

MISO

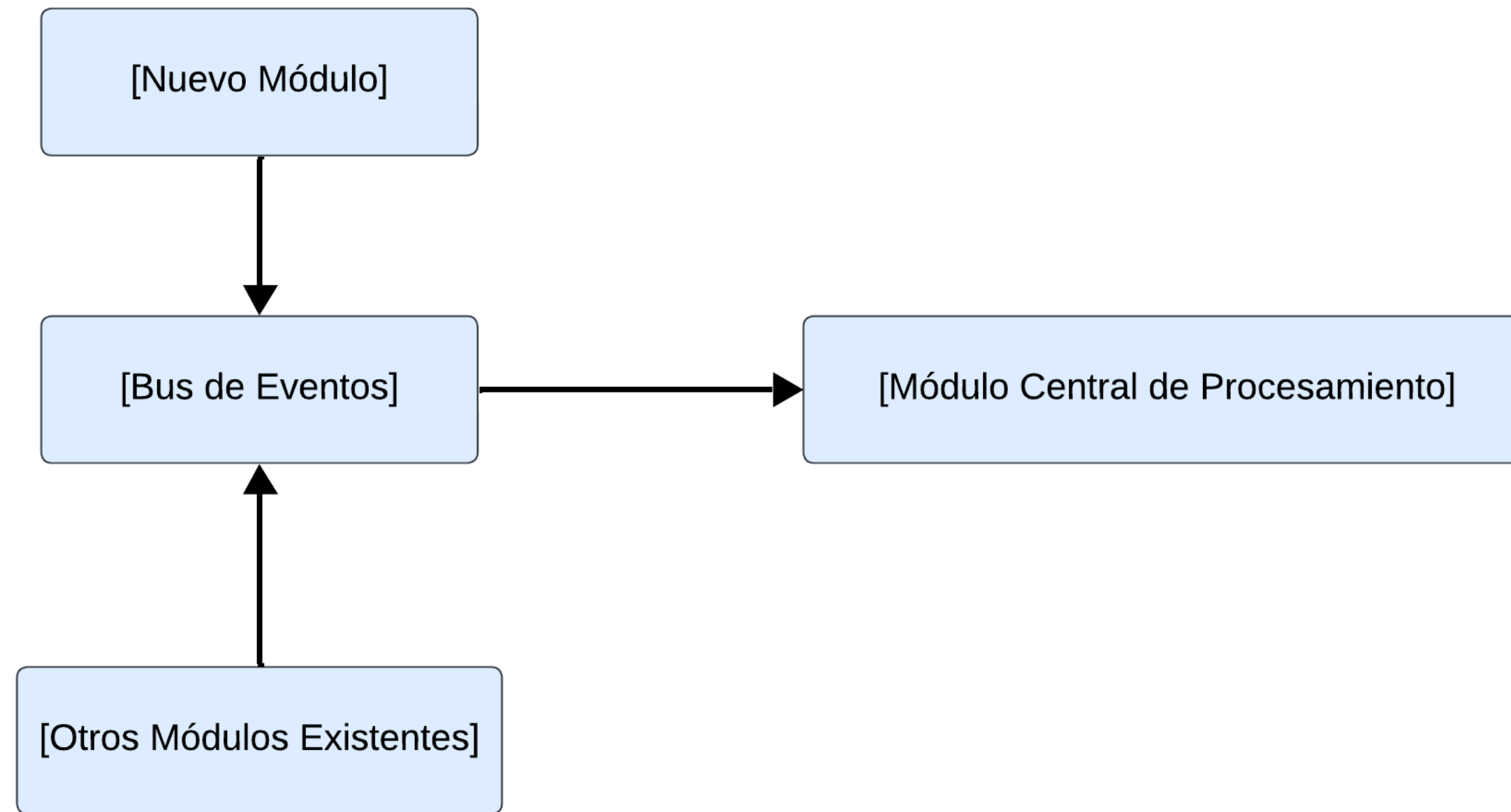
Maestría en Ingeniería de Software

Entrega 3: Diseño de experimentación

Atributo de calidad 1: Modularidad

Escenario de calidad: Integración Dinámica de Nuevos Módulos de Procesamiento			
Escenario #: 1	Integración Dinámica de Nuevos Módulos de Procesamiento		
Fuente	Propuesta de un nuevo algoritmo de procesamiento de imágenes por parte del equipo de I+D.		
Estímulo	Se recibe una solicitud para integrar un nuevo módulo (por ejemplo, un algoritmo de mejora de contraste) en el pipeline de procesamiento.		
Ambiente	Ambiente de pruebas con simulación de tráfico elevado		
Artefacto	El módulo específico de procesamiento que se integrará.		
Respuesta	El sistema debe permitir la incorporación del nuevo módulo sin afectar los módulos existentes, integrándose de forma aislada.		
Medida de la respuesta	Tiempo de integración (idealmente menor a 30 minutos) y validación exitosa mediante pruebas de regresión (100% de tests aprobados).		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
Implementación de una arquitectura de microservicios basada en eventos, donde cada módulo expone un contrato de eventos y se comunica a través de un bus de eventos.Puntos de sensibilidad: Definición y mantenimiento de c	Definición y mantenimiento de contratos (interfaces) entre módulos y la correcta orquestación de eventos.	Mayor flexibilidad e independencia en el desarrollo frente a una complejidad añadida en la gestión del bus de eventos.	Incompatibilidades en la definición de eventos y la posibilidad de que la integración genere efectos colaterales no previstos en módulos ya existentes.
Justificación	La capacidad de integrar nuevos módulos sin alterar el sistema global refuerza la modularidad y facilita la innovación continua en el procesamiento de imágenes.		
Diagrama de arquitectura			

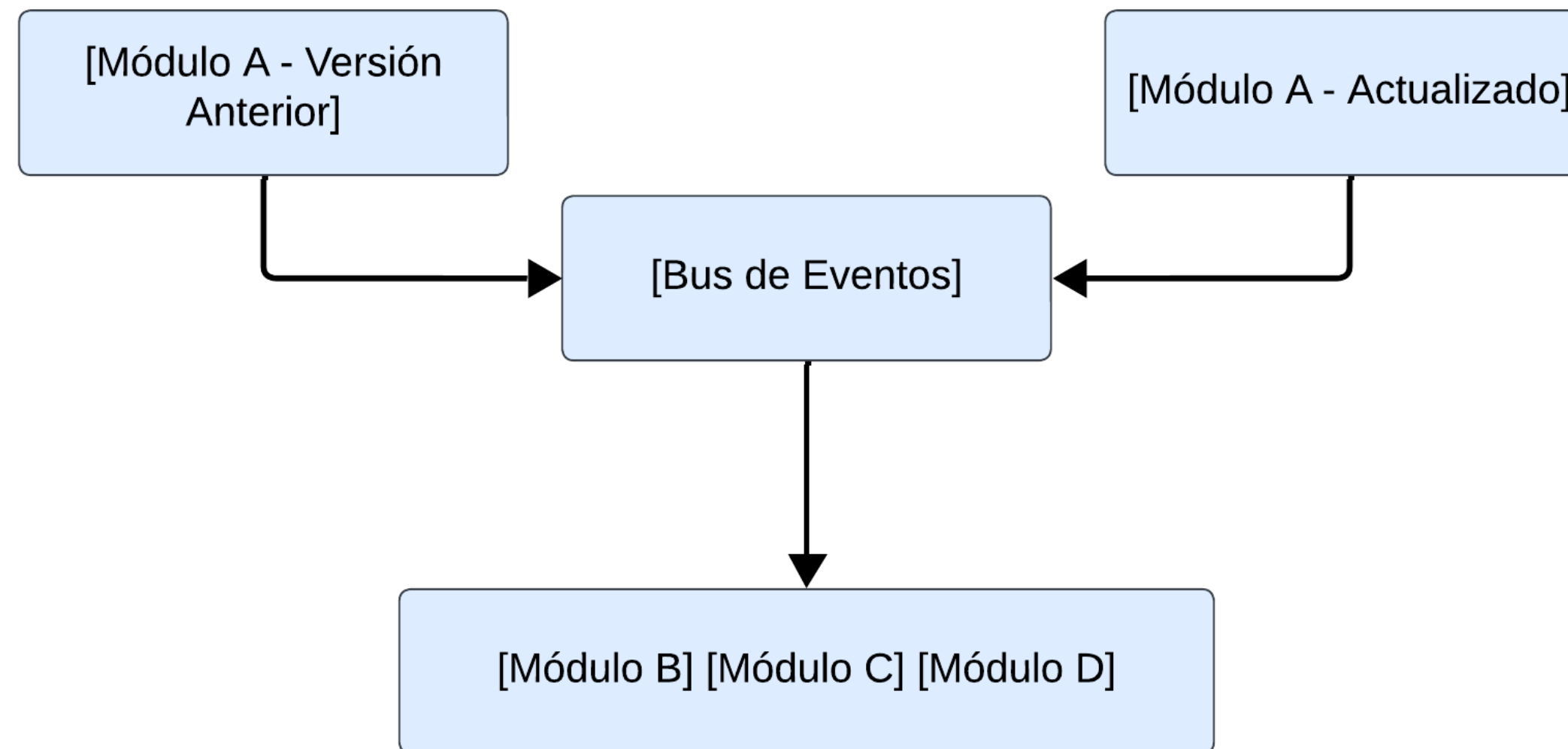
Diagrama de arquitectura



Atributo de calidad 1: Modularidad

Escenario de calidad: Actualización y Mantenimiento Aislado de Módulos			
Escenario #: 2	Actualización y Mantenimiento Aislado de Módulos		
Fuente	Detección de un error o necesidad de mejora en un módulo existente		
Estímulo	Se identifica un fallo en el módulo de procesamiento de imágenes que requiere una actualización.		
Ambiente	Ambiente de staging/QA que replica condiciones de producción con datos históricos y tráfico simulado.		
Artefacto	El módulo afectado que debe ser actualizado.		
Respuesta	El módulo debe actualizarse de forma independiente sin interrumpir el funcionamiento de otros módulos, permitiendo un despliegue continuo.		
Medida de la respuesta	Tiempo de despliegue (< 15 minutos), sin interrupción en la disponibilidad del servicio		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
Uso de contenedores para cada módulo y despliegue continuo (CI/CD) que facilite la actualización aislada, acompañado de pruebas unitarias e integración.	Manejo de versiones y compatibilidad entre módulos durante la actualización.	Aislamiento y facilidad de mantenimiento frente a la duplicación de infraestructura o esfuerzo adicional en la orquestación de pruebas.	Posible inconsistencia en la comunicación intermodular si no se sincroniza correctamente la versión del API o del contrato de eventos.
Justificación	Permitir actualizaciones aisladas sin afectar la operación global garantiza que los errores se puedan corregir rápidamente y con bajo impacto en el servicio.		
Diagrama de arquitectura			

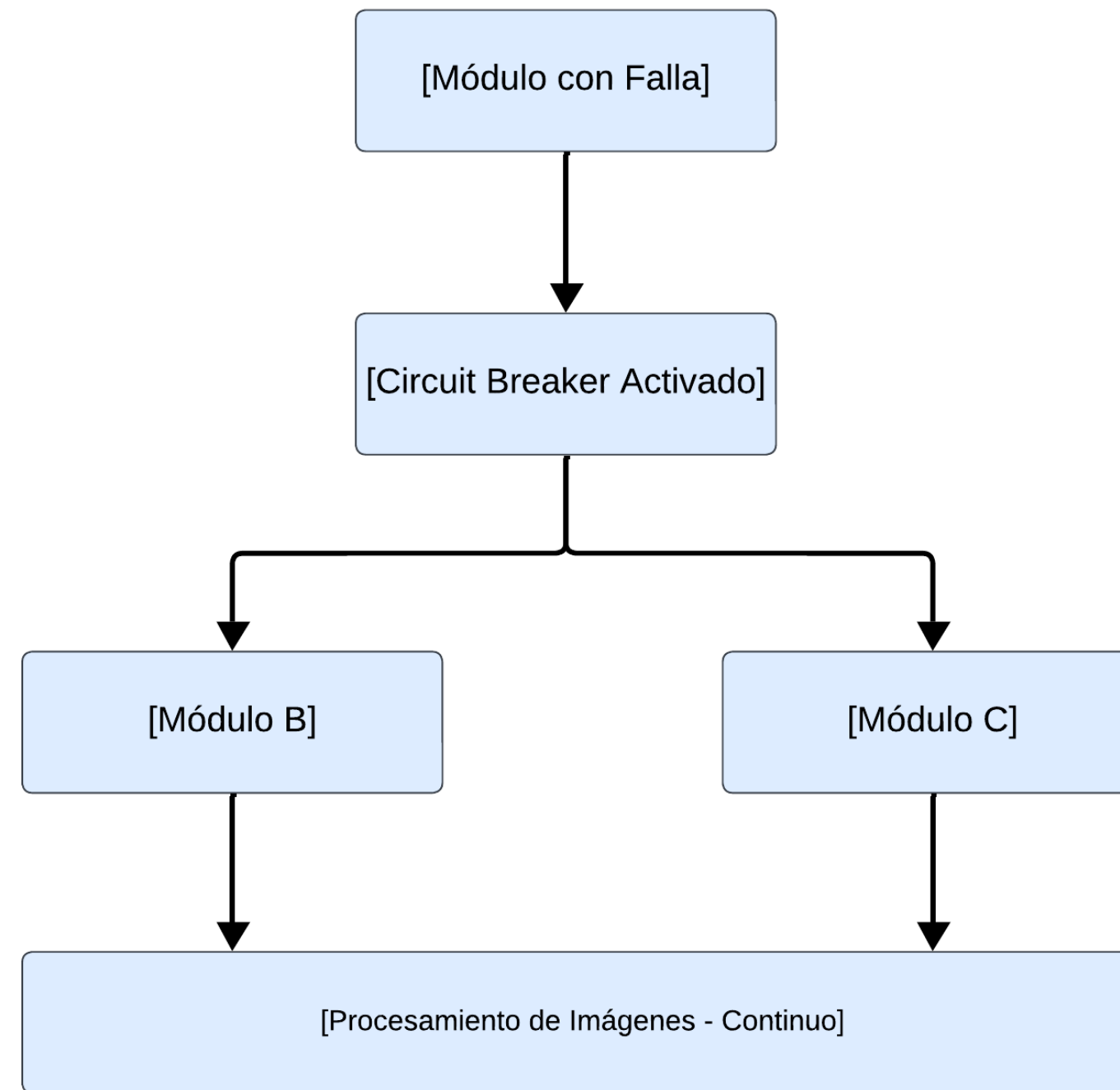
Diagrama de arquitectura



Atributo de calidad 1: Modularidad

Escenario de calidad: Aislamiento y Recuperación ante Fallos en Módulos			
Escenario #: 3	Aislamiento y Recuperación ante Fallos en Módulos		
Fuente	Fallo crítico en uno de los módulos durante la operación en producción.		
Estímulo	Un módulo (por ejemplo, el encargado de aplicar filtros de imagen) falla durante el procesamiento.		
Ambiente	Ambiente de producción simulado con tráfico realista y condiciones de carga normal.		
Artefacto	El módulo que ha presentado el fallo.		
Respuesta	El sistema debe aislar el módulo defectuoso, activar mecanismos de recuperación y continuar operando con los demás módulos		
Medida de la respuesta	Tiempo de detección y aislamiento del fallo (< 5 segundos) y porcentaje de imágenes procesadas correctamente (idealmente > 95%).		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
Implementación de patrones de resiliencia como circuit breakers y retry patterns, junto con monitoreo basado en eventos para detectar fallos.	Detección oportuna de errores y correcta propagación de eventos de fallo sin afectar la totalidad del sistema.	Mayor complejidad en la lógica de manejo de errores y potencial duplicación de lógica de recuperación en cada módulo.	Riesgo de fallo en la detección de errores, lo que podría llevar a un fallo en cascada y degradar el servicio.
Justificación	Asegurar que un fallo en un módulo no impacte a todo el sistema es vital para mantener la disponibilidad y confiabilidad del servicio.		
Diagrama de arquitectura			

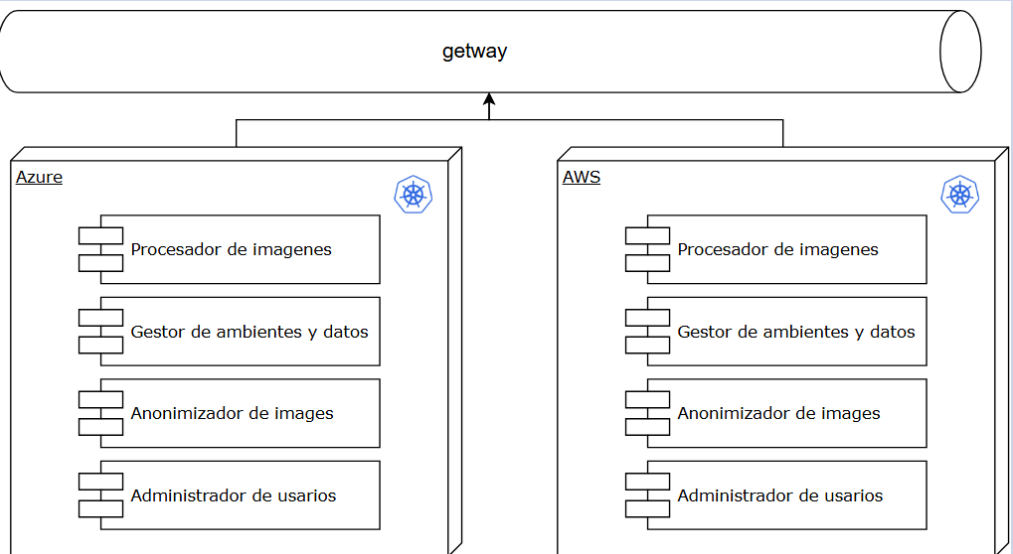
Diagrama de arquitectura



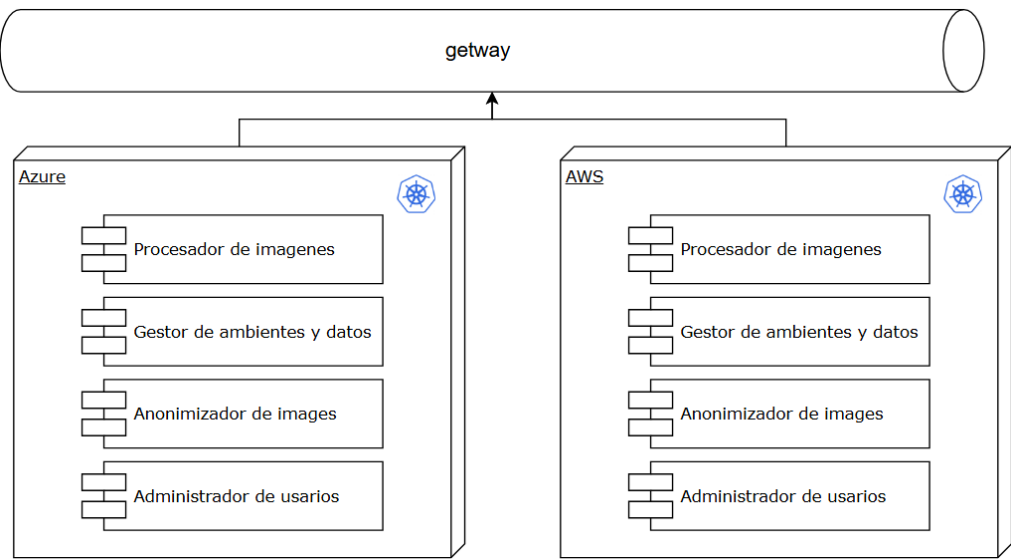
Atributo de calidad 2:Escalabilidad

Escenario de calidad: <Nombre escenario>			
Escenario #: 4	Recuperación ante Fallo de Escalado Automático		
Fuente	Sistema de monitoreo detecta un fallo en el mecanismo de escalado automático.		
Estímulo	El componente responsable del escalado automático no responde durante un aumento repentino de la carga.		
Ambiente	<ul style="list-style-type: none">Entorno de producción normal durante un evento de alta demanda inesperada.		
Artefacto	Módulo de escalado automático y gestion de ambientes y datos		
Respuesta	<ul style="list-style-type: none">El sistema debe activar un plan de contingencia que permita la redistribución de la carga hacia otros servicios disponibles para mantener la operatividad.		
Medida de la respuesta	Tiempo de activación del plan de contingencia inferior a 2 minutos; mantenimiento del tiempo de respuesta de los servicios críticos por debajo de 3 segundos durante la incidencia.		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
	Implementación de mecanismos de detección de fallos en el escalado automático y procedimientos manuales de escalado como respaldo.	Incremento en la complejidad operativa y necesidad de capacitación adicional para el personal en procedimientos manuales de escalado.	Dependencia en la rapidez y precisión de la intervención humana durante la contingencia.
Justificación	Contar con un plan de contingencia para fallos en el escalado automático asegura la continuidad del servicio y minimiza el impacto en la experiencia del usuario durante eventos de alta demanda.		
Diagrama de arquitectura			

Atributo de calidad 2: Escalabilidad

Escenario de calidad: <Nombre escenario>			
Escenario #: 5	Escalabilidad en Caso de Indisponibilidad de un Centro de Datos		
Fuente	Notificación de indisponibilidad de un centro de datos por parte del proveedor de infraestructura en la nube.		
Estímulo	Fallo crítico en el centro de datos principal que aloja la mayoría de los microservicios.		
Ambiente	Entorno de producción con usuarios activos en tiempo real.		
Artefacto	Servicios desplegados en kubernetes		
Respuesta	El sistema debe redistribuir automáticamente las cargas de trabajo hacia otros centros de datos disponibles, escalando los recursos según sea necesario para absorber la carga adicional.		
Medida de la respuesta	Tiempo de redistribución y escalado inferior a 5 minutos; mantenimiento de la disponibilidad del servicio en un 99.9% durante la incidencia.		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
	Diseño de una arquitectura multi-región con capacidad de balanceo de carga global y replicación de datos en tiempo real.	Costos adicionales asociados con la replicación de datos y recursos en múltiples regiones.	Posibles inconsistencias de datos si la replicación no se realiza correctamente o si hay latencias significativas entre regiones.
Justificación	Una arquitectura resiliente y distribuida geográficamente garantiza la continuidad del servicio incluso ante fallos catastróficos en un centro de datos, protegiendo la integridad del negocio y la confianza de los usuarios.		
Diagrama de arquitectura			

Atributo de calidad 2: Disponibilidad

Escenario de calidad: <Nombre escenario>			
Escenario #: 6	Escalabilidad en Respuesta a Picos de Carga Inesperados		
Fuente	Incremento inesperado de usuarios debido a un evento viral o una mención en medios de comunicación de alto alcance.		
Estímulo	El sistema experimenta un aumento repentino del 500% en el tráfico de usuarios en un período de 10 minutos.		
Ambiente	Entorno de producción durante una situación no planificada de alta demanda.		
Artefacto	Microservicios de autenticación, gestión de perfiles de usuario y procesamiento de contenido.		
Respuesta	El sistema debe detectar automáticamente el aumento abrupto en la carga y escalar los recursos necesarios para mantener el rendimiento y la disponibilidad, implementando mecanismos de balanceo de carga y distribución eficiente del tráfico.		
Medida de la respuesta	Tiempo de respuesta promedio de las solicitudes se mantiene por debajo de 2 segundos; el escalado de recursos se completa en menos de 3 minutos desde la detección del incremento de tráfico; cero caídas del servicio durante el evento.		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
	Implementación de un sistema de monitoreo en tiempo real que identifique rápidamente aumentos anómalos en el tráfico y active políticas de escalado automático.	Posible incremento en los costos operativos debido al aprovisionamiento dinámico de recursos adicionales durante picos de carga.	Riesgo de sobreaprovisionamiento si los picos de tráfico son de corta duración, lo que podría generar costos innecesarios.
Justificación	Preparar el sistema para manejar aumentos inesperados en la carga garantiza la continuidad del servicio y una experiencia de usuario consistente, incluso en situaciones imprevistas que podrían afectar la reputación y la confianza en la plataforma.		
Diagrama de arquitectura	 <p>El diagrama de arquitectura muestra un sistema distribuido con un gateway centralizado que se conecta a dos entornos de nube: Azure y AWS. Cada entorno contiene cuatro componentes de microservicios: Procesador de imágenes, Gestor de ambientes y datos, Anonimizador de imágenes y Administrador de usuarios. Los componentes están organizados en una estructura de árbol, con el gateway en la raíz y los microservicios como hijos. El diagrama ilustra la redundancia y la escalabilidad del sistema al distribuir los componentes en dos proveedores de nube.</p>		

Atributo de calidad 3: Seguridad

Escenario de calidad: <Nombre escenario>			
Escenario #: 7	Ataque de Inyección a la API		
Fuente	Atacante externo		
Estímulo	Envío de solicitudes maliciosas que incluyen payloads para inyección de código (SQL, scripts) a través de la API REST.		
Ambiente	Operación normal bajo ataque dirigido; pico de tráfico malicioso.		
Artefacto	Endpoints de la API REST de recepción de datos médicos.		
Respuesta	El sistema debe detectar y bloquear de forma inmediata las solicitudes maliciosas, rechazarlas, registrar el incidente y activar alertas en el sistema de monitoreo de seguridad.		
Medida de la respuesta	Bloqueo del 100% de solicitudes maliciosas detectadas; tiempo de respuesta inferior a 1 segundo; registro y notificación en el 100% de los casos.		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
	Vulnerabilidad a inyección si no se implementan validaciones robustas	Incorporar filtros y validaciones exhaustivas puede aumentar la latencia en picos de alto tráfico.	Exposición de datos sensibles y compromisos en la integridad del sistema si no se controla adecuadamente.
Justificación	La implementación de mecanismos de validación y filtrado en la entrada (por ejemplo, mediante un Web Application Firewall y sanitización de inputs) garantiza la detección temprana de ataques. Aunque se puede incurrir en una leve degradación del rendimiento, este impacto se mitiga con escalabilidad horizontal y redundancia en el procesamiento, protegiendo la confidencialidad e integridad de los datos.		
Diagrama de arquitectura	<pre>graph LR; PW[Portal Web] -- "Solicitud Maliciosa" --> AG[Api Gateway]; subgraph AG [Api Gateway]; V[Validador]; end; AG -- "Ataque Dectado" --> N[Noficador]; N -- "Alerta" --> A((Alerta));</pre>		

Atributo de calidad 3: Seguridad

Escenario de calidad: <Nombre escenario>			
Escenario #: 8	Falla en el Proceso de Anonimización de Datos		
Fuente	Sistema (error interno)		
Estímulo	Ejecución fallida del módulo de anonimización, lo que provoca que datos sensibles no sean correctamente procesados y queden expuestos.		
Ambiente	Operación normal, alterada por un fallo inesperado en el proceso crítico.		
Artefacto	Módulo de anonimización de datos y base de datos de imágenes/metadatos.		
Respuesta	El sistema debe detectar el fallo de inmediato, detener el flujo de datos no anonimados, activar alertas y redirigir el proceso a un módulo de respaldo o iniciar un protocolo de recuperación para evitar la exposición de información sensible.		
Medida de la respuesta	Tiempo de detección inferior a 30 segundos; activación y respuesta en el 100% de los incidentes; menos del 5% de datos potencialmente comprometidos.		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
	Dependencia crítica del módulo de anonimización para la protección de datos sensibles.	La implementación de redundancia y monitoreo continuo puede aumentar la complejidad del sistema y la latencia en el procesamiento de datos.	Exposición de datos sensibles y violación de normativas de privacidad (por ejemplo, HIPAA) en caso de fallo en la anonimización.
Justificación	Al integrar mecanismos de monitoreo y redundancia en el proceso de anonimización, se asegura una respuesta inmediata ante fallos, minimizando el riesgo de exposición de información. El incremento en complejidad se compensa con la necesidad crítica de proteger la confidencialidad de los datos, asegurando el cumplimiento normativo y la confianza del usuario.		
Diagrama de arquitectura	<pre>graph LR PW[<<component>> Portal Web] -- Imagen --> A[<<component>> Anonimizador] subgraph A [<<component>> Anonimizador] P[<<component>> Procesador] V[<<component>> Validador] P -- "Imagen Procesada" --> V end A -- Metadatos --> BD[<<component>> Base de Datos] A -- "Imagen Anonimada" --> R[<<component>> Repositorio]</pre>		

Atributo de calidad 3: Seguridad

Escenario de calidad: <Nombre escenario>			
Escenario #: 9	Ataque de Fuerza Bruta en el Módulo de Autenticación		
Fuente	Atacante externo		
Estímulo	Múltiples intentos de autenticación fallidos desde la misma o diferentes IPs, característicos de un ataque de fuerza bruta.		
Ambiente	Operación normal bajo ataque de fuerza bruta; actividad sospechosa detectada en el sistema de autenticación.		
Artefacto	Módulo de autenticación basado en OAuth2 y JWT.		
Respuesta	El sistema debe identificar la actividad anómala, aplicar medidas de rate limiting y bloqueo temporal de IPs, registrar los incidentes y notificar al equipo de seguridad, sin afectar el acceso de usuarios legítimos.		
Medida de la respuesta	Bloqueo del 100% de intentos maliciosos detectados; tiempo de respuesta ante el ataque inferior a 1 minuto; tasa de falsos positivos inferior al 1%.		
Decisiones Arquitecturales	Punto de sensibilidad	Tradeoff	Riesgo
	Vulnerabilidad a ataques de fuerza bruta y acceso no autorizado a través de la autenticación.	Las estrategias de rate limiting y bloqueo pueden impactar a usuarios legítimos durante periodos de alta demanda si no se calibran correctamente.	Acceso no autorizado a información sensible y posible compromiso del sistema si el ataque no se mitiga a tiempo.
Justificación	La implementación de mecanismos de detección y mitigación de fuerza bruta, como el rate limiting, bloqueo de IPs y monitoreo de patrones de acceso, permite proteger el módulo de autenticación sin comprometer la experiencia del usuario. Estos controles, aunque pueden generar bloqueos erróneos en casos excepcionales, son críticos para prevenir accesos no autorizados y mantener la seguridad del sistema.		
Diagrama de arquitectura	<pre>graph LR subgraph "API Gateway" direction TB IG["<<service>> API Gateway"] end subgraph "Components" direction TB GR["<<component>> GestorRegistro"] GL["<<component>> GestorLogin"] BD["<<component>> BaseDatos"] end IG -- "Informacion Usuario" --> GR IG -- "Solicitud Acceso" --> GL GR -- "Registro" --> BD GL -- "Token" --> IG GL -- "Usuario" --> BD BD -- "SQL" --> BD</pre>		