Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

ACUERDO MARCO NUBE PÚBLICA V
FORMATO RFI PARA OPERACIÓN SECUNDARIA

1. Contexto estratégico de la Entidad

1.1 Información general

- Nombre de la Entidad: Secretaria General de la Alcaldía Mayor de Bogotá
- Sector: Distrito
- Rol misional: La Secretaría General de la Alcaldía Mayor de Bogotá es la entidad que lidera la articulación y coordinación de la administración distrital, dedicada a desarrollar capacidades institucionales para contribuir al bienestar integral de la ciudadanía, fomentar la confianza en la gestión pública y promover un orden institucional eficiente.

1.2 Contexto y motivación para el uso de nube pública

La Secretaría General de la Alcaldía requiere fortalecer su estrategia de continuidad operativa mediante la implementación de una plataforma de Recuperación ante Desastres (Disaster Recovery Plan - DRP) sobre servicios de nube pública, que permita proteger los sistemas de información misionales y de apoyo actualmente alojados en infraestructura local (On-Premise).

La adopción de servicios de nube pública busca atender las siguientes necesidades institucionales:

• Continuidad del negocio y resiliencia operativa: garantizar la disponibilidad de los sistemas críticos de la entidad ante eventos de falla tecnológica, indisponibilidad de infraestructura, incidentes de seguridad o desastres que afecten el centro de datos principal.

• Recuperación ante desastres (DRP): implementar una infraestructura alterna que permita la recuperación controlada de los servicios tecnológicos, minimizando los tiempos de interrupción y reduciendo la pérdida potencial de información.

• Reducción del riesgo tecnológico: disminuir la dependencia de una única ubicación física para la operación de los servicios institucionales, incorporando capacidades de redundancia geográfica y recuperación de servicios.

• Fortalecimiento de la disponibilidad de los servicios institucionales: asegurar la continuidad de aplicaciones críticas, bases de datos y plataformas tecnológicas que soportan la operación administrativa y la prestación de servicios a ciudadanos, entidades públicas y demás grupos de interés.

• Escalabilidad y flexibilidad tecnológica: disponer de recursos tecnológicos bajo demanda para atender requerimientos futuros de capacidad, crecimiento de información o ampliación de los servicios institucionales.

• Seguridad de la información: aprovechar las capacidades avanzadas de seguridad, monitoreo, auditoría, cifrado y control de acceso ofrecidas por plataformas de nube pública líderes en el mercado.

• Eficiencia operativa: reducir la complejidad asociada a la administración de infraestructura física destinada exclusivamente a contingencia, optimizando la gestión tecnológica y los tiempos de recuperación.

• Cumplimiento de lineamientos de Gobierno Digital: fortalecer la arquitectura tecnológica institucional mediante la adopción de modelos de nube alineados con las políticas y lineamientos emitidos por el Gobierno Nacional en materia de transformación digital, continuidad de negocio y gestión de riesgos tecnológicos.

En este contexto, la Entidad requiere una solución de nube pública que permita implementar un ambiente de recuperación ante desastres para sus componentes de bases de datos, servidores de aplicaciones y servicios de soporte, garantizando niveles adecuados de disponibilidad, seguridad, resiliencia y continuidad operativa.

Estado actual:

La Secretaría General de la Alcaldía actualmente soporta parte de sus servicios tecnológicos críticos sobre infraestructura On-Premise ubicada en su centro de datos institucional, donde se alojan plataformas de bases de datos, aplicaciones misionales y sistemas de apoyo administrativo.

Dentro de los componentes identificados como críticos para la continuidad operativa se encuentran:

Plataforma de Bases de Datos

La entidad dispone de una plataforma Oracle Database implementada bajo arquitectura Oracle RAC (Real Application Clusters), conformada por dos nodos de base de datos, sobre sistema operativo Oracle Linux. Esta plataforma soporta información institucional utilizada por múltiples sistemas de la entidad y constituye uno de los componentes más sensibles desde el punto de vista de disponibilidad y continuidad del servicio.

Plataformas Aplicativas

La infraestructura actual incluye servidores de aplicaciones que soportan diferentes procesos institucionales, entre los cuales se encuentran:

- Sistema SIGA.
- Plataforma SAT WEB.
- Plataforma Administrativa y Financiera.
- Componentes WebLogic para servicios empresariales.
- Servidores de integración y automatización de procesos.

Estos servicios se encuentran desplegados sobre servidores Linux con diferentes capacidades de procesamiento, memoria y almacenamiento, distribuidos en múltiples instancias de aplicación.

Infraestructura Tecnológica

El ambiente identificado para continuidad operativa está compuesto por aproximadamente:

- 2 servidores de bases de datos Oracle RAC.
- 2 servidores asociados a la plataforma SIGA.
- 5 servidores asociados a la plataforma SAT WEB.
- 2 servidores Oracle WebLogic para servicios administrativos y financieros.

Adicionalmente, algunos sistemas utilizan almacenamiento externo para el procesamiento y conservación de información institucional.

Situación actual de continuidad del negocio

La operación de los sistemas descritos depende inicialmente de la infraestructura tecnológica instalada en el centro de datos principal de la entidad. Ante eventos que afecten la disponibilidad de dicha infraestructura, la entidad podría enfrentar riesgos asociados a:

- Interrupción de servicios institucionales.
- Afectación de procesos administrativos y operativos.
- Indisponibilidad de aplicaciones de soporte a la gestión pública.
- Pérdida temporal de acceso a información crítica.
- Incremento en los tiempos de recuperación ante incidentes mayores.

Si bien la infraestructura actual permite la operación normal de los servicios, la entidad requiere fortalecer sus capacidades de continuidad de negocio mediante la implementación de un ambiente de Recuperación ante Desastres (DRP) que permita contar con una plataforma alterna para la recuperación controlada de los servicios tecnológicos críticos.

Necesidad identificada

Con el fin de reducir los riesgos operativos y tecnológicos asociados a la dependencia de una única ubicación física para la prestación de los servicios, la entidad requiere implementar una solución de recuperación ante desastres sobre nube pública que permita replicar y recuperar los componentes críticos de infraestructura, bases de datos y aplicaciones institucionales, garantizando niveles adecuados de disponibilidad, resiliencia y continuidad operativa.

1.3 Horizonte del proyecto

x Corto plazo (0–12 meses)
☐ Mediano plazo (1–3 años)

☐ Largo plazo (más de 3 años)

2. Objetivos del uso de la nube pública

Priorice los siguientes objetivos según su relevancia para la Entidad de 1 a 5 (5 = mayor prioridad):

5 Continuidad del negocio y recuperación ante desastres
4 Escalabilidad y elasticidad bajo demanda
5 Seguridad y gestión de riesgos
5 Cumplimiento normativo y regulatorio
4 Optimización y control de costos
3 Innovación tecnológica (IA, analítica, automatización, IoT, otros)

2.1 Criterios de éxito esperados:

La implementación de la solución de Recuperación ante Desastres (DRP) se considerará exitosa cuando se cumplan los siguientes criterios:

Disponibilidad de la infraestructura de contingencia

- La infraestructura de recuperación ante desastres deberá encontrarse implementada, configurada y operativa en la plataforma de nube pública seleccionada.
- Los componentes de cómputo, almacenamiento, red y seguridad deberán estar disponibles para soportar los servicios definidos dentro del alcance del proyecto.

Protección de los sistemas críticos

- Los servidores, aplicaciones y bases de datos identificados por la entidad como objeto del DRP deberán encontrarse replicados o protegidos mediante los mecanismos definidos durante la implementación.
- La solución deberá garantizar la capacidad de recuperación de los servicios priorizados por la entidad.

Recuperación de servicios

- Deberá demostrarse mediante pruebas controladas la capacidad de recuperación de los sistemas incluidos en el alcance.
- Los procedimientos de recuperación deberán permitir el restablecimiento de los servicios tecnológicos dentro de los tiempos definidos por la entidad para escenarios de contingencia.

Integridad de la información

- La información replicada hacia el ambiente de recuperación deberá conservar su integridad, consistencia y disponibilidad.

- Las pruebas realizadas deberán evidenciar que los datos pueden ser recuperados sin afectaciones funcionales atribuibles al proceso de replicación o recuperación.

Validación funcional

- Los sistemas incluidos dentro del alcance deberán superar satisfactoriamente las pruebas funcionales definidas por la entidad.
- Los usuarios responsables de cada sistema deberán validar la disponibilidad y correcto funcionamiento de los servicios recuperados.

Seguridad y control

- La solución implementada deberá cumplir con las políticas institucionales de seguridad de la información y control de acceso.
- Los mecanismos de monitoreo, auditoría y trazabilidad deberán encontrarse habilitados para los componentes implementados.

Documentación y transferencia de conocimiento

- Deberá entregarse la documentación técnica y operativa de la solución implementada.
- Deberá realizarse transferencia de conocimiento al personal designado por la entidad para la administración y operación del ambiente de recuperación.

Cierre del proyecto

El proyecto se considerará finalizado satisfactoriamente cuando:

- La infraestructura de recuperación ante desastres se encuentre operativa.
- Las pruebas de recuperación hayan sido ejecutadas y aprobadas.
- Se hayan entregado los documentos técnicos y operativos correspondientes.
- La entidad emita la aceptación de los entregables definidos en el proyecto.

3. Clasificación de la información, riesgos y cumplimiento

3.1 Clasificación de la información

Indique el nivel de sensibilidad de la información involucrada:

x Información pública
x Información de uso interno
x Información confidencial
x Información sensible / datos personales / datos críticos

3.2 Restricciones de ubicación geográfica de los datos

x Colombia
x Región específica (indicar): East US 2
☐ Sin restricción geográfica

3.3 Regulaciones y lineamientos aplicables

- Ley 1581 de 2012 – Protección de datos personales y normas asociadas (Habeas Data).
- Decreto 1377 de 2013 – Reglamentación parcial de la Ley 1581.
- Ley 1712 de 2014 – Transparencia y acceso a la información pública.
- Resolución 500 de 2021 - Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Decreto 767 de 2022 - Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Resolución 2277 de 2025 - Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- Resolución 373 de 2025 – Adopción de Política de seguridad digital y estrategia de seguridad digital de la Secretaria General de la Alcaldía Mayor de Bogota
- Lineamientos de Seguridad y Privacidad de la Información aplicables al sector público (políticas internas, MIPG/seguridad digital, etc.).
- Lineamientos/guías de SIC (Superintendencia de Industria y Comercio) en materia de datos personales.
- Políticas internas de gestión documental y archivo, y clasificación de información.
- Requisitos de auditoría (Contraloría/entes de control) y retención de logs según política institucional.

4. Tipo de necesidad

Seleccione el(los) escenario(s) que aplican:

x Nueva solución en nube pública
x Migración de infraestructura o sistemas On-Premise a nube
☐ Migración entre nubes públicas
☐ Expansión de solución cloud existente
☐ Renovación de servicios cloud
☐ Conectividad entre nubes públicas
x Conectividad nube pública – datacenter on-premise
x Sitio alterno / recuperación ante desastres

PARA CADA ESCENARIO DE LA NECESIDAD DE LA ENTIDAD SELECCIONADO, DILIGENCIE LA INFORMACIÓN APLICABLE EN LAS SECCIONES SIGUIENTES:

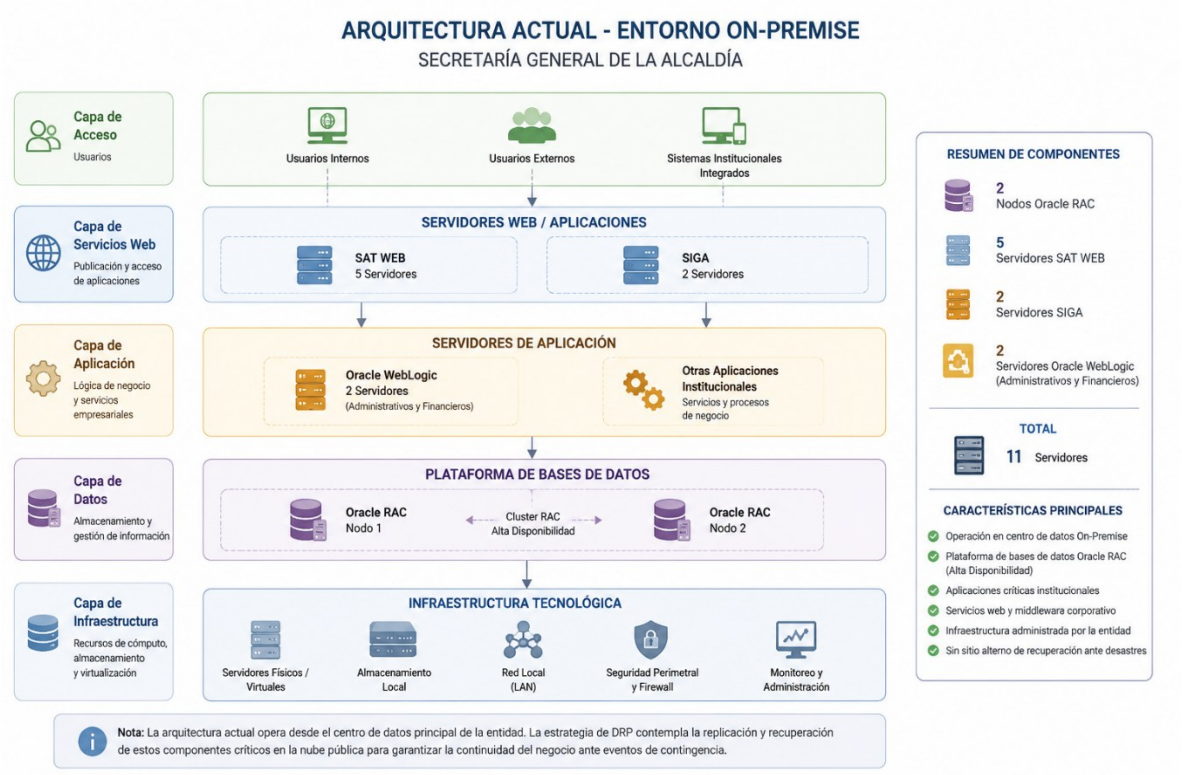
5. Arquitectura actual y estado objetivo

5.1 Arquitectura actual (si aplica)

Descripción general:

La Secretaría General de la Alcaldía dispone actualmente de una arquitectura tecnológica basada en infraestructura local (On-Premise), desde la cual se soportan aplicaciones misionales, administrativas y de apoyo que resultan fundamentales para la operación institucional.

La arquitectura actual se encuentra compuesta por una capa de bases de datos, una capa de aplicaciones y una capa de servicios web, desplegadas sobre servidores virtualizados y sistemas operativos Linux, que interactúan para garantizar la prestación de los servicios tecnológicos de la entidad.



Capa de Datos

La gestión y almacenamiento de la información institucional se soporta sobre una plataforma Oracle Database implementada bajo arquitectura Oracle Real Application

Clusters (RAC), conformada por dos nodos de base de datos que operan de manera integrada para proporcionar disponibilidad, balanceo de carga y continuidad de los servicios de información.

Esta plataforma constituye el repositorio principal de datos para los sistemas administrativos, financieros y de gestión institucional.

Capa de Aplicaciones

La capa de aplicaciones está conformada por servidores dedicados a la ejecución de sistemas institucionales y servicios empresariales, entre los cuales se encuentran:

- Plataforma SIGA.
- Plataforma SAT WEB.
- Aplicaciones administrativas y financieras.
- Servicios empresariales basados en Oracle WebLogic.

Estos componentes soportan los procesos operativos y administrativos de la entidad, permitiendo la gestión de información, ejecución de trámites y acceso a servicios internos y externos.

Capa de Servicios Web

La publicación de servicios y aplicaciones se realiza mediante servidores de aplicaciones y servidores web especializados, encargados de atender las solicitudes de usuarios internos y externos, así como la integración entre los diferentes sistemas institucionales.

Infraestructura Tecnológica

El ambiente objeto de la estrategia de recuperación ante desastres está conformado aproximadamente por:

Componente	Cantidad
Nodos Oracle RAC	2
Servidores SIGA	2
Servidores SAT WEB	5
Servidores Oracle WebLogic	2
Total Servidores	11

Esquema General de Operación

Actualmente la operación de los sistemas se concentra en el centro de datos principal de la entidad, donde residen los componentes de infraestructura, almacenamiento, bases de datos y aplicaciones.

La interacción entre los componentes tecnológicos puede resumirse de la siguiente manera:

1. Los usuarios acceden a los servicios institucionales mediante aplicaciones web y servicios empresariales.
2. Los servidores de aplicaciones procesan las solicitudes y ejecutan la lógica de negocio.
3. Los servidores Oracle WebLogic administran los componentes empresariales y las integraciones entre sistemas.
4. La información es almacenada y consultada desde la plataforma Oracle Database RAC.
5. Todos los componentes operan actualmente sobre infraestructura local administrada por la entidad.

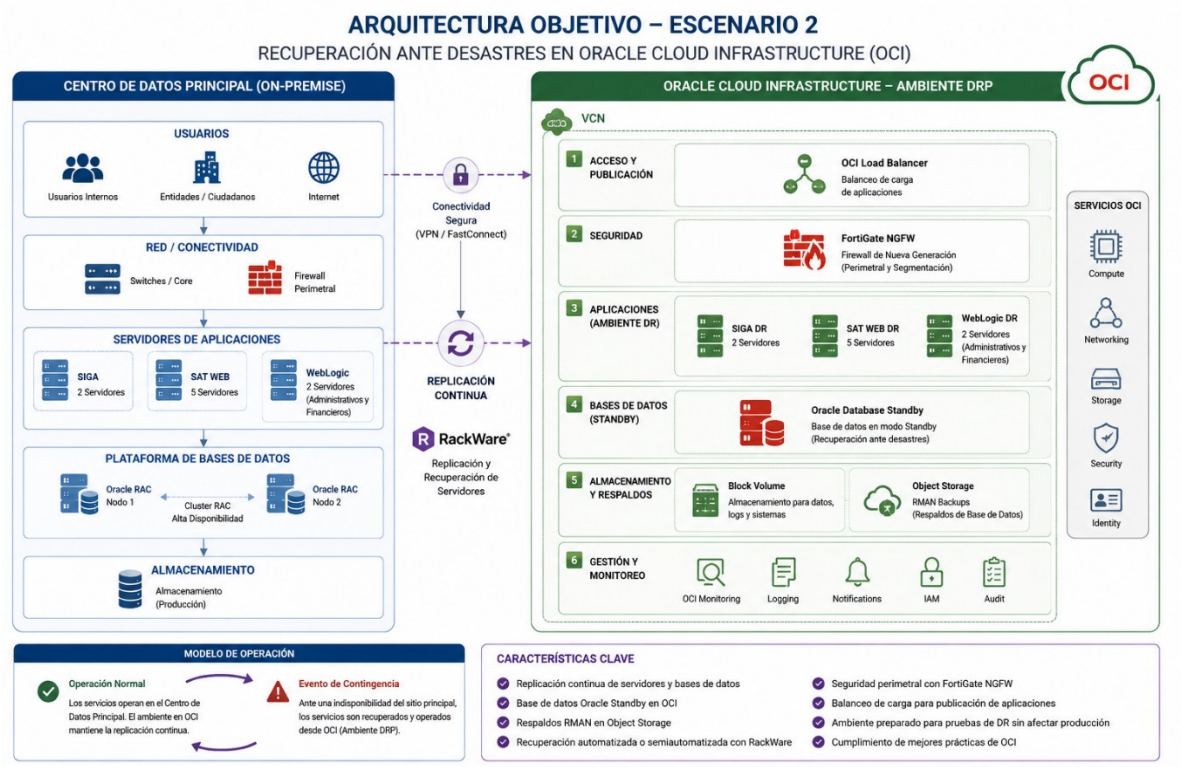
Situación Actual

La arquitectura actual permite la operación normal de los servicios institucionales; sin embargo, la continuidad de dichos servicios depende principalmente de la disponibilidad del centro de datos principal. Por esta razón, la entidad requiere complementar su arquitectura tecnológica mediante la implementación de una solución de Recuperación ante Desastres (DRP) en nube pública que permita disponer de una infraestructura alterna para la recuperación de los servicios críticos ante escenarios de contingencia.

5.2 Arquitectura objetivo esperada

La Entidad requiere implementar una arquitectura de Recuperación ante Desastres (DRP) sobre una plataforma de nube pública que permita garantizar la continuidad operativa de los sistemas críticos institucionales mediante la replicación y recuperación de los componentes de infraestructura, aplicaciones y bases de datos actualmente alojados en el centro de datos principal.

La arquitectura objetivo deberá operar como un sitio alterno de contingencia, preparado para asumir la operación de los servicios priorizados ante eventos que afecten la disponibilidad de la infraestructura principal.



Componentes de la arquitectura objetivo

La solución deberá estar conformada, como mínimo, por los siguientes componentes:

Capa de Bases de Datos

La arquitectura deberá incorporar una plataforma de base de datos de contingencia que permita mantener una copia actualizada de la información institucional alojada actualmente en Oracle Database.

La solución deberá contemplar:

- Base de datos Oracle Standby en nube pública.
- Almacenamiento dedicado para bases de datos.
- Mecanismos de sincronización y recuperación de información.
- Capacidades de recuperación ante fallas del sitio principal.

Adicionalmente, la entidad requiere una estrategia complementaria de respaldo mediante almacenamiento de objetos para la conservación de copias de seguridad de las bases de datos institucionales.

Capa de Aplicaciones

La solución deberá permitir la recuperación de los servidores de aplicaciones asociados a los sistemas institucionales incluidos dentro del alcance del proyecto, garantizando la disponibilidad de:

- Plataforma SIGA.
- Plataforma SAT WEB.
- Servicios basados en Oracle WebLogic.
- Componentes administrativos y financieros.
- Servicios de soporte e integración.

La recuperación de dichos servidores deberá realizarse mediante mecanismos de replicación y orquestación que permitan reducir los tiempos de indisponibilidad ante eventos de contingencia.

Capa de Replicación y Recuperación

La arquitectura deberá incorporar una plataforma especializada para la replicación de servidores y recuperación de cargas de trabajo entre el centro de datos principal y el ambiente de contingencia en nube pública.

Esta plataforma deberá permitir:

- Replicación continua de servidores.
- Recuperación automatizada o semiautomatizada.
- Pruebas de recuperación sin afectar la operación productiva.
- Gestión centralizada del proceso de recuperación.

Capa de Seguridad

La solución deberá incorporar controles de seguridad perimetral para proteger el ambiente de recuperación ante desastres, incluyendo:

- Firewall virtual de nueva generación.
- Control de tráfico entrante y saliente.
- Segmentación de redes.
- Aplicación de políticas de seguridad.
- Monitoreo y registro de eventos.

Capa de Acceso y Publicación

La arquitectura deberá incluir mecanismos que permitan distribuir y gestionar el tráfico de los servicios recuperados durante escenarios de contingencia, mediante componentes de balanceo de carga y publicación segura de aplicaciones.

Capa de Infraestructura

La plataforma de nube pública deberá proporcionar recursos de:

- Cómputo.
- Almacenamiento.
- Redes virtuales.
- Balanceo de carga.
- Seguridad.
- Monitoreo.

Estos componentes deberán dimensionarse para soportar la recuperación de los servicios incluidos en el alcance del proyecto.

Modelo de Operación Esperado

Bajo condiciones normales de operación, los sistemas continuarán ejecutándose en el centro de datos principal de la entidad, mientras que el ambiente de nube pública permanecerá sincronizado y preparado para asumir la operación en caso de contingencia.

Ante un evento de indisponibilidad del sitio principal, la entidad deberá poder activar los procedimientos de recuperación para habilitar la operación de los servicios desde el ambiente de contingencia, garantizando la continuidad de los procesos institucionales críticos.

La solución deberá permitir la ejecución periódica de pruebas de recuperación, validación de procedimientos y actualización de los mecanismos de sincronización, con el fin de asegurar la efectividad del plan de recuperación ante desastres.

6. Requisitos funcionales y no funcionales

6.1 Requisitos de negocio

La solución deberá permitir:

Continuidad Operativa

- Garantizar la continuidad de los servicios tecnológicos que soportan los procesos institucionales críticos.
- Minimizar el impacto operativo ante eventos de indisponibilidad del centro de datos principal.
- Disponer de una plataforma alterna para la recuperación de los servicios priorizados.

Disponibilidad de la Información

- Garantizar la protección de la información institucional.
- Reducir el riesgo de pérdida de datos ante eventos de contingencia.
- Mantener mecanismos de respaldo y recuperación que aseguren la disponibilidad de la información.

Gestión del Riesgo Tecnológico

- Reducir la dependencia de una única ubicación física para la operación de los servicios tecnológicos.
- Fortalecer las capacidades institucionales de recuperación ante desastres.
- Incrementar la resiliencia de la infraestructura tecnológica.

Cumplimiento Normativo y Gobierno Digital

- Fortalecer el cumplimiento de los lineamientos asociados a continuidad del negocio, gestión de riesgos, seguridad de la información y transformación digital aplicables a entidades públicas.
- Mantener capacidades de auditoría, trazabilidad y monitoreo de la operación tecnológica.

6.1.2 Requisitos Funcionales

La solución deberá proporcionar como mínimo las siguientes capacidades:

Recuperación de Servicios

- Recuperar los servicios tecnológicos incluidos dentro del alcance del proyecto.
- Permitir la activación controlada del ambiente de contingencia.
- Permitir la restauración de la operación normal una vez superada la contingencia.

Replicación de Información

- Mantener mecanismos de sincronización y replicación de información entre el ambiente principal y el ambiente de recuperación.
- Garantizar la consistencia e integridad de los datos replicados.

Respaldo y Recuperación

- Permitir la generación y almacenamiento de respaldos de información.
- Permitir la recuperación de bases de datos, servidores y servicios incluidos en el alcance.
- Mantener históricos de respaldo conforme a las políticas definidas por la Entidad.

Seguridad

- Implementar mecanismos de autenticación y control de acceso.
- Mantener capacidades de monitoreo y auditoría.
- Permitir el cifrado de la información almacenada y transmitida.

Monitoreo

- Disponer de herramientas de monitoreo de infraestructura, almacenamiento y servicios.

- Generar registros de eventos y alertas operativas.
- Facilitar la supervisión de los componentes de recuperación.

Pruebas de Recuperación

- Permitir la ejecución periódica de pruebas de recuperación.
- Validar la capacidad de recuperación de los servicios sin afectar la operación productiva.
- Generar evidencias y reportes de resultados de las pruebas realizadas.

6.2 Requisitos técnicos

Procesos Críticos Soportados

La solución deberá soportar la continuidad de los procesos institucionales que dependen de los sistemas incluidos dentro del alcance del proyecto.

Gestión Administrativa y Financiera

Procesos asociados a:

- Gestión financiera.
- Gestión presupuestal.
- Gestión contable.
- Gestión contractual.
- Gestión administrativa.

Gestión Institucional

Procesos asociados a:

- Administración de información institucional.
- Gestión documental y administrativa.
- Seguimiento y control de actividades institucionales.
- Soporte a la toma de decisiones.

Atención a Usuarios y Servicios Institucionales

Procesos soportados por las plataformas web y aplicativos institucionales que permiten la interacción de usuarios internos y externos con la Entidad.

Servicios de Información

Procesos que dependen de la disponibilidad de las bases de datos institucionales, incluyendo:

- Consulta de información.
- Registro y actualización de datos.

- Integración entre sistemas.
- Intercambio de información entre aplicaciones.

Servicios Tecnológicos Transversales

Procesos relacionados con:

- Autenticación y acceso a aplicaciones.
- Servicios empresariales soportados en middleware.
- Integración de aplicaciones.
- Publicación de servicios web.

Sistemas objeto de protección

La solución deberá contemplar la recuperación de los siguientes componentes tecnológicos identificados por la Entidad:

Componente	Cantidad
Oracle RAC	2 nodos
Servidores SIGA	2
Servidores SAT WEB	5
Servidores Oracle WebLogic	2
Total de servidores	11

La recuperación de estos componentes deberá realizarse de acuerdo con la estrategia de recuperación definida por la Entidad y los niveles de servicio establecidos para la solución.

6.3 Seguridad, privacidad y gobierno

La solución de Recuperación ante Desastres (DRP) deberá incorporar mecanismos de seguridad, control, monitoreo y gobierno que permitan proteger los servicios tecnológicos críticos de la Entidad, garantizar la integridad de la información replicada y facilitar la administración segura de los recursos desplegados en la nube pública.

La arquitectura propuesta deberá preservar los principios de confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional durante los procesos de replicación, almacenamiento, respaldo y recuperación.

6.3.1 Seguridad de la Infraestructura

La solución deberá proporcionar mecanismos que permitan proteger los recursos desplegados en la nube pública mediante controles de acceso, segmentación de red y monitoreo permanente.

Como mínimo deberá contemplar:

- Redes virtuales aisladas para los componentes de recuperación.

- Segmentación lógica de servicios y recursos.
- Políticas de control de acceso a nivel de red.
- Protección de los recursos de cómputo y almacenamiento.
- Registro de actividades administrativas y operativas.

Para arquitecturas que contemplen recuperación integral de aplicaciones, la solución deberá incorporar capacidades de protección perimetral mediante firewall virtual de nueva generación o mecanismo equivalente.

6.3.2 Gestión de Identidades y Accesos

La solución deberá utilizar mecanismos de gestión de identidades que permitan administrar el acceso a los recursos tecnológicos desplegados en la nube.

Deberá permitir:

- Definición de usuarios, grupos y roles.
- Administración centralizada de permisos.
- Aplicación del principio de mínimo privilegio.
- Control de acceso a recursos de infraestructura, almacenamiento y bases de datos.
- Trazabilidad de actividades administrativas.

La Entidad deberá conservar el control sobre los permisos y accesos asociados a la solución implementada.

6.3.3 Protección de la Información

La solución deberá garantizar la protección de la información institucional durante los procesos de replicación, almacenamiento y recuperación.

Información en tránsito

La sincronización de datos entre el centro de datos principal y la nube pública deberá realizarse mediante canales seguros de comunicación.

La conectividad utilizada para la replicación y administración del servicio deberá contar con mecanismos que permitan proteger la información transmitida entre los ambientes.

Información en reposo

Los componentes de almacenamiento utilizados por la solución deberán permitir la protección de la información almacenada, incluyendo:

- Bases de datos de contingencia.
- Volúmenes de almacenamiento.
- Copias de seguridad.
- Archivos de configuración.

Cuando aplique, la solución deberá permitir la utilización de mecanismos de cifrado para proteger la información almacenada.

6.3.4 Protección de Bases de Datos y Respaldos

La arquitectura deberá garantizar la protección de la información crítica mediante mecanismos de recuperación y respaldo.

La solución deberá contemplar:

- Replicación de bases de datos hacia el ambiente de contingencia.
- Almacenamiento de respaldos institucionales.
- Conservación de copias de seguridad.
- Recuperación de información ante eventos de contingencia.
- Validación periódica de la capacidad de recuperación de los datos.

Para los escenarios contemplados por la Entidad, los respaldos deberán poder almacenarse en servicios de almacenamiento de objetos y mantenerse disponibles para procesos de restauración cuando sea requerido.

6.3.5 Monitoreo y Auditoría

La solución deberá proporcionar capacidades de monitoreo y auditoría sobre los recursos desplegados en la nube pública.

Como mínimo deberá permitir:

- Monitoreo de disponibilidad de servicios.
- Monitoreo de infraestructura.
- Generación de alertas operativas.
- Registro de eventos administrativos.
- Registro de cambios sobre configuraciones críticas.
- Consulta de eventos de auditoría.

La Entidad deberá contar con acceso a los registros generados por la solución para fines de seguimiento, control y auditoría.

6.3.6 Gobierno de la Plataforma

La solución deberá facilitar la administración y gobierno de los recursos desplegados en la nube pública mediante mecanismos que permitan:

- Organización lógica de recursos tecnológicos.
- Administración de ambientes.
- Gestión de configuraciones.
- Administración de consumo y costos.
- Gestión de inventario de recursos.
- Aplicación de políticas de operación y seguridad.

La arquitectura deberá permitir el crecimiento futuro de la solución sin afectar la operación de los servicios existentes.

6.3.7 Seguridad para Recuperación ante Desastres

La solución deberá garantizar que los procesos de recuperación se ejecuten de forma controlada y segura.

Deberá permitir:

- Validar la integridad de la información replicada.
- Ejecutar pruebas de recuperación sin afectar los ambientes productivos.
- Recuperar bases de datos y servicios de acuerdo con la estrategia definida por la Entidad.
- Mantener trazabilidad sobre las actividades de recuperación ejecutadas.

Para arquitecturas que contemplen recuperación completa de aplicaciones y servidores, la solución deberá permitir la recuperación coordinada de infraestructura, aplicaciones y bases de datos.

7. Demanda y capacidad esperada

7.1 Usuarios o transacciones estimadas

Actualmente no se dispone de métricas consolidadas de usuarios ni de transacciones, dado que la plataforma corresponde a una implementación nueva y aún no ha iniciado operación productiva.

En esta fase inicial, el dimensionamiento se ha realizado con base en las capacidades técnicas actuales y en los requerimientos funcionales definidos en el diseño, lo que asegura la cobertura adecuada para la puesta en marcha.

Las métricas de uso y volumen de transacciones serán recolectadas y documentadas una vez se cuente con datos reales de operación, permitiendo establecer proyecciones más precisas en etapas posteriores.

7.2 Proyección de crecimiento

Dado que la solución corresponde a una implementación nueva, no se proyecta crecimiento adicional en esta etapa. Las capacidades definidas en el diseño actual cubren plenamente los requerimientos funcionales, operativos y de rendimiento previstos para el servicio.

El dimensionamiento inicial contempla los recursos necesarios para garantizar la estabilidad, disponibilidad y desempeño de la plataforma bajo las condiciones normales de operación, sin necesidad de ampliaciones o escalamiento inmediato.

8. Capacidades esperadas del Proveedor

El proveedor deberá describir:

Modelo de prestación del servicio y operación (SLA, soporte 7x24 si aplica)

La entidad requiere para el desarrollo de sus proyectos requerimiento servicios profesionales en el enfoque de continuación del proyecto de DRP y desarrollo de proyectos los siguientes Perfiles.

Código	Servicio	Zona	Tipo	Horas
CO-EX-16-01	Arquitecto Senior en Nube Publica	Remoto	Servicios profesionales	35
CO-MI-01-01	Servicio de migración	Remoto	Servicios profesionales	15
CO-EX-02-01	Experto Senior en Recuperación ante Desastres	Remoto	Servicios profesionales	250

9. Enfoque de solución propuesto por el Proveedor

El proveedor deberá presentar un enfoque integral que garantice la cobertura técnica, operativa y de seguridad de la solución, incluyendo como mínimo los siguientes elementos:

- Descripción del alcance de la solución: Definición clara de los servicios, funcionalidades y componentes que serán entregados, alineados con los objetivos de la Entidad.

- Resumen ejecutivo: Síntesis de la propuesta, destacando beneficios, valor agregado y cumplimiento de requerimientos estratégicos.

- Arquitectura propuesta: Presentación de un diagrama lógico y un diagrama de red a alto nivel, que evidencien la estructura, interconexiones y componentes principales.

- Supuestos y dependencias: Identificación de condiciones necesarias para la implementación (conectividad, licencias, ventanas de mantenimiento, recursos de terceros).

- Plan por fases y cronogramas:
  - Descubrimiento y evaluación.
  - Diseño de landing zone y seguridad.
  - Piloto.
  - Migración por oleadas.
  - Estabilización y operación.

- Riesgos y mitigaciones: Análisis de riesgos técnicos, de seguridad, operativos y de cumplimiento, con estrategias de mitigación documentadas.

- Diseño y documentación del plan de desastre: Plan de recuperación ante fallos, con definición de RTO/RPO y procedimientos de continuidad.

- Estimación de costos: Presentación en tabla comparativa que incluya:
  - Costos recurrentes (mensuales/anuales).

- Costos únicos (migración/servicios profesionales).
- Supuestos de consumo.

- Evidencias de seguridad y cumplimiento: Certificaciones, reportes y prácticas que respalden la conformidad con estándares internacionales (ISO 27001, NIST, OWASP, entre otros).

- Capacitación y transferencia de conocimiento: Plan de formación para el equipo de la Entidad, incluyendo sesiones, manuales y mecanismos de apropiación tecnológica.

10. Condición especial para MiPymes (Manifestación de MYPYMES)

No aplica, teniendo en cuenta el monto del presente proceso de contratación.

Nota para la Entidad Compradora

La calidad y nivel de detalle de la información suministrada por la Entidad en el presente RFI incide directamente en la **precisión, pertinencia y valor** de las respuestas entregadas por los Proveedores de Servicios de Nube Pública (CSP).

En la medida en que la Entidad proporcione información **suficiente, clara y contextualizada** sobre sus objetivos, restricciones, riesgos, demanda y visión futura, los CSP podrán:

- Dimensionar de forma más precisa las soluciones propuestas.
- Presentar arquitecturas y servicios alineados con las necesidades reales de la Entidad.
- Proveer estimaciones más confiables de capacidades, costos y modelos operativos.
- Identificar y mitigar riesgos técnicos, operativos, de seguridad y de cumplimiento.

Lo anterior permitirá a la Entidad realizar una **toma de decisiones basada en datos**, reduciendo la incertidumbre, minimizando riesgos y aumentando la probabilidad de seleccionar la alternativa de nube pública más adecuada para el cumplimiento de su misión institucional.

El presupuesto de contratación de créditos Universales es de $460.950.680 y el presupuesto total seria de $580.448.148