**UNIVERSIDAD PERUANA LOS ANDES**

**FACULTAD DE INGENIERÍA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y**

# COMPUTACIÓN



Base de Datos II

Arquitectura Centralizada

**AUTOR**

VICENTE RAMOS, Elian

**DOCENTE**

RAUL FERNANDEZ, Bejarano

**CICLO**

V

# HUANCAYO – PERÚ – 2025

Arquitectura Centralizada

1. Portada

Título: Proyecto Técnico de Arquitectura Centralizada

Cliente / Organización: [Nombre de la organización]

Autor: Eli Mar (o nombre del responsable)

Fecha: 02/10/2025

2. Resumen ejecutivo

Este documento describe el diseño técnico, el plan de implementación y los requisitos para desplegar una arquitectura centralizada de servicios TI para [Nombre de la organización]. El objetivo es concentrar servicios críticos (aplicaciones empresariales, datos y autenticación) en una plataforma central gestionada, mejorando la administración, seguridad y cumplimiento, reduciendo la duplicidad de servicios y optimizando costos operativos.

3. Objetivos

* Centralizar los servicios de aplicaciones y datos en un datacenter local o en un proveedor de nube privada/colocación.
* Asegurar accesos controlados y trazabilidad mediante IAM (gestión de identidades y accesos).
* Garantizar alta disponibilidad (HA) para servicios críticos.
* Implementar políticas de respaldo y recuperación ante desastres (DR).
* Proveer un marco de seguridad que cubra red, host y aplicación.

4. Alcance

Incluye:

* Diseño lógico y físico de la arquitectura centralizada.
* Requisitos de hardware y software para servidores, almacenamiento y red.
* Políticas de seguridad, backup y DR.
* Plan de migración de sistemas heredados.
* Cronograma y estimación de costos.

No incluye:

* Implementación de estaciones de usuario final (salvo ajustes de red y acceso).
* Integración con terceros fuera del alcance acordado (a menos que se especifique).

5. Requisitos

5.1 Requisitos funcionales

* Autenticación central (LDAP/Active Directory).
* Servidor(es) de aplicaciones centralizados.
* Servidor(es) de base de datos centralizados con replicación.
* Servicio de archivos centralizado (NFS/SMB).
* Portal de administración central.

5.2 Requisitos no funcionales

* Disponibilidad objetivo: 99.95% para servicios críticos.
* Tiempo de recuperación objetivo (RTO): 2 horas.
* Punto de recuperación objetivo (RPO): 1 hora.
* Escalabilidad horizontal mediante balanceo de carga.
* Cumplimiento con políticas de seguridad locales y normativas aplicables.

6. Diseño arquitectónico

6.1 Arquitectura lógica

* Capa de presentación: Clientes web/móviles y VPN/Proxy de acceso seguro.
* Capa de aplicaciones: Cluster de servidores de aplicaciones detrás de balanceadores.
* Capa de datos: Cluster de bases de datos con réplica primaria-secundaria.
* Servicios transversales: Autenticación (LDAP/AD), registro/auditoría, backup, monitoreo.

6.2 Arquitectura física (resumen)

* Datacenter/colocation o proveedor de nube privada.
* VLAN separadas: administración, aplicaciones, base de datos, DMZ, backup.
* Firewall perimetral y sistema de prevención de intrusiones (IDS/IPS).
* Balanceador de carga (HAProxy, F5 o equivalente).

6.3 Diagrama (texto)

Internet

|

Firewall Perimetral (HA)

|

Load Balancer (HA)

|

+-----------------------------+

| VLAN aplicaciones (Cluster) |

| - App1 (VM/Conteiner) |

| - App2 |

+-----------------------------+

|

+-----------------------------+

| VLAN base de datos (Cluster) |

| - DB primaria |

| - DB réplica |

+-----------------------------+

|

Storage SAN/NAS (Snapshots, Backup)

|

Backup & DR Site (replicación asincrónica)

7. Componentes y especificaciones

7.1 Infraestructura de cómputo

* Servidores de aplicaciones (x3 VMs): CPU 8 vCPU, RAM 32 GB, 200 GB SSD.
* Servidores de base de datos (cluster): 2 nodos (Primario/Replica) CPU 16 vCPU, RAM 64 GB, NVMe 1 TB.
* Servidor de administración y monitoreo (x1): CPU 4 vCPU, RAM 16 GB.

7.2 Almacenamiento

* SAN/NAS con snapshots: 10 TB usable inicial, expansión por volumen.
* Políticas de IOPS para DB (asegurar latencia baja).

7.3 Red

* Routers y switches administrables con soporte VLAN y QoS.
* VLANs: 10 (gestion), 20 (aplicaciones), 30 (bd), 40 (DMZ), 50 (backup).
* VPN de sitio a sitio y acceso remoto con MFA.

7.4 Software

* Sistema operativo: Linux Enterprise (RHEL/Ubuntu LTS) o Windows Server según necesidad.
* Base de datos: PostgreSQL / MariaDB / MS SQL (según requisito).
* Balanceo: HAProxy / Nginx / F5.
* Directory: Active Directory o OpenLDAP.
* Monitoreo: Prometheus + Grafana o Zabbix.
* Backup: Bacula / Veeam / solución compatible con snapshots.

7.5 Seguridad

* Firewall perimetral y reglas por aplicación.
* IDS/IPS y segmentación de red.
* Encriptación in transit (TLS 1.2/1.3) y at-rest para datos sensibles.
* Gestión de parches automatizada.
* Control de accesos basado en roles (RBAC).

8. Plan de migración

Fase 0 - Preparación (2 semanas)

* Inventario de sistemas actuales.
* Copia de seguridad completa.
* Pruebas de compatibilidad.

Fase 1 - Infraestructura base (3 semanas)

* Provisionamiento de hardware/VMs.
* Configuración de red y VLANs.
* Despliegue de directorio y certificados.

Fase 2 - Servicios y datos (3 semanas)

* Instalación de servidores de aplicaciones.
* Migración de bases de datos a entorno controlado.
* Pruebas de rendimiento y carga.

Fase 3 - Validación y puesta en producción (2 semanas)

* Pruebas integradas (UAT).
* Corte y monitoreo 24/7 inicial.

Fase 4 - Optimización y cierre (2 semanas)

* Ajustes de configuración.
* Documentación final y capacitación.

9. Pruebas y validación

* Pruebas unitarias en cada servicio.
* Pruebas de integración entre capas.
* Pruebas de rendimiento (stress, carga y endurance).
* Pruebas de failover para HA y DR.
* Pruebas de seguridad (scan de vulnerabilidades y pentest básico).

10. Plan de contingencia y DR

* Replicación de datos a sitio secundario (asincrónica o síncrona según RPO).
* Procedimiento de conmutación por error (failover) documentado.
* Copias de seguridad diarias y retención por 30 días (ajustable).