PLAN DE CONTINGENCIA Y SOSTENIBILIDAD DE INFRAESTRUCTURA TI

Version 1.0

V° B°

Firmado digitalmente por RUBIO SANCHEZ Roxana FAU 20453744168 hard
Motivo: Viso en señal de conformidad
Fecha: 20/02/2026 09:44 a. m.

V° B°

Firmado digitalmente por PEREZ CERNA Carlos Alfonso FAU 20165645325 hard
Motivo: Viso en señal de conformidad
Fecha: 19/02/2026 03:06 p.m.

V° B°

Firmado digitalmente por BECERRA NOVOA Gustavo Pierre FAU 20165645325 soft
Motivo: Viso en señal de conformidad
Fecha: 19/02/2026 10:44 p.m.

V° B°

Firmado digitalmente por VELASQUEZ DIAZ Ronald Heenry FAU 20453744168 soft
Motivo: Viso en señal de conformidad
Fecha: 20/02/2026 09:14 a.m.

CONTROL DE VERSIONES				
Versión	**Elaborado por**	**Aprobado por**	**Fecha**	**Descripción**
1.0	Ing. Gustavo Novoa Becerra	Ing. Carlos Pérez Cerna	30/12/2025	Versión inicial

1. Introducción

La Dirección Regional de Salud (DIRESA) Cajamarca tiene como misión fundamental garantizar adecuados procesos de gestión para la atención integral de salud a favor de las comunidades de diversas culturas y creencias, proporcionándoles los medios necesarios para salvaguardar su salud y propiciando la participación activa de la sociedad civil. En este sentido, la institución ha desarrollado un ecosistema digital que actúa como el vehículo principal para operativizar dicha gestión. Los sistemas "One Vision" y los Tableros de Indicadores representan los "medios necesarios" que la DIRESA pone a disposición de la región para asegurar que la atención de salud sea eficiente, equitativa y basada en información técnica veraz. La estabilidad de estas plataformas es, por lo tanto, un requisito indispensable para cumplir con la promesa institucional de salvaguardar la salud de todos los cajamarquinos.

Actualmente, la capacidad de la DIRESA para ejercer este control y proporcionar una atención integral descansa sobre una infraestructura tecnológica híbrida de alta complejidad, la cual combina la virtualización tradicional en Microsoft Hyper-V con la orquestación moderna de contenedores mediante Kubernetes (K8s). Esta arquitectura ha sido diseñada para evolucionar desde modelos centralizados hacia un entorno de Alta Disponibilidad (HA), buscando eliminar los Puntos Únicos de Fallo (SPOF) que históricamente ponían en riesgo la continuidad de los servicios. No obstante, la sofisticación de componentes como el cluster de base de datos Patroni, el sistema de caché Redis y la red de microservicios, exige una gobernanza técnica de alto nivel para garantizar que la tecnología sea un soporte fiable y no un obstáculo para la gestión sanitaria regional.

El presente documento, denominado **Plan de Contingencia y Sostenibilidad de Infraestructura de TI**, constituye el marco normativo y estratégico para proteger esta infraestructura en el Data Center de la sede central. Su propósito es establecer los lineamientos y Procedimientos

Operativos Estándar (POEs) que permitan mitigar riesgos operativos antes de que estos afecten la atención al ciudadano. Un punto neurálgico de este plan es la gestión proactiva de los recursos limitados, especialmente el monitoreo crítico de la memoria RAM y CPU de los servidores físicos. Dado el actual nivel de demanda de los sistemas, la administración eficiente de este hardware es vital para asegurar que los "procesos de gestión" mencionados en la misión institucional no se vean interrumpidos por limitaciones de capacidad técnica.

Más allá de la operación diaria, este plan detalla la Estrategia de Recuperación ante Desastres (DRP), estableciendo protocolos rigurosos para la protección de los datos sensibles de salud. Mediante el uso de herramientas especializadas como Barman para la persistencia de datos y Velero para la infraestructura de contenedores, se garantiza que el Punto de Recuperación (RPO) y el Tiempo de Recuperación (RTO) cumplan con los estándares de seguridad necesarios. El objetivo final es garantizar que, incluso ante escenarios de falla catastrófica, la información clínica y administrativa de la DIRESA permanezca íntegra, inmutable y disponible para su pronta restauración, minimizando cualquier impacto negativo en las comunidades beneficiarias.

Finalmente, el documento proyecta la sostenibilidad del modelo a largo plazo, identificando la necesidad imperativa de cerrar las brechas de calidad detectadas. Esto incluye la remediación estratégica de la Deuda Técnica de 193 días y la formalización de un perfil de Aseguramiento de la Calidad (QA) que proporcione la red de seguridad necesaria para las actualizaciones del software. Asimismo, el plan define una hoja de ruta tecnológica que promueve la observabilidad proactiva con Prometheus y Grafana, establece las bases para el diagnóstico de seguridad recurrente con OWASP ZAP y propone la centralización del conocimiento técnico en una Wiki institucional. Con esta visión prospectiva, la DIRESA Cajamarca reafirma su compromiso con una gestión moderna, transparente y orientada a la mejora continua de sus servicios digitales.

2. Objetivos

2.1. Objetivo General

Asegurar la continuidad operativa de los servicios digitales de la DIRESA Cajamarca, minimizando el impacto de fallos tecnológicos, humanos o naturales, y garantizando la sostenibilidad de la plataforma tecnológica a largo plazo

2.2. Objetivos Específicos

a) Garantizar la Resiliencia de los datos asegurando el RPO (Punto de Recuperación) cercano a cero para las bases de datos Postgres mediante Patroni y Barman.
b) Mitigar la Saturación de Recursos estableciendo un protocolo de "Apagado Selectivo" (Load Shedding) ante la caída de un nodo físico, dado que el consumo actual de RAM (70% por nodo) impide un failover total automático.
c) Formalizar la Recuperación ante Desastres implementando la estrategia de backups 3-2-1 utilizando la nube de Claro como repositorio externo.

3. Alcance

El plan cubre todos los activos críticos ubicados en el Data Center del Jr. Mario Urteaga N° 500:

- **Capa Física:** 2 Servidores HP (Hyper-V Cluster), Storage SAN (Fibre Channel), Switches Core y Perímetro (Fortinet HA).
- **Capa Virtual:** 70 Máquinas Virtuales (Windows/Linux).
- **Capa de Aplicación:** Clusters de Kubernetes (Vanilla), Sistemas One Vision, Superset
- **Capa de Datos:** Clusters PostgreSQL con Patroni, Redis Sentinel.

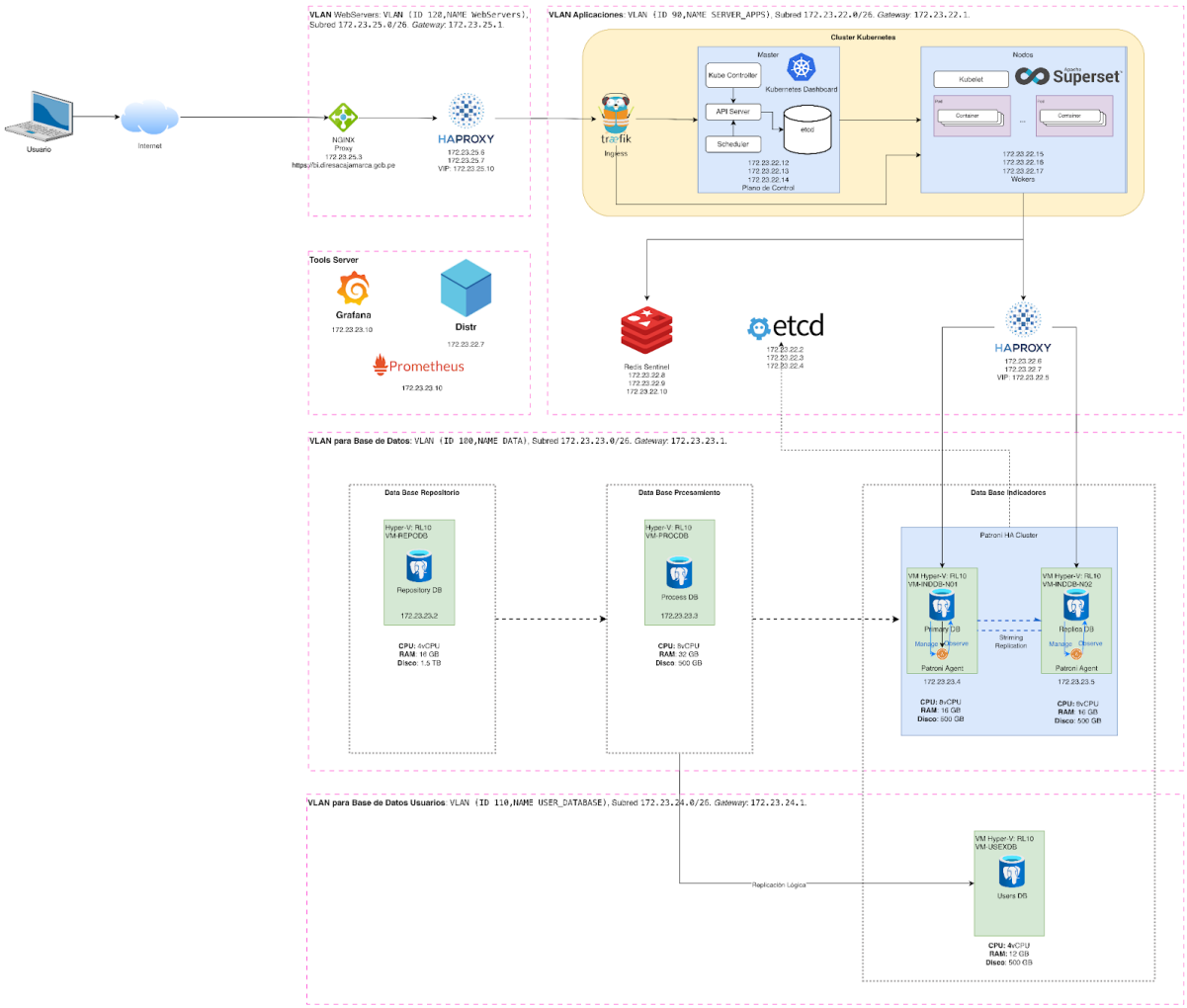
Exclusiones*:* Equipamiento de usuario final y conectividad interna de las redes de salud periféricas

4. Arquitectura

La infraestructura virtual se divide en dos ecosistemas que comprten segmentos de VLANs y estas separan las diversas capas para garantizar seguridad y rendimiento

4.1. Ecosistema de Análisis de Datos

Orientado al procesamiento de indicadores y business intelligence (BI). Se basa en una cadena de datos que fluye desde la obtención de datos sin procesar y los guarda en las bases de datos de repositorios, hasta la visualización de indicadores.

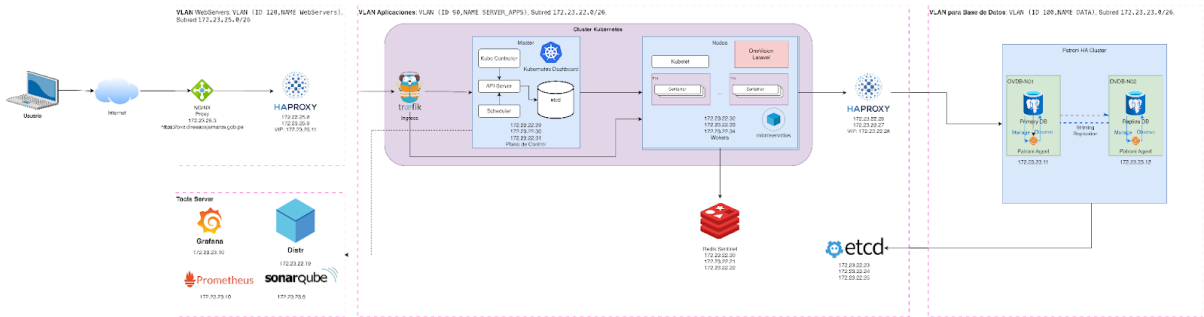


Img. 1: Arquitectura del Ecosistema de Análisis de Datos

- **Capa de Acceso:** SSL mediante NGINX Proxy y balanceo mediante HAProxy (VIP 172.23.25.10).
- **Orquestación:** Cluster K8s dedicado para la instancia de Apache Superset y otras aplicaciones que se irán construyendo
- **Capa de Datos:** Estructura dividida en:
- **Bases de Datos de Repositorio:** Datos sin procesar información ontenida de doversas fuentes.
- **Bases de Datos de Procesamiento:** Datos transformados a partir de las bases de datos de Repositorio .
- **Bases de Datos de Indicadores:** Cluster Patroni de alta disponibilidad para exponer los indicadores en los tableros que serán consultados por los usuarios finales.
- **Bases de Datos de usuario:** Información replicada mediante procesos ETL para consulta de usuarios externos.

4.2. Ecosistema One Vision y Microservicios

Orientado para la operación transaccional en tiempo real de los servicios de salud de las IPRES que han implementado el One Vision Clinico y One Vision Administrativo. Se basa en un flujo de datos que va desde los usuarios de los sistemas web de las distintas IPRES hasta el alamacenamiento en bases de datos de alta disponibilidad en postgresql.



Img. 2: Arquitectura del Ecosistema de One Vision y Microservicios

- **Capa de Acceso:** SSL mediante NGINX Proxy y balanceo mediante HAProxy (VIP 172.23.25.11).
- **Orquestación:** Cluster K8s dedicado para la instancia de One Vision Clinico y Administrativo y microservicios necesarios para el correcto funcionamiento de la plataforma
- **Capa de Datos:** Cluster Patroni de alta disponibilidad para alamacenar y consultar los datos e información generada por los usuarios, ademas se usa Redis Sentinel para caché de sesiones de la plataforma One Vision.
- **Herramientas de Soporte:** Monitoreo centralizado con Prometheus y Grafana además de calidad con SonarQube como también repositorio de artefatos K8s con Distr.

5. Análisis FODA

Este diagnóstico estratégico integral surge de la necesidad de evaluar nuestra situación competitiva actual. A través del análisis de factores internos y externos, buscamos potenciar nuestras fortalezas, mitigar debilidades y, fundamentalmente, anticipar riesgos latentes que podrían comprometer la continuidad de la operación.

FORTALEZAS (Internas)	OPORTUNIDADES (Externas)
1. **Alta Disponibilidad en Capas:** Diseño redundante en Firewall, Hyper-V, K8s y BD (Patroni). 2. **Protección Eléctrica:** UPS + Grupo Electrógeno con transferencia automática. 3. **Sistemas Modernos:** Uso de contenedores y microservicios facilita la recuperación y despliegue. 4. **Personal Capacitado:** Equipo OITE con dominio de tecnologías complejas (K8s/Linux). 5. **Repotenciación de Infraestructura:** Existen planes de adquisición de Tecnología a corto plazo	1. **Nube de Claro:** Posibilidad de externalizar backups críticos fuera de la zona sísmica. 2. **Optimización de Recursos:** Reducción de consumo mediante refactorización de VMs a contenedores. 3. **Virtualización de Escritorios:** Para reducir la carga administrativa local.

DEBILIDADES (Internas)	AMENAZAS (Externas)
1. **Saturación Crítica de RAM:** 70% de ocupación por nodo. Si un nodo falla, el restante **no soporta el 140% de carga**, provocando caída total. 2. **SPOF en Almacenamiento:** La SAN es un punto único de fallo; no hay réplica de SAN. 3. **Ubicación Única:** No existe un sitio de contingencia (DR Site) físico. 4. **Sobrecarga de vCPU:** Ratio de 190% puede degradar el rendimiento en picos de demanda.	1. **Desastres Naturales:** Sismos severos en Cajamarca que afecten la estructura física. 2. **Ciberataques:** Ransomware dirigido a entornos de salud (sector crítico). 3. **Fallas de Cadena de Suministro:** Demora en reposición de discos SAS/SSD para la SAN o repuestos HP.

6. Identificación de Riesgos, Matriz y BIA

6.1. Matriz de Riesgos

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO	
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**ZONA DE RIESGO**	**ACCIONES PREVENTIVAS**	**ACCIONES DE CONTINGENCIA**
Colapso Hyper-V por falta de RAM	Fallo de un nodo físico. El nodo vivo no soporta el 140% de carga (70%+70%).	Caída total de los sistemas One Vision y Superset.	**BAJO**	**ALTO**	**INACEPTABLE**	Rightsizing de VMs	Ejecución de Load Shedding: apagado automático de VMs no críticas
Pérdida de Acceso a SAN (Storage)	Falla en controladoras Fibre Channel o múltiples discos.	Indisponibilidad de todas las VMs y pérdida de persistencia.	**BAJO**	**ALTO**	**IMPORTANTE**	Monitoreo predictivo de controladoras y discos; mantenimiento de switches FC.	Restauración de servicios críticos desde la Nube o Cintas en discos locales de servidores (DAS).
Corrupción de BD (Split-Brain Patroni)	Fallo de red entre nodos que genera dos "líderes" escribiendo.	Inconsistencia de datos clínicos e historias corruptas.	**MEDIO**	**ALTO**	**IMPORTANTE**	Configuración de Watchdog y monitoreo estricto de latencia en el cluster etcd.	Promoción manual de nodo mediante patronictl y restauración PITR con Barman.
Ataque de Ransomware	Vulnerabilidades en Windows 2016 o brechas en microservicios Laravel.	Encriptación de datos y extorsión institucional.	**MEDIO**	**ALTO**	**INACEPTABLE**	Escaneos DAST con OWASP ZAP y segmentación estricta de VLANs.	Aislamiento de red y restauración desde backups inmutables en la Nube.
Fallo de Climatización	Avería de los aires de precisión en Jr. Mario Urteaga.	Apagado térmico preventivo de los servidores HP.	**BAJO**	**MEDIO**	**MODERADO**	Mantenimiento preventivo trimestral del aire de precisión en el datacenter	Ventilación forzada de emergencia y apagado preventivo de equipos de desarrollo.
Saturación del Enlace de Internet	Consumo excesivo en el enlace de 200Mbps por backups o ataques.	Lentitud extrema en el acceso externo a One Vision.	**MEDIO**	**MEDIO**	**MODERADO**	Implementación de QoS en Fortinet para priorizar tráfico de las VLANs de aplicaciones.	Conmutación manual o automática a la línea de backup de internet.
Fallo de Sincronización etcd	Latencia de red o saturación de CPU en nodos Master de K8s.	Inestabilidad del cluster Kubernetes; los pods no despliegan.	**BAJO**	**ALTO**	**IMPORTANTE**	Monitoreo de latencia de escritura en disco para los nodos del plano de control.	Restauración de snapshots de etcd y reinicio de servicios de orquestación.

Desincronización de Redis Sentinel	Fallo de quórum entre las instancias de Redis.	Fallas en el manejo de sesiones y caché de One Vision.	**BAJO**	**MEDIO**	**TOLERABLE**	Pruebas de quórum (mínimo 3 nodos) en la VLAN de aplicaciones.	Reseteo manual de estados y reconfiguración de punteros de caché en microservicios.
Error en Despliegue (Deuda Técnica)	Código con errores lógicos o deuda técnica sin probar.	Error 500 en la plataforma One Vision.	**MEDIO**	**MEDIO**	**MODERADO**	Análisis de código con SonarQube e integración de pruebas en Staging.	Rollback inmediato a la versión anterior mediante GitLab/Git.
Pérdida de Configuración de Firewalls	Error humano en la consola de Fortinet, fallo de hardware o actualizaciones de firmware fallidas	Incomunicación total de las VLANs.	**BAJO**	**ALTO**	**IMPORTANTE**	Backups automáticos de configuración tras cada cambio en el Fortinet.	Restauración inmediata del archivo de configuración desde repositorio de backups
Fallo de Energía (UPS/Grupo)	Agotamiento de baterías de UPS, Fallo mecánico del grupo electrógeno o Desabastecimiento de combustible en emergencias prolongadas		**BAJO**	**ALTO**	**IMPORTANTE**	Pruebas mensuales de arranque del grupo electrógeno y transferencia automática. Monitoreo preventivo del estado de baterías del UPS.	Apagado ordenado de sistemas si el tiempo de autonomía del UPS es menor al 20%.

6.2. Análisis de Impacto al Negocio (BIA)

El Análisis de Impacto al Negocio permite cuantificar la criticidad de los procesos institucionales y determinar los umbrales de tolerancia ante una interrupción. En la DIRESA Cajamarca, la infraestructura tecnológica es el soporte directo de la continuidad asistencial; por ello, la degradación de los servicios digitales se traduce inmediatamente en un riesgo para la gestión de la salud regional.

a) Evaluación de Procesos Críticos: Ecosistema "One Vision"

La plataforma **One Vision**, en sus versiones Clínica y Administrativa, se clasifica como un **Servicio de Misión Crítica**. Su indisponibilidad genera un efecto dominó que paraliza la cadena de valor de las Instituciones Prestadoras de Servicios de Salud (IPRES):

- **Impacto Asistencial:** La caída del módulo clínico impide el acceso a historias clínicas electrónicas, programación de citas y registro de atenciones, forzando un retorno a procesos manuales que incrementan el error humano y los tiempos de espera del paciente.
- **Impacto Administrativo:** La interrupción del flujo administrativo detiene la gestión de suministros, farmacia y procesos de referencia/contra-referencia, afectando la logística sanitaria de la región.
- **Umbrales de Tolerancia:** Se ha definido un **Tiempo Máximo Tolerable de Disrupción (MTPD)** de **1 hora**. Superar este umbral implica una afectación crítica de la capacidad operativa institucional.

b) Evaluación de Procesos de Soporte: Tableros de Indicadores

Los sistemas de inteligencia de negocios basados en Apache Superset se clasifican como Servicios de Prioridad Alta, pero no inmediata. Su rol es vital para la toma de decisiones estratégicas de la alta dirección y la vigilancia epidemiológica.

- **Impacto en la Gestión:** La indisponibilidad de los tableros impide la visualización de indicadores en tiempo real.
- **Umbrales de Tolerancia:** Dado que estos procesos permiten una gestión asíncrona, se ha establecido un Tiempo Objetivo de Recuperación (RTO) de 2 horas. Durante este periodo, la OITE debe priorizar el restablecimiento de las bases de datos transaccionales antes que la capa de visualización.

c) Matriz de Objetivos de Continuidad (RTO / RPO)

Para garantizar que la recuperación sea coherente con las necesidades del negocio, se establecen los siguientes parámetros técnicos de cumplimiento obligatorio:

Servicio Crítico	Criticidad	RTO (Tiempo de Recuperación)	RPO (Punto de Recuperación)	Impacto de la Falla
One Vision Clínico	**Muy Alta**	< 60 Minutos	< 15 Minutos (PITR)	Paralización de la atención médica en las IPRES.
One Vision Administrativo	**Alta**	< 60 Minutos	< 15 Minutos	Detención de procesos logísticos y de farmacia.
Bases de Datos (Patroni)	**Crítica**	< 30 Minutos	Próximo a cero (0)	Colapso total de todas las aplicaciones dependientes.
Indicadores (Superset)	**Media**	< 120 Minutos	< 24 Horas	Incertidumbre estratégica por falta de indicadores
Gestión Documental	**Baja**	< 4 Horas	< 24 Horas	Retraso en trámites administrativos internos.

7. Estrategia de Protección de Datos

La integridad de la información es el activo más crítico de la DIRESA, especialmente considerando que los sistemas "One Vision" y los Tableros de Indicadores gestionan datos sensibles de salud regional. Esta estrategia define los mecanismos técnicos para garantizar un Punto de Recuperación (RPO) cercano a cero y la disponibilidad de la información ante fallos lógicos o físicos. El enfoque aquí es la resiliencia del dato en reposo y en tránsito, asegurando que existan copias íntegras y seguras antes de cualquier incidente

7.1. Arquitectura de Respaldo para Bases de Datos (PostgreSQL)

La protección de las bases de datos transaccionales y de indicadores se centraliza en un servidor dedicado que ejecuta Barman (Backup and Recovery Manager). Este sistema está diseñado para gestionar el ciclo de vida de los respaldos de los clusters de Patroni, eliminando el riesgo de pérdida de transacciones.

a) **Sincronización mediante WAL Archiving:** Se establece un flujo constante de registros de transacciones (Write-Ahead Logs) desde el cluster Patroni hacia el servidor de backup. Esto garantiza un **RPO (Objetivo de Punto de Recuperación)** de apenas segundos
b) **Gestión de Backups "Full" y "Incrementales":** Se define una política de backups de base completa semanal, complementada con la retención de logs diarios para permitir la reconstrucción de la base de datos ante fallos de integridad.
c) **Seguridad del Repositorio:** El acceso al servidor Barman está restringido exclusivamente al equipo de infraestructura de la OITE, utilizando llaves SSH cifradas para la comunicación con los nodos de base de datos.

7.2. Estrategia de Persistencia en Entornos Contenedorizados

Para la capa de aplicaciones (One Vision, Superset), se implementa Velero como orquestador de backups de infraestructura y datos.

a) **Respaldo de la Capa de Control:** Se asegura la copia de seguridad de los metadatos dado que Velero captura todos los objetos de la API de Kubernetes, incluyendo Namespaces, ConfigMaps, Secrets, despliegues de servicios críticos como One Vision y Superset y volúmenes lógicos del cluster.
b) **Lógica de Backups por Namespace:** La estrategia segmenta los respaldos por criticidad, priorizando los espacios de nombres produccion-clinica y estadistica-bi.
c) Integridad de Volúmenes Persistentes (PV): Se utiliza tecnología de *snapshots* para capturar el estado exacto de los discos virtuales donde residen las configuraciones de las aplicaciones.

7.3. Normativa de Retención y Almacenamiento (Regla 3-2-1)

Para garantizar la resiliencia ante desastres de gran magnitud (sismos o incendios en el Data Center), la DIRESA se adhiere al estándar internacional de protección 3-2-1 para mitigar riesgos de desastres físicos.

1. **Tres Copias de Seguridad:** Se mantienen al menos tres instancias de cada dato crítico (Producción, Backup Local y Backup Externo en Nube).

2. **Dos Medios Diferentes:** Los respaldos deben residir en plataformas tecnológicas distintas, combinando almacenamiento en disco de alta velocidad para recuperaciones rápidas y almacenamiento en cinta o sistemas inmutables para preservación.

3. **Una Copia Fuera de Sede (Cloud):** Como medida de contingencia geográfica, se sincronizará una copia de los respaldos críticos hacia el

repositorio en la **Nube de Claro**, actuando como sitio de contingencia externa ante la inhabilitación física del local central.

7.4. Matriz de Retención y Frecuencia de Respaldos

Sistema / Capa	Herramienta	Frecuencia	Retención	Almacenamiento
Bases de Datos (One Vision)	Barman	Continuo (WAL)	30 días	Local + Claro Cloud
Bases de Datos (Superset)	Barman	Diario (Full)	15 días	Local
Configuración K8s	Velero	Cada 4 horas	7 días	Almacenamiento Interno
Máquinas Virtuales (Hyper-V)	Snapshots	Semanal	2 versiones	SAN Storage

8. Estrategia de Continuidad Operativa

La Estrategia de Continuidad Operativa de la DIRESA Cajamarca define el conjunto de procedimientos técnicos y administrativos necesarios para restablecer los servicios críticos tras una interrupción. El enfoque principal es la resiliencia de los sistemas One Vision (Clínico y Administrativo) y los Tableros de Indicadores Estadísticos (Superset), los cuales son de gran importancia.

8.1. Protocolo de Gestión de Carga Crítica (Load Shedding)

Dada la restricción técnica de memoria RAM en los nodos del cluster (uso actual ~70%), la caída de un nodo físico (SPOF parcial) disparará una saturación inmediata en el nodo superviviente. Se establece el siguiente procedimiento de "Apagado Selectivo" para preservar los sistemas críticos

a) Niveles de Alerta y Umbrales de Memoria

1. **Nivel Verde (Operación Normal):** Uso de RAM < 75%. No se requieren acciones.

2. **Nivel Amarillo (Precaución):** Uso de RAM entre 76% - 89%. Monitoreo intensivo de procesos "zombie".
3. **Nivel Rojo (Pánico de RAM):** Uso de RAM > 90%. Activación inmediata del Protocolo de Apagado.

b) Matriz de Ejecución de Apagado de Servicios

En caso de Nivel Rojo, el administrador de infraestructura procederá al apagado manual o mediante scripts de los siguientes servicios en orden de prioridad baja a alta

Orden	Servicio/Maquina Virtual	Comando de Suspensión	Impacto
1°	MV-GIT01	Stop-VM -VMName " MV-GIT01"	Suspensión del Servicio git
2°	VM-APPSDEV	Stop-VM -VMName " VM-APPSDEV "	Suspensión del entorno de desarrollo del área de informática
3°	VM-CONTREG	Stop-VM -VMName " VM- CONTREG "	Suspensión de actualización de artefacto para Kubernetes
4°	VM-KEYCLOAKDEV	Stop-VM -VMName " VM- KEYCLOAKDEV "	Suspensión del servicio de autenticacion oauth2 en entorno de desarrollo
5°	VM-SONARQUBE	Stop-VM -VMName " VM- SONARQUBE "	Suspensión del servicio de escaneo de código estatico
6°	VM-SRVMCPTEST01	Stop-VM -VMName " VM- SRVMCPTEST01"	Suspension del entorno de dearrolo para el MAD
7°	VM-SRVTAIGA	Stop-VM -VMName " VM- SRVTAIGA "	Suspension del servicio de gestion de historias de usuario
8°	VM-SUPERSETDEV	Stop-VM -VMName " VM- SUPERSETDEV "	Suspensión del entorno de desarrollo superset
9°	VM-SUPERSETSRC	Stop-VM -VMName " VM- SUPERSETSRC "	Suspensión del entorno de desarrollo superset con codigo fuente
10°	VM-USERSDB	Stop-VM -VMName " VM- USERSDB "	Suspensión del servicio de base de datos para usuarios externos

Orden	Servicio/Maquina Virtual	Comando de Suspensión	Impacto
11°	VM-SW04	Stop-VM -VMName " VM- SW04"	Suspensión servicio Git
12°	VM-NIFI	Stop-VM -VMName " VM- NIFI "	Suspensión del proceso ETL

8.2. Procedimientos Operativos de Recuperación (DRP)

Esta sección detalla los pasos técnicos para la restauración de servicios tras una pérdida confirmada de datos o caída del sistema.

a) Restauración de la Base de Datos

Ante una corrupción lógica o pérdida del cluster de datos, el DBA de la OITE seguirá estos pasos:

1. **Aislamiento del Cluster:** Se debe proceder a pausar la gestión del cluster para evitar que Patroni intente auto-corregirse durante la restauración, se debe pausar mediante el comando:
   `patronictl -c /etc/patroni/patroni.yml pause`
   Esto evita conflictos de escritura durante la recuperación.
2. **Identificación del Punto de Recuperación:** Consultar en el servidor Barman la lista de backups disponibles:
   `barman list-backup [nombre_servidor]`
3. **Ejecución de la Restauración (PITR):** La ejecución de la recuperación se realiza mediante el comando:
   `barman recover --target-time "YYYY-MM-DD HH:MM:SS" --remote-ssh-command "ssh postgres@SERVIDOR_POSTGRES" [server] [ID_del_backup] /var/lib/pgsql/17/data/`
4. **Reactivación de Patroni:** Una vez recuperado el flujo de datos, se reactiva el servicio iniciando el nodo principal y posteriormente sus réplicas.
   `patronictl -c /etc/patroni/patroni.yml resume`
   `patronictl -c /etc/patroni/patroni.yml list`

b) Restauración del Orquestador y Aplicaciones (Velero)

Si los objetos del cluster (Deployments, Services, ConfigMaps) han sido borrados o alterados:

1. **Verificación de Inventario:** Listar los respaldos almacenados en el repositorio:
   `velero backup get`
2. **Restauración Total o Parcial:** Ejecución de la restauración filtrando por el namespace afectado:
   `velero restore create --from-backup [BACKUP_NAME] --include-namespaces [NAME_SPACE].`
3. **Validación de Persistencia:** Comprobar que los columenes se han montado correctamente
   `kubectl get pvc -n [NAME_SPACE]`
   O listamos todos los volumenes
   `kubectl get pvc -A`

8.3. Plan de Comunicación y Árbol de Llamadas

Ante un desastre, se activa el siguiente flujo de comunicación:

1. **Detección:** El sistema de alertas (Alertmanager) notifica al Especialista de Infraestructura.
2. **Evaluación (T+5 min):** El especialista determina si el incidente es corregible en < 15 min. Si no, notifica al Director de OITE.
3. **Declaración de Crisis (T+15 min):** El Director de OITE informa a la Dirección Regional de Salud sobre la posible interrupción del servicio.
4. **Resolución y Cierre:** Una vez restaurado el servicio, se emite un "Informe Post-Mortem" detallando la causa raíz y las medidas adoptadas.

8.4.Contingencia de Infraestructura Física (Hyper-V)

Para las 70 máquinas virtuales alojadas en Hyper-V que no forman parte del cluster de contenedores:

1. **Reversión de Snapshots:** Ante una actualización fallida de Windows Server o corrupción del sistema operativo, se procederá a la reversión al snapshot más reciente (máximo 7 días de antigüedad).
2. **Procedimiento:**
    1) Apagar VM.
    2) Aplicar Punto de Control.
    3) Validar consistencia de red e IP estática.

9. Sostenibilidad y Mantenimiento

La sostenibilidad de la plataforma tecnológica de la DIRESA Cajamarca no depende únicamente de la configuración inicial, sino de un modelo de gestión proactiva que evolucione con las necesidades institucionales. Este capítulo define los pilares de visibilidad operativa, seguridad proactiva y aseguramiento de la calidad, estableciendo los estándares que el equipo de la OITE deberá seguir para garantizar que los ecosistemas se mantenga operativos, seguros y eficientes a largo plazo.

9.1. Marco de Monitoreo

Para garantizar la estabilidad del cluster Kubernetes y la capa de persistencia de datos (PostgreSQL), se utiliza un stack de monitoreo de estándar industrial basado en Prometheus, Grafana y Alertmanager. Este sistema permite pasar de una administración reactiva a una basada en datos en tiempo real.

a) Recolección de Métricas y Dashboards de Control

1. **Monitoreo de Infraestructura (Node Exporter):** Supervisa la salud de los servidores físicos y máquinas virtuales, con énfasis en

el uso de CPU, la latencia de escritura en los discos SAS de la SAN y el rendimiento de las interfaces de red de 10GbE.

2. **Métricas de Orquestación (Kube-state-metrics):** Provee visibilidad sobre el ciclo de vida de los contenedores, permitiendo identificar pods en estado de error, reinicios inesperados o saturación de recursos en los microservicios de "One Vision".
3. **Visualización en Grafana:** Se han diseñado tableros de control específicos que centralizan la telemetría. El dashboard de "Capacidad Crítica" debe ser el punto de referencia diario, mostrando el consumo agregado de RAM para anticipar la activación de protocolos de contingencia.

b) Protocolo de Notificaciones y Alertas Críticas

El sistema **Alertmanager** actúa como el primer respondiente técnico, clasificando las alertas según su severidad:

1. **Severidad Crítica (Pánico de RAM >90%):** Dispara una notificación inmediata que exige la intervención del administrador para evaluar el desalojo de servicios no esenciales.
2. **Severidad Alta (Falla de Nodo Patroni):** Indica una conmutación de base de datos (failover). Requiere la revisión del log para asegurar que la alta disponibilidad se mantiene activa.
3. **Severidad Advertencia (Almacenamiento >90%):** Alerta preventiva para la gestión de volúmenes persistentes antes de que afecten la capacidad de escritura de las bases de datos.

9.2. Estándar de Seguridad Dinámica (Hoja de Ruta DAST)

Como parte de la estrategia de seguridad a largo plazo, la DIRESA adopta la metodología de Análisis Dinámico de Seguridad (DAST). Se establece el uso de OWASP ZAP como la herramienta estándar para evaluar la resiliencia de las aplicaciones web frente a ciberataques.

a) **Requerimiento de Escaneo Mensual:** Se define como política institucional la ejecución de un escaneo completo de vulnerabilidades cada 30 días sobre las URLs de producción.

b) **Gestión de Vulnerabilidades:** Los hallazgos derivados de OWASP ZAP deberán integrarse en un registro de riesgos. Aquellos catalogados como "Críticos" (Inyección SQL, Broken Authentication) deben ser remediados en un plazo no mayor a 72 horas.

c) **Actualización de Reglas:** La OITE será responsable de mantener la herramienta actualizada con el último "Top 10 de OWASP" para asegurar que las nuevas amenazas sean detectadas oportunamente.

9.3. Aseguramiento de la Calidad y Remediación de Deuda Técnica

La auditoría del sistema ha identificado una Deuda Técnica acumulada de 193 días y un Coverage (cobertura de pruebas) del 0.0%. Este escenario representa un riesgo crítico para la sostenibilidad, ya que cualquier actualización podría generar fallos en cascada.

a) **Necesidad del Perfil QA:** Se establece como requisito estratégico la formalización de una función de Aseguramiento de la Calidad (QA) dentro de la OITE. Este rol será el encargado de diseñar la malla de pruebas automáticas que hoy el sistema carece.

b) **Estrategia de Remediación:** La sostenibilidad requiere que el equipo de desarrollo priorice la resolución de los "Bugs" y "Vulnerabilidades" detectados en SonarQube, utilizando los reportes de calidad como guía obligatoria para el paso a producción de cualquier mejora.

9.4. Gestión del Conocimiento y Documentación (Estándar Wiki)

Para mitigar el riesgo de dependencia técnica y asegurar la continuidad ante la rotación de personal, se establece la necesidad de un Repositorio Centralizado de Conocimiento (Wiki Técnica).

a) **Contenido Obligatorio:** La Wiki deberá alojar de forma digitalizada todos los Procedimientos Operativos Estándar (POEs) detallados en

este plan, los diagramas de arquitectura actualizados y el inventario de máquinas virtuales.

b) **Actualización de la "Línea Base":** Cualquier cambio estructural en el cluster o en la base de datos debe ser documentado en la Wiki en un plazo máximo de 48 horas, garantizando que el conocimiento permanezca en la institución y no en personas aisladas.

10. Inventario Técnico de Activos Críticos

El inventario de activos constituye la "Línea Base" de la infraestructura. Cualquier cambio en estos activos debe reflejar una actualización en la versión de este plan.

10.1. Infraestructura de Servidores Físicos (Capa de Cómputo)

Estos son los "Hosts" físicos que sostienen toda la virtualización de la DIRESA.

ID Activo	Equipo	Especificaciones Técnicas	Función	Estado
SRV-01	HP ProLiant 380 Gen10	2x Intel Xeon Gold, 512GB RAM	Nodo 01 Hyper-V (Cluster)	Operativo
SRV-02	HP ProLiant 380 Gen10	2x Intel Xeon Gold, 512GB RAM	Nodo 02 Hyper-V (Cluster)	Operativo
SAN-01	HPE MSA 2050 Storage	65TB Útiles (RAID 10) - Conectividad FC	Almacenamiento Centralizado	Operativo
SW-CORE	Cisco Catalyst 3850	24 Puertos 10GbE	Backbone de Red	Operativo

10.2. Inventario de Máquinas Virtuales (Capa de Virtualización)

Se gestionan aproximadamente 70 Máquinas Virtuales (VMs). A continuación, se detallan las más críticas para la continuidad:

Nombre VM	vCPU	RAM (GB)	Dirección IP	Sistema Operativo	Descripción / Función
VM-K8SEST[01-06]	24	24	172.23.22.12-17	Rocky Linux 10.1	Cluster Kubernetes (3 Master / 3 Workers)
VM-K8SINF[01-06]	24	24	172.23.22.29-34	Rocky Linux 10.1	Cluster Kubernetes (3 Master / 3 Workers)
VM-ETCD[01-03]	12	12	172.23.22.2-4	Rocky Linux 10.1	Cluster ETCD para Postgres Patroni (Estadística)
VM-ETCDOV[01-03]	12	12	172.23.22.23-25	Rocky Linux 10.1	Cluster ETCD para Postgres Patroni (One Vision)
VM-HAPWEB[01-02]	24	24	172.23.25.6-7	Rocky Linux 10.1	Balanceadores HA Proxy para Cluster Kubernetes
VM-DC01 / DC02	4	4	172.18.20.1-2	Windows Server 2016	Controladores de Dominio y Servidores DNS
VM-DHCP	2	3.0	172.18.20.6	Windows Server 2016	Servidor de Resolución de Direcciones IP
VM-NPM	2	4.0	172.23.25.3	Rocky Linux 10.1	Nginx Proxy Manager
VM-WAF	2	6	172.23.25.5	Rocky Linux 10.1	Firewall de Aplicaciones (SafeLine)
VM-OVDB[01-02]	4	12	172.23.23.11-12	Rocky Linux 10.1	Cluster Postgres-Patroni para One Vision
VM-INDDB-N0[1-2]	8	16	172.23.23.4-5	Rocky Linux 10.1	Nodos Cluster Postgres (Estadística)
VM-PROCDB	8	32	172.23.23.3	Rocky Linux 10.1	Postgres para Procesamiento de Indicadores
VM-REPODB	4	16	172.23.23.2	Rocky Linux 10.1	Postgres Repositorio Central

Nombre VM	vCPU	RAM (GB)	Dirección IP	Sistema Operativo	Descripción / Función
VM-USERSDB	4	12	172.23.24.2	Rocky Linux 10.1	Postgres para Usuarios Externos
VM-REDIS[01-03]	2	4	172.23.22.8-10	Rocky Linux 10.1	Cluster Redis Sentinel (Soporte Superset)
VM-HAPDB-01	2	4	172.23.22.6	Rocky Linux 10.1	Balanceador HA Proxy para Base de Datos
VM-TDDB	14	50	172.18.20.16	Windows Server 2016	Servidor DB One Vision (Legacy/Soporte)