacia KADABRA.

**ISO 27017**, Guía de implementación para controlar la red perimetral y el acceso a la nube Cloud Computing.

**ISO 27018**, Guía de implementación para controlar la protección de datos para los servicios de Cloud Computing. (privadas, publicas e hibridas)

**ISO 27032**, teniendo en cuenta que se van exponer Api’s a los canales digitales se recomienda la implementación de este ISO que aborda "Ciberseguridad" o "la seguridad del ciberespacio", definida como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio". A su vez, "el ciberespacio" se define como "el entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos y redes conectadas a él, que no existe en ningún entorno físico.

**ISO 27035**, Guía para la implementación de incidentes de seguridad

**ISO 27039**, Guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión.

### Componentes

#### Gestor de accesos & identidades (IAM)

Componente que se usara para cubrir las siguientes capacidades:

1. Accesos y autorización
2. Identificación y autenticación
3. Auditoria

#### Web Application Firewall (WAF)

Componente que se encargará de analizar el tráfico web y que será manejada en el balanceador ubicado en la DMZ de presentación para el acceso de las aplicaciones en los canales de da cada AFP.

#### Gestor de Políticas

Componente que se encargara de manejas las políticas de red y accesos configuradas en KADABRA, este se integra con el IAM para la sincronización, replicación y ejecución de políticas en tiempo real.

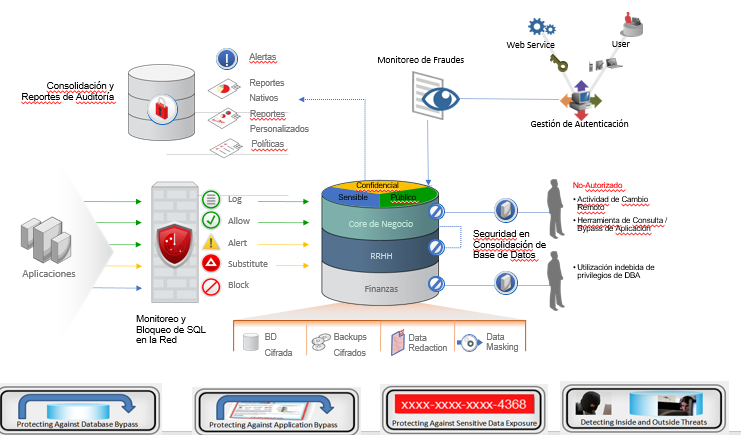
#### Firewall

Componente que se encargara de gestionar el tráfico de red entre la DMZ de presentación, la VLAN de aplicación y la VLAN de datos mediante políticas y reglas de acceso, fijarse en el gráfico de la vista de red perimetral.

#### Gestor de Auditoria

Componente que se encargara de centralizar la auditoria de cada uno de los componentes de KADABRA en cada una de las capas propuestas en la arquitectura.

### Vista de Seguridad de Datos



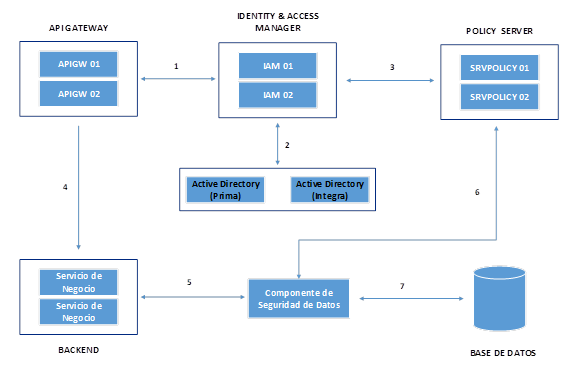
### Vista de Seguridad Perimetral



**Externos**, son las empresas terceras con las que KADABRA va a comunicarse para realizar sus operaciones como la SBS, AFPNet, Bancos, Estudios Abogados, ..etc.

### Caso de Uso

Muestra el flujo de cómo se ejecutarían las políticas de seguridad a nivel de servicios y datos.



1. El API Gateway envía mediante los datos de cabecera los parámetros de seguridad para la autenticación y autorización hacia los recursos del BACKEND y BASE DE DATOS.
2. El IAM recibe los parámetros y los valida contra cada uno de los repositorios de cada AFP si es correcta la validación, este procede a validar si en los datos enviados hay políticas que se tengan que ejecutar.
3. El Policy Server valida las políticas y las envía a ejecutar mediante el IAM y el API Gateway para luego dejar pasar hacia los servicios de negocios ubicados en el backend.
4. Los servicios de negocio reciben si es que fuera el caso parámetros de seguridad para ser ejecutadas por el componente de seguridad de datos.
5. El Componente de seguridad de datos recibe los parámetros de los servicios de negocio para luego validarlos con el Policy Server.
6. El componente de seguridad de base de datos procede a validar si hay políticas de accesos a datos como restricción de datos sensibles o protección de datos según sea el caso.
7. Si el punto 6 es satisfactorio el servicio procede a realizar operaciones sobre las filas seleccionadas.

### Lineamientos

En este apartado se describirán algunos lineamientos de seguridad que se tendrán que tomar en cuenta para desarrollarlos en la etapa de implementación.

1. El componente IAM utilizara recursos de computo comunes para ambas AFPs pero se crearan instancias y dominios por separado.
2. Al igual que el punto anterior los componentes Policy Server y el componente de seguridad de datos utilizaran recursos de computo compartido, pero para ambos instancias y grupos de políticas separados para cada asociada.
3. Se manejará un esquema de alta disponibilidad local para los componentes de seguridad como el IAM, Policy Server, API Gateway y el componente de seguridad de datos. Para el site de contingencia o DRP estos componentes serán configurados sin alta disponibilidad.
4. Se configurarán 3 segmentos de red con la siguiente finalidad:

**DMZ de Presentación**, esta será de cara a los canales de cada AFP e internet en caso ambas asociadas deseen desarrollar productos digitales y necesiten exponer datos de KADABRA, para ello se manejara un balanceador de tipo ADC (Application Delivery Controller) para manejar las capacidades de certificados digitales mediante un WildCard (Generación de certificados bajo un dominio o sub-dominio) y activar la capacidad de WAF (Web Application Firewall) para cubrir las vulnerabilidades manejadas en el OWASP Top Ten.

**VLAN de Aplicación,** esta VLAN alojara los componentes de las capas de KADABRA tanto del Backend y Experiencia de Usuario, por esta VLAN se conectarán las AFP asociadas más los socios estratégicos y terceros.

**VLAN de datos,** esta VLAN alojara las bases de datos de KADABRA, estas trabajaran bajo un esquema de infraestructura y recursos separados para ambas asociadas, como best-practice la norma **ISO/IEC 27001** en capítulo tecnológico relacionado al diseño de una red perimetral recomienda que se separe de forma independiente el acceso y la gestión de la persistencia de los datos sensibles.

1. Se trabajará bajo un esquema de replicación del Active Directory o LDAP de cada AFP hacia los componentes de KADABRA, salvo que no existe restricción técnica alguna para conectarse directamente a cada AFP.
2. El desarrollo de las políticas será parametrizables, personalizadas y configuradas para cada AFP asociada según sus requerimientos de negocio.
3. Como lineamiento las políticas y roles de cada AFP serán configuradas de forma independiente.