ESPECIFICACIONES TÉCNICAS

REPOSICIÓN E IMPLEMENTACIÓN DE UN DATACENTER CLOUD PARA METRO S.A

Versión B

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍAS

Marzo 2024

Tabla de contenido

1. Objetivo

El presente llamado a licitación tiene por objeto seleccionar una empresa que provea servicios de infraestructura en nube pública para la implementación y realojamiento del actual Datacenter de Metro de Santiago, con el objetivo de respaldar, mejorar y optimizar la infraestructura existente, aprovechando las ventajas de la nube para mejorar la escalabilidad, disponibilidad y eficiencia operativa.
La presente especificación solicitará dos productos de similar característica, pero con diferentes alcances, los productos son los siguientes:

Producto N°1 Infraestructura de Datacenter en modalidad de host dedicado y con virtualizador de (Bare-metal). Este producto tiene como objetivo establecer una infraestructura de datacenter en un entorno dedicado y flexible, facilitando una disposición que permita adaptarse a necesidades futuras de expansión o transición. Solo se podrán utilizar en la propuesta los siguientes virtualizadores,: VMware Cloud, HyperV Cloud, Oracle KVM (con soporte directo de Oracle), RedHat KVM (con soporte directo de Red Hat) y Nutanix. Estos virtualizadores asegurarán una infraestructura que optimiza la interoperabilidad con plataformas y servicios administrativos actuales, al mismo tiempo que habilita el uso de estándares tecnológicos avanzados y protocolos necesarios para garantizar una estructura adaptable y de amplia integración tecnológica.

Es importante destacar que está restringido la instalación de un virtualizador sobre otro virtualizador, ya que esto impactaría negativamente en el rendimiento y la estabilidad del sistema. Además, los hosts dedicados no deben encontrarse alojados en datacenter de terceros, así como tampoco es posible compartir o vincular con terceros.

Producto N°2 Infraestructura nativa nube pública (máquinas virtuales, sistemas operativos y motores de base de datos) para 3 ambientes (desarrollo, QA y producción) del sistema denominado “Sistema de Gestión y Control de transacciones de ventas y usos (CVU)”

Se debe considerar en el diseño de la solución que Metro utiliza la autenticación de acceso a la plataforma de servidores y cuentas de servicio mediante Active Directory.

Para aplicativos externos o interna con autenticación moderna, Metro utiliza los servicios de autenticación provista por su plataforma 365 mediante entra ID, para aquellas aplicaciones legacy, Metro utiliza Active Directory locales para la validación de credenciales. Con la finalidad de gestionar adecuadamente el acceso de usuarios y recursos a los aplicativos que serán montados en nube, el oferente deberá considerar estos antecedentes en el diseño de su arquitectura, considerando los mecanismos de seguridad robustos para garantizar la confidencialidad, integridad y disponibilidad del AD, cuentas de servicios y de las máquinas que sean parte del Datacenter Cloud independiente de la nube en la que estén implementadas.

2. Descripción de la situación actual.

Metro en la actualidad cuenta con un Datacenter corporativo que provee servicios de back Office a la organización, este Datacenter está implementado en una superficie de 78 Mt² y está ubicado en el edificio corporativo.

El Datacenter corporativo aloja un total de 20 rack, en los cuales están implementados los sistemas de comunicaciones corporativos (Core de Comunicaciones), sistemas de respaldos, UPS y los clústeres[1] de servidores que dan el cómputo y almacenamiento necesario para 60+ sistemas corporativos, bases de datos, sistemas de almacenamiento y correo electrónico que utilizan 4 . 4 7 5 colaboradores.

Los servicios que el Datacenter corporativo entrega a sus usuarios están implementados en entornos virtualizados. Estos entornos utilizan VMware como hipervisor y se dividen en 3 site[2] los cuales son descritos a continuación.

Site1:
Compuesto por dos clústeres, cada uno con 9 y 2 host respectivamente, los host son servidores PowerEdge M630 (Intel Xeon E5-2660 v3 de 2.60 GHz con 128 GB Ram) y M620 (Intel Xeon E5-2670 0 de 2.60 GHz con 128)

Site2:
Compuesto por dos clústeres, cada uno con 3 y 4 host respectivamente, los host son servidores PowerEdge M630 (Intel Xeon E5-2660 v3 de 2.60 GHz con 128 GB Ram), M620 (Intel Xeon E5-2670 0 de 2.60 GHz con 128) y M640 (Intel Xeon Gold 6234 de 3.3

GHz con 128)

[1] Conjunto de servidores que se gestionan como una única unidad de computo
[2] site: conjunto de Rack que integran servidores, almacenamiento y comunicaciones.

Site3:
Compuesto por un clúster productivo con 6 host, los host son servidores Cisco Hiperconvergente HX220C-M4S (Intel Xeon E5-2630 v4 de 2.20 GHZ.)

En su conjunto estas infraestructuras virtuales entregan cómputo y almacenamiento a un total de 180 máquinas virtuales (el detalle de consumo de las máquinas virtuales por cada site es parte del detalle del anexo N° 1.)

3. Alcance Producto 1 : requerimientos generales.

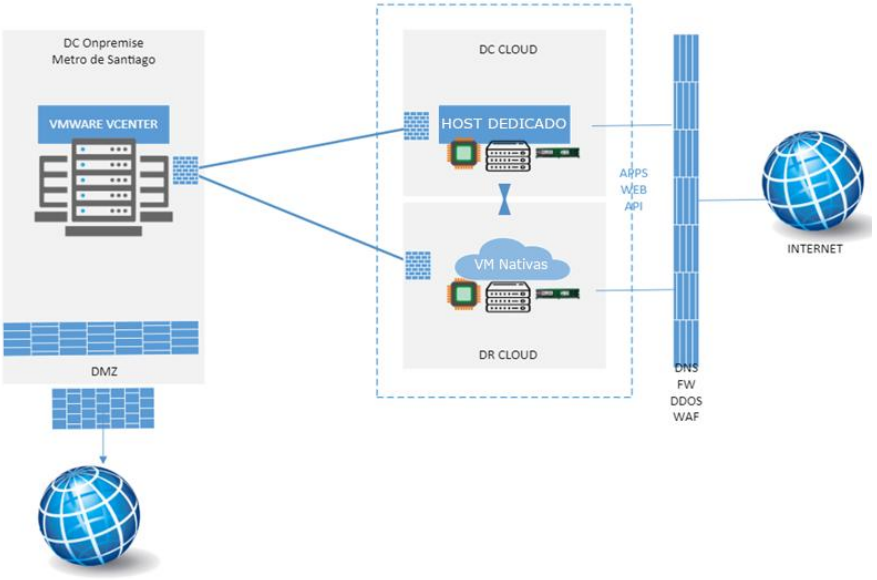
REQ01: El Proponente debe considerar el suministro de los servicios de infraestructura en modalidad de nube pública provista por hyperscalers, con host dedicado y la utilización de hipervisor Bare-metal (tipo1) para el total de máquinas virtuales que soporta la actual plataforma virtualizada de Metro de Santiago considerando mantener la división lógica de site descrita en el apartado N°2.

El servicio considera la habilitación de equipamiento, conectividad, seguridad, almacenamiento, DR, configuración y puesta en marcha del hardware y software necesario para la correcta operación de la infraestructura antes descrita.

La nube publica ofertada deberá estar al homologado a un estándar TIER III o superior.

El diseño e implementación de la infraestructura deberán seguir las mejores prácticas reconocidas en la industria para entornos de nube pública, aplicando metodologías y marcos de referencia validados por cada proveedor, garantizando así un diseño que cumpla con estándares de alta disponibilidad, seguridad, resiliencia, escalabilidad y eficiencia operativa. Asimismo, se debe considerar un marco de gobernanza robusto que facilite la administración de la infraestructura y permita una evolución y adaptación eficiente a futuras necesidades tecnológicas sin impactar los objetivos operativos actuales.

A continuación, se presenta un diagrama conceptual de la solución requerida.



ImagenN°1 Diagrama Conceptual Datacenter

REQ02: El Proponente será responsable de la migración de la plataforma y sistemas que se encuentran en los actuales clústeres VMware on-premise que componen la solución virtual que Metro de Santiago administra en su Datacenter. Para ello el oferente deberá presentar el diseño del modelo, método y una evaluación exhaustiva de riesgos potenciales de la migración, incluyendo incompatibilidades, fallas en aplicaciones críticas y pérdida de datos. Este análisis debe ser entregado a la organización para su revisión y aprobación. Además, deberá garantizar la seguridad en la comunicación entre ambos sitios, implementando medidas de protección avanzadas para asegurar la integridad y confidencialidad de los datos transferidos entre la nube y el datacenter local, cumpliendo con los estándares de seguridad necesarios para la operación crítica de la infraestructura

REQ03: La Nube propuesta deberá proveer servicios IaaS, PaaS, SaaS, lo anterior para asegurar la migración de servicios desde infraestructura montada en hipervisor Bare-metal a servicios nativos VM, serverless o contendedores como parte de la modernización de aplicaciones que lleva adelante Metro de Santiago.
Los servicios deberán cumplir con un nivel de disponibilidad 99,7% al año y una latencia máxima de 50 milisegundos en la misma región.

REQ04: El proponente deberá considerar como parte de su propuesta un servicio DR

del cual no requiere Host Dedicado, implementado en un site secundario en una región diferente. Que permita en caso de indisponibilidad del site principal prestar los servicios ofertados. Las máquinas que serán parte del DR están declaradas en el anexo N° 3, estos ambientes deben tener los mismos niveles de seguridad y disponibilidad que aquellos sistemas que están en el site principal.

Objetivos de Recuperación (RTO/RPO):

- RTO (Recovery Time Objective): El tiempo máximo de recuperación deberá ser de 30 minutos para sistemas críticos. La maquinas deben ser respaldadas diariamente en forma automática.

- RPO (Recovery Point Objective): La pérdida máxima de datos permitida será de 8 horas.

- El proponente deberá presentar un plan de pruebas trimestrales de conmutación (failover) y recuperación para validar el cumplimiento de estos objetivos.

REQ05: El oferente adjudicado deberá incluir en su propuesta un modelo operacional que permita la activación del site de contingencia (DR) y el procedimiento de vuelta atrás. En caso de ser necesaria la activación del site de contingencia, este deberá estar operativo en un tiempo no superior a 30 minutos desde que se declare la indisponibilidad del site principal, asegurando que el proceso de conmutación no genere indisponibilidad de los servicios contratados por un periodo mayor a dicho tiempo, y que el número de activaciones no supere los 4 eventos al año.
Asimismo, se requiere que el proveedor garantice acuerdos de nivel de servicio (SLA) comprometidos tanto para el site principal como el site de contingencia (DR), con un SLA mínimo de 99.97% de disponibilidad anual.
El proceso de vuelta atrás deberá ser ejecutado de manera controlada y programada, asegurando la disponibilidad del servicio y evitando la perdida de datos.

REQ06: El oferente adjudicado deberá proporcionar toda la documentación técnica necesaria, incluyendo la topología formal de la infraestructura propuesta, configuraciones detalladas procedimientos operativos y de contingencia, y cualquier otra documentación relevante para asegurar la continuidad y el correcto funcionamiento de los servicios.

3.1.Descripción de ambientes requeridos, Producto 1.

REQ07: El Proveedor deberá considerar segmentación de ambientes lógicos (Producción, Desarrollo, QA) como parte de su diseño ofertado. Los entornos de **Producción, Desarrollo y QA** deberán ser segmentados en **redes virtuales independientes (VPCs)** para garantizar un **aislamiento completo** entre ellos.
El proveedor deberá asegurar que **no exista comunicación directa** entre los entornos de Producción y Desarrollo, excepto a través de **puntos de control** predefinidos y seguros.

REQ8: El Proveedor Adjudicado deberá considerar que la infraestructura a implementar prestará servicio de procesamiento y almacenamiento para sistemas de uso interno de metro y para servicios que estarán expuestos a internet, por lo tanto, deberá considerar Zonas de Seguridad en donde se publiquen aquellos servicios que deben ser expuestos a internet, para lo cual se debe considerar, implementar y configurar los mecanismos, equipos y servicios de seguridad necesarios, tanto para las redes internas (nube) como para aquellas que estén expuestas a internet.

3.2. Instalación y configuración de máquinas virtuales y motores de base de datos.

REQ9 El Oferente adjudicado será el responsable del diseño, implementación y puesta en marcha de los ambientes antes descritos en conjunto con el equipo técnico de Metro (Producción, desarrollo y QA) considerando al menos a las siguientes actividades:

- Instalación, configuración y puesta en marcha de la infraestructura de Hardware: Configuración de host dedicado, requerida para la migración de las máquinas virtuales que conforman cada ambiente y los motores de bases de datos que son descritos en anexo N° 1.
- Instalación y configuración de Hipervisor bare metal y creación de los ambientes lógicos necesarios para la puesta en servicios de la totalidad de máquinas virtuales declaradas en anexo 1.
- Migración de máquinas virtuales: Ejecución de la migración de máquinas virtuales desde el Datacenter onpremise a la infraestructura implementada en nube, asegurando la integridad de los datos y minimización el tiempo de inactividad

- Configuración y disponibilización de Dashboard de monitoreo: Implementación de un panel de control que permita el monitoreo en tiempo real de los ambientes de Producción, QA y Desarrollo. Este dashboard deberá mostrar el estado de las máquinas virtuales y de los motores de bases de datos, proporcionando información de rendimiento, consumo de recursos y alertas de sistema.
- Servicio de reportería que genere informes de monitoreo: periódicos de máquinas virtuales y motores de bases de datos, cubriendo aspectos como consumo de recursos, rendimiento de los sitios alojados, uso y tráfico, seguridad, optimización y respaldos (espacio en disco, RAM, procesamiento, conectividad, y tiempo de actividad). Los reportes básicos deberán ser provistos desde el día 0 de implementación de la plataforma.

- Separación lógica y seguridad de los ambientes: Implementación de la separación lógica de los ambientes de producción, QA y Desarrollo. Deberán implementar mecanismos de seguridad que impidan la intervención o acceso a los ambientes productivos por personal no autorizado,

- Transferencia de conocimiento: Realización de sesiones de transferencia de conocimiento con el equipo de Metro, complementadas con documentación detallada de la implementación, configuraciones y mejores prácticas para el manejo y mantenimiento de los ambientes.

3.3.Conectividad y acceso a plataforma.

REQ10: El Proponente deberá suministrar mecanismos de acceso seguro a los ambientes y aplicativos implementados en los data center del oferente, considerando aspectos de encriptación de la información en tránsito y aquella que está almacenada en las instalaciones del proveedor, además de considerar mecanismos de autentificación de acceso. Para esto, debe considerar por ejemplo la habilitación de VPN Site to Site u otros mecanismos de conexión que permitan asegurar la conectividad y seguridad de acceso hacia el sistema entre los extremos (data center proveedor y las instalaciones de Metro S.A.) Esta información deberá ser entregada al momento de presentar la oferta. Estos accesos deberán considerar redundancia en su implementación lo anterior considerando posibles fallas de los

accesos principales.

Se podrá presentar conectividad a puntos de acceso locales provistos por las nubes o carriers que permita disminuir la latencia propia de Internet. Este item deberá ser consignado en la oferta económica como un item opcional y quedará a criterio de Metro su aplicación.

4. Provisión del licenciamiento requerido.

REQ11: El Oferente adjudicado deberá proveer todo el licenciamiento que sea necesario (Hipervisor, Sistemas operativos, motores de base de datos SQL), y cualquier otro licenciamiento que sea necesario para el correcto funcionamiento de los servicios contratados, este licenciamiento deberá ser provisto por toda la duración del contrato. En el caso del licenciamiento SQL, este deberá ser adquirido a nombre de Metro y con Software Assurance que permita la portabilidad de la licencia a ambientes onpremise u otras nubes en caso de que metro así lo requiera. La cantidad de licencias SQL está consignada en el ANEXO N°4

REQ12: El Oferente adjudicado deberá ofertar licenciamiento Microsoft EMS E3 de acuerdo al formulario económico (precio unitario), considerando un desde de 250 licencias, este licenciamiento deberá ser consignado en la oferta económica como un item opcional y quedará a criterio de su adjudicación en forma total o parcial.

5. Soporte requerido.

REQ12: La Nube propuesta por el oferente adjudicado deberá contar con soporte y una plataforma de gestión de tickets, en donde se pueda registrar, escalar y dar seguimiento de incidentes detectados, además de seguimiento a las gestiones realizadas y tiempo de resolución.

El oferente deberá describir en su propuesta el proceso de soporte y la matriz de escalamiento respectivo. (Incluir SLA ante casos de baja y alta criticidad).

6. Calidad de Partner y Certificaciones.

REQ13: El oferente deberá:

- Tener la calidad de Partner que permita la implementación de servicios (solicitados en el presente documento) en la nube, esta condición deberá ser acreditada con carta / certificado emitido por la nube en la cual se realizará la implementación. A Adicionalmente, el Partner deberá tener la capacidad de realizar compras, gestionar cuentas, adquirir y administrar créditos, así como gestionar la facturación directamente con el proveedor de la nube, asegurando una administración integral y eficiente de los servicios contratados.
- Tener experiencia comprobada de 10 años o más en el mercado con proyectos de implementación de plataformas TI con VMware, HyperV, Nutanix o KVM en sus versiones comerciales, con 5 o más implementaciones Cloud exitosas de envergadura similar a la propuesta para Metro de Santiago en entorno nube. Se deberán adjuntar los certificados que acrediten la condición solicitada, y el detalle de las implementaciones realizadas con sus correspondientes contactos y a lo menos 5 cartas de recomendación por parte de los clientes

El Equipo implementador deberá estar compuesto por un mínimo de 2 roles técnicos y un rol de líder, todos con al menos 4 años de experiencia demostrable en la implementación de soluciones Vmware, HyperV, Nutanix o KVM en sus versiones comerciales en la Nube. Los roles técnicos deberán ser Arquitecto de soluciones Cloud e Ingeniero Implementador de soluciones Cloud, ambos con acreditaciones y certificaciones de acuerdo a su función. Se deberán adjuntar los certificados que acrediten la condición de certificación solicitada, y el detalle de las implementaciones en las que ha participado cada uno de los integrantes del equipo implementador, con su correspondiente contacto.

- El proveedor deberá acreditar la formación profesional /certificaciones de cada uno de los miembros del equipo implementador.

7. Requerimiento de ciberseguridad y Seguridad de la Información.

7.1.Requerimiento de ciberseguridad

El Proponente deberá desarrollar en su propuesta en forma detallada los puntos que a continuación se solicitan como requerimientos de ciberseguridad y seguridad de la información, adjuntando la documentación que sea necesaria para respaldar la solución ofertada:

REQ14: El proveedor deberá considerar en su propuesta la implementación de una o varias soluciones de software que permitan cubrir al menos los siguientes aspectos de ciberseguridad Cloud. A su vez, el proveedor deberá utilizar su experiencia y las buenas prácticas para proponer una estrategia de uso y/o consumo de cada solución, velando que se cumpla con el objetivo pero que también se produzca una economía de costos para Metro de Santiago:

- Autenticación de Identidad: Solución(es) que permita(n) realizar un efectivo control y gestión de accesos y privilegios a la infraestructura, las aplicaciones y los datos.

- Protección de la red e Infraestructura: Solución(es) que permita(n) administrar redes privadas Cloud (VPC) y a su vez implementar medidas de seguridad Este/Oeste (medidas de ciberseguridad dentro de la misma capa de red) y Norte/Sur (protección del tráfico perimetral entre redes internas y externas). El proveedor deberá incorporar en su propuesta y diseño una infraestructura de seguridad perimetral que permita exponer servicios (Apps, web, API) hacia internet, protegiendo la infraestructura de accesos no autorizados, Anti DDoS, e incorporando servicios de Firewall y DNS. La solución también deberá permitir realizar microsegmentación de la red, es decir, dividir lógicamente el centro de datos a nivel de carga de trabajo individual, de manera de poder definir los controles de ciberseguridad adecuados.

- Protección de Servidores: Solución(es) que permita(n) reforzar la seguridad para hardware crítico.

- Protección de Datos: Solución(es) que permita(n) gobernar la seguridad y

privacidad de los datos, realizar descubrimiento de datos confidenciales, etiquetado y cifrado.

- Recuperación y Respaldos: Solución(es) que permita(n) realizar copias de seguridad de los datos, configuraciones e infraestructura. Del mismo modo deben permitir realizar pruebas de restauración.

- Controles de detección: Solución(es) que permita(n) realizar la detección de amenazas de manera transversal, registro de actividades y cambios de configuración(log). Las alertas generadas deben poder integrarse con sistemas de correlación de eventos top del mercado (Ej: QRadar y Splunk).

- Monitoreo y observabilidad Cloud: Solución que permita tener una visibilidad completa del ambiente Cloud, del tráfico y de las comunicaciones, así como de la accesibilidad a los datos.

7.2.Requerimiento de Seguridad de la Información.

REQ 15 El Proponente deberá desarrollar en su propuesta en forma detallada como abordará los requerimientos seguridad de la información que a continuación se detallan, adjuntando la documentación que sea necesaria para respaldar la solución ofertada:

- El oferente adjudicado será el responsable de suministrar el sistema y proceso de respaldo de la información contenida en los servidores, y en los motores de base de datos. En este contexto, deberá considerar servicios y plataforma de respaldo propios de la nube, distinto de donde se implemente la infraestructura principal, debiendo resguardar la confidencialidad, integridad y disponibilidad de los datos, mediante un ambiente aislado lógicamente. El almacenamiento ofrecido debe quedar con acceso restringido, normado por los procedimientos de accesos que deben ser indicados como parte del servicio del proponente. Lo anterior debe ser descrito en detalle en la oferta técnica presentada.

- Respaldo de Infraestructura: El oferente adjudicado deberá implementar

un sistema de respaldo para la infraestructura crítica (máquinas virtuales, configuraciones de hipervisores y redes) que cumpla con criterios estandarizados de disponibilidad y seguridad, orientado a la rápida recuperación de entornos operativos en caso de fallas o incidentes. Los respaldos deberán realizarse de la siguiente manera:

- Diarios: Retención de 7 días, para restauración rápida de configuraciones recientes.
- Semanales y mensuales: Retención de 1 mes, para garantizar la restauración de configuraciones previas, en caso de problemas tras actualizaciones o cambios accidentales.

Estos respaldos de infraestructura deberán cumplir con las normativas de seguridad, incluyendo cifrado de datos en tránsito y en reposo, y adherirse a normativas locales e internacionales relevantes como ISO 27001. El proveedor deberá ejecutar pruebas periódicas de restauración para validar la integridad y confiabilidad de los respaldos de infraestructura, almacenándolos en ubicaciones seguras para minimizar el riesgo de pérdida de datos.

- Respaldo Incremental de Datos:
  El proveedor adjudicado deberá implementar una estrategia de respaldo incremental de datos, enfocada en la protección y recuperación de información crítica generada por usuarios y operaciones del sistema, para garantizar la continuidad del negocio. La política de respaldo deberá considerar:
  - Respaldos incrementales diarios: Con retención de 7 días, capturando solo los cambios recientes desde el último respaldo completo, optimizando almacenamiento y tiempos de procesamiento.
  - Respaldos completos semanales y mensuales: Con retención de 1 mes, permitiendo la recuperación completa de los datos en caso de incidentes mayores.
  - Respaldos de largo plazo (trimestrales): Para respaldos históricos que cumplan con requerimientos de auditoría y regulaciones, donde el último trimestre se conservará durante toda la duración del contrato.

  Todos los respaldos de datos deberán contar con cifrado robusto y cumplir

con las normativas de protección de datos aplicables, como ISO 27001, ISO 22301 y GDPR. Esta estrategia permitirá una restauración confiable de los datos, asegurando la continuidad operativa y minimizando los tiempos de recuperación. El proveedor deberá realizar pruebas regulares para confirmar la integridad de los respaldos y deberá disponer de instructivos claros de restauración de información en caso de ser necesario.

- Respaldo del Ambiente de Recuperación ante Desastres (DR): Una vez activado el ambiente de Recuperación ante Desastres (DR), el oferente adjudicado deberá realizar respaldos de este entorno con la misma periodicidad y bajo los mismos estándares que los definidos para el ambiente principal. Esto incluye respaldos diarios, semanales y mensuales según los criterios establecidos de retención y seguridad, con el fin de asegurar la disponibilidad y recuperación de la información durante el tiempo en que el sitio de DR esté en operación.
- El proveedor deberá implementar un sistema de monitoreo constante del estado de los sistemas de respaldo en el ambiente de DR, verificando que se ejecuten correctamente y que los respaldos sean íntegros y restaurables en caso de necesidad. Esta estrategia deberá mantenerse activa mientras dure la contingencia, hasta que los servicios se restablezcan completamente en el sitio principal, garantizando una recuperación continua y segura.

- Será responsabilidad del oferente generar los mecanismos que permitan a Metro de Santiago el monitoreo 7x24 y generación de alarmas a sus equipos de soporte interno, informando a Metro según SLA establecidos de la indisponibilidad de algún servicio. El proveedor entregará al equipo de Operaciones TI de Metro, el acceso a dashboard de monitoreo donde se pueda visualizar el estado de salud de cada uno de los servidores y servicios contratados, particularmente parámetros tales como consumo de recursos de las VM (CPU, RAM, Espacio de discos), estado de sitios internos y externos, tráfico, y cualquier otro que permita tomar medidas proactivas de mantenimiento y mejora necesarias del ambiente. Además, el Oferente adjudicado deberá realizar inducción del uso y generación de nuevos dashboard. La descripción del modelo de operación del monitoreo

y alarmas asociada a incidentes en la plataforma deberá ser descrito en detalle en la oferta técnica del oferente.

- El proveedor de servicios de Nube deberá contar con un proceso, procedimientos y un equipo de respuesta a incidentes, que le permita detectar eventos, incidentes y ataques, monitorearlos, analizarlos, escalar a Metro, contener el daño de forma efectiva, neutralizar al atacante o vector y restaurar la integridad y disponibilidad de los sistemas y la red de manera oportuna y efectiva, para lo cual deberá contar con certificaciones adhoc a sus procesos de seguridad en cuanto a manejo de información y administración de sistemas de terceros. Esta información debe ser parte de las propuestas técnicas que debe entregar el oferente.

- La información "Confidencial" de Metro, deberá estar debidamente protegida frente a robos, mal uso y/o exposición sin autorización de Metro. La información "Confidencial" debe estar protegida de manera que solo las personas autorizadas puedan accederla, las cuales deben estar definidas explícitamente por el propietario de la información. No se debe divulgar esta información a menos que tenga la autorización correspondiente del propietario. Ejemplos de información "Confidencial" es, pero no limitada a: Informes de auditoría, Informes financieros y de contabilidad, Registros de Incidentes y evidencias, Actas y minutas de Directorio y junta de accionistas, Bases de licitación privada, Cláusulas o acuerdos de confidencialidad, Documentos legales, contratos y anexos, Notificación juzgado civil, Información de nuevos proyectos, planes estratégicos, Metodologías propietarias (desarrolladas por Metro o adquiridas para un grupo específico de trabajadores), Antecedentes personales, documentos de postulación e ingreso como trabajador, Antecedentes laborales, Antecedentes, licencias y Exámenes médicos, Certificados, Contraseñas, Contratos de trabajo, Cotización previsional, Evaluaciones de trabajadores, Información de sueldos, Proceso disciplinario, Información de clientes, Documentación disponible en web de Auto consulta, Documentación disponible en web de Rankmi, Documentación disponible en web de Exámenes preventivos.

8. Otros requerimientos.

REQ16 El proveedor de servicios deberá suministrar un espacio inicial de 60 TB y las herramientas y procedimientos de respaldo para el almacenamiento de data histórico que Metro mantiene actualmente en su Datacenter onpremise.

REQ17: La infraestructura principal para el servicio de datacenter cloud y servicios asociados deberá estar implementada en regiones del continente Americano . La solución de DR deberá estar implementado en una región distinta a la utilizada para el Datacenter principal.

REQ18 El Proveedor de servicios de nube adjudicado deberá mantener registros de los eventos (logs) de la actividad realizada sobre los sistemas por un periodo de retención mínimo de un año. Estos registros de eventos deberán estar protegidos contra escritura y acceso no autorizado. Asimismo, deberá colaborar activamente en la remediación y mitigación de los eventos o incidentes de seguridad o ciberseguridad que se relacionen con su servicio.

REQ19: Desde el inicio del proyecto, el proveedor deberá entregar los accesos con privilegios de Administrador a todas las plataformas cloud y de ciberseguridad implementadas.

REQ20: El proveedor deberá realizar traspaso de conocimiento, manuales, procedimientos, configuraciones e instructivos relacionado a los sistemas y la implementación realizada, este traspaso se realizará a personal Metro o a quien él determine.

9. Producto 2: Infraestructura nativa nube (Servidores virtuales) para sistema CVU.

REQ21 El Proponente debe considerar el suministro de los servicios IAAS para el sistema CVU, para lo cual deberá implementar 3 ambientes (Producción, QA y Desarrollo), compuesto cada uno por un número determinado de servidores, los cuales se detallan en anexo N° 4. Los servidores que componen estos ambientes deberán contar con sus respectivos sistemas operativos Windows server en su última versión soportada y motores de base de datos SQL en su última versión según la descripción de ambientes (Anexo 5). El licenciamiento para los sistemas operativos y motores de base de datos SQL deberá considerar Software Assurance y deberá ser adquiridos a nombre de Metro con una vigencia de soporte de 6 años, permitiendo mover las licencias a ambientes onpremise u otras nubes si Metro así lo requiere.

Estos servidores virtuales utilizarán las mismas capacidades de conectividad, seguridad, respaldo, soporte y monitoreo que se implementarán para el producto N°1.

REQ22 El ambiente productivo deberá ser parte del DR descrito en el producto 1.

REQ23 A esta infraestructura se aplicarán los mismos requerimientos de Ciberseguridad y seguridad de la información consignados para el producto 1.

10. Duración del contrato producto 1 y 2.

El contrato adjudicado tendrá una duración de 36 meses, desde la implementación de la infraestructura.

11. ANEXOS

11.1. Anexo N°1: Infraestructura y almacenamiento actual sistemas

El detalle de la infraestructura, consumos y almacenamiento se describe en los links de la siguiente tabla:

ID	CPUs	Memory	NICs	Disks	Provisioned MiB	OS according to the configuration file
1	4	16.384	1	1	139.374	Microsoft Windows Server 2019 Standar
2	4	12.288	1	1	114.799	Microsoft Windows Server 2008 R2 (64-bit)
3	4	8.192	1	1	161.903	Microsoft Windows Server 2012 (64-bit)
4	4	16.384	1	1	139.41	Microsoft Windows Server 2019 Standar
5	4	8.192	1	1	100.601	Microsoft Windows Server 2012 (64-bit)
6	4	8.192	2	1	264.303	Microsoft Windows Server 2012 (64-bit)
7	2	1.024	1	2	72.818	Microsoft Windows Server 2022 Standard (64-bit)
8	4	16.384	1	5	475.273	Microsoft Windows Server 2016 Standar
9	2	8.192	1	1	161.903	Microsoft Windows Server 2019 Standar
10	4	8.192	2	1	264.303	Microsoft Windows Server 2016 Standard (64-bit)
11	8	20.48	1	1	174.191	Microsoft Windows Server 2016 (64-bit)
12	4	8.128	2	8	2.993.443	Microsoft Windows Server 2022 Standard (64-bit)
13	2	8.192	2	9	1.228.912	Microsoft Windows Server 2022 Standard (64-bit)
14	4	4.08	1	1	55.391	Microsoft Windows Server 2022 Standard (64-bit)
15	1	4.096	1	1	20.6	Microsoft Windows Server 2022 Standard (64-bit)
16	2	4.096	1	2	110.805	Microsoft Windows Server 2022 Standard (64-bit)
17	4	16.384	2	11	2.924.953	Microsoft Windows Server 2022 Standard (64-bit)
18	2	12.288	1	2	94.32	Microsoft Windows Server 2012 (64-bit)
19	2	12.288	1	1	94.319	Microsoft Windows Server 2019 Standar
20	4	12.288	2	4	733.54	Microsoft Windows Server 2008 R2 (64-bit)
21	2	8.192	1	1	161.903	Microsoft Windows Server 2016 or later (64-bit)
22	4	8.192	1	1	161.903	Microsoft Windows Server 2019 Standard (64-bit)
23	16	16.384	2	23	6.867.055	Microsoft Windows Server 2012 (64-bit)
24	8	20.48	1	1	174.191	Microsoft Windows Server 2016 Standard (64-bit)
25	8	16.384	1	13	2.064.508	Microsoft Windows Server 2019 Standar (64-bit)
26	8	20.48	1	1	174.191	Microsoft Windows Server 2016 Standard (64-bit)
27	8	8.192	1	1	90.223	Microsoft Windows Server 2012 (64-bit)
28	8	8.192	1	1	90.223	Microsoft Windows Server 2012 (64-bit)
29	8	26.624	1	7	1.219.728	Microsoft Windows Server 2012 (64-bit)
30	4	6.144	1	2	139.379	Microsoft Windows Server 2012 (64-bit)

31	4	4.096	1	2	188.527	Microsoft Windows Server 2012 (64-bit)
32	2	24.1	1	11	2.702.013	Microsoft Windows Server 2012 (64-bit)
33	8	32.768	1	6	1.650.798	Microsoft Windows 8 (64-bit)
34	2	4.064	1	2	268.426	Microsoft Windows Server 2022 Standard (64-bit)
35	8	20.48	1	1	174.192	Microsoft Windows Server 2016 Standard (64-bit)
36	3	16.384	1	7	774.255	Microsoft Windows Server 2012 (64-bit)
37	4	16.384	1	12	292.845	Microsoft Windows Server 2022 Standard (64-bit)
38	2	24.576	2	7	301.189	Microsoft Windows Server 2012 (64-bit)
39	4	2.048	1	1	104.562	Microsoft Windows Server 2022 Standard (64-bit)
40	8	49.152	1	3	817.297	Microsoft Windows Server 2019 Standard (64-bit)
41	2	10.24	1	8	1.026.160	Microsoft Windows Server 2022 Standard (64-bit)
42	2	8.192	1	2	213.126	Microsoft Windows Server 2019 Standard
43	4	8.192	1	1	161.957	Microsoft Windows Server 2012 (64-bit)
44	1	4.096	2	2	77.817	Microsoft Windows Server 2003 Standard (32-bit)
45	2	3.904	2	1	38.833	Microsoft Windows 2000
46	2	4.096	2	2	157.913	Microsoft Windows Server 2003 (32-bit)
47	1	2.048	2	1	17.655	Microsoft Windows 2000 Server
48	4	8.192	1	2	284.794	Microsoft Windows Server 2016 Standard
49	2	3.072	2	3	280.451	Microsoft Windows Server 2003 Standard (32-bit)
50	2	12.288	1	2	166.058	Microsoft Windows Server 2012 (64-bit)
51	4	4.096	1	2	209.019	Microsoft Windows Server 2022 Standar
52	4	16.384	1	7	1.013.896	Microsoft Windows Server 2019 Standar
53	4	12.288	1	2	319.601	Microsoft Windows Server 2022 Standar
54	2	16.384	1	8	1.178.780	Microsoft Windows Server 2012 (64-bit)
55	6	12.288	1	1	166.264	Microsoft Windows Server 2022 Standard (64-bit)
56	4	8.192	1	1	161.95	Microsoft Windows Server 2016 Standard
57	4	20.48	1	2	264.312	Microsoft Windows Server 2016 Standard
58	4	12.288	1	2	268.439	Microsoft Windows Server 2016 Standard
59	4	16.384	2	2	272.495	Microsoft Windows Server 2022 Standar
60	4	8.192	1	1	213.145	Microsoft Windows Server 2012 (64-bit)
61	4	16.384	1	7	1.013.884	Microsoft Windows Server 2019 Standar
62	2	8.192	2	1	161.93	Microsoft Windows Server 2019 Standar
63	2	8.192	1	1	161.912	Microsoft Windows Server 2022 Standar
64	2	8.192	1	2	417.93	Microsoft Windows Server 2012 (64-bit)
65	4	8.192	1	1	213.222	Microsoft Windows Server 2012 (64-bit)
66	4	8.192	1	1	161.979	Microsoft Windows 10 (64-bit)
67	4	32.768	1	7	2.029.709	Microsoft Windows Server 2012 Standar
68	2	8.192	1	1	161.917	Microsoft Windows Server 2016 Standard
69	4	12.288	1	2	217.205	Microsoft Windows Server 2022 Standar
70	4	12.288	1	2	288.907	Microsoft Windows Server 2016 Standard
71	4	12.288	1	2	217.212	Microsoft Windows Server 2022 Standar
72	2	8.192	1	1	161.943	Microsoft Windows Server 2016 Standar
73	2	6.144	1	1	190.615	Microsoft Windows Server 2008 R2 Standar
74	4	8.192	2	1	264.377	Microsoft Windows Server 2012 (64-bit)
75	4	12.288	2	2	217.216	Microsoft Windows Server 2022 Standar
76	2	8.192	1	1	213.178	Microsoft Windows Server 2016 Standard
77	2	6.144	1	1	159.953	Microsoft Windows 10 (64-bit)
78	4	16.384	1	4	477.32	Microsoft Windows Server 2016 Standard
79	16	14.336	1	2	526.516	Microsoft Windows Server 2012 (64-bit)
80	4	12.288	3	2	268.429	Microsoft Windows Server 2016 Standard
81	4	12.288	1	2	217.203	Microsoft Windows Server 2022 Standar
82	4	12.288	1	2	204.936	Microsoft Windows Server 2016 Standard
83	4	12.288	1	2	268.411	Microsoft Windows Server 2022 Standar
84	2	8.192	1	8	1.065.393	Microsoft Windows Server 2022 Standard (64-bit)
85	2	8.192	1	1	90.222	Microsoft Windows Server 2022 Standar
86	10	10.24	2	4	1.157.263	Microsoft Windows Server 2012 (64-bit)
87	2	4.032	1	1	266.31	Microsoft Windows Server 2008 R2 (64-bit)
88	2	12.288	1	2	166.057	Microsoft Windows Server 2012 (64-bit)
89	4	12.288	1	2	268.423	Microsoft Windows Server 2016 Standard
90	8	16.384	2	38	11.290.735	Microsoft Windows Server 2012 (64-bit)
91	4	8.192	1	2	284.806	Microsoft Windows Server 2016 Standard
92	4	8.192	1	2	315.52	Microsoft Windows Server 2008 (64-bit)

93	12	24.576	1	4	403.589	Microsoft Windows Server 2012 (64-bit)
94	4	8.192	1	2	192.629	Microsoft Windows Server 2008 R2 (64-bit)
95	2	3.072	1	2	95.469	Microsoft Windows 7 (32-bit)
96	6	8.192	3	7	1.442.046	Microsoft Windows Server 2008 (64-bit)
97	4	6.144	2	2	272.586	Microsoft Windows Server 2008 (32-bit)
98	8	12.288	1	3	913.604	Microsoft Windows Server 2012 (64-bit)
99	2	4.096	1	2	1.313.740	Microsoft Windows Server 2008 R2 (64-bit)
100	2	3.944	1	2	203.796	Microsoft Windows 7 (64-bit)
101	4	4.096	1	2	321.673	Microsoft Windows Server 2012 (64-bit)
102	4	8.192	1	2	377.026	Microsoft Windows Server 2012 (64-bit)
103	8	24.576	1	4	653.443	Microsoft Windows Server 2008 Enterprise
104	8	24.576	1	4	215.178	Microsoft Windows Server 2008 Enterprice (64-bit)
105	4	12.288	2	5	1.149.149	Microsoft Windows Server 2003 (32-bit)
106	2	8.192	2	1	110.825	Microsoft Windows Server 2012 (64-bit)
107	2	4.096	1	2	106.67	Microsoft Windows Server 2008 R2 (64-bit)
108	2	8.192	2	8	2.496.666	Microsoft Windows Server 2012 (64-bit)
109	4	4.032	2	1	86.113	Microsoft Windows Server 2008 R2 (64-bit)
110	2	4.096	1	2	106.638	Microsoft Windows Server 2008 Enterprise
111	2	1.024	1	1	75.364	Microsoft Windows Server 2022 Standard (64-bit)
112	4	8.192	1	2	264.39	Microsoft Windows Server 2008 (64-bit)
113	4	4.096	1	3	440.446	Microsoft Windows Server 2012 (64-bit)
114	2	4.096	2	2	376.374	Microsoft Windows Server 2012 (64-bit)
115	2	12.288	1	5	1.333.383	Microsoft Windows Server 2012 (64-bit)
116	4	12.288	1	2	288.888	Microsoft Windows Server 2016 Standard
117	2	16.384	1	1	221.329	Microsoft Windows Server 2012 (64-bit)
118	2	8.192	1	3	745.598	Microsoft Windows Server 2012 (64-bit)
119	4	16.384	1	4	477.31	Microsoft Windows Server 2016 Standard
120	2	8.192	1	1	161.918	Microsoft Windows Server 2016 or later (64-bit)
121	4	12.288	1	1	166.102	Microsoft Windows Server 2016 or later (64-bit)
122	6	24.576	1	2	239.933	Microsoft Windows Server 2012 (64-bit)
123	4	6.144	1	2	313.532	Microsoft Windows Server 2012 (64-bit)
124	2	12.288	1	1	114.802	Microsoft Windows Server 2012 (64-bit)
125	2	12.288	1	1	114.883	Microsoft Windows Server 2012 (64-bit)
126	4	12.288	1	2	370.835	Microsoft Windows Server 2022 Standard (64-bit)
127	2	10.24	1	12	245.746	Microsoft Windows Server 2022 Standard (64-bit)
128	2	16.384	1	3	753.858	Microsoft Windows Server 2012 (64-bit)
129	2	8.192	1	2	59.897	Microsoft Windows Server 2012 (64-bit)
130	2	8.192	1	1	162.002	Microsoft Windows Server 2016 or later (64-bit)

11.2. Anexo N°2: Indicadores de desempeño y calidad de servicio

A continuación, en documento adjunto se describen los indicadores en base a los cuales se medirá el desempeño y calidad en la prestación de los servicios contratados.

INDICADOR	SLA
Disponibilidad del ambiente de Producción	El ambiente productivo deberá tener una disponibilidad del 99,97% Anual
Disponibilidad del ambiente de Pruebas (QA y Desarrollo)	El servicio en ambiente QA y Desarrollo deberá tener una disponibilidad del 99,94% mensual

11.3. Anexo N°3: Maquinas en modalidad DR.

VM	Powerstate	CPUs	Memory	NICs	Disks	Capacidad Disco	OS according to the VMware Tools	SQL
1	poweredOn	4	12	1	2	256	M. Windows Server 2016 or later (64-bit)	
2	poweredOn	4	20	1	2	256	M. Windows Server 2016 or later (64-bit)	
3	poweredOn	4	8	1	1	256	M. Windows Server 2012 (64-bit)	
4	poweredOn	2	8	2	1	153	M. Windows Server 2016 or later (64-bit)	
5	poweredOn	4	8	1	1	204	M. Windows Server 2012 (64-bit)	
6	poweredOn	4	12	1	2	276	M. Windows Server 2016 or later (64-bit)	
7	poweredOn	4	8	1	2	204	M. Windows Server 2016 or later (64-bit)	
8	poweredOn	4	12	1	2	256	M. Windows Server 2016 or later (64-bit)	
9	poweredOn	4	12	1	2	204	M. Windows Server 2016 or later (64-bit)	
10	poweredOn	2	12	1	2	153	M. Windows Server 2012 (64-bit)	
11	poweredOn	4	12	1	2	256	M. Windows Server 2016 or later (64-bit)	
12	poweredOn	4	6	2	2	266	M. Windows Server 2008 (32-bit)	
13	poweredOn	4	4	1	2	317	M. Windows Server 2012 (64-bit)	
14	poweredOn	4	12	2	5	1.136	M. Windows Server 2003 (32-bit)	
15	poweredOn	2	8	2	1	102.	M. Windows Server 2012 (64-bit)	
16	poweredOn	4	4	2	1	81	M. Windows Server 2008 R2 (64-bit)	
17	poweredOn	2	16	1	1	204	M. Windows Server 2012 (64-bit)	
18	poweredOn	2	12	1	1	102	M. Windows Server 2012 (64-bit)	
19	poweredOn	4	16	1	1	122	M. Windows Server 2016 or later (64-bit)	
20	poweredOn	4	8	1	1	153	M. Windows Server 2012 (64-bit)	
21	poweredOn	4	16	1	1	122	M. Windows Server 2016 or later (64-bit)	
22	poweredOn	2	8	1	1	153	M. Windows Server 2016 or later (64-bit)	
23	poweredOn	2	8	1	1	153	M. Windows Server 2016 or later (64-bit)	
24	poweredOn	4	8	1	1	153	M. Windows Server 2016 or later (64-bit)	
25	poweredOn	4	6	1	2	133	M. Windows Server 2012 (64-bit)	
26	poweredOn	2	24	1	10	2.370	M. Windows Server 2012 (64-bit)	
27	poweredOn	2	24	2	7	276	M. Windows Server 2012 (64-bit)	
28	APP	4	16	2	1	1024	M. Windows Server última versión soportada(64-bit)	
29	BD	8	32	2	1	6144	M. Windows Server última versión soportada(64-bit)	SI
30	Integrador	4	16	2	1	1024	M. Windows Server última versión soportada(64-bit)	SI
31	ETL	4	16	2	1	512	M. Windows Server última versión soportada(64-bit)	

1.1.Anexo N°4: Motores de Base de datos SQL Para el Producto 1

ID	MOTOR DE BASE DATOS	Ent / Std
1	SQL Server 2000	Microsoft SQL Server Standard Edition
2	SQL Server 2008 R2	Microsoft SQL Server 2008 (RTM)
3	SQL Server 2016	Microsoft SQL Server Enterprise: Core-based Licensing (64-bit)
4	SQL Server 2012	Microsoft SQL Server Enterprise Edition (64-bit)
5	SQL Server 2008 R2	Microsoft SQL Server Enterprise Edition (64-bit)
6	SQL Server 2012 R2	SQL Server 2012 R2
7	SQL Server 2016	Microsoft SQL Server Enterprise: Core-based Licensing (64-bit)
8	SQL Server 2008 SP4	Microsoft SQL Server 2008 (SP4)
9	SQL Server 2016	Microsoft SQL Server Enterprise: Core-based Licensing (64-bit)
10	SQL Server 2008 SP4	Microsoft SQL Server 2008 (SP4)

1.2.Anexo N°5: Infraestructura y almacenamiento Sistemas CVU

			Servidor			
Ambiente	Servicio	Cantidad de Core	RAM	Disco	Sistema operativo	Motor de BD
Producción	APP	4	16	1 TB	Windows Server	N/A
	BD	8	32	6 TB	Windows Server	SQL Server Enterprise
	Integrador	4	16	1 TB	Windows Server	SQL Server Estándar
	ETL	4	16	512 GB	Windows Server	N/A
QA	APP	4	16	1 TB	Windows Server	N/A
	BD	4	32	6 TB	Windows Server	SQL Server Estándar
	Integrador	4	16	1 TB	Windows Server	SQL Server Estándar
	ETL	4	16	512 GB	Windows Server	N/A
Desarrollo	APP	4	16	1 TB	Windows Server	N/A
	BD	4	32	6 TB	Windows Server	SQL Server Estándar
	Integrador	4	16	1 TB	Windows Server	SQL Server Estándar.
	ETL	4	16	512 GB	Windows Server	N/A

1.1.Anexo N°6: Licenciamiento SQL para el sistema Sistemas CVU

Tipo	Cantidad	Versión	Soporte
SQL Server Enterprise + SA	1	Última versión disponible	A 6 años
SQL Server Estándar + SA	5	Última versión disponible	A 6 años