PREVIRED

ES HACERLO FÁCIL, RÁPIDO Y BIEN

LICITACIÓN PRIVADA DE SERVICIOS OUTSOURCING DE TI Y DATACENTER

Bases Técnicas

26/05/2023

Índice de Contenidos

Introducción 8

Glosario 11

1. Antecedentes 12

1.1 Misión y Visión de Previred 12

1.2 Propósito de la Licitación 12

1.3 Servicios que el área de TI provee a la organización 12

1.4 Estructura organizacional áreas de Negocio 13

1.5 Principales Servicios por líneas de negocios 13

2 Situación actual 14

2.1 Servicios de Data Center 14

2.2 Licencias 15

2.3 Sistemas Operativos, Motores de Datos, Storage y Otros 15

2.4 Infraestructura de Servidores On-premises y Cloud 17

2.5 Infraestructura máquinas virtuales y base de datos Productivas 17

2.6 Infraestructura máquinas virtuales Contingencia 20

2.7 Características Storage Productivo y de Contingencia 20

2.8 Infraestructura máquinas virtuales y de Base de Datos de Preproducción 21

2.9 Características Storage Preproductivo Cloud. 22

2.10 Red de Datos, Comunicaciones y Seguridad actuales 23

2.11 Servicio de Monitoreo 25

2.12 Software Base utilizado por PREVIRED 26

3 Requerimiento de la licitación 28

3.1 Visión del servicio 28

3.2 Administración del Servicio 28

3.3 Comité Ejecutivo y Operativo 29

3.4 Servicio de Datacenter 29

3.5 Propuesta para llevar servicios a la Cloud en el futuro. 30

3.6 Infraestructura para Servidores, Bases de Datos y Storage 30

3.7 Infraestructura y crecimiento de Producción y Contingencia 31

3.8 Infraestructura y crecimiento de Preproducción 31

3.9 Housing equipamiento de terceros o PREVIRED 31

3.10 Migración de Servicios 32
3.11 Plazos de Implementación y Pruebas 33
3.12 Migración de Cintas Históricas 33
3.13 Provisión de Servicio de Dominio 33
3.13.1 Servicio dominio y DNS para usuarios internos 33
3.13.2 Servicio de dominio y DNS para servidores 33
3.14 Servicio de Sincronización de hora 34
3.15 Servicio de Antivirus 34
3.16 Servicio de parchado de seguridad de la plataforma 34
3.17 Inventario y capacidades de equipos 35
3.18 Escritorios Virtuales 36
3.19 Mesa de Ayuda Técnica 24x7 37
3.20 Soporte y Mantención Preventiva y Correctiva Hardware 39
3.21 Renovación Tecnológica 39
3.22 Operación, Mantención y Soporte del Software Base 39
3.22.1 Operación de servicio 39
3.22.2 Mantención de equipos 40
3.23 Licencia, garantías, suscripciones 40
3.24 Cobertura horaria Servicios de Ingeniería 40
3.25 Servicios 24x7 41
3.26 Horas para trabajos programados adicionales de Consultoría 41
3.27 Servicio de Ingeniería de Sistemas 41
3.28 Servicios de Administración de Base de Datos 44
3.29 Servicio de Ingeniería DevOps 46
3.30 Servicio de Administración de Redes y Seguridad 48
3.31 Servicios Internos y de Colaboración 49
3.32 Administración de otros Servicios de Capa Media Críticos 50
3.33 Servicio de Administración de Colas de Mensajería 51
3.33.1 Servicio de Administración de RedHat AMQ Broker 51
3.33.2 Servicio de Administración de WebSphere MQ 52
3.34 Gestión de los Pasos a Producción 53
3.35 Servicios Adicionales 54
3.35.1 Servicio de administración de contraseñas y claves maestras, desbloqueo de claves para los dominios de Previred 54

3.35.2 Servicio de Relay de Correo. 54
3.35.3 Envío de Email para campañas de Marketing 55
3.36 Responsabilidad del Software Aplicativo 56
3.37 Servicios de Respaldo, Retención y Recuperación 56
3.38 Estudio de la Capacidad y Rendimiento 58
3.39 Licencias de Software 59
3.40 Seguridad de la Información y Ciberseguridad 60
3.40.1 Requerimiento de Certificación en Seguridad 60
3.40.2 Servicios Base de seguridad 63
3.40.3 Servicios Adicionales de Seguridad 64
3.41 Requerimientos de Auditoria 66
3.41.1 Requisitos relacionados con estándares de auditoría 66
3.41.2 Inspecciones o auditorias por parte de PREVIRED 66
3.42 Continuidad de Negocio 67
3.42.1 Site secundario y/o contingencia 67
3.42.2 Planes de Contingencia y Restauración de servicios 69
3.43 Servicio de Monitoreo y Observabilidad 70
3.43.1 Monitoreo de servicios transversal 73
3.43.2 Monitoreo transaccional Atentus 73
3.44 Red de Datos, Comunicaciones y Seguridad 74
3.44.1 Requerimientos de comunicaciones 75
3.44.2 Servicio de Acceso a Internet 77
3.44.3 RED WAN de las AFP Y SUPEN 77
3.44.4 Conexión a Red WAN Terceros 80
3.44.5 Monitoreo de Redes 81
3.44.6 Concentrador VPN 81
3.44.7 Capa Balanceadores 82
3.44.8 WAF 82
3.44.9 Anti DDOS / Ataques Volumétricos 83
3.44.10 IPS 83
3.44.11 DNS Público 84
3.44.12 Conectividad con Redbanc 84
3.44.13 Red LAN Oficina 85

3.44.14 Servicio Internet Oficina....85
3.44.15 VPN para trabajo Remoto....86
3.44.16 WIFI Oficina....86
3.44.17Seguridad para Acceso Internet usuarios Oficina Previred o Escritorios Virtuales....87
3.44.17.1 Filtro de Contenido o Tecnología de última generación que permita:....87
3.45 Enlaces de Datos....89
3.45.1 Enlaces contratados por Data Center Kyndryl para servicio WAN....89
3.45.2 Enlaces para interconexión Oficina – Data Center....90
3.44.3 Enlaces exclusivos para interconexión Data Center primario y secundario, enlaces de fibra en HA 90
3.44.4 Enlaces Internet Negocio contratados por Data Center Kyndryl....90
3.44.5 Enlaces contratados por Previred....91
4 Requerimientos de Informes de Gestión....92
4.1 Informes de Eventos No Programados....92
4.2 Informes de Eventos Programados....92
4.3 Informes de Eventos Acceso al Data Center....93
4.4 Informes de Respaldos....94
4.4.1 Informe semanal del estado del proceso de respaldo.....94
4.4.2 Informe con detalle de los backups/restore de las BDs....94
4.4.3 Informe con detalle de todos los Backup realizados en el mes....95
4.4.4 Informe con tasa de éxito/falla de los respaldos diarios.....95
4.5 Informe de Modificación de Ambientes....96
4.5.1 Informe de Versionamiento a nivel de firmware de la plataforma....97
4.5.2 Informe de Inventario de Hardware....97
4.5.3 Informe de Seguridad....97
4.5.4 Informe de Gestión Mensual....98
5 Niveles de Servicios....99
5.1 Niveles de servicio asociados a Site Productivo....99
5.2 Indicadores niveles de servicio....101
5.3 Niveles de servicio definidos para servicios asociados a Data Center productivo y para Red de Datos y Comunicaciones....101
5.4 Niveles de servicio centro de procesamiento alterno....105
5.5 Niveles de servicio definidos para servicios adicionales (Servicio de administración de contraseñas y claves maestras, desbloqueo de claves y Escritorios Virtuales):....107

6 Multas 108
6.1 Multas definidas por incumplimiento de servicios asociados a Data Center productivos, red de datos y comunicaciones en Data Center productivo y alterno 108
6.1.1 UPTIME 108
6.1.2 Requerimientos 109
6.1.3 Máquinas virtuales 109
6.1.4 Respaldos 109
6.1.5 Informes 109
6.1.6 Calidad del Servicio 110
6.1.7 Aplicación Controles de Cambio 110
6.1.8 Cumplimiento de proyectos 111
6.2 Multas definidas para incumplimientos centro de procesamiento alterno 111
7 Tabla de Precios 113
7.1 Se entiende por Servicio BASE los ítems siguientes: 113
7.2 Formato de Entrega Oferta Económica 113
7.3 Crecimiento a Demanda 115
7.4 Bajas de Servicios o Máquinas 119
8 Anexos 120
8.1 Anexo de requerimientos físicos y ambientales del Data Center 120
8.2 Anexo de listado de servidores ambientes Producción, Preproducción y Contingencia 120
8.3 Anexo de licencias propiedad de Previred 120
8.4 Anexo de fichas de diagramas de servicio 120
8.5 Anexo de procedimientos de respaldo, retención y recuperación de la información 120
8.6 Anexo de consideraciones para la arquitectura servidores de base de datos 120
8.7 Anexo de templates utilizados para la solicitud de creación de máquinas virtuales 121
8.8 Anexo del protocolo de aceptación de los servicios 121
8.9 Anexo de grupos de migración según etapas de migración definidos (ETM) 121
8.10 Anexo de Inventario Base, matriz de software 121
8.11 Anexo de Inventario de comunicaciones 121

Índice de Ilustraciones

Ilustración 1: Imagen Referencial Arquitectura Host VMWare 17
Ilustración 2: Imagen referencial Arquitectura base de datos Mssql Always On. 18
Ilustración 3: Imagen referencial Arquitectura base de datos Oracle RAC. 19
Ilustración 4: Arquitectura referencial de Contingencia. 21
Ilustración 5: Arquitectura general de Preproducción. 23
Ilustración 6: Diagrama red de comunicaciones actual 25
Ilustración 7: Ejemplos de Monitoreos 26
Ilustración 8: Flujo actual de solicitudes de servicio (incidentes/requerimientos) 37
Ilustración 9: Diagrama de Conectividad Arquitectura de Réplica de Contingencia 68
Ilustración 10: Ejemplos de Monitoreos 71
Ilustración 11: Diagrama Simple de Red Actual 75
Ilustración 12: WAN AFP: Situación Actual 79
Ilustración 13: Plano oficina PREVIRED y zonas de cobertura WIFI (Referencial) 87

Introducción

El 12 de mayo del año 2000 nace Previred, con la visión de convertirse en un socio estratégico del sistema de seguridad social chileno.

Constituida formalmente como "Pago Electrónico Previsional S.A.", el primer desafío de la compañía fue ayudar a las Administradoras de Fondos de Pensiones y a terceros, mediante la prestación de servicios operacionales e informáticos de calidad, que permitieran hacer más ágil y eficientes los procesos y procedimientos, tanto para las instituciones como para las personas.

Debido al positivo impacto que rápidamente generaron sus productos y servicios, Previred comenzó a desarrollar nuevas soluciones para toda la industria previsional, a saber: Isapres, Cajas de Compensación de Asignación Familiar, Mutualidades de Empleadores y diversas instituciones públicas a través de soluciones que se destacan por ser innovadoras, seguras y de calidad.

De esta manera, y hasta el día de hoy, Previred ha ampliado su alcance, fortaleciendo su rol como socio estratégico del sistema de seguridad social, mediante la creación sostenida de valor para clientes, trabajadores, accionistas y la comunidad.

En la actualidad Previred posee un destacado rol a nivel país en lo que a materia de recaudación de cotizaciones previsionales se refiere, debiendo al respecto mencionar el gran volumen de transacciones en el servicio de recaudación, administrando un porfolio de más de 70 servicios del ámbito previsional, con diferentes niveles de criticidad, no sólo por el volumen de los procesos, sino por las exigencias normativas que deben cumplirse y la dependencia de éstos con otros servicios de impacto a nivel nacional.

Los principales servicios otorgados son: Sitio Recaudación www.previred.com, Sitio Servicio de Certificados de Cotizaciones (InfoCotizaciones), Servicios de Clave Única para AFP (SACU), Servicio de Notificaciones a Empleadores, Portal AFP (CAPRI), Centro de Movimiento Histórico AFP (CMH), Traspaso Web, Preguntas Previsionales, Registro Histórico APV y APVC (RHAPVC), Aclaración y Notificación de Morosos Presuntos (DNPA), STI, Servicios de Gestión de Cobranza, entre otros.

Previred gestiona la seguridad basada en el cumplimiento de la Norma de Seguridad ISO 27001 y de Continuidad Operativa ISO 22301, de forma de garantizar la confidencialidad, integridad y disponibilidad de la información, como también la Continuidad Operativa. Respecto al riesgo operacional, controla y audita sus procesos sobre la base del Estándar AT801 Tipo II y AT-205 Tipo II. Adicionalmente es auditada en distintos aspectos anualmente por consultoras externas: Auditoría de Estados Financieros, Evaluación de Riesgos, Auditoría de TI, y Assesment de Seguridad según ISO 27002.

El propósito de esta licitación es contar con un socio de alto nivel de infraestructura de Data Center y servicios de plataformas tecnológicas, los cuales permitan cumplir los objetivos estratégicos de la compañía, obteniendo altísimos niveles de continuidad operativa, entregarnos una seguridad y ciberseguridad tecnológica que logre protegernos de cualquier tipo de ciberataques, proveernos una excelente observabilidad que permita anticipar y resolver degradaciones o fallas en toda la trazabilidad de los servicios y así lograr entregar el más alto nivel de uptime, SLA y disponibilidad de servicios a los usuarios e instituciones.

En segunda prioridad, contar con una plataforma de infraestructura preproductiva que permita a la compañía el desarrollo óptimo de productos y sus evoluciones, con una infraestructura ágil, robusta, elástica y segura que apoye todo el desarrollo de servicios.

Para ello, buscamos un oferente que pueda brindarnos servicios de data center con un enfoque en la transformación digital, garantizando una alta disponibilidad y escalabilidad de nuestra plataforma en línea, para ofrecer un mejor servicio a nuestros clientes. Asimismo, nos interesa que el oferente cuente con sólidas políticas de seguridad y ciberseguridad, para garantizar la integridad y confidencialidad de la información que se maneja en nuestra plataforma. Un oferente que tenga experiencia y conocimientos en el diseño, implementación y gestión de infraestructuras de data center, y que pueda ofrecernos soluciones innovadoras y eficientes que cumplan con nuestros requerimientos específicos, tales como:

- Escalabilidad: nuestra plataforma está diseñada para manejar grandes cantidades de datos y usuarios, por lo que requerimos del oferente un estándar transaccional de gran capacidad.
- Rendimiento: nuestra plataforma proporciona un alto rendimiento y disponibilidad, garantizando ello, la continuidad operativa de sus procesos y servicios.
- Seguridad: nuestra plataforma cuenta con medidas de seguridad robustas para proteger los datos que a causa de su labor procesa y/o trata, asegurando la disponibilidad, confidencialidad e integridad de la información.
- Integración: nuestra plataforma puede integrarse fácilmente con otros sistemas y aplicaciones, permitiendo una gestión más eficiente y automatizada de los procesos de negocios.
- Observabilidad: nuestros servicios requieren de una óptica transversal, siendo el monitoreo continuo y sistemático, un pilar fundamental de cara a los usuarios e instituciones.

El objetivo fundamental para Previred es que, a través de este servicio, se asegure la continuidad operacional de sus sistemas y la seguridad, proporcionando una adecuada gestión de la calidad de sus servicios, aumentando la eficiencia de sus procesos de negocio, alineando dichos procesos e infraestructura TI y reduciendo los riesgos asociados a su actividad, con un contrato que cuente con niveles de servicio acorde a la dinámica y exigencia del negocio.

Para cumplir con los objetivos planteados Previred considera fundamental la experiencia, metodología, calidad y compromiso del recurso humano del oferente, de manera de contar y ser avalado por un socio tecnológico capaz de enfrentar las diversas problemáticas que puedan presentarse en la ejecución de sus actividades.

- El servicio requerido por parte de Previred incluye, en grandes líneas: Plataforma On Premises para servicios de negocio productivos.
- Outsoursing Operación y administración de plataforma productiva.
- Plataforma Cloud en distintas nubes públicas, y modalidades IaaS, PaaS, SaaS. Para servicios de colaboración, y ambientes preproductivos.
- Plataforma de comunicaciones y seguridad
- Soporte de especialistas para infraestructura, telecomunicaciones y seguridad.
- Mesa de Ayuda y Soporte
- Servicio de Observabilidad en toda la plataforma.
- SOC de Seguridad y Servicio de ciberseguridad.

Los servicios de infraestructura y servicios a prestar por parte del Oferente deberán abarcar todos los ambientes existentes en Previred, tales como:

- Producción.
- Preproducción, este ambiente contempla Desarrollo, Calidad, Staging y ambiente de servicios transversales
- Openshift 4.11 (actual) o en su defecto N-1.
- Contenedores y microservicios desplegados.
- Servicios de seguridad y Ciberseguridad
- Dominios de acceso (Active Directory, LDAP, SSO)
- Cualquier otro entorno que PREVIRED pueda requerir a futuro.

Dada la criticidad de los servicios otorgados por Previred y atendida la normativa aplicable en la materia, es requerimiento contar con un Plan de Continuidad de Negocios y un Plan de Recuperación de Desastres, de los que Previred dispone en la actualidad y respecto de los cuales el oferente debe estar alineado bajo esta directriz.

Glosario

- **Plataforma On Premises:** Infraestructura TI en Data Center local.
- **Plataforma Cloud**: Infraestructura TI en Data Center del tipo nubes públicas o privada
- **Modalidad de Servicios**: IaaS, PaaS, SaaS.
- **Ambiente Productivo:** Infraestructura y servicios necesarios para la operación de los sistemas y aplicaciones explotados por el usuario final.
- **Ambiente Preproductivo:** Infraestructura y servicios necesarios para el proceso de Desarrollo. Dividido en ambientes intermedios como (Dev/Calidad/Staging, etc.)
- **Mesa de Ayuda:** Sistema tecnológico que ayuda a los equipos de atención al cliente a recibir, administrar, organizar, automatizar, responder e informar sobre las preguntas o problemas.
- **Observabilidad:** Proceso mediante el cual se detecta, visualizan y priorizan acciones ante problemas para mejorar la experiencia del usuario final, mientras se administra la eficiencia operativa.
- **POD Team :** Equipo dedicado para Previred.
- **Hardening:** Medidas de seguridad sobre los equipos de trabajo
- **EOL:** Se refiere a cuando caduca el soporte del oferente en cuestión "End of Life"

1. Antecedentes

1.1 Misión y Visión de Previred

Como contexto general, el objetivo principal de esta licitación es permitir a Previred cumplir a cabalidad su misión y visión:

Misión: Brindar servicios en el ámbito de la Seguridad Social, mediante soluciones innovadoras, seguras y de calidad, reconociendo el impacto social de nuestra labor y asegurando la creación de valor para nuestros clientes, trabajadores, accionistas y la comunidad.

Visión: Ser el socio estratégico más ágil y eficiente del Sistema de Seguridad Social. Otorgando, más y mejores servicios a los trabajadores, empleadores e instituciones que lo componen.

1.2 Propósito de la Licitación

El propósito de esta licitación es contar con un socio de alto nivel de infraestructura de Data Center y servicios de plataformas tecnológicas, los cuales permitan cumplir los objetivos estratégicos de la compañía, obteniendo altísimos niveles de continuidad operativa, entregarnos una seguridad y ciberseguridad tecnológica que logre protegernos de cualquier tipo de ciberataques, proveernos una excelente observabilidad que permita anticipar y resolver degradaciones o fallas en toda la trazabilidad de los servicios y así lograr entregar el más alto nivel de uptime, SLA y disponibilidad de servicios a los usuarios e instituciones.

En segunda prioridad, contar con una plataforma de infraestructura preproductiva que permita a la compañía el desarrollo óptimo de productos y sus evoluciones, con una infraestructura ágil, robusta, elástica y segura que apoye todo el desarrollo de servicios.

1.3 Servicios que el área de TI provee a la organización

La Gerencia de Tecnología es la responsable del desarrollo y la administración de todos los servicios de Previred, esta gerencia está compuesta por un área de Desarrollo y Mantención de aplicaciones, Control de Calidad y Testing, Arquitectura y Gestión de Datos y de la Subgerencia de Sistemas, esta última, es la responsable de la gestión y administración de toda la plataforma de infraestructura tecnológica de la compañía.

Actualmente, Previred tiene definido los servicios, tanto en Data Center propios como en entornos de Cloud Privada (Ambiente de PreProducción) y Cloud Públicas (que no es parte del alcance de esta RFP), los servicios solicitados incluyen la administración de las infraestructuras instaladas en el Data Center y Cloud Privada.

Todos los servicios son proporcionados internamente por el área de TI de Previred, contando con los soportes nivel 3 de los fabricantes.

1.4 Estructura organizacional áreas de Negocio

Previred administra y gestiona 5 líneas de negocio actualmente:

1) Recaudación
2) Certificados
3) Notificación
4) Apoyo al Giro
5) Gestión de Cobranzas

La Gerencia de Tecnología provee a cada línea de negocio: Desarrollo y Mantención de aplicaciones, Especialistas Devops, Analistas de Control de Calidad y Testing, Arquitecturas (Infraestructura, Software y de Datos), Gestión de Datos y BI, Administración de los Sistemas en ambientes PreProductivos, Productivos y Contingencia.

1.5 Principales Servicios por líneas de negocios

La distribución de servicios por cada línea de negocio es la siguiente:

1) Recaudación
    I. Sitio Publico PREVIRED.com
    II. Sitio Privado PREVIRED.com
    III. BackOffice recaudación
    IV. Plataforma de Pagos MQSeries
    V. Procesos rendición y publicación Batch C
    VI. Demonios Batch Java
    VII. Granja de Pagos
    VIII. Granja Integración
    IX. Granja Servicios
    X. Granja de Servicios/Integración
    XI. UNIRED, consulta DT
    XII. Workload Automation (CAWA)
    XIII. Preguntas Previsionales
    XIV. Recaudación Previred (REC en AFP)
    XV. SFTP
    XVI. SICOP
    XVII. Api Login
    XVIII. Preguntas Previsionales
    XIX. Botón embebido Previred
    XX. Ejecutor de Procesos REC

2) Certificados
    I. Servicio de información de cotizaciones - Infocotizaciones
    II. Control contratistas

3) Notificación
    I. Notificación OT

II. Notificación Funes
III. Notificador PREVIRED

4) Apoyo al Giro
I. Servicio autenticación clave única Afiliados AFP – SACU AFP
II. Servicio autenticación clave única Beneficiarios AFP – SACU Beneficiario
III. Servicio autenticación clave única Afiliados AFC – SACU AFC
IV. Centro de movimientos Histórico – CMH
V. CMH Cotizaciones
VI. Traspaso Web AFP
VII. Bloqueo TWEB AFP
VIII. TVI
IX. CAPRI
X. Fidelización
XI. Groot
XII. SFTP
XIII. SIDEP
XIV. RHAPVC
XV. CONPAG
XVI. SVI
XVII. STI
XVIII. SAGCOM 1.0, 1.5
XIX. Pilar Solidario
XX. Formularios Retiro 10% y Retiro Extranjero.
XXI. Subtrab – SEJ
XXII. Ejecutor de Procesos BEST
XXIII. Compin
XXIV. WS Dirección del trabajo
XXV. Servicio Rezagos

5) Gestión de Cobranzas
I. Gestión DNPA
II. Aclaración, regularización e interposición de DNP
III. Ejecutor de Procesos

Para mayor detalle ver anexo 4. Fichas Diagramas de servicios.

2 Situación actual

2.1 Servicios de Data Center

Los servicios de Previred operan sobre un único contrato con nuestro actual proveedor de Servicios Kyndryl, los servicios productivos son entregados desde el data center principal y contamos con servicios de Data Center Contingencia.

Los servicios para ambientes preproductivos son entregados desde la nube privada de IBM Cloud en EEUU (Dallas).

Datacenter	Dirección	Ambientes-Servicios
San Bernardo	Av Puerta Sur #03320, San Bernardo	Ambientes Productivos, Backbone de comunicaciones, balanceo y seguridad (Activo).
Providencia	Av. Providencia #655, Providencia	Site de contingencia, Backbone de comunicacioones, balanceo y seguridad (Activo) para los servicios: Recaudación, infocotizaciones, control contratistas, CMH, SACU, Traspaso WEB, interposición de demandas, SAGCOM, Openshift, entre otros
CLOUD IBM-Dallas	EEUU	Ambientes PreProductivos

2.2 Licencias

Previred pone a disposición del oferente todas las licencias que son su propiedad, pero que no cubren el 100% de las necesidades actuales, para cubrir la diferencia, el oferente deberá proponer en modalidad servicio las licencias faltantes.

Ver detalle "Anexo N°3 Licencias propiedad PREVIRED"

2.3 Sistemas Operativos, Motores de Datos, Storage y Otros

Previred utiliza los siguientes productos para su operación general:

- Sistemas Operativos
    - Red Hat Enterprise Linux
    - Windows Server
    - Openshift
    - AIX
    - Windows 11
    - Citrix

- Motores de bases de datos utilizados

- Oracle RAC - Enterprise
- Microsoft SQL Server AON – Enterprise y Standard
- PostgreSQL
- MySQL
- MongoDB
- MariaDB (Galera-Wordpress)
- REDIS

Para mayor detalle ver anexo: "Anexo N° 10 Inventario BASE - Matriz Software"

- Equipos de comunicaciones y seguridad

  Para mayor detalle ver anexo: "Anexo N° 11 Inventario Comunicaciones Seguridad"

  - Equipos físicos de terceros o PREVIRED en operación actual.Guardium, herramienta de firewall de bases de datos, administrada por Neosecure.
  - Fortigate: Equipos para trabajo remoto (2U)

Todo lo descrito en este punto se encuentra detallado en Anexos "Anexo N° 10 Inventario BASE - Matriz Software", "Anexo N° 11 Inventario Comunicaciones Seguridad" y "Anexo N° 2 Listado Servidores"

2.4 Infraestructura de Servidores On-premises y Cloud

PREVIRED tiene en la actualidad 6 plataformas para cubrir la demanda de los ambientes:

- Plataforma ON-Premise para todos los servicios productivos, con infraestructura dedicada.
- IBM-Cloud para ambientes preproductivos.
- Citrix, para escritorios virtuales y servicios RPA.
- Openshift On-premise para ambientes productivos.
- Openshift Cloud para ambiente preproducción
- Plataforma de Contingencia On-premise en Data Center secundario

2.5 Infraestructura máquinas virtuales y base de datos Productivas

La Infraestructura actual esta implementada sobre VMware 7.X en equipos físicos dedicados, replicados con site de contingencia, ver imagen 1, para alojar máquinas virtuales con sistemas operativos RedHat Enterprise y Windows Server.

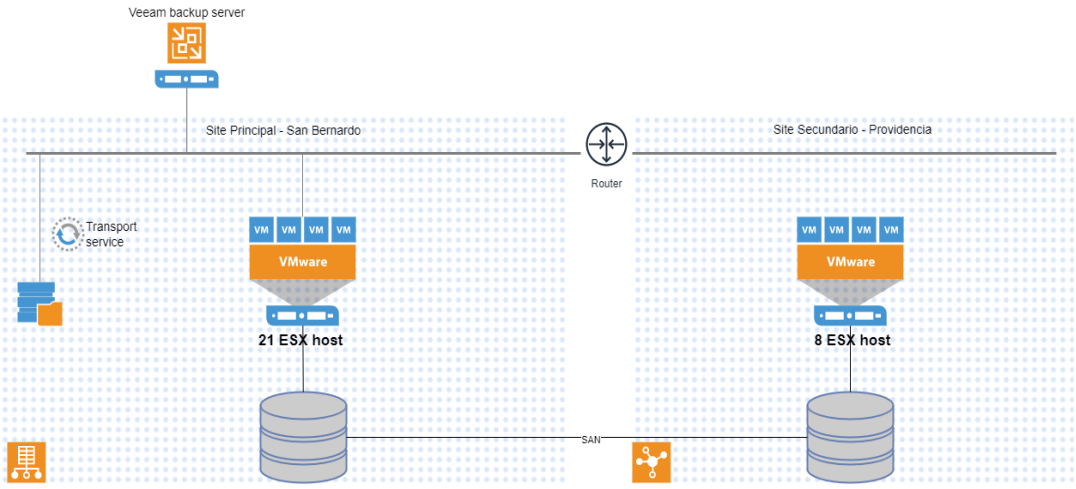


Ilustración 1: Imagen Referencial Arquitectura Host VMWare

Para el caso de los servidores de Base de Datos Productivos, se cuenta con máquinas físicas exclusivas, considerando el nivel transaccional necesario para los servicios de Previred, ver imagen 2 y 3, manteniendo contingencia para cada motor de datos, ya sea MSSQL Always On y Oracle RAC.

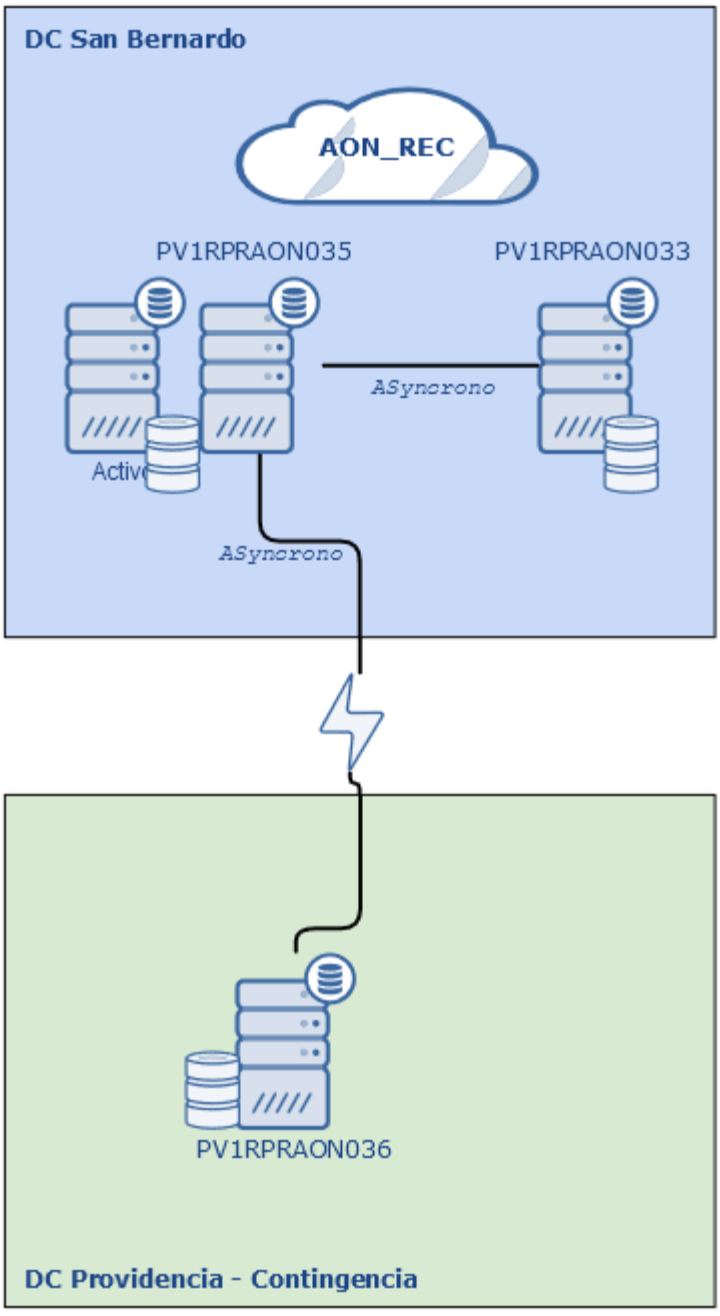


Ilustración 2: Imagen referencial Arquitectura base de datos Mssql Always On.

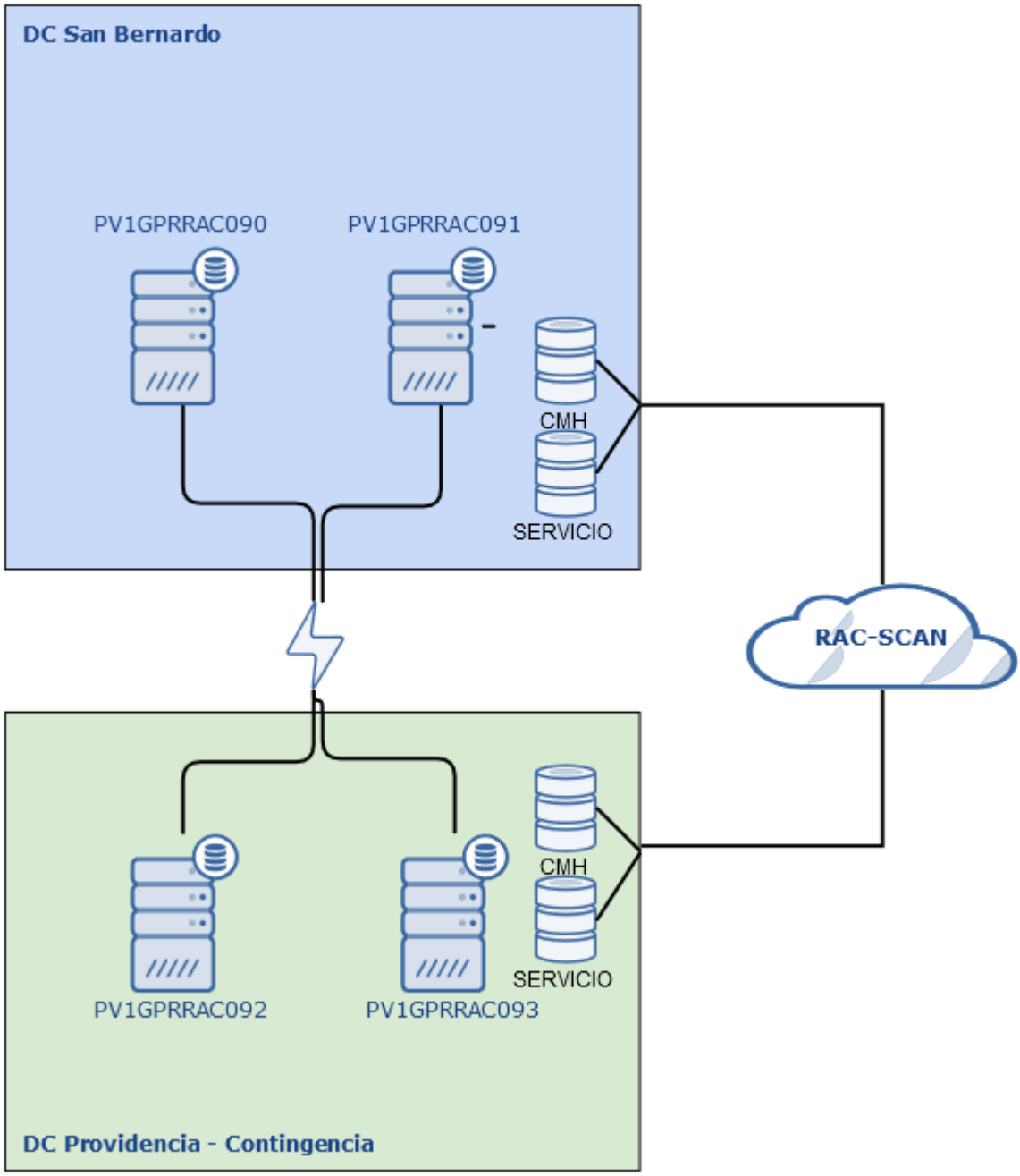


Ilustración 3: Imagen referencial Arquitectura base de datos Oracle RAC.

Para detalles respecto de los equipos que soportan o incluyen esta infraestructura ver Anexo: "Anexo N° 2 Listado Servidores"

Capacidad Vserver On Premise:

	Core	Memoria RAM (GB)	Storage (GB SSD)
Total	1600	2500	90.000

2.6 Infraestructura máquinas virtuales Contingencia

La Infraestructura actual esta implementada en VMware 7.X, basada en máquinas virtuales con sistemas operativos RedHat Enterprise y Windows Server. La actual plataforma cuenta con una réplica de base de datos MSSQL a un host físico y un RAC Oracle extendido. para detalles ver Anexo: "Anexo N° 2 Listado Servidores", el total de infraestructura dedicada a la entrega general de servicios de Contingencia es:

	Core	Memoria RAM (GB)	Storage (GB)
Total	1200	2200	60.000

El oferente debe considerar la contingencia de Escritorios Virtuales, detallado en punto 3.18.

2.7 Características Storage Productivo y de Contingencia

Las características actuales del Storage se componen de 2 Equipos Flash System 9200 con 150 TB SSD, los cuales tienen altísimos niveles de desempeño que permite un máximo de 18M IOPS y 180 GB/s, con latencias mínimas de 70 µs. El oferente debe disponibilizar Storage de igual o mejor tecnología, capacidad y rendimiento, igual o mejor velocidad de discos, todo, en función del óptimo y correcto funcionamiento de los servicios de Previred.

Algunas de las características actuales de nuestro Storage Flash System 9200 son:

- Menor Ocupación en DataCenter
- Tecnología 100 % Flash
- Compresión por Hardware
- Umbral de IOPS alta
- Conectividad 16 Gb
- Hardware última tecnología (NVME-FCMs)
- Encriptación
- Escalabilidad

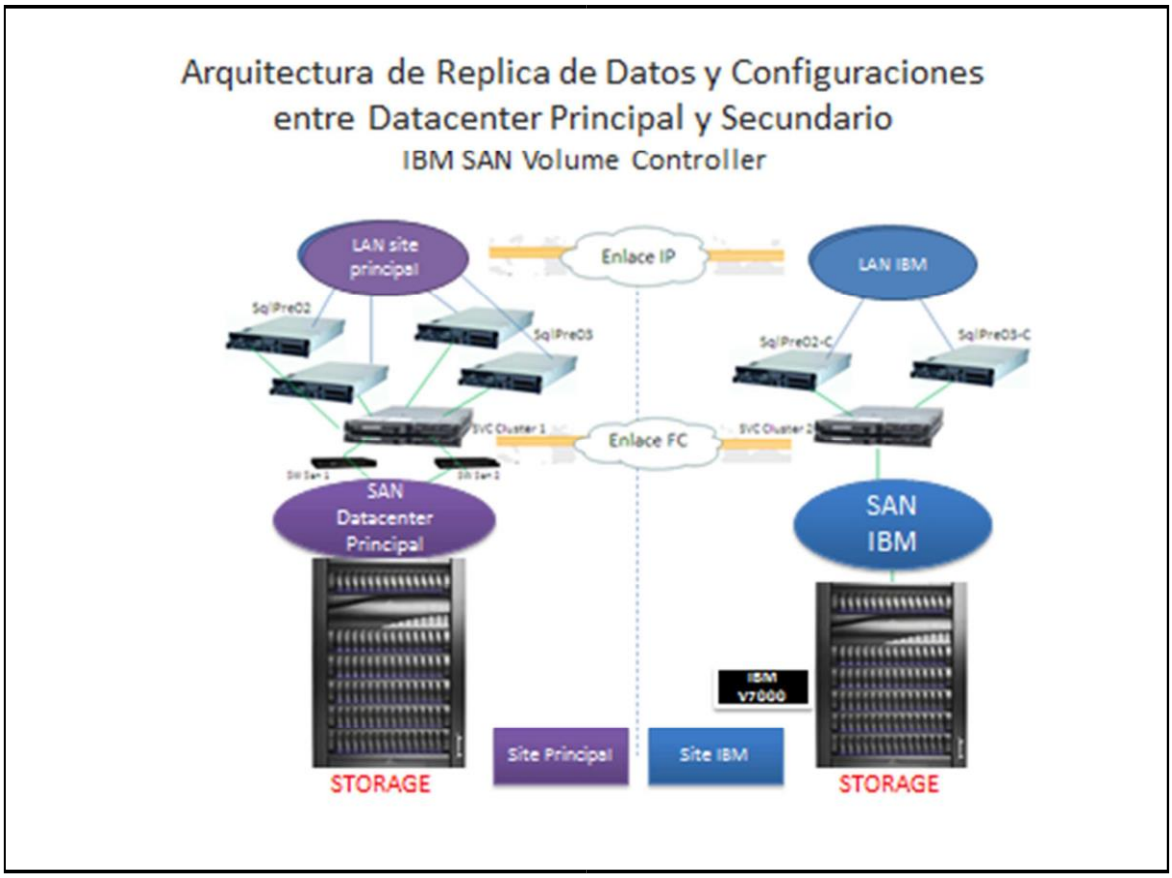


Ilustración 4: Arquitectura referencial de Contingencia.

2.8 Infraestructura máquinas virtuales y de Base de Datos de Preproducción

La Infraestructura actual esta implementada en VMware 7.X, basada en máquinas virtuales con sistemas operativos RedHat Enterprise y Windows Server.

La actual plataforma de preproducción está compuesta por 106 servidores virtuales. Ver cuadro de potencias totales que se encuentran en los servidores, para detalles ver Anexo: "Anexo N° 2 Listado Servidores"

El total de infraestructura dedicada a la entrega general de servicios Preproductivo es:

	VCore	**Memoria RAM (GB)**	**Storage (GB)**

Total	600	2000	50.000

Cabe señalar que este ambiente se encuentra comprendido de la siguiente forma:

- Servidores Barmetal en IBM cloud para contener las máquinas virtuales existentes.
- Servidores Barmetal para el motor de base de datos Oracle.
- Una plataforma de Openshift 4.X para lo que corresponde a Contenedores y microservicios.

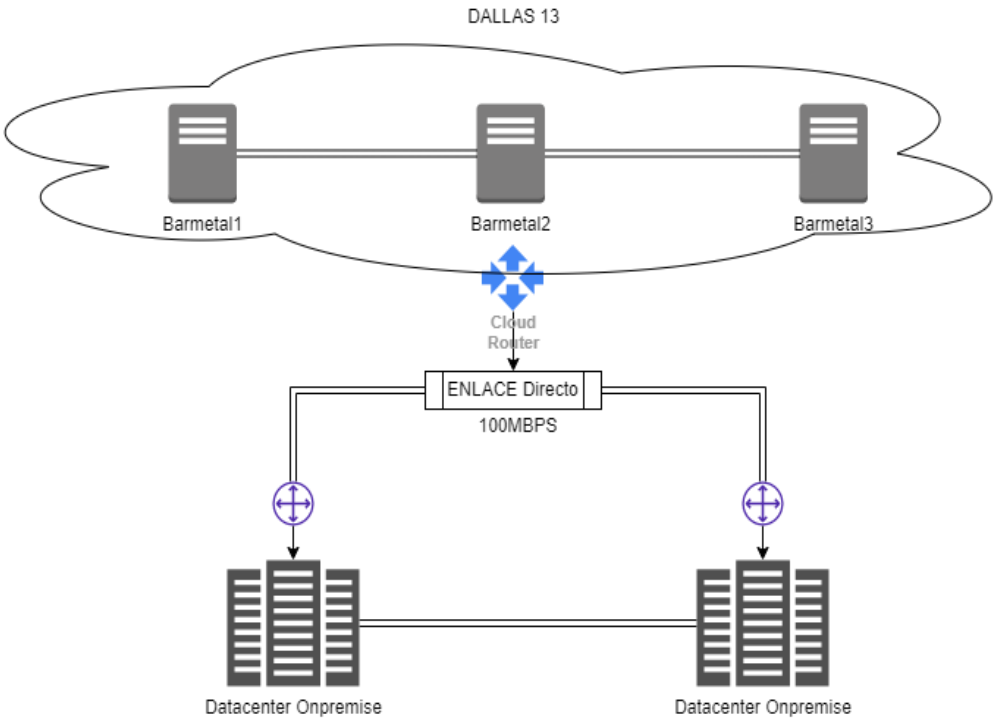


IMAGEN GENERAL DE PREPRODUCCIÖN

2.9 Características Storage Preproductivo Cloud.

Las características actuales del Storage se compone de 50 TB de discos SSD, los cuales tienen altísimos niveles de desempeño que permite una baja latencia. El oferente debe disponibilizar Storage Cloud de igual o mejor tecnología, capacidad y rendimiento, igual o mejor velocidad de discos, todo, en función del óptimo y correcto funcionamiento de los servicios de Previred.

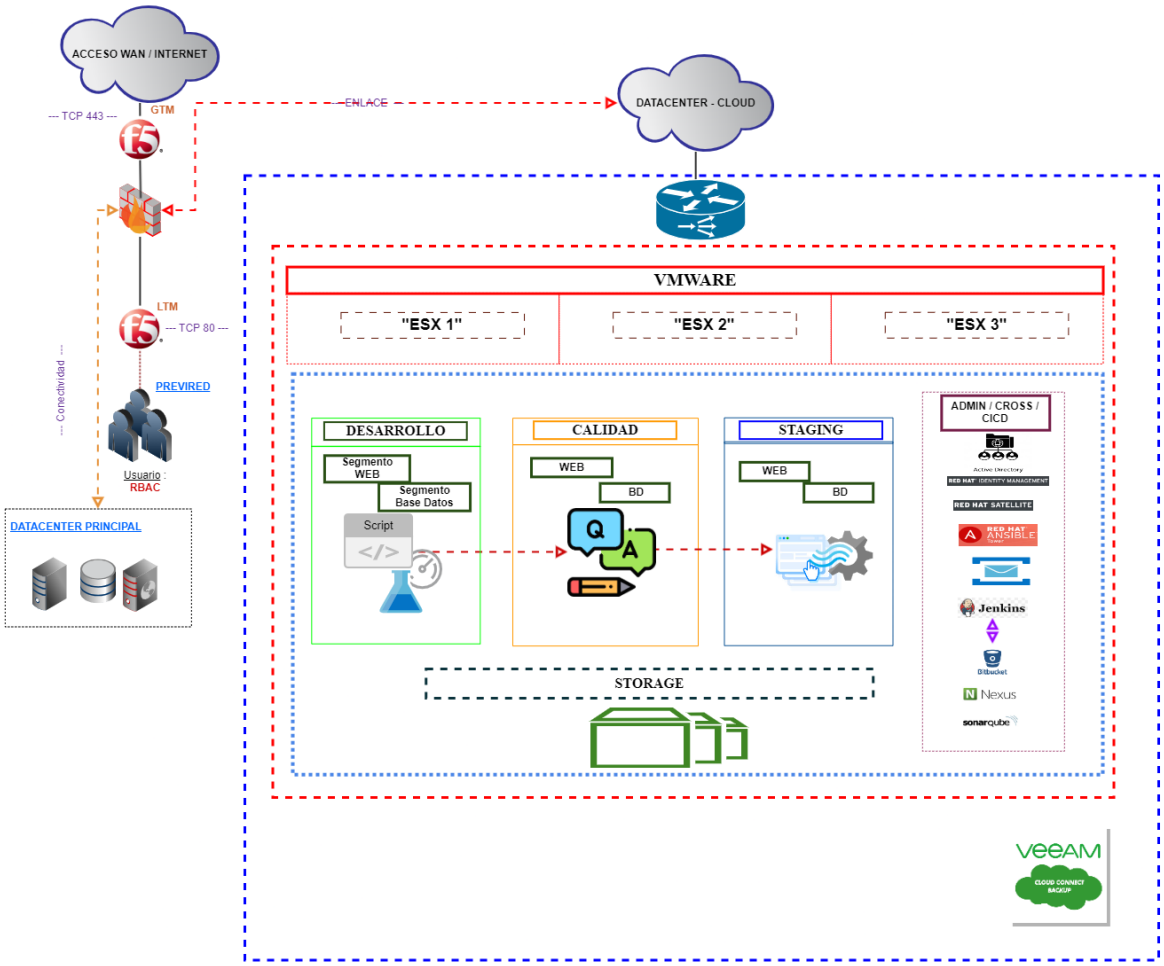


Ilustración 5: Arquitectura general de Preproducción.

2.10 Red de Datos, Comunicaciones y Seguridad actuales

En la actualidad, Previred, cuenta, para toda su operación, con dos Data Center en IBM y administrados por Kyndryl, esto es:

- Kyndryl San Bernardo : Data Center Principal
- Kyndryl Providencia : Data Center Secundario

Previred cuenta con una plataforma de comunicaciones y seguridad configuradas en HA en todas sus capas y enlaces que permite operar en Data Center principal o secundario de forma transparente y con los mismos niveles de servicio.

También contamos con servicios de seguridad Cloud con AKAMAI, los servicios contratados son KONA SITE DEFENDER, PROLEXIC Y FASTDNS, loa cuales deben ser considerados por el oferente.

Previred mantiene múltiples integraciones hacia diferentes instituciones a través de las plataformas de comunicaciones:

- **WAN AFPs** – integración a través de enlaces dedicados hacia todas las AFP y la Superintendencia de AFP (Provista por el OFERENTE)
- **REDBANC** – integración a través de enlaces dedicados hacia Redbanc permite acceder a los servicios de la RBI, estos son provistos por Redbanc
- **RED DE TERCEROS** – integración de otras instituciones que requieran integrar a PREVIRED a través de enlaces dedicados (Enlaces contratados por PREVIRED y Terceros a través de MPLS capa 2 de GTD)
- **CLOUD PRIVADA** – Acceso a través de túneles con ancho de banda asegurado para acceder a los ambientes previos provistos por Kyndryl en EEUU.
- **VPNs** – Integraciones VPN para instituciones que requieran este tipo de accesos a través de un concentrador de VPN dedicado para este objetivo

Previred cuenta con 2 segmentos IP clase C propios que deberán ser utilizadas/migradas hacia el nuevo oferente de servicios, estos segmentos son utilizados para publicación de servicios a Internet o con las integraciones anteriormente señaladas, se deberá definir la estrategia para mover los servicios y direccionamientos para generar la menor indisponibilidad posible.

Toda la red de Previred y sus integraciones opera hoy en día exclusivamente con IPv4 y se requiere incorporar IPv6. A continuación, Diagrama Simple de Red Actual:

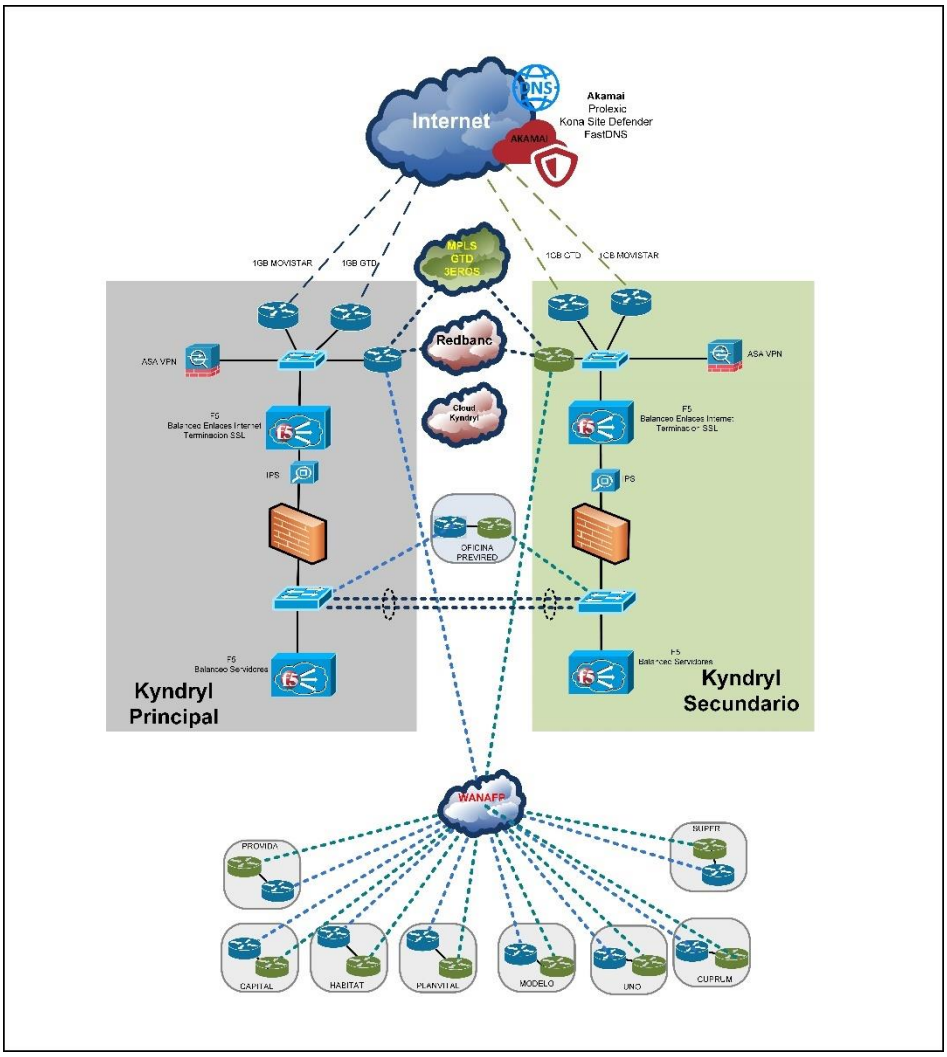


Ilustración 6: Diagrama red de comunicaciones actual

2.11 Servicio de Monitoreo

Actualmente Previred cuenta con distintas herramientas de Monitoreo, tales como Nagios, New Relic, entre otros para observación interna y Atentus como monitoreo externo (experiencia usuarios), todo con el objetivo de identificar el comportamiento de los sistemas e infraestructura TI en toda su trazabilidad,

La siguiente imagen ejemplifica monitoreo servicio de Recaudación y en la segunda imagen, monitoreo servicio SACU, lo que se aprecia en la imagen corresponde a los servidores que conforman el servicio, y el monitoreo permite detectar fallas puntuales de componentes o servicios completos.

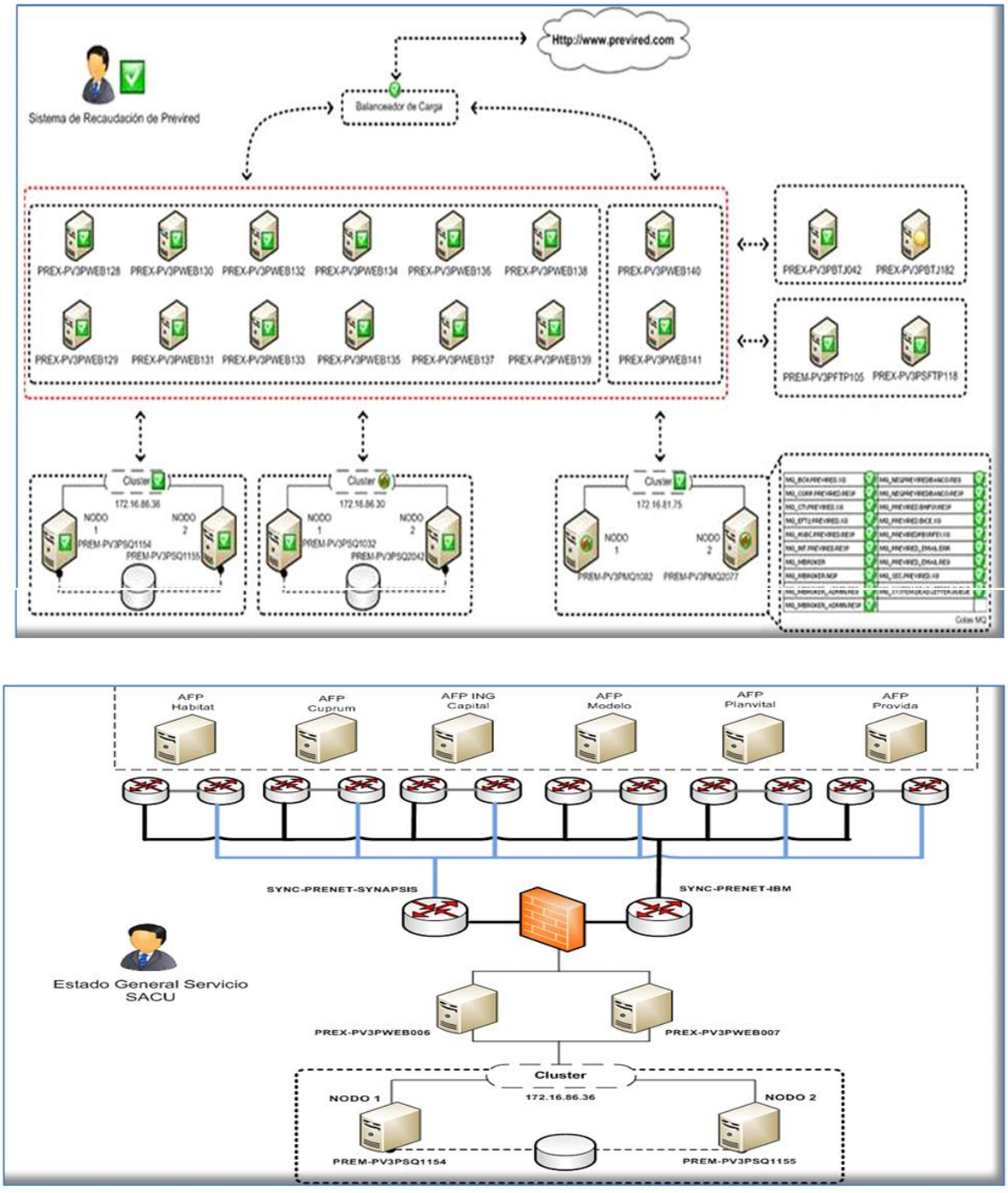


Ilustración 7: Ejemplos de Monitoreos

2.12 Software Base utilizado por PREVIRED

Es requisito del servicio que el oferente cuente con personal certificado y/o calificado, en las plataformas y software utilizadas por Previred. A modo de resumen, las plataformas y software principales utilizadas son:

- Productos RedHat
  - Red Hat Enterprise Linux Server
  - RHEL Server High Availability - RHEL Server Resilient Storage
  - JBoss EAP
  - JBoss EWS
  - Jboss Fuse-karaf
  - Satellite
  - Ansible
  - Openshift
  - AMQ
  - Podman

- Productos IBM
  - AIX
  - WebSphere MQ Series
  - Guardium

- Productos Oracle
  - Oracle Database Enterprise Edition 19C
  - Oracle Active Data Guard

- Productos Microsoft
  - Windows Server
  - Windows Workstation
  - SQL Server STD y Enterprise

- Otros (Ver Anexo: "Anexo N° 10 Inventario BASE - Matriz Software")

Para detalles como también verificar otros softwares utilizados, Ver Anexo: "Anexo N° 10 Inventario BASE - Matriz Software",

3 Requerimiento de la licitación

El servicio por ofertar por parte del oferente debe cumplir cabalmente el propósito de esta licitación, permitiendo el procesamiento y operación en forma eficiente y segura de las aplicaciones y bases de datos pertenecientes a Previred, en un esquema de servicio continuo 24x7 y que además permita incorporar nuevos requerimientos de espacio o recursos, equipamientos y servicios, que pudiesen presentarse en el tiempo de acuerdo con la dinámica del negocio.

3.1 Visión del servicio

Enfoque en la transformación digital, garantizando una alta disponibilidad y escalabilidad de nuestra plataforma en línea, para ofrecer un mejor servicio a nuestros clientes.

Así mismo, nos interesa que el oferente cuente con sólidas políticas de seguridad y ciberseguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información que se maneja en nuestra plataforma.

Buscamos un oferente que tenga experiencia y conocimientos en el diseño, implementación y gestión de infraestructuras de data center, y que pueda ofrecernos soluciones innovadoras y eficientes que cumplan con nuestros requerimientos específicos.

Buscamos flexibilidad en alta y baja de servicios, con el objetivo de mejorar la eficiencia en los costos.

3.2 Administración del Servicio

A. El oferente como Previred deberá nominar formalmente a un Administrador de Contrato, con la autoridad para representar y comprometer al oferente y Previred, respectivamente, en relación con todos los aspectos del contrato. El administrador del contrato del oferente será el encargado de controlar y coordinar la correcta ejecución de los Servicios.
B. Antes de nominar a la persona como Administrador del Contrato, el oferente deberá presentar a dicha persona a Previred, entregando los antecedentes que se requieran en relación a la experiencia de la persona.
C. En el evento que el oferente decida cambiar al Administrador de Contrato, deberá dar aviso escrito y anticipado a Previred, quien podrá aprobar o rechazar la designación.
D. El oferente deberá tomar las medidas destinadas a que el Administrador de Contrato designado sea en definitiva aceptado a satisfacción de Previred.
E. El oferente deberá destinar un equipo dedicado a la operación y gestión del contrato, este equipo debe estar compuesto por al menos:
    a. Gerente de Servicio.
    b. Líder Técnico.
    c. Líder de Servicio
    d. POD Team, equipo conformado por especialistas de exclusiva dedicación a Previred, debe cubrir la administración y gestión de todos los servicios y la infraestructura asociada en el rango de 24x7.
    e. Este equipo en conjunto con Previred opera diariamente y sesionara semanalmente.
F. El oferente deberá destinar a la prestación de los Servicios contratados personal de su exclusiva dependencia laboral y que cumplan con los requisitos curriculares y técnicos adecuados a la industria para la prestación de los servicios que a cada trabajador corresponda. Sin perjuicio de lo anterior, el oferente tendrá la facultad de subcontratar servicios específicos

con terceros proveedores con el fin de complementar los Servicios. En el evento que el oferente requiera subcontratar el todo o parte de los Servicios contratados requerirá autorización previa y escrita de PREVIRED.

3.3 Comité Ejecutivo y Operativo

A. El Oferente como Previred deberá nominar formalmente a representantes de un Comité Ejecutivo, con el objeto de que supervisen la administración del contrato.
B. Este Comité Ejecutivo debe estar compuesto por el Gerente General del oferente y Gerente General de Previred, más los respectivos Gerentes de 2da. línea y Administradores del Contrato.
C. Este Comité realizará revisiones semestrales de la ejecución del contrato, incluido los planes operativos, y los cambios al contrato.
D. Este Comité asistirá a pedido de cualquiera de las partes en la resolución de conflictos o discrepancias durante la ejecución del servicio o en la negociación de modificaciones del contrato.
E. El Comité Operativo estará conformado por Gerentes de 2da. línea y Administradores del Contrato y quienes ellos definan.
F. Este comité Operativo sesionará semanalmente y revisará la operación del servicio.

3.4 Servicio de Datacenter

En el Data Center del oferente se alojará el equipamiento que dará la capacidad de procesamiento a los ambientes de Producción, Pre-Producción, Gestión de Datos, Colaboración y otros Servicios de Apoyo transversal.

Para asegurar el funcionamiento 24x7, el oferente debe contar con personal especializado, herramientas y suministros adecuados que proporcionen monitoreo, seguridad y continuidad de servicios en el tiempo. Por medio de este servicio, se garantizará la administración y resguardo del equipamiento, en el que almacena data sensible tanto de PREVIRED, como de sus clientes.

Se requerirá que el Data Center ofertado cuente con certificaciones TIER 3 o superior.

Ver "Anexo N° 1 Requerimientos Físicos y ambientales del Data Center".

Responsabilidades del oferente:

- Dar acceso a Previred al Site en el horario y circunstancias que estime convenientes.
- Lo anterior significa que Previred se reserva el derecho a realizar visitas de auditorías (técnicas y aplicativas), ante lo cual el oferente deberá facilitar la realización de dicha actividad, sin presentar inconvenientes, los cuales de existir serán considerados como baja en los SLA establecidos.
- Mantener actualizados y disponibles Procedimientos de acceso al Data Center en condiciones normales o por emergencia.
- Mantener actualizados y disponibles Procedimientos escritos de sistemas de prevención / Seguridad contra siniestros.

- Entregar los procedimientos de autorización de ingreso al Data Center al personal de Previred o subcontratistas autorizados por Previred y acompañados por personal de Previred.

3.5 Propuesta para llevar servicios a la Cloud en el futuro.

El oferente, dentro del primer año de iniciada la operación del servicio deberá entregar una propuesta técnica y económica para implementar a los menos 3 servicios productivos de negocio o colaboración de Previred en Cloud, esta propuesta, una vez aprobada por Previred, debe ser implementada por el oferente dentro de los siguientes 12 meses, en conjunto con Previred.

Esta propuesta, debe contener un detalle de servicios, ventajas y desventajas, mínimo evaluación de 2 proveedores de Cloud. Adicionalmente debe contener una tabla de costo comparativa y el valor de descuento del servicio evaluado en on premises, para ser descontado del servicio en curso.

3.6 Infraestructura para Servidores, Bases de Datos y Storage

Será responsabilidad del oferente realizar la propuesta de equipamiento, su dimensionamiento y disponibilidad, basándose en la información aportada por Previred. Para revisar las capacidades, remitirse a sección 2.2, 2.3, 2.4, 2.5, 2.6 y 2.7 de este documento.

Para detalle ver anexos:

- Anexo: "Anexo N° 4 Fichas Diagramas de Servicio"
- Anexo: "Anexo N° 2 Listado Servidores"
- Anexo: "Anexo N° 10 Inventario BASE - Matriz Software"

Consideraciones

- Para servicios Productivos, se solicita ofertar equipamiento dedicado y con una tecnología de última generación, según lo descrito en punto 2.5 "Infraestructura máquinas virtuales Productivas" y punto 2.7 "Características Storage Productivo".
- Servidores de Base de datos Productivos, deben ser maquinas físicas. Ver Anexo N° 6 Consideraciones al momento de generar la arquitectura de servidores de Base de Datos.
- Para ambientes preproductivos se solicita ofertar ambientes cloud, esto con el objeto de bajar costos y otorgar flexibilidad y elasticidad para satisfacer demandas variables de los recursos en una modalidad de pago a demanda y/o porcentaje de crecimiento anual sobre la infraestructura contratada. Para el caso de máquinas de Bases de Datos MSSQL y Oracle para ambientes preproductivo que requieren, éstas deben prestar el rendimiento óptimo, por lo que Previred queda abierto a recibir otras propuestas que puedan garantizar la operatividad de los servicios, según descripción de punto 2.5 "Infraestructura máquinas virtuales Productivas" y punto 2.7 "Características Storage Productivo".
- Para Servidores Productivos y preproductivo que almacenan las Bases de Datos Oracle, se debe tener en consideración tipo y cantidad de licencias Oracle declaradas por Previred, ver Anexo

N°3, "Licencias propiedad de Previred", de manera de asegurar no requerir licencias adicionales (revisar restricciones de licenciamiento de Oracle).

- En caso de que el tipo de máquinas ofertada requiera otro tipo de licenciamiento o licencias adicionales de cualquier tipo, estás deberán declararse y cotizarse por separado.
- Es responsabilidad del oferente asegurar el cumplimiento del licenciamiento requerido para cumplir con los requerimientos de licenciamiento de los diferentes proveedores de software.
- Previred podrá solicitar como parte del servicio, reconvertir o rehacer máquinas virtuales de acuerdo con las necesidades de negocio. Sin que esta labor implique costos adicionales. Esto aplica a todos los ambientes proporcionados.
- El oferente en conjunto con Previred deberá definir template bases de manera de facilitar la creación de nuevas máquinas virtuales. Ver Anexo N°7 "Template Para Máquinas Virtuales".
- El oferente deberá garantizar compatibilidad de versiones de software base utilizado por Previred con las herramientas que utilizará para prestar el servicio, por ejemplo: software de virtualización, de respaldo, agentes de monitoreo u otras herramientas requeridas para prestar el servicio.
- El oferente deberá garantizar un rendimiento de la plataforma otorgada sea igual a o superior a la actual.
- El oferente debe considerar lo necesario para cumplir el propósito de esta licitación.

3.7 Infraestructura y crecimiento de Producción y Contingencia

La infraestructura está descrita en punto 2.5 "Infraestructura máquinas virtuales y base de datos Productivas" y punto 2.6 "Infraestructura máquinas virtuales Contingencia" y 2.7 "Características Storage Productivo y de Contingencia". como mínimo, el oferente debe presentar una arquitectura igual o suprior, con tecnología de punta y óptima para la correcta operación de los servicios productivos de Previred, en todas sus capas: Aplicativas, Bases de Datos, Storage, entre otros.

Previred tiene planificado poder incorporar nuevos servicios en ambientes de producción, por cual el oferente debe considerar un crecimiento anual del 10% de la plataforma de producción, con tecnología homóloga de la existente, que asegure el propósito de esta licitación.

3.8 Infraestructura y crecimiento de Preproducción

La infraestructura está descrita en punto 2.8 "Infraestructura máquinas virtuales y de Base de Datos de Preproducción" y punto 2.7 "Características Storage Productivo". como mínimo, el oferente debe presentar una arquitectura igual o superior, con tecnología de punta y óptima para la correcta operación de los servicios productivos de Previred, en todas sus capas: Aplicativas, Bases de Datos, Storage, entre otros.

Previred tiene planificado poder incorporar nuevos servicios en ambientes de preproducción, por cual el oferente debe considerar un crecimiento anual del 10% de la plataforma de preproducción, con tecnología homóloga de la existente, que asegure el propósito de esta licitación. El primer incremento del 10% es al inicio del servicio.

3.9 Housing equipamiento de terceros o PREVIRED

El oferente debe considerar el espacio de rack para alojar equipos proporcionados por terceros, esto debe ser equivalente a 12U (6U en Site 1 y 6U en Site 2).

3.10 Migración de Servicios

Será responsabilidad del oferente proponer un plan de migración, que garantice una mínima pérdida de uptime de los servicios. se considerar las migraciones en días y horarios no laborales, considerando que la mayoría de los servicios operan 7x24x365.

Migración lógica de los servicios y data almacenada en la actual plataforma, como las configuraciones de los equipos de comunicaciones y seguridad de propiedad del actual proveedor de Data Center a la nueva plataforma proporcionada por el oferente. Implementación, configuración, tunning, pruebas de rendimiento y puesta en marcha.

El plan de migración propuesto se debe detallar en la propuesta del oferente, el cual debe contemplar al menos los siguientes puntos:

- Estrategia de migración.
- Plan de Implementación y cronograma completo el cual considere las pruebas necesarias para certificar funcionamiento de los servicios.
- El oferente deberá especificar qué información y colaboración requiere de parte del proveedor actual de Data Center y de Previred.
- El oferente deberá proveer un enlace directo hacia el Data Center actual, con alta disponibilidad y con las capacidades suficientes para realizar la transferencia de archivos en forma óptima, mientras dure la migración.
- Previo a migración se debe considerar y realizar Respaldo Masivos a los Activos de Información de Previred.
- Para servicios productivos, las migraciones deben planificarse fuera de horario, noches o fines de semana, dependiendo del servicio y su ventana de mantenimiento.
- Es requisito que la fecha tope para que los servicios estén productivos y operando en nuevo site sea el 31 de julio 2024.
- Previred estima que desde el punto de vista de las dependencias aplicativas o de infraestructura, las etapas de migración (ETM) que deben migrarse a la nueva plataforma en forma conjunta son los siguientes, independiente que se puedan migrar más de un ETM por vez:

    - ETM 1: Servicios básicos para la operatividad y migración hacia el nuevo DataCenter.
    - ETM 2: Servicios base para las aplicaciones en despliegue continuo
    - ETM 3: Servicios de preproducción
    - ETM 4: Servicios Productivos de Notificación y Certificados y Bases de datos
    - ETM 5: Servicios Productivos Recaudación y plataforma de Pago
    - ETM 6: Servicios de Apoyo y Cobranza.
    - ETM 7: Servicios de Gestión de datos
    - ETM 8: Servicios de Colaboración.

Para mayor detalle, ver Anexo: "Anexo N° 9 Grupos Migración ETM"

Nota: La migración del servicio de los diferentes servicios deberán planificarse fuera de los días peak de cada uno.

3.11 Plazos de Implementación y Pruebas

Para evitar cualquier contratiempo, el plazo TOPE de implementación y de migración deberá ser el 31 de julio 2024. El cual se entenderá por finalizado con la aceptación por parte de Previred, a través del documento correspondiente. Favor ver anexo, "Anexo N° 8 Protocolo de Aceptación de Servicios"

Los oferentes deberán especificar estrategia y plan de implementación para el proyecto completo, incluyendo carta Gantt y especificando responsables.

3.12 Migración de Cintas Históricas

Como servicio adicional el oferente deberá cotizar la conversión de las cintas de respaldos históricas, correspondiente a los últimos 10 años, que son aproximadamente 400 cintas de formato Ultrium LTO6. Los respaldos son realizados utilizando Unidad de Respaldo Tivoli Service Management (TSM)

Cintas actuales corresponden a modelo LT06. Si servicio de respaldo no considera integración con este formato, también deberá considerarse la migración de estas cintas.

Adicionalmente debe entregar una mejora de propuesta a largo plazo de generación de respaldo y almacenamiento de este:

Ejemplo

- Tecnología LTO9
- Respaldo Cloud u otra alternativa

Considerar, adicionalmente, que Previred debe quedar o tener una copia y acceso a la información.

3.13 Provisión de Servicio de Dominio

3.13.1 Servicio dominio y DNS para usuarios internos

El oferente de proveer el servicio de dominio para los usuarios internos (hoy llamado "Previred.com"), brindando además los servicios de NTP y DNS correspondientes. Deben considerarse al menos dos controladores de dominio, en plataforma exclusiva, con alta disponibilidad y contingencia, más un tercero que sea réplica de lectura, en la plataforma de preproducción.

Se valorará una contingencia alternativa en ambientes Cloud

3.13.2 Servicio de dominio y DNS para servidores

El oferente debe proveer del servicio de dominio, DNS y NTP para la plataforma de servidores (hoy llamado "Previred.neg"). Debe considerar al menos dos controladores de dominio, en plataforma exclusiva, con alta disponibilidad y contingencia.

También debe considerarse un controlar de dominio replicado en Cloud, una vez se implementen servicios en ese ambiente.

3.14 Servicio de Sincronización de hora

El oferente de considerar el servicio de:

- Sincronización horaria a través de Servicio NTP para toda la plataforma que aloja los servicios y servidores de Previred, esto incluye equipos de comunicaciones.
- Parchado y actualización ante cambio de hora previstos para la zona horaria vigente en plataforma que soporta los servicios y servidores de Previred.
- Monitorear el correcto funcionamiento del servicio, sincronización e integración de los clientes del servicio NTP.

3.15 Servicio de Antivirus

El oferente de considerar el servicio de:

- Software de Antivirus en modalidad dedicada, con administración centralizada para todos los servidores de Previred, sin distinción de ambiente.
- Se solicita que el oferente mantenga las versiones del motor y la definición de antivirus actualizadas, serán parte de los niveles de servicios exigidos
- Se solicita acceso de lectura para Previred a la consola central de antivirus.
- Se solicita mantener una política y un control exhaustivo de actualización del cliente de antivirus tanto en los servidores que dan servicio al negocio de Previred, como también los servidores que usará el oferente para prestar los diferentes servicios.
- Se solicita la entrega de un informe mensual con el estado del servicio, esto incluye detecciones o alertas registradas, inventario de máquinas, versión del antivirus instalada, entre otros que requiera Previreed.

3.16 Servicio de parchado de seguridad de la plataforma

El oferente debe considerar:

- Servicio de parchado y actualización de seguridad de la infraestructura, servidores, equipos de conectividad, middleware y clientes de base de datos relacionados con todos los servicios de Previred.

- Administrar los repositorio y proceso de parchado de seguridad de la plataforma de forma centralizada, eficiente y segura.
- El proceso de este servicio debe cubrir los requerimientos de instalación, administración, reportería y seguridad para todas las interacciones sobre la infraestructura, servidores, middleware y equipos sin excepción (Incluidos los ambientes de Preproductivos, Productivos y Contingencia)
- La herramienta/as utilizada para realizar esta actividad, deben permite la distribución de los parches y actualizaciones publicadas por los proveedores tecnológicos de forma centralizada para los distintos elementos administrados (Productos Microsoft, RedHat Linux, VMWare, SQL Server, AIX, entre otros).
- El servicio debe cumplir un calendario mensual de acuerdo a lo definido por PREVIRED.
    - Calendario de parches:
        - Ambientes Transversales y de Preproducción:
            - Servidores Transversales Días 07 de cada mes o hábil siguiente
            - Servidores Desarrollo Días 11 de cada mes o hábil siguiente
            - Servidores Calidad Días 15 de cada mes o hábil siguiente
        - Servicios Apoyo al Giro y Cobranzas
            - Servidores Productivos Días 21 de cada mes o hábil siguiente.
        - Recaudación, Notificaciones, Apoyo al Negocio y Colaboración.
            - Servidores Productivos Días 25 de cada mes o hábil siguiente

3.17 Inventario y capacidades de equipos

Se solicita que el oferente mantenga el inventario de todos los Servidores, Storage, Equipos de comunicaciones y seguridad actualizadas, donde la información mínima a entregar mensualmente es:

- Nombre de Equipo
- Firmware
- Sistema Operativo
- Versión de Sistema Operativo
- SW Ambiental
- Versión SW Ambiental
- Procesador
- Memoria RAM
- Espacio de Storage asignado
- Espacio de Storage disponible

Se deberá entregar un informe mensual con esta información, con el detalle del inventario actualizado.

Para más información, ver anexos: “Anexo N° 2 Listado Servidores” y “Anexo N° 10 Inventario BASE - Matriz Software”.

3.18 Escritorios Virtuales

Actualmente, Previred cuenta con un grupo de 40 escritorios virtuales en plataforma Citrix, que en su mayoría son utilizados para la ejecución de tareas mediante robots RPA y otros para usuarios críticos.

Se solicita al oferente brindar una plataforma similar (ya sea con Citrix u otra) que permita la ejecución de robot RPA como para uso de usuarios críticos, **con servicio de respaldo, alta disponibilidad y contingencia**. Considerar además crecimiento anual de un 10% de la cantidad y potencias de Escritorios Virtuales.

Para los RPA actuales Previred utiliza el producto UIPATH, por recomendación del proveedor, idealmente estén sobre máquinas virtuales en AWS.

Cómo base, los escritorios virtuales deben tener las siguientes características: 8 Vcores, 16 GB. RAM, 150 GB. HDD, Licenciamiento Base, Operación Base, respaldo, monitoreo.

Nota: Licenciamiento base corresponde a todo aquello que permita a la máquina en cuestión operar de manera correcta y lista para poder ser utilizada. Esto considera: sistema operativo, antivirus si aplica, monitoreo, respaldo, anclamiento a dominio según definición, entre otros.

3.19 Mesa de Ayuda Técnica 24x7

En el siguiente diagrama se muestra el flujo actual para lo que es la gestión de procesos TI, proceso actualmente aplica a la Subgerencia de Sistemas como contraparte del oferente:

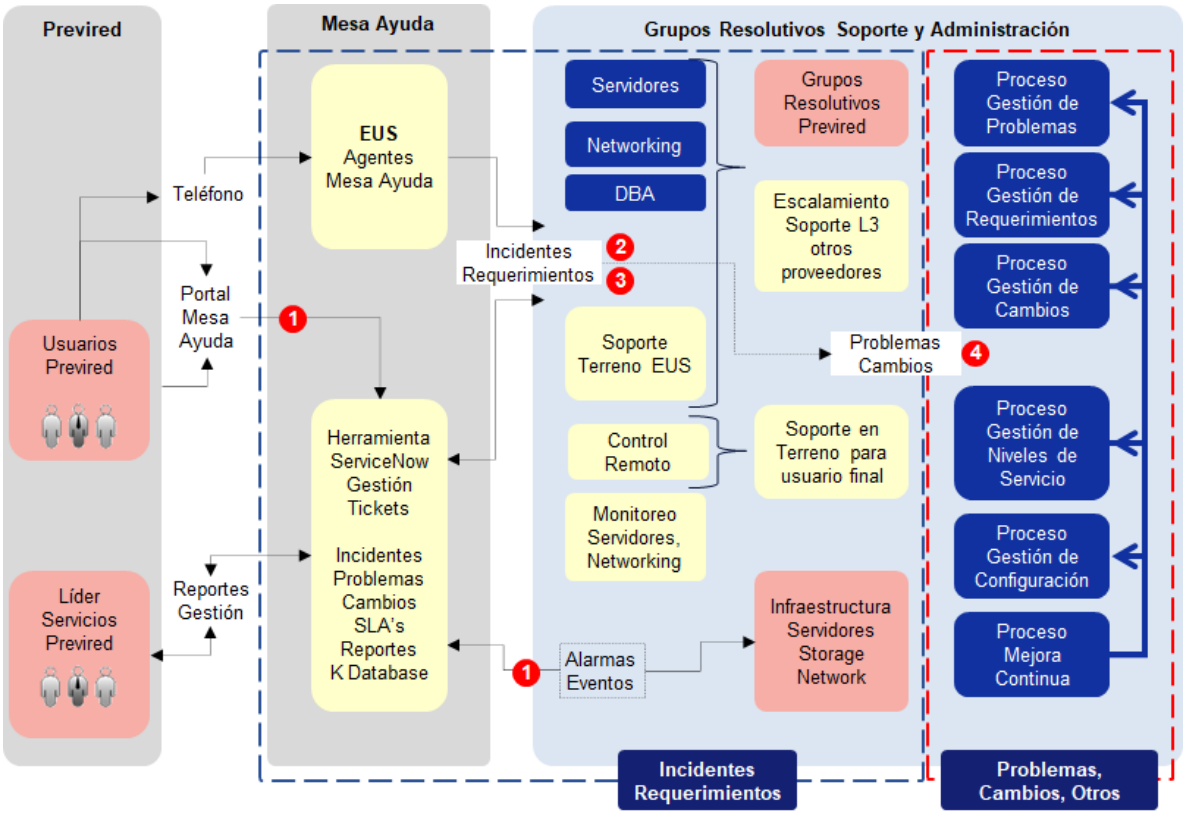


Ilustración 8: Flujo actual de solicitudes de servicio (incidentes/requerimientos)

En el diagrama anterior, se puede observar que las solicitudes de servicios -1- (Incidentes/Requerimientos) pueden ingresar a través de la mesa de ayuda o a través de la gestión de eventos vía monitoreo/observabilidad o llamado telefónico. Los incidentes no resueltos -2- pasan a categoría de "Problemas" y se aplica el proceso de gestión de problemas.

Los requerimientos -3- pasan directo al proceso de gestión de requerimientos.

En -4- puede ocurrir que los procesos de gestión de problemas y/o gestión de requerimientos activen el proceso de gestión de cambios.

La mesa de servicios debe ser el punto único de contacto para el personal de Sistemas de Previred, la gestión del servicio debe ser gestionada por el Líder de Servicio, donde se cursan todas las incidencias, peticiones, problemas, cambios y en general solicitudes relacionadas con el servicio.

En específico, el requerimiento es:

- Mesa de ayuda de estándar mundial y reconocida en el mercado que cumpla normas ITIL. Ej. Service Now.
- Es requisito que los procesos estén soportados, bajo metodología ITIL.
- El acceso a la mesa de ayuda se restringe al personal técnico de Previred y no más de 40 personas de la Subgerencia de Sistemas de Previred.
- Las alertas por fallas de servicios de terceros que afecten al servicio de Previred y su monitoreo y seguimiento será responsabilidad del oferente, por ejemplo: AFP, Bancos u otras.
- Las alertas e incidencias de servicios automáticamente tendrán que generar un ticket e internamente, generarse la solución del mismo.
- Informes en línea de tickets (listado de pendientes, atrasados, resueltos, entre otros)
- Servicio 24x7
- Uso de herramienta de Service Desk (con acceso web), que permita generar tickets, llevar control y seguimiento de ellos.
- La herramienta de Service Desk debe proveer un primer nivel que realice la categorización y derivación de los tickets ingresados. Previred sólo deberá especificar el problema / requerimiento / Cambio u otro y el primer nivel de la mesa de ayuda gestionarlo internamente.
- Atención de llamadas con N° único de contacto y/o correo electrónico, Registro, categorización, derivación a la plataforma correspondiente, escalamiento, seguimiento y cierre de las peticiones de servicio.
- Envío de informe semanal de tickets y estatus, en especial los ticket pendientes, con detalle del motivo de su estado.
- Informe mensual de servicio con SLAs.
- Plataforma debe permitir tipificado de Requerimientos acorde a lo requerido por Previred, detalle de categorías serán entregadas por Previred.
- Plataforma debe permitir control de SLAs y escalado.
- Gráfica con volúmenes actuales de Tickets abiertos por Previred.
    - La tasa de crecimiento anual de los requerimientos en el año 2022 ha correspondido a un factor de 1,25.
    - Promedio de tickets mensuales 2º semestre 2022.
    - Solicitudes: 20
    - Cambios: 150
    - Incidencias: 30

3.20 Soporte y Mantención Preventiva y Correctiva Hardware

Dado que la provisión de la infraestructura, servidores, storage, equipos de comunicaciones, de seguridad, entre otros. serán de propiedad del oferente, éste debe asegurar que cuentan con garantías vigentes y/o contratos de soporte y mantención con los fabricantes respectivos y acorde a la criticidad del negocio (SLA contratados), por toda la duración del contrato.

Previred exigirá que el oferente disponga y exhiba el Plan de Mantención Preventiva del Hardware, esto incluye un informe mensual de estado del hardware utilizado en toda la plataforma.

3.21 Renovación Tecnológica

En relación al plazo de contratación de los servicios, el oferente deberá considerar renovación tecnológica de toda la infraestructura que soporta la plataforma, en todas sus capas, cómo mínimo debe contener lo señalado en "Anexo N° 2 Listado Servidores" , "Anexo N° 10 Inventario BASE - Matriz Software" y "Anexo N° 11 Inventario Comunicaciones Seguridad",) en los siguientes periodos.

- Servicio a 48 meses, no considera renovación.
- Servicio a 72 meses, se debe considerar renovación al 3er año
- Servicio a 96 meses, se debe considerar renovación al 4to año

También se considera que toda renovación tecnológica debe incluir CPU, Memoria y Storage, esto con el fin de contar con generación de componentes acorde al mercado

Esta Renovación Tecnológica debe aplicar también a equipos de Storage y toda cada de servicios y equipos de Seguridad, Comunicaciones, Conexión e Interconexión, entre otros.

3.22 Operación, Mantención y Soporte del Software Base

3.22.1 Operación de servicio

Es responsabilidad del Oferente garantizar la compatibilidad del hardware y software durante la operación y mantención de los servicios. Se debe asegurar el monitoreo, respaldo, actualización y/o renovación de los equipos o aplicaciones según las recomendaciones de los fabricantes en base a la matriz de compatibilidad respectiva, también, se debe considerar la operación y soporte del software Base, con cobertura 24x7.

Será responsabilidad del oferente el coordinar e informar oportunamente este tipo de actividades y contar con el visto bueno de Previred previo a la actualización del firmware, o aplicación de parches.

Siendo especialmente sensible a estos cambios los ambientes de contingencia en Data Center secundario.

La coordinación establecida debe ser fijada para la aplicación de las actividades mensuales en el caso de ser repetitivas y periódicas de origen mensual y bajo una calendarización a definir en conjunto con Previred (calendario lo debe presentar el oferente), acorde a la posibilidad de cada servicio según su nivel de criticidad.

3.22.2 Mantención de equipos

El software existente en los servidores debe tender a ser la versión N-1 de la última versión disponible. Será responsabilidad del oferente la instalación de parches y la seguridad del Software Base, según los procedimientos estándares estipulados para cada plataforma.

Se debe considerar la mantención del software Base, con cobertura 24x7, el oferente se debe comprometer a mantener la Operatividad del Hardware y Software Base, desempeñando actividades mínimas lo que le permitirá asegurar la continuidad operativa, para ello debe realizar al menos las siguientes labores:

a. Revisiones de disponibilidad de los servicios y sistemas.
b. Mantenciones preventivas y correctivas.
c. Revisiones periódicas de prevención sobre los servicios activos.
d. Detección y alertas de eventos.
e. Verificación de las existencias y niveles de software instalados en los servidores.
f. Detección y eliminación de virus.
g. Instalaciones de parches críticos definidos por el oferente, proveedores calificados por Previred o por indicados por Previred directamente.
h. Plan de estrategia e instalación en caso de existir una vulnerabilidad o actualización critica de un software o hardware.
i. Emisión de sugerencias y alertas a personal válido designado por Previred.

3.23 Licencia, garantías, suscripciones

Será parte del servicio otorgado por el oferente el pago anual del Soporte de licencias de software base de uso por parte de Previred (Sistema Operativo y elementos ambientales que permitan la operación de servidor (Firmware, Antivirus, entre otros)

El oferente debe llevar el control de las licencias cuando éstas estén próximas a su vencimiento y con ello coordinar debidamente sus respectivas renovaciones.

3.24 Cobertura horaria Servicios de Ingeniería

Los servicios de Previred operan 24x7 y deben contar con soporte de Ingeniería de Sistemas, Administración de Base de Datos, Redes, Comunicaciones, Seguridad y cualquier otra necesidad que permita asegurar su operación y continuidad operativa.

3.25 Servicios 24x7

Los servicios 24x7 que, como mínimo, deben operar y entregar servicio, asegurando la continuidad operativa y la seguridad, deben ser:

- Mesa de Ayuda.
- Monitoreo de trazabilidad completa, end to end (Observabilidad general del negocio, la Infraestructura, Servicios, Networking, Seguridad, entre otros)
- Operación de Plataforma de Servicios
- Respaldo y Recuperación
- Aplicación de controles de cambio
- Atención de Incidentes
- Trabajos programados fuera de horario (mantenciones en general, Trabajos de Base de Datos, Ingeniería de Sistemas, Networking, Seguridad)
- Cualquier otra necesidad que pueda surgir según necesidad en pro a la continuidad operativa, la seguridad y la óptima operatividad de los servicios

3.26 Horas para trabajos programados adicionales de Consultoría

Para la correcta operación de los servicios de Previred, se requiere disponer de un paquete mensual de 80 horas de Ingeniero experto para ser usadas como consultoría o algún servicio no cubierto por este contrato.

En caso de no usarse en el mes calendario se acumularán en el período de 6 meses móviles.

3.27 Servicio de Ingeniería de Sistemas

En lo referente a los servicios de Ingeniería de Sistemas, el oferente deberá realizar labores de administración, instalación, configuración, monitoreo y mantención de niveles adecuados de la plataforma, sistemas operativos, capa media e integración de servicios, para garantizar la correcta operatividad, disponibilidad, performance, niveles de SLA contratados y definidos por Previred, llevando a cabo las tareas de toma de control, puesta en marcha, securitizar y soporte proactivo de los servicios.

Deberá adaptarse al cambio de tecnologías monitoreando y observando el continuo ciclo de vida del desarrollo del software, administrando la infraestructura TI que se necesita para implementar el software en entornos de Cloud o híbridos resguardando las normas y políticas asociadas a seguridad de la información.

Entre otras, las actividades previstas son:

- Administrar, instalar, configurar, mantener y monitorear la plataforma e infraestructura que soporta los servicios con enfoque a la optimización de recursos y mejora continua.
- Resguardar la confidencialidad, integridad y disponibilidad de los servicios.
- Crear y analizar alertas, errores, archivos logs, resolución de problemas y ajustes de parámetros para un desempeño óptimo de la plataforma y servicios middleware.
- 'Hardening' de plataforma para asegurar la seguridad de los servicios.
- Analizar y resolver requerimientos de cambios, mejoras, solicitudes, incidentes, problemas asignados
- Realizar y registrar el proceso de escalamiento, en caso de que le sean asignados ticket de incidentes y el grupo de soporte no sea capaz de solucionarlo, a las unidades resolutivas según corresponda.
- Realizar y registrar el proceso de derivación en caso de que le sean asignados ticket de incidentes que no estén dentro de las responsabilidades del grupo de soporte, a las unidades resolutivas según corresponda.
- Proveer el escalamiento de problemas e interactuar con otros proveedores según sea necesario, en caso de tiempo de resolución incierto, incorporar una mesa técnica para revisión.
- Coordinar el mantenimiento de hardware con el oferente correspondiente para la infraestructura bajo el alcance del servicio.
- Actualización de versiones, de acuerdo con las necesidades del negocio y las recomendaciones del fabricante, esto incluye calendario EOL.
- Realizar la apertura de ticket de incidentes, requerimientos y problemas en la Mesa de Ayuda Previred, frente a una condición anormal del servicio.
- Manejo, administración y supervisión de cuentas, accesos y permisos de usuarios. Las políticas utilizadas para estas operaciones serán definidas en acuerdo con el Previred.
- Mantener y proveer la información necesaria en forma oportuna en la relación con los equipos que interactúan en el ciclo de desarrollo de aplicaciones de Previred, Networking, proveedores y fabricantes, entre otros.
- Registro continuo del rendimiento y uso de las componentes de CPU, memoria y disco, y mantención de la información histórica de acuerdo con las capacidades de almacenamiento existentes.
- Mantener actualizadas las normas y procedimientos relacionados con actividades de soporte técnico antes mencionadas.
- Propuesta de cambios o mantención de componentes, parámetros o condiciones del hardware y software de los servidores que permitan el mejoramiento continuo de la plataforma.
- Proveer soporte al proceso de Gestión de Cambios, realizando el análisis y evaluación de impacto de los cambios solicitados.
- Interactuar con las áreas técnicas de terceros proveedores designados por Previred, sobre temas bajo el alcance del servicio.
- Manejo, resguardo y supervisión de cuentas privilegiadas y usuarios finales.
- Recibir de los proveedores de Previred información relacionada con nuevos productos y/o versiones de sistemas operativos y Programas de Sistemas dentro del alcance del Servicio.
- Entregar mensualmente los errores conocidos y repetitivos en la plataforma con el fin de tomar acciones tempranas de mantención.
- Supervisar, controlar y ejecutar los procedimientos de contingencia que involucren actividades a realizar en este servicio.

- Llevar el registro en las bitácoras respectivas de los eventos, cambio técnicos y aplicativos sobre los servicios.
- Liderar y fomentar las necesidades de automatización tecnológica de los servicios.
- Generar la información para el control del cumplimiento de los Niveles de Servicio acordados.
- Generar informes mensual estadísticos, de acuerdo con el Manual de Procedimientos, que entreguen las métricas asociadas al servicio.
- Coordinar e implementar despliegues de software sobre las plataformas que administra (nuevas funcionalidades – mantenciones, entre otros), adhiriendo al proceso de control de cambios/Gestion del Cambio y control de versiones solicitado por Previred.
- Brindar soporte para la solución de problemas según el proceso de Gestión de Problemas.
- Revisar, mantener y actualizar los planes y procedimientos correspondientes a la recuperación ante desastres y contingencias
- Velar por el Uptime y los SLA de los servicios e infraestructura donde residen.
- Atención de incidentes, contribuyendo con equipos multidisciplinarios a resolver problemas y documentar las oportunidades de mejora.
- Incorporar, colaborar, participar y fortalecer integralmente el proceso de integración y despliegue continuo del ciclo del desarrollo de aplicaciones.
- Evaluar, explotar e incorporar herramientas que permitan automatizar actividades y recursos de infraestructura, monitoreo, testing, control y administración relacionados a los servicios.
- Contribuir, colaborar y participar activamente de mesas de cooperación y coordinación con las distintas áreas, proyectos, jefes de Proyecto y células multidisciplinarias, según se estime conveniente por parte de Previred.
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE), cuentas vigentes de acceso, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

Previred contempla para una correcta administración ajustada a las normas de seguridad que se exige, el utilizar políticas de seguridad a través de Active Directory e IPA (RedHat).

Previred actualmente tiene implementadas varias herramientas de apoyo a la administración las que se detallan a continuación:

Administración centralizada Plataforma RedHat:

La administración de máquinas RHEL es realizada con la plataforma RedHat IPA, la cual permite el control centralizado de perfiles de usuario, y política de contraseñas así como a través de ésta poder establecer reglas que controlan de mejor manera los accesos entre servidores como también la convivencia entre los usuarios y los distintos servicios radicados en éstos servidores, teniendo de esta manera una administración más acotado según las necesidades que se requiera y con ello muy bien controlado.

Complementariamente a esta plataforma tenemos instalado RedHat Satellite, que es utilizado para llevar el control de versiones, del Software base ejemplo: RHEL, Jboss, entre otros, generación de templates y aplicación de parches y/o upgrade de máquinas RHEL, incluido todo el software base.

Administración centralizada Plataforma Microsoft:

Se utiliza Dominio Microsoft, manejado sobre Active Directory que administra el control de accesos y políticas de seguridad.

Para los servidores Microsoft se utiliza WSUS para la aplicación de parches críticos o recomendados.

Previred está abierta a que el oferente proponga, para la administración, herramientas diferentes a estas, con la garantía que permite iguales o mejores prestaciones que la plataforma actual.

3.28 Servicios de Administración de Base de Datos

Respecto a las bases de Datos, el oferente deberá instalar/crear/configurar/monitorear y mantener los niveles adecuados de la plataforma especificada. Asimismo, deberá realizar las tareas de mantención y administración los motores de base de datos de forma segura y considerando los niveles de criticidad operacional de cada servicio, como a su vez, apoyo en planes de rendimiento, performance y modificaciones a las bases de datos para ajustar sus especificaciones ante requerimientos de los servicios de Previred.

Entre otras, las actividades previstas son:

- Instalar, configurar y mantener actualizados los motores de bases de datos en base a lo recomendado de los proveedores de los servicios.
- Mantener, observar y monitorear los respaldos, restauraciones de los motores de bases de datos.
- Administrar y monitorear tareas aplicativas sobre los motores de bases de datos.
- Administrar y realizar la agenda de mantenimiento, administrar cambios para minimizar disrupciones del servicio.
- Implementar y ejecutar recomendaciones, buenas prácticas, parches de seguridad y de mejoras sobre el servicio para minimizar disrupciones como: (parches de seguridad del motor, actualizaciones, migraciones o cambios de versión, correcciones de errores y de rendimiento).
- Instalar y mantener la vigencia y soporte del software del motor de bases de datos. (Mantener informados a Previred sobre estas iniciativas y su impacto)
- Crear y mantener links a otras bases de datos.
- Reorganizar la data e impacto sobre el Storage o disco de almacenamiento para mejorar el desempeño.
- Verificar la ejecución de los respaldos de acuerdo con las Políticas de Respaldo y los scripts debidamente aprobados por Previred.
- Buscar errores y advertencias en archivos de logs y traces y sugerir medidas correctivas.
- Verificar y corregir niveles de fragmentación de las Bases de Datos.
- Realizar mantenciones semanales y mensuales a base de datos, de manera de asegurar el desempeño.
- Medir ejecuciones de proceso, crear alertas y realizar recomendaciones a los niveles de rendimiento de las Bases de Datos.
- Disponer acceso al aplicativo de monitoreo del oferente 24x7, perfil de sólo lectura.
- Mantener las tareas administrativas tales como indexaciones, reorganizaciones.
- Analizar los problemas de rendimiento (performance), y sugerir acciones de mejora.
- Revisar las políticas para la seguridad de acceso y privilegios a los motores y base de datos.

- Validar réplicas en instalación de contingencia de acuerdo con las Políticas de Replicación y los scripts debidamente aprobados.
- Liderar y fomentar las necesidades de automatización tecnológica de los servicios.
- Revisar las políticas de respaldo y recuperación ante catástrofes (pérdida total o parcial de la Base de Datos) de acuerdo con las Políticas de Contingencia y los procedimientos debidamente aprobados y provistos por Previred.
- Asesorar el dimensionamiento de las necesidades de almacenamiento, procesamiento y servicio de acuerdo con las especificaciones de la aplicación con el soporte de las áreas de desarrollo de software de Previred, quienes conocen las necesidades de negocio y de sus aplicaciones.
- Proveer reportes de crecimiento en tamaño y procesamiento para cada DBMS a los fines de anticipar problemas por falta de espacio y/o capacidad de procesamiento.
- Implementar procedimientos de subida y bajada de instancias y/o Base de Datos para grupos externos al grupo de Base de Datos.
- Revisiones permanentes de alertas y logs propios de los motores de Bases de Datos que pudiesen ser necesarios para mantener y/o aumentar el performance de los servicios.
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE), cuentas vigentes de acceso al motor y Base de Datos asociadas, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

3.29 Servicio de Ingeniería DevOps

Respecto a las plataformas y servicios necesarios en el ciclo de vida del desarrollo de aplicaciones definido por Previred. El oferente deberá instalar/configurar/monitorear y mantener los niveles adecuados de la plataforma especificada, colaborando en el proceso de desarrollo de software, apoyando a los equipos multidisciplinarios del área de tecnología a través de técnicas de integración y despliegue continuo que favorezcan reducir el tiempo y eficiencia para el negocio.

También es responsabilidad de el oferente de definir una arquitectura segura y de alta disponibilidad, que se pueda adaptar a diferentes tipos de integraciones y necesidades del negocio, siendo competitivo al reducir la tasa de errores y el tiempo de recuperación tras errores de forma eficiente, rápida y de calidad, a fin de promover y capacitar el modelo DevOps y organizacional que fomente la colaboración con los equipos de TI, consigan los objetivos alineados al negocio.

Deberá innovar y adaptarse al cambio de tecnologías monitorizando y observando el continuo ciclo de vida del desarrollo del software, administrando la infraestructura TI que se necesita para implementar el software en entornos de Cloud o híbridos y con acceso de múltiples usuarios, resguardando las normas y políticas asociadas a seguridad de la información. Desde los ambientes preproductivos hasta la puesta en marcha en los ambientes Productivos.

Entre otras, las actividades previstas son:

- Encargado de aprovisionar los recursos o infraestructura requeridos para los proyectos
- Asegurar la integración y despliegue continuo del ciclo del desarrollo de aplicaciones de forma segura.
- Seleccionar un modelo de implementación apropiado para los proyectos e implementar la estrategia de crecimiento tecnológico y la plataforma en general (Base de Datos, Infraestructura, Software, Seguridad).
- Análisis de resultados obtenidos en cada una de las fases del ciclo de vida del software.
- Monitorización continua de los procesos de Desarrollo, Testing y Operación.
- Mantener una comunicación constante con las áreas involucradas sobre problemas, mejoras, soluciones y cambios que impactan sobre la plataforma tecnológica.
- Soportar servicios provistos a clientes internos en el ámbito de la plataforma en general relacionado a todos los ambientes de la compañía.
- Proponer las mejoras acordadas en el proyecto de continuidad de negocio y apoyar a clientes internos a mantener la estabilidad en los servicios y aplicaciones, asistiendo oportunamente a los cambios.
- Coordinarse con las áreas de Ingeniería de Sistemas, Administración de Redes y Seguridad, Administración de Base de Datos, Desarrollo y Calidad en la implementación de nuevos proyectos. Entregando soporte de excelencia con alto experticia técnica.
- Participar de reuniones de arquitectura y análisis de proyectos. Evaluación de componentes relacionado y el posible impacto o riesgo que pueda originar el proyecto.
- Supervisar el diagnóstico y la resolución de problemas en los procesos. Mantiene la cohesión de los proyectos para que el esfuerzo invertido.
- Contribuir y participar activamente de mesas de cooperación y coordinación con las distintas áreas, proyectos, jefes de Proyecto y células multidisciplinarias.
- Ser un actor y gestor del cambio respecto de la entrega continua y su implementación End to End
- Entregar informes mensuales con indicadores definidos permitiendo ser proactivos respecto a la detección de degradación en los servicios.

- Apoyar a las áreas productivas cuando se presenten contingencias e incidencias o trabajos fuera de horario y/o fines de semanas.
- Mantener siempre una actitud proactiva, formal, de apoyo y comprensiva respecto de todos los usuarios que interaccionan con Previred.
- Fortalecer integralmente el proceso de la integración y despliegue continuo del ciclo del desarrollo de aplicaciones, incorporando herramientas modernas de administración y optimización de los recursos involucrados.
- Adquirir y promover conocimiento funcional de los productos y beneficios para el cliente, proponiendo soluciones técnicas que agreguen valor.
- Evaluar e incorporar herramientas que permitan automatizar los recursos de infraestructura, monitoreo, testing, control y administración relacionados a la integración y despliegue continuo del código fuente.
- Liderar y fomentar las necesidades de automatización tecnológica de los servicios.
- Documentar y actualizar información relevante de uso vigente para desempeñar el trabajo (monitoreo, inventarios de uso y capacidades, vigencia de infraestructura y base de conocimiento del trabajo diario)
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE), cuentas vigentes de acceso, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

3.30 Servicio de Administración de Redes y Seguridad

Respecto a las plataformas de Comunicaciones y Seguridad, el oferente deberá instalar/configurar/monitorear y mantener los niveles adecuados de la plataforma especificada.

También es responsabilidad del oferente, definir una arquitectura segura y de alta disponibilidad, que se pueda adaptar a diferentes tipos de integraciones y necesidades del negocio. Debiendo realizar las tareas de administración necesarias para garantizar la continuidad y performance de la plataforma de red y equipos de seguridad.

Entre otras, las actividades previstas son:

- Asegurar la mantención, operación y requerimientos en general asociados a las plataformas de comunicaciones y seguridad.
- Implementar, administrar y gestionar políticas en los Firewall y equipos de comunicaciones que atienden la red de Previred.
- Realizar las configuraciones a nivel de Firewall según los requerimientos definidos/solicitados
- Realizar configuraciones en los equipos de capa 2 y capa 3 de toda la plataforma de Previred
- Contraparte y apoyo para nuevas implementaciones de sistemas/servicios o integraciones, donde se requiere participar activamente en la definición del diseño y arquitectura de red.
- Gestion y monitoreo de otros enlaces como WAN, Redbanc o WAN Terceros
- Revisar configuraciones y arquitectura para ofrecer e indicar mejoras que se puedan aplicar
- Monitoreo transversal de Enlaces y Equipos de comunicaciones y seguridad, revisiones de Log de FW, routers, switches, etc.
- Realizar revalidación de reglas de firewall de forma semestral
- Monitoreo, revisión y análisis a eventos de seguridad que se presenten en alguna de las plataformas como IPS, WAF, entre otros.
- Generar respaldos periódicos de todas las configuraciones de los equipos de comunicación y seguridad
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE, si aplica), cuentas vigentes de acceso, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

3.31 Servicios Internos y de Colaboración

Respecto a los servicios internos, llámese dominio de usuarios, y otros servicios de apoyo al negocio, el oferente deberá instalar/configurar/monitorear y mantener los niveles adecuados de la plataforma especificada.

También es responsabilidad del oferente, definir una arquitectura segura y de alta disponibilidad, que se pueda adaptar a diferentes tipos de integraciones y necesidades del negocio. Debiendo realizar las tareas de administración necesarias para garantizar la continuidad y performance de la plataforma que soporte los servicios internos.

Entre otras, las actividades previstas son:

- La función principal es la mantención, operación, monitoreo, respaldo y aseguramiento de la continuidad de los servicios internos o de colaboración.
- Mantener actualizado los sistemas de seguridad que protejan la plataforma de servicios internos.
- Asegurar la confidencialidad en la administración de los servicios internos o de colaboración.
- Monitorear la plataforma de servicios internos de colaboración, asegurando la disponibilidad.
- Mantener actualizada, monitoreada y supervisada, la plataforma de virtualización en que residan los diferentes servicios internos
- Mantener actualizado, monitoreado y supervisados, los servidores y máquinas virtuales que brinden servicios internos.
- Realizar las reasignaciones de usuarios y las reinstalaciones necesarias de los escritorios virtuales, de forma oportuna.
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE), cuentas vigentes de acceso, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

3.32 Administración de otros Servicios de Capa Media Críticos

Para la correcta administración, el profesional a cargo debe innovar, gestionar, mantener, promover, explotar y adaptarse a las tecnologías utilizadas e instaladas en las plataformas y servicios utilizados e implementados por Previred.

Debe contar con capacitaciones, certificaciones y habilidades técnicas para planificar, controlar, automatizar, resolución de problemas y apoyar en la continuidad operacional de los servicios tecnológicos descritos de forma segura y proactiva.

Pudiesen existir instancias en los que se vayan a requerir mesas de trabajo multidisciplinar ante la necesidad de implementación de algún proyecto o alguna resolución crítica de incidencia con lo cual se va a requerir apoyo de profesionales cualificados, quienes puedan brindar apoyo desde su punto de vista, así como para aportar soluciones a las distintas casuísticas que vayan existiendo a lo largo de la operación.

3.33 Servicio de Administración de Colas de Mensajería

3.33.1 Servicio de Administración de RedHat AMQ Broker

Con relación al servicio RedHat AMQ, el oferente deberá mantener los niveles adecuados de la plataforma especificada. Asimismo, deberá realizar las tareas de Mantención y administración adecuadas al nivel de criticidad de esta plataforma de mensajería especificada, como a su vez apoyo en planes de rendimiento y performance. Cada vez que se requiera se realizarán las modificaciones a las colas AMQ para ajustar sus especificaciones a los aplicativos internos. Para ello, se permitirá el acceso al personal de Previred con privilegios de administración.

Entre otras, las actividades previstas son:

- Instalación, mantención y configuración del servicio.
- 'Tunning' y resolución de problemas del software para cumplir con niveles de servicio.
- Actualizaciones periódicas propias del software y actualización del producto según EOL.
- Revisión y optimización avanzada del producto. Se requiere conocimiento avanzado.
- Revisión, análisis de performance e implementación de mejoras según sea necesario.
- Revisión de disponibilidad del servicios e integridad de los datos o mensajes.
- Revisión y análisis de Log.
- Análisis, seguimiento y corrección ante incidencias y su posterior documentación.
- Revisiones permanentes de alertas y log propios de la aplicación.
- Documentar y mantener un registro periódico de las mantenciones, actualizaciones de hardware y software, cambios en las aplicaciones.
- Monitoreo de objetos propios de AMQ (profundidad de cola, conexiones abiertas, estado de los canales, etc.)
- Informes mensuales: cambios relevantes de cluster RedHat AMQ Broker, log, parches, vulnerabilidades, plan de mejoras.
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE), cuentas vigentes de acceso, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

El servicio actualmente operando, se encuentra en la versión: RedHat AMQ 7.9.2

3.33.2 Servicio de Administración de WebSphere MQ

Con relación al servicio WebSphere MQ, el oferente deberá mantener los niveles adecuados de la plataforma especificada. Asimismo, deberá realizar las tareas de Mantención y administración adecuadas al nivel de criticidad de esta plataforma de pagos especificada, como a su vez apoyo en planes de rendimiento y performance. Cada vez que se requiera se realizarán las modificaciones a las colas MQ para ajustar sus especificaciones a los aplicativos internos. Para ello, se permitirá el acceso al personal de PREVIRED con privilegios de administración.

Entre otras, las actividades previstas son:

- Instalación, mantención y configuración del servicio.
- 'Tunning' y resolución de problemas del software para cumplir con niveles de servicio.
- Actualizaciones periódicas propias del software y actualización del producto según EOL.
- Revisión y optimización avanzada del producto. Se requiere conocimiento avanzado.
- Revisión, análisis de performance e implementación de mejoras según sea necesario.
- Revisión de disponibilidad del servicios e integridad de los datos o mensajes.
- Revisión y análisis de Log.
- Análisis, seguimiento y corrección ante incidencias y su posterior documentación.
- Revisiones permanentes de alertas y log propios de la aplicación.
- Documentar y mantener un registro periódico de las mantenciones, actualizaciones de hardware y software, cambios en las aplicaciones.
- Monitoreo de objetos propios de MQ (profundidad de cola, conexiones abiertas, estado de los canales, etc.)
- Informes mensuales: cambios relevantes de clúster MQ, log, parches, vulnerabilidades, plan de mejoras.
- Generar y entregar a Previred, informe de gestión mensual con información que contemple: Estado de la seguridad, rendimiento, alertas, uso de los recursos, inventarios y crecimiento esperado de (CPU, RAM, STORAGE), cuentas vigentes de acceso, validación del cumplimiento de la política de accesos y contraseñas. Cambios relevantes, visor de eventos, plan de mejoras y recomendaciones.

El servicio actualmente operando se encuentra en la versión: WebSphere MQ versión 9.1.2

3.34 Gestión de los Pasos a Producción

Será el oferente el encargado de la gestión de cambio tanto a nivel de configuraciones como cambios aplicativos en los ambientes Productivos de Negocio.

Todos los cambios en plataformas productivas deben programarse fuera de horario o en ventana de mantención definida para cada uno de los servicios, por ejemplo: aplicación de parches de seguridad, cambios en configuraciones tanto a nivel de sistema operativo como a nivel aplicativo, entre otros.

Existen 3 tipos de controles de cambio: a) por incidencias, b) cambios planificados y c) no planificados. Los controles de cambio aplicativos se rigen en el siguiente marco:

a) Los controles de cambio por incidencia, que corrigen errores que se encuentran en producción y requieren urgencia de resolución y deben ser aplicados en cualquier horario, en coordinación con Previred.
b) Los controles de Cambio planificados, provenientes de la aplicación de mantenciones que son una agrupación de requerimientos menores y de menor urgencia o la implementación de algún nuevo servicio o proyecto que se planifica anticipadamente su puesta en producción y que son aplicados de lunes a viernes durante la ventana 00:00 hrs a 07:00 hrs., en coordinación con Previred.
c) Los controles de cambio no programados, de forma similar al anterior con la salvedad que este no fue coordinado previamente su ejecución, por la cual no se encuentra calendarizado su aplicación. Estos son coordinados internamente durante la misma ventana entre las 00:00 hrs a 07:00 hrs.

La gestión, coordinación y ejecución del control de cambio en producción debe ser llevada a cabo por el equipo de especialistas dedicado para Previred (equipo POD Team) o los especialistas necesarios para llevar a cabo el control de cambio, todo esto bajo el procedimiento entregado por Previred en un Consejo Asesor de Cambio (CAB), para asegurar, coordinar, evaluar, revisar y aprobar los cambios que afecten la operación y continuidad alineada con el negocio.

Es responsabilidad del oferente controlar el cambio y garantizar que quede bien implantado. El objetivo es maximizar la productividad minimizando los errores. Previred certifica los controles de cambio previo al paso a producción en el ambiente de QA y también certifica post paso a producción.

El flujo establecido a seguir tras la recepción de la solicitud de control de cambio por parte del área de Calidad viene establecido por el Procedimiento de Solicitud de Control de Cambios Aplicativos a Data Center.

3.35 Servicios Adicionales

3.35.1 Servicio de administración de contraseñas y claves maestras, desbloqueo de claves para los dominios de Previred

Servicio complementario al soporte telefónico provisto por la Mesa de Ayuda de Previred y consiste en que se deja a disposición del usuario final una aplicación web que le permite realizar el desbloqueo de su(s) clave(s) de acceso a él o los dominios de Previred.

La disponibilización y construcción de la aplicación debe ser realizada de acuerdo a las políticas de manejo de claves de PREVIRED y de acuerdo a los flujos aprobadores. Esta aplicación debe permitir la administración centralizada de contraseñas y claves maestras

Se debe administrar la plataforma donde radica la aplicación y con administrar se entiende, como mínimo, por:

- Monitorear
- Respaldar
- Actualizar
- Parchar
- Mitigación de vulnerabilidades

Esto aplica tanto para la aplicación como para las herramientas e infraestructura que la soportan.

3.35.2 Servicio de Relay de Correo.

Servicio requerido para el envío masivo de correos electrónicos, debe ser una plataforma pensada en alta disponibilidad, capaz de procesar al menos 300.000 correos diarios, actualmente soportado por servidores Linux con Postfix y Dovecot que responden a dominios o registros MX de propiedad de Previred.

Los correos enviados son de distinta índole, pero es prioritario que los correos sean enviados o despachados de forma rápida ya que podrían estar asociados a recuperación de contraseñas, estatus de servicios en las plataformas, notificaciones normativas, cuadraturas de información de procesos y monitoreo alertas.

Los aplicativos de Previred sólo pueden configurar una dirección IP o FQDN con su respectiva seguridad para el envío de correos, por lo que el servicio debe contar con acceso VIP y alta disponibilidad y tolerancia a envíos masivos de los servicios de notificación.

El servicio debe brindar:

- Obtener estatus e información y reportes de correos entregados, rechazados, rebotes, etc...
- Poder enviar correos desde múltiples direcciones IP para evitar bloqueos.
- Implementar normas y políticas de seguridad sobre el servicio de envió de correo, por ejemplo, SPF, DKIM entre otros.
- Direcciones IPs Publicas exclusivas.
- Envío de correos diarios aprox.:300.000
- La plataforma debe ser actualizadas y mantenida para cumplir con el ciclo de vida vigentes de sus componentes y protocolos de forma segura.

3.35.3 Envío de Email para campañas de Marketing

Previred utiliza Sendgrid para realizar campañas de envío masivo de correo electrónico hacia sus clientes. El oferente debe proporcionar una plataforma o servicio de igual características o mejor para este servicio que cumpla, como mínimo, con lo siguiente:

- Manejo de contactos y grupos de contactos
- IPs públicas exclusivas.
- Configuraciones de seguridad como mínimo SPF y DKIM
- Editor de Templates
- Campos personalizables.
- Reportería asociada a las campañas de envió masivo de correos.
- Analítica personalizable en tiempo real.
- Crear informes basados en el calendario, la categoría de email, el ISP, la región y el tipo de dispositivo.

3.36 Responsabilidad del Software Aplicativo

Es responsabilidad de Previred la correcta operación de la capa aplicativa de negocio, es responsabilidad del oferente el monitoreo del desempeño óptimo de la plataforma y de los tiempos de respuesta de cada componente que aseguren los SLA para cada servicio. Se indica explícitamente que la plataforma que soporta la aplicación es de total responsabilidad del oferente.

El oferente deberá permitir el acceso para la administración y mantención a los Software Aplicativos vía acceso remoto y físico a las instalaciones a personal de Previred.

En el caso que se requiera proporcionar soporte al aplicativo a través de otros proveedores, el oferente deberá dar las facilidades para que los aplicativos reciban el soporte establecido.

3.37 Servicios de Respaldo, Retención y Recuperación

Se solicita al oferente el servicio de realizar y asegurar la correcta operación de respaldo, retención y recuperación de data e información corresponde a:

- Implementar los respaldos en la plataforma, de acuerdo a las políticas y procedimientos definidos y documentados en conjunto con Previred.
- Ejecutar, monitorear y verificar la ejecución de los respaldos de acuerdo a las políticas y procedimientos acordados entre el oferente y Previred.
- Controlar y ejecutar los procesos de respaldo y restauración en la infraestructura suministrada por Previred, según las políticas definidas por Previred, o en caso de que sea requerido.
- Definir una red de datos específica para respaldos para que los procesos productivos/otros no sean afectados por estos.
- Se debe considerar la provisión de cintas necesarias para otorgar el servicio, según corresponda y sea necesario según la propuesta del oferente.
- Los respaldos de máquinas es 100% responsabilidad del oferente, el que tiene que garantizar una correcta recuperación y en tiempos acorde a los SLAs establecidos para cada servicio
- Velar por la instalación, configuración y actualización de los agentes de respaldo en los servidores.
- Realizar controles diarios a los logs de respaldo y mantener una bitácora diaria del control de los respaldos en la infraestructura suministrada y administrada por el oferente.
- Monitorear el software y hardware de respaldo.
- Controlar que los respaldos se realicen en la ventana horaria definida de tal forma de no entorpecer la operación normal de los sistemas.
- Entrega de Informes diarios con resultados de los respaldos, detallado por máquina.
- Generar propuestas de mejoras o cambio de parámetros o condiciones de los equipos de respaldo que permitan el mejoramiento continuo de la plataforma de respaldos.
- Escalar al grupo de soporte los problemas de respaldo y restauración.
- Generar métricas de control como las siguientes: cantidad de respaldos / restauraciones planificadas, porcentaje de respaldos / restauraciones exitosas, porcentaje de procesos cancelados.

- Realizar periódicamente pruebas de restauración de los respaldos a objeto de probar la capacidad, seguridad, efectividad y tiempo estimado para restablecer la información contenida en ellas.
- Velar por la efectividad de los respaldos efectuados en la plataforma e informar cancelaciones, errores y omisiones.
- Mantener actualizado los manuales y procedimientos asociados al servicio de respaldo.
- Proveer la infraestructura para efectuar las restauraciones de información para las pruebas de validación de procedimientos o recuperación de información histórica.
- Proveer el soporte de mantenimiento de hardware, de la plataforma histórica (En caso de ser requerida)
- Responder a las solicitudes de restauración y respaldo dentro de los plazos establecidos.
- Velar por la custodia física de todos los medios magnéticos, tanto históricos como vigentes, en los Centros de Cómputo del oferente.
- Verificar el estado de los soportes físicos que contienen las copias de seguridad, comprobando que los respaldos son capaces de recuperar la información respaldada.
- Copia de seguridad de respaldo mensual, que debe ser entregado en las oficinas de Previred, es requisito que el traslado de las cintas sea realizado por personal del Datacenter en transporte especializado en transporte de especies valoradas, de manera de minimizar riesgos de robo, las cintas deben entregarse rotuladas acorde a los procedimientos de PREVIRED y con un detalle del contenido.
- El Data Center debe entregar el servicio de almacenaje en cintoteca externa al data center, la cual debe contar con todas las garantías para que las cintas sean resguardadas en forma adecuada, y con la seguridad requerida.
- Realizar la apertura de ticket de incidentes, requerimientos, problemas y cambios en la Mesa de Ayuda de Previred, frente a una condición anormal del servicio.
- Resolver los tickets de incidentes, requerimientos, problemas y cambios que le han sido asignados.
- Realizar y registrar el proceso de escalamiento, en caso de que le sean asignados ticket de incidentes que no estén dentro de las responsabilidades del oferente, a las unidades resolutivas según lo indicado en el Procedimiento de Escalamiento.
- Realizar y registrar el proceso de derivación en caso de que le sean asignados ticket de incidentes que no estén dentro de las responsabilidades del oferente, a las unidades resolutivas según lo indicado en el Procedimiento de Derivación.
- Supervisar, controlar y ejecutar los procedimientos de contingencia que involucren actividades a realizar en este servicio.
- Llevar el registro en las bitácoras respectivas de los eventos del servicio.
- Generar la información para el control del cumplimiento de los Niveles de Servicio acordados.
- Brindar soporte para la solución de problemas según el proceso de Gestión de Problemas.
- Brindar soporte para la solución de cambios según el proceso de Gestión de Cambios.
- Revisar, mantener y actualizar los planes y procedimientos correspondientes a la recuperación ante desastres y contingencias de este servicio.
- Las cintas al final de contrato son propiedad de PREVIRED, según si aplique dependiente de la propuesta del oferente.

Para mayor detalle, ver anexo: "Anexo N° 5 Procedimiento de Respaldo, Retención y Recuperación de la Información"

3.38 Estudio de la Capacidad y Rendimiento

Este servicio tiene como objetivo contar con un análisis permanente del rendimiento y capacidad de hardware de la plataforma en su totalidad, tasas de crecimientos de data, tráfico de red y calidad de servicio, identificando carencias o riesgos en el día a día del servicio, y en particular los días peak de cada negocio.

Producto de este análisis, más los datos de crecimiento del negocio a proporcionar por Previred, se espera un estudio de capacidad mensual y anual que le permita a Previred planificar y provisionar oportunamente la infraestructura o desarrollos requeridos.

El oferente debe entregar un informe mensual de toda la plataforma Previred, indicando la media de uso de cada componente de la plataforma, a su vez declarar los riesgo y mejoras necesarias detectadas con su respectivo plan de trabajo.

Una vez al año, en el mes de agosto, el oferente debe entregar un informe anual consolidado. Este informe anual consolidado, debe señalar la variación mes a mes por el transcurso de un año del estado de algunos de los parámetros representativos que conforman la infraestructura y plataforma TI, como ancho de banda, consumo de CPU, I/O, porcentaje de uso de memoria, porcentaje de utilización de disco detallado por servicio, entre otros, y con ello, las recomendaciones en cuanto a crecimientos de capacidad, rendimiento y optimizaciones de la Infraestructura de tal manera de asegurar la continuidad del negocio y seguridad, para el año siguiente.

3.39 Licencias de Software

Se debe distinguir entre 2 tipos de licencias: el primer tipo: son las licencias que el Data Center requiere para la habilitación de los servicios, sobre las cuales el oferente será el responsable de su provisión, entiéndase por éstas Licencias de Antivirus, Software especializados de Respaldo y Recuperación, Plataforma de Monitoreo, Virtualización, entre otras, y un segundo tipo de licencias que denominaremos Software Base, estas son licencias de Sistema Operativo, Base de Datos, MQ Series, en que Previred declara tener el listado descrito en Anexo N° 3 "Licencias Propiedad de Previred" y que el oferente podrá disponer para habilitar los servicios, en caso que estas licencias no sean suficientes por cambio de arquitecturas, o procesador de servidores ofertados, el oferente deberá declarar cual es el delta faltante y cotizar en forma separada.

Como parte del servicio, el oferente deberá considerar el pago anual de Soporte y Actualización del total de las licencias Microsoft y MQ Series u otras, tanto de las que son propiedad de Previred, como las posibles adicionales que deba contratar. Adicionalmente debe contratar la suscripción Anual del S.O. Red Hat, para todo el parque de máquinas, actual o nuevas.

Se exceptúan de este pago las licencias Oracle que Previred cancelará directamente.

3.40 Seguridad de la Información y Ciberseguridad

El oferente debe garantizar los principios básicos de la seguridad de la información, cumpliendo el propósito de esta licitación y sobre la base de:

- Disponibilidad.
- Confidencialidad.
- Integridad

3.40.1Requerimiento de Certificación en Seguridad

Se requiere que el servicio ofrecido cuente con una certificación en la norma ISO/IEC 27001 de Seguridad de la Información u homóloga, en caso de existir actualizaciones y/o reemplazo de la misma, por parte de una firma acreditada ante la United Kingdom Accreditation Service (UKAS), la Deutsche Akkreditierungsstelle (Dakks) u otra que acredite el oferente a conformidad de Previred.

La certificación antes mencionada, deberá acreditarse anualmente ante Previred mediante el certificado correspondiente y/o los informes de auditoría de seguimiento realizados por el certificador. En este contexto, el oferente se compromete a abordar todos los hallazgos emanados de dichos informes, los cuales deberán ser comunicados a Previred.

La certificación deberá estar vigente a la fecha de la licitación y a la fecha de la adjudicación e implementación del servicio, de ser el caso, y deberá permanecer válida mientras el contrato no haya expirado y/o caducado. Cabe señalar que la Declaración de Aplicabilidad (SOA) que conlleva toda certificación, deberá, asimismo, ser comunicada a Previred.

La implementación de la Política de Seguridad será responsabilidad del oferente, siendo Previred el dueño de la política de seguridad.

Los contenidos que al menos debe considerar esta declaración (SOA) son los siguientes:

N°	Descripción
5	**Controles organizativos**
5.1	Políticas de seguridad de la información
5.2	Funciones y responsabilidades de seguridad de la información
5.3	Segregación de funciones
5.4	Responsabilidades de gestión
5.5	Contacto con autoridades
5.6	Contacto con grupos de interés especial
5.7	Inteligencia de amenazas
5.8	Seguridad de información en gestión de proyectos
5.9	Inventario de información y otros activos asociados
5.10	Uso aceptable de información y otros activos asociados
5.11	Retorno de activos
5.12	Clasificación de información
5.13	Etiquetado de información
5.14	Transferencia de información
5.15	Control de acceso
5.16	Gestión de identidad
5.17	Información de autenticación
5.18	Derechos de acceso
5.19	Seguridad de la información en la relación con los proveedores
5.20	Acercamiento a la seguridad de la información en acuerdos con proveedores
5.21	Gestión de seguridad de la información en la cadena de suministro de ICT
5.22	Monitoreo, revisión y gestión de cambios de servicios del proveedor
5.23	Seguridad de la información para uso de servicio en la nube
5.24	Planificación y preparación de gestión de incidentes de seguridad de la información
5.25	Evaluación y decisión sobre eventos de seguridad de la información
5.26	Respuesta a incidentes de seguridad de la información
5.27	Aprendizaje sobre incidentes de seguridad de la información
5.28	Recolección de pruebas
5.29	Seguridad de la información durante interrupción
5.30	Preparación de ICT para continuidad de actividad
5.31	Requisitos legales reglamentarios y contractuales
5.32	Derechos de propiedad intelectual
5.33	Protección de registros
5.34	Privacidad y protección de PII
5.35	Revisión independiente de seguridad de la información
5.36	Cumplimiento de políticas, reglas y normas de seguridad de la información
5.37	Procedimientos operativos documentados
6	Controles de personas
6.1	Control

6.2	Términos y condiciones de trabajo
6.3	Concientización, educación y capacitación de seguridad de la información
6.4	Proceso disciplinario
6.5	Responsabilidades tras el cese o cambio de empleo
6.6	Acuerdos de confidencialidad o no divulgación
6.7	Trabajo a distancia
6.8	Informe de eventos de seguridad de la información
7	Controles físicos
7.1	Perímetros de seguridad física
7.2	Acceso físico
7.3	Aseguramiento de oficinas, salas e instalaciones
7.4	Supervisión de seguridad física
7.5	Protección contra amenazas físicas y medioambientales
7.6	Trabajo en zonas seguras
7.7	Escritorio y pantalla despejados
7.8	Ubicación y protección de equipos
7.9	Seguridad de activos fuera de las instalaciones
7.10	Medios de almacenamiento
7.11	Servicios de apoyo
7.12	Seguridad de cableado
7.13	Mantenimiento de equipo
7.14	Eliminación segura o reutilización de equipos
8	Controles tecnológicos
8.1	Dispositivos terminales de usuario
8.2	Derechos de acceso privilegiado
8.3	Restricción de acceso a la información
8.4	Acceso a código fuente
8.5	Autenticación segura
8.6	Gestión de capacidad
8.7	Protección contra "malware"
8.8	Gestión de vulnerabilidades técnicas
8.9	Gestión de configuración
8.10	Supresión de información
8.11	Enmascaramiento de datos
8.12	Prevención fuga de datos
8.13	Respaldo de información

N°	Descripción
8.14	Redundancia de instalaciones de tratamiento de información
8.15	Registro

8.16	Actividades de monitoreo
8.17	Sincronización de reloj
8.18	Uso de programas privilegiados de utilidad
8.19	Instalación de "software" en sistemas operativos
8.20	Seguridad de redes
8.21	Seguridad de servicios de red
8.22	Segregación de redes
8.23	Filtro web
8.24	Uso de criptografía
8.25	Ciclo de vida de desarrollo seguro
8.26	Requisito de Seguridad de las aplicaciones
8.27	Principios de ingeniería y arquitectura de sistemas seguros
8.28	Codificación segura
8.29	Pruebas de seguridad de desarrollo y aceptación
8.30	Desarrollo externo
8.31	Separación de entornos de desarrollo, prueba y producción
8.32	Gestión de cambio
8.33	Información de prueba
8.34	Protección de sistemas de información durante pruebas de auditoría

En caso de que alguno de los controles no aplique, se deberá indicar argumento de su exclusión en el proceso de la licitación.

3.40.2 Servicios Base de seguridad

Este requerimiento constituye un requerimiento mínimo a proporcionar en materia de seguridad, el objetivo es contar con plataformas protegidas por dispositivos de seguridad y en alta disponibilidad en todas sus capas.

Es ideal que todos los componentes cuenten con una interfaz web para que Previred o quien defina pueda tener accesos full a todos los equipos/dispositivos, todos los accesos entregados a Previred serán en modo lectura, la administración de los dispositivos debe ser de responsabilidad del oferente.

Se deberán realizar reuniones, como mínimo, mensuales para revisión de eventos y mejoras del servicio, además contar con un Informe mensual de Seguridad con descripción de eventos y las recomendaciones de mejora.

Los requerimientos mínimos a nivel de seguridad son:

- **Contar con un SOC** de Seguridad 24x7, cuyas funciones mínimas correspondan a supervisar, prevenir, detectar, investigar y responder a las amenazas cibernéticas.
- **Firewall Perimetral PRO (HA)** para ambientes de producción, exclusivos para Previred, con acceso WEB. Se puede ofrecer plataformas virtualizadas, considerando que soporten el volumen de tráfico/tiempos de respuesta en los periodos de mayor acceso a la plataforma.
- **Firewall Perimetral PREVIOS (HA)** para ambientes previos como Desarrollo, QA, Homologación, etc.., exclusivos para Previred, con acceso WEB. Se puede ofrecer plataformas virtualizadas.

- **IPS** o equipamiento equivalente a la fecha de la puesta en marcha. Es importante señalar que, dado el plazo del contrato y evolución tecnológica, es indispensable el oferente actualice las plataformas de seguridad según las nuevas tecnologías que estén vigentes y que permitan cumplir con las mejores prácticas en materia de seguridad.
- **SIEM**, sistema de gestión de eventos e información de seguridad que recopile, normalice y correlacione datos para identificar los incidentes de seguridad que se puedan producir en la plataforma, considerando equipos de comunicación, seguridad y servidores, entre otros, que se definan.
- **Anti DDOS** sistema para proteger la infraestructura frente a ataques DDoS de forma continua a través del filtrado y limpieza en la nube, Anti DDos debe evitar que los ataques colapsen las conexiones/enlaces/plataforma, permitiendo recibir solo el tráfico habitual de los usuarios y clientes.
- **WAF**, Web Application Firewall, para proteger a las aplicaciones web de diversos ataques en la capa de aplicación, como cross-site scripting (XSS), inyección de SQL o envenenamiento de cookies, entre otros.

El servicio base de seguridad debe contar con una solución de monitoreo y administración automatizado de usuarios privilegiados, capacidad de control de acceso y monitoreo de los usuarios privilegiados de servidores y aplicaciones. Por ejemplo, administradores de firewalls u otros. También debe contar con la capacidad de asignación de credenciales temporales a los usuarios privilegiados y de mecanismos heurísticos o reglas configurables (eliminar el resguardo de cuentas de administración en sobres), para la generación de alertas ante comportamientos de acceso sospechosos.

3.40.3 Servicios Adicionales de Seguridad

- Ethical Hacking
  - El servicio de Ethical hacking para los servicios de PREVIRED debe garantizar la confidencialidad, integridad y disponibilidad de los servicios.
  - Se debe realizar análisis interno y externo de los servicios priorizados por PREVIRED, mínimo 3 veces al año.
  - El proceso de este servicio debe cubrir los requerimientos de instalación, administración, reportería, apoyo en la remediación y verificación post mitigación.
  - DEFINIR ALACANCE, EJ. SERVICIOS CRÍTICOS

- Análisis Forense
  - El servicio de análisis de seguridad forense sobre posible ataques o eventos se seguridad sobre la plataforma, equipos o servicios de PREVIRED.
  - Este servicio debe cubrir los requerimientos propuestos por PREVIRED, para identificar, preservar, obtener, documentar y análisis de la información.
  - DEFINIR ALACANCE, EJ. SERVICIOS CRÍTICOS

- Especialista Blue Team.
  - El servicio de experto en ciberseguridad especializado en analizar el comportamiento de los sistemas de PREVIRED.

  - Este servicio debe cubrir los requerimientos propuestos por PREVIRED de análisis, recomendaciones y remediaciones manera proactiva sobre la plataforma sobre ataques de ciberseguridad.
  - DEFINIR ALACANCE, EJ. SERVICIOS CRÍTICOS

- Análisis Pentesting.
  - El servicio para determinar el alcance de los fallos de seguridad de los sistemas de PREVIRED.
  - Especialista debe seguir los procesos determinados para garantizar las mitigaciones de los fallos o vulnerabilidades en los sistemas detectados
  - Este servicio debe cubrir los requerimientos propuestos por PREVIRED de análisis, determinar, recopilación de la información y elaboración del informe sobre la plataforma auditada.
  - DEFINIR ALACANCE, EJ. SERVICIOS CRÍTICOS

- Análisis de Vulnerabilidades
  - El servicio para determinar el análisis, riesgo y la capacidad de predecir problemas de seguridad de acuerdo con el tipo de impacto.
  - Este servicio debe proporcionar información y control de las vulnerabilidades de los sistemas detectados sobre los activos que PREVIRED defina.
  - DEFINIR ALACANCE, EJ. SERVICIOS CRÍTICOS

3.41 Requerimientos de Auditoria

3.41.1 Requisitos relacionados con estándares de auditoría

Se requiere que el servicio ofrecido sea auditado anualmente bajo los estándares SSAE18 Tipo 2 y AT-205 Tipo 2.

La auditoría deberá ser realizada por una firma de auditoría externa (de las denominadas BIG FOUR) inscrita debidamente en los registros de la Comisión para el Mercado Financiero (CMF), empresa que deberá emitir el resultado de la evaluación en un informe dirigido a la Gerencia de Riesgos y Contraloría de Previred y a sus Auditores Externos de Estados Financieros.

El informe deberá entregarse a más tardar al 31 de enero de cada año o hábil siguiente (respecto del año anterior evaluado).

El informe emitido deberá tener la característica de un reporte Tipo II. Esta característica implica que la revisión deberá contemplar la evaluación por diseño e implementación de los controles internos más el testeo de efectividad operacional respecto de al menos 10 meses del año calendario evaluado.

3.41.2Inspecciones o auditorias por parte de PREVIRED

El oferente deberá proporcionar oportunamente las facilidades correspondientes ante requerimientos de parte de Previred, cuando se requiera documentación, antecedentes, evidencias o visitas, para comprobar el adecuado desempeño de los servicios entregados, como, asimismo, deberá dar estas mismas facilidades a auditores externos que haya contratado PREVIRED en el contexto de un trabajo que requiera realizar. En este último caso, el costo de la auditoría será de cargo del oferente.

3.42 Continuidad de Negocio

3.42.1 Site secundario y/o contingencia

Previred, consciente de su importancia dentro del sistema de seguridad social, necesita asegurar la continuidad de su negocio para satisfacer los requerimientos acordados con las partes interesadas, en particular, para asegurar la calidad y la disponibilidad de sus servicios hacia sus clientes.

En ese contexto, como parte de su Sistema de Gestión de Continuidad del Negocio, certificado en la ISO 22301:2019, Previred ha definido su Business Continuity Plan (BCP), el que contiene los procedimientos para responder a los distintos tipos de disrupciones que pudiesen interrumpir la operación normal de sus servicios. Uno de estos procedimientos es el Disaster Recovery Plan (DRP), por el que Previred en la actualidad posee un Site de Contingencia ante Desastres con plataforma 100% redundante y réplica de datos a nivel de Storage online.

La solución debe considerar enlaces FC redundates y con diferentes proveedores de servicio.

Los requerimientos respecto a la solución Disaster Recovery Plan (DRP) de PREVIRED son los siguientes:

- Se solicita al oferente realizar pruebas de DRP 6 veces al año asegurando la Continuidad Operativa de los servicios de Previred, en sus líneas de negocio.
- Se solicita que el oferente del Data Center Principal participe activamente en la realización de las pruebas programadas anualmente y que sea contraparte en la activación y desactivación de la réplica de datos. Por tanto, se debe considerar la participación de un team multidisciplinario compuesto al menos de: Líder de Servicios, POD TEAM, Ingenieros de Comunicaciones, Ingeniero de Sistemas, Administrador de Base de Datos, entre otros necesarios, tanto en las tareas previas de preparación como el día mismo de la ejecución de las pruebas (activación y desactivación), tareas a realizarse fuera de horario laboral.

La solución utilizada actualmente, como se observa en la imagen, es réplica de Storage a Storage y exige la conexión de las SAN entre Data Center principal y secundario a través de los Switch SAN, estos Switch deben disponer de 4 bocas disponibles para la interconexión. Los equipos SVC requeridos para implementar esta solución son provistos por el oferente del Data Center Secundario.

La solución de réplica considera, el caso de Servidores de BD Físicos, sólo la réplica de las bases de datos, en el caso de Servidores Virtuales, se replican Servidores completos.

El oferente puede realizar contingencia tanto on-premise o cloud, siempre asegurando la calidad, rendimiento, la continuidad operativa y la seguridad de los servicios.

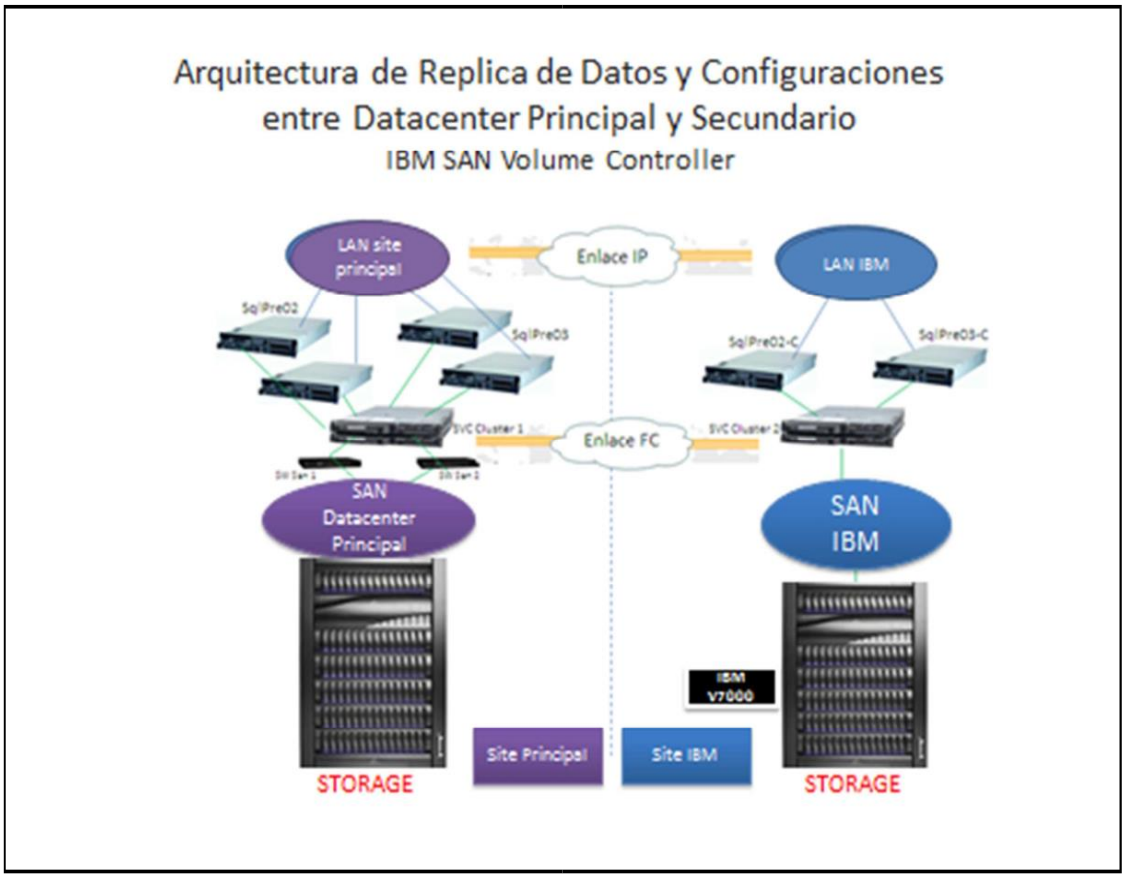


Ilustración 9: Diagrama de Conectividad Arquitectura de Réplica de Contingencia

La modalidad propuesta por el oferente debe permitir mantener el desempeño y los tiempos de respuesta acordados en los SLA de cada servicio dentro de esta modalidad, por lo que sus RTO (Recovery Time Objetive) deben ser capaz de responder en menor o igual tiempo a los MTPD (Maximum Tolerable Period of Disruption) de cada servicio definido en el BIA (Business Impact Analysis) de Previred.

Previred privilegiará a aquellos oferentes que propongan modalidad Activo-Activo en la solución de DRP, esto incluye todo lo necesario para tener adicionalmente un diseño de RED extendida entre sites.

3.42.2 Planes de Contingencia y Restauración de servicios

Se debe contar con planes de contingencia que consideren procedimientos de recuperación y restauración del servicio en los SLA definidos, específicos para el total de la plataforma y los servicios prestado, incluidas la plataforma de comunicaciones y seguridad.

El plazo de entrega de este plan no debe exceder 90 días contados desde la puesta en marcha del servicio.

3.43 Servicio de Monitoreo y Observabilidad

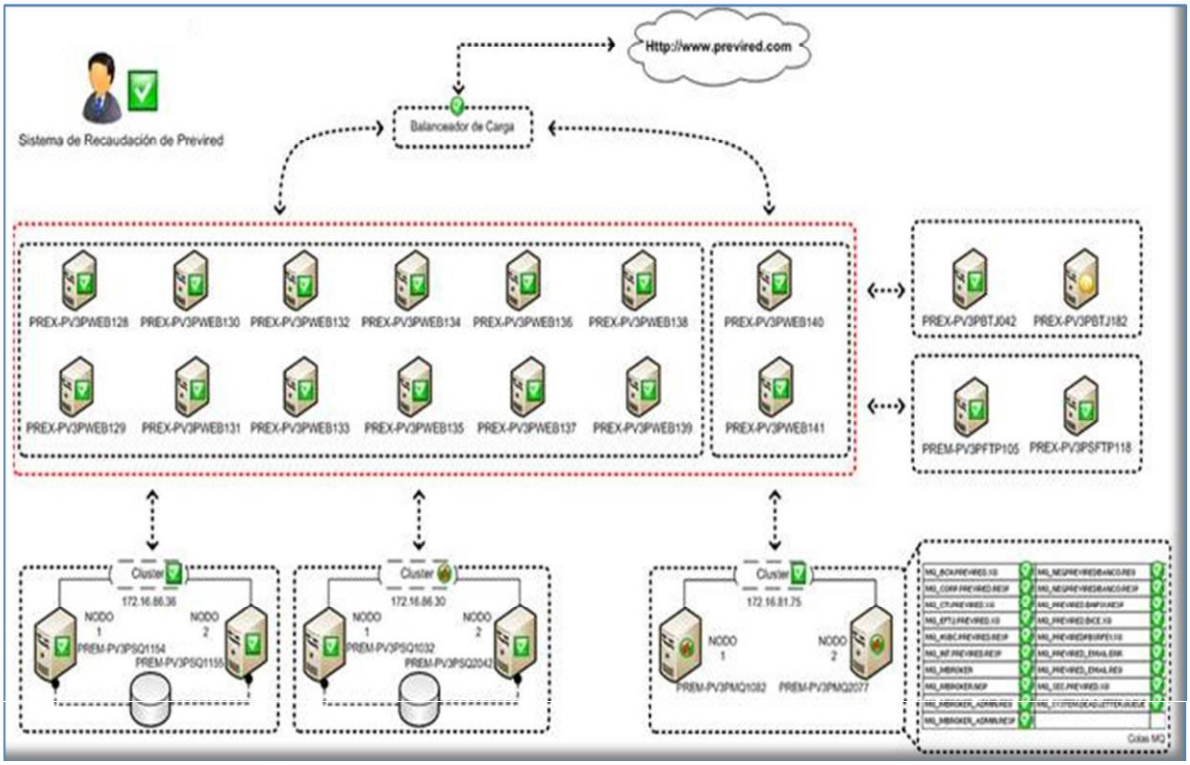
El objetivo del servicio de Monitoreo y Observabilidad deberá ser capaz de identificar el comportamiento de los sistemas e infraestructura TI en toda su trazabilidad, End to End, que puedan presentar posibles riesgos, eventos, intrusos, fallos de seguridad, amenazas y errores, con la finalidad de ayudar a mitigar y anteponerse a la materialización de incidentes y problemas que impidan las operaciones del sistema mediante cambios proactivos y apoyar en la reducción del tiempo de inactividad y pérdidas de servicio del negocio.

Se deberá monitorear, observar, analizar y securitizar el desempeño, la disponibilidad y trazabilidad de los componentes de los diferentes servicios en tiempo real mediante la recopilación, visualización y control de los registros de eventos y métricas, garantizando la disponibilidad de los servicios involucrados.

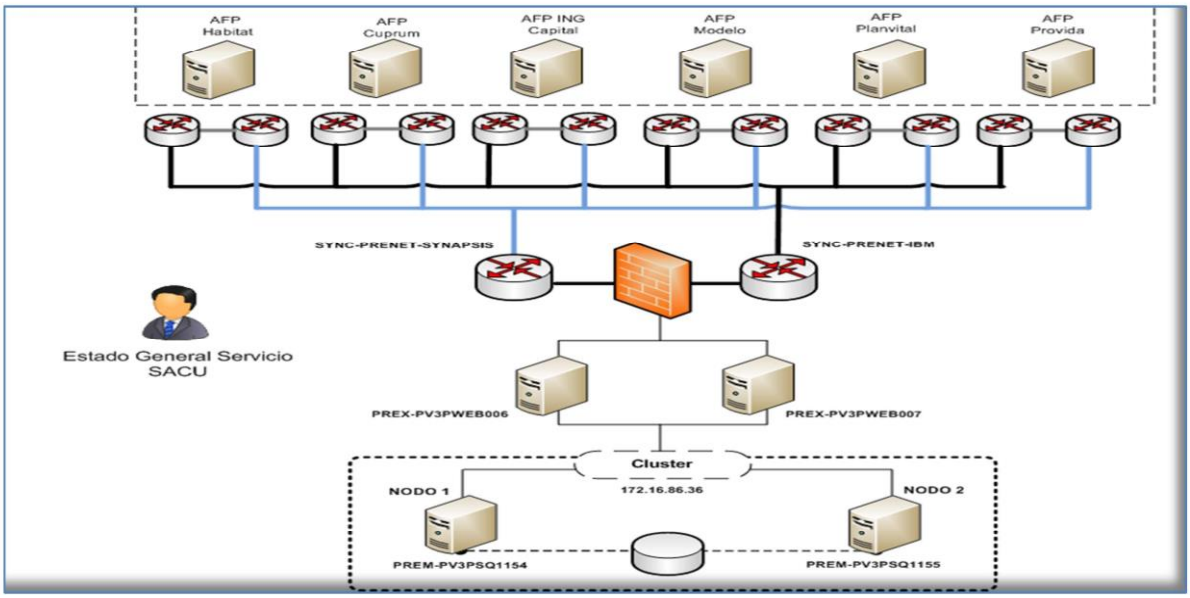
Se requiere de Monitoreo y Observabilidad de todos los componentes definidos según inventario y que componen la arquitectura e integración de los servicios, de manera de asegurar la correcta operación de cada uno de ellos, tales como utilización base de cada sistema operativo, memoria, procesador, middleware, utilización del espacio en disco y en dispositivos de bases de datos (Datafiles o similares), monitoreo de la conectividad y equipos de Networking, MQ (profundidad de colas, conexiones abiertas, estado de canales, entre otros), de manera de informar el alcance de niveles de criticidad y proponer cambios en el servicio para mantener los niveles de disponibilidad acordados.

La visualización del monitoreo y observabilidad debe estar disponible a través de internet, dashboard y/o consolas para Previred. Este debe ser considerado como un servicio, y debe ser capaz de cubrir en forma transversal todas las capas de los sistemas, desde el negocio, las comunicaciones, pasando por HW y SW base hasta la capa aplicativa e integración con terceros.

La siguiente imagen ejemplifica monitoreo servicio de Recaudación y en la segunda imagen, monitoreo servicio SACU, lo que se aprecia en la imagen corresponde a los servidores que conforman el servicio, y el monitoreo permite detectar caídas puntuales de componentes o servicios completos.



Ejemplo: Monitoreo Gráfico Servicio de Recaudación



Ejemplo: Monitoreo Gráfico Servicio SACU

Ilustración 10: Ejemplos de Monitoreos

Previred deberá contar con acceso de lectura a toda la o las plataformas de monitoreo y las actividades mínimas que se requiere realizar por parte del oferente son:

- Proveer la infraestructura, instalar, configurar y mantener operativa la plataforma de monitoreo.
- Instalar en la plataforma los agentes de monitoreo provistos por oferente, posteriormente darles mantenimiento, soporte y compatibilidad con los productos utilizados por Previred.
- Aplicar las definiciones de los umbrales de alarma para cada componente de la plataforma del Previred, previamente acordados entre el oferente y Previred.
- Proveer una herramienta de monitoreo unificada para los diferentes componentes de la plataforma del Previred.
- Establecer en conjunto con Previred grupos de recursos factibles de ser monitoreados por la herramienta. Estos grupos deben representar dependencias e interrelaciones de las diferentes componentes de la plataforma, de manera tal de tener una visión integral de las alertas, eventos y/o fallas que componen los servicios de negocio.
- Realizar monitoreo de la plataforma administrada por el oferente.
- Realizar monitoreo del estado de salud de los servicios para el negocio.
- Identificar posibles fallas en la plataforma; y evaluación de posteriores acciones preventivas y/o correctivas, mediante el uso de la herramienta de monitoreo.
- Utilizar la información provista por la herramienta de monitoreo, a través de interfaces automatizadas toda vez que esto sea posible, para que los grupos de soporte tomen acciones preventivas y correctivas en la plataforma.
- Informar a Previred de las alertas e indisponibilidad de alguno de los servicios utilizando la herramienta de gestión de incidentes y problemas.
- Ejecutar el escalamiento acordado entre las partes, dejando registro de este en la herramienta de gestión de incidentes y problemas.
- Almacenar el comportamiento en el tiempo de los componentes y la plataforma monitoreada por la herramienta.
- Realizar los análisis de tendencias para alertas tempranas.
- Informar a PREVIRED de las posibles restricciones que impidan la normal instalación de los agentes de software en la plataforma, comprometiendo acciones de análisis para su corrección.
- Realizar la apertura de ticket de incidentes, requerimientos, problemas y cambios en la Mesa de Ayuda de Previred, frente a una condición anormal del servicio.

- Realizar y registrar el proceso de escalamiento, en caso de que le sean asignados ticket de incidentes al oferente y este no sea capaz de solucionarlos, a las unidades resolutivas según lo indicado en el Procedimiento de Escalamiento.
- Realizar y registrar el proceso de derivación en caso de que le sean asignados ticket de incidentes que no estén dentro de las responsabilidades de oferente, a las unidades resolutivas según lo indicado en el Procedimiento de Derivación.
- Supervisar, controlar y ejecutar los procedimientos de contingencia que involucren actividades a realizar en este servicio.
- Llevar el registro en las bitácoras respectivas de los eventos del servicio.
- Generar la información para el control del cumplimiento de los Niveles de Servicio acordados.
- Revisar, mantener y actualizar los planes y procedimientos correspondientes a la recuperación ante desastres y contingencias de este servicio.

3.43.1 Monitoreo de servicios transversal

Previred tiene contratado el servicio de monitoreo NEW RELIC el cual proporciona a los clientes información sobre el rendimiento de su infraestructura, recursos en la nube, contenedores y aplicaciones mediante la incorporación de datos de telemetría en un solo lugar y la entrega de datos procesables a los clientes en tiempo real.

El oferente debe entregar y disponibilizar monitoreo para cubrir las necesidades de observabilidad sobre la plataforma y servicios transversales de aplicación similar en calidad y forma.

3.43.2 Monitoreo transaccional Atentus

Previred tiene contratado el servicio de monitoreo de negocio Atentus, el cual simula de forma permanente la actividad de un usuario desde 5 distintos ISP´s que interactúan con las aplicaciones de Previred. A través de este servicio que permite medir disponibilidad y tiempos de respuesta, Previred controla los SLA o cumplimiento de acuerdos de Niveles de Servicios con el Data Center Principal y de Contingencia (cuando aplica).

El oferente tendrá acceso a través del servicio contratado por Previred al monitoreo Atentus en línea.

3.44 Red de Datos, Comunicaciones y Seguridad

En la actualidad, Previred, cuenta, para toda su operación, con dos Data Center en IBM y administrados por Kyndryl, esto es:

- Kyndryl San Bernardo : Data Center Principal
- Kyndryl Providencia : Data Center Secundario

Previred cuenta con una plataforma de comunicaciones y seguridad configuradas en HA en todas sus capas y enlaces que permite operar en Data Center principal o secundario de forma transparente y con los mismos niveles de servicio.

También contamos con servicios de seguridad Cloud con AKAMAI, los servicios contratados son KONA SITE DEFENDER, PROLEXIC Y FASTDNS, loa cuales deben ser considerados por el oferente.

Previred mantiene múltiples integraciones hacia diferentes instituciones a través de las plataformas de comunicaciones:

- **WAN AFPs** – integración a través de enlaces dedicados hacia todas las AFP y la Superintendencia de AFP (Provista por el OFERENTE)
- **REDBANC** – integración a través de enlaces dedicados hacia Redbanc permite acceder a los servicios de la RBI, estos son provistos por Redbanc
- **RED DE TERCEROS** – integración de otras instituciones que requieran integrar a PREVIRED a través de enlaces dedicados (Enlaces contratados por PREVIRED y Terceros a través de MPLS capa 2 de GTD)
- **CLOUD PRIVADA** – Acceso a través de túneles con ancho de banda asegurado para acceder a los ambientes previos provistos por Kyndryl en EEUU.
- **VPNs** – Integraciones VPN para instituciones que requieran este tipo de accesos a través de un concentrador de VPN dedicado para este objetivo

Previred cuenta con 2 segmentos IP clase C propios que deberán ser utilizadas/migradas hacia el nuevo oferente de servicios, estos segmentos son utilizados para publicación de servicios a Internet o con las integraciones anteriormente señaladas, se deberá definir la estrategia para mover los servicios y direccionamientos para generar la menor indisponibilidad posible.

Toda la red de Previred y sus integraciones opera hoy en día exclusivamente con IPv4 y se requiere incorporar IPv6.

A continuación, Diagrama Simple de Red Actual

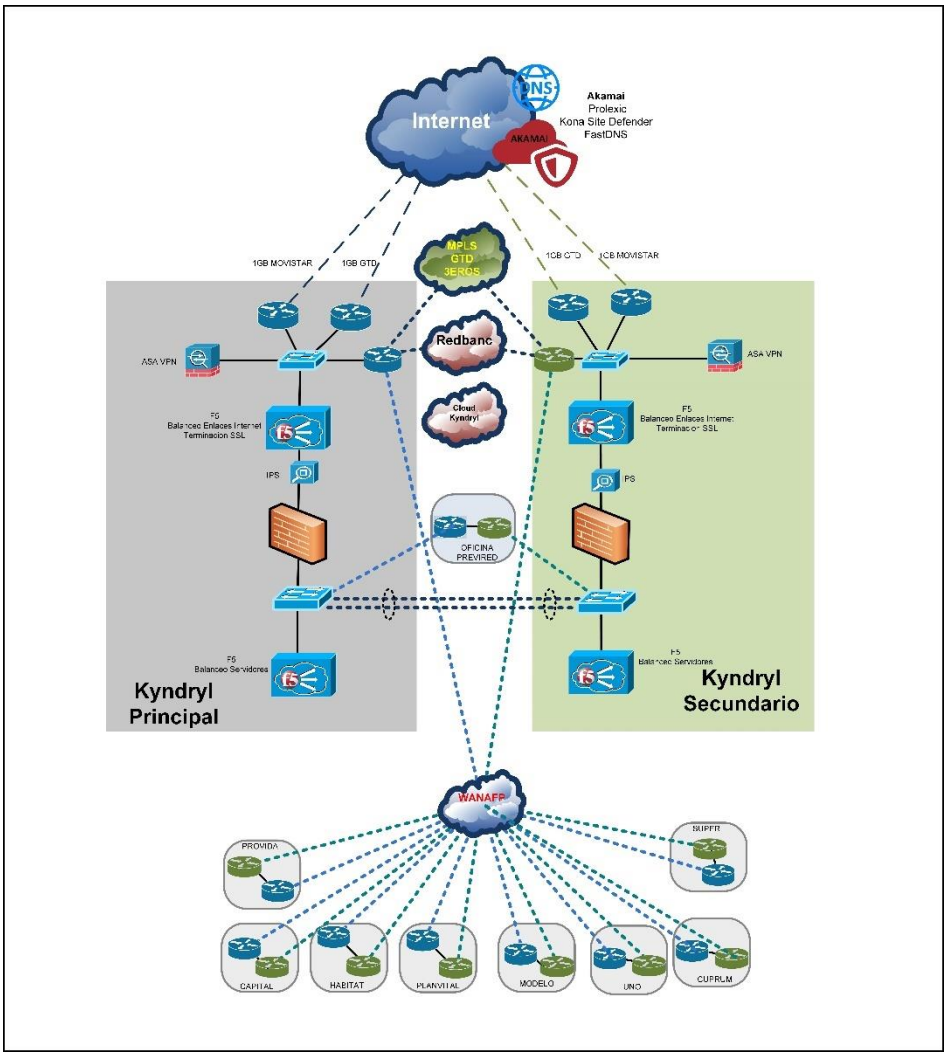


Ilustración 11: Diagrama Simple de Red Actual

3.44.1 Requerimientos de comunicaciones

El oferente debe considerar los siguientes requerimientos a nivel de comunicaciones:

- Cotizar enlaces por separado, ya que Previred podría tomar la decisión de contratarlos directamente o en otros casos por motivos de negocio
- Considerar 2 o más enlaces para las diferentes integraciones, para asegurar alta disponibilidad debido a incremento en problemas físicos de enlaces de los últimos años.
- Proveer equipos de comunicación: Firewalls, Routers, Switches, Balanceadores, concentrador VPN, entre otros, considerar marcas que sean lideres de mercado

- Servicios de Administración de toda la plataforma de comunicaciones (Configuración, revisión, respaldos, actualizaciones, entre otros).
- Evaluar/implementar SD-WAN
- Evaluar/implementar Microsegmentación
- Se deberá planificar/implementar IPv6 post migración de todos los servicios
- Para integración a Cloud considerar enlace/túnel privado que asegure ancho de banda.
- Todos los equipos deben contar con soporte de fábrica y correspondiente vigentes hasta el final del contrato.
- Acceso a Previred en modo lectura o auditoría a toda la plataforma de comunicaciones y seguridad.
- Plataforma de comunicaciones debe ser de uso exclusivo para Previred: Firewall, Routers, Balanceadores, Switches, etc.
- Plantear mejoras sobre arquitectura de redes.
- Implementar WAN AFP.
- Implementar Balanceadores, LTM y Link Controler que sean compatibles con las integraciones y necesidades de Previred
- Balanceadores deben soportar la carga de terminación SSL de todos los servicios WEB
- Prestar servicio DNS Publico para múltiples dominios de PREVIRED: 20 dominios (Puede ser DNS compartido con otros clientes), se debe garantizar un uptime de 99,99% mensual
- Implementar IPS para tráfico Internet y otras integraciones (Redbanc, WAN AFP, entre otros).
- Filtro de Contenido/aplicación para acceso Internet Usuarios internos de Previred /Servidores o tecnología de última generación
- Salida internet en alta disponibilidad en oficina de Previred independiente del Negocio, descrito en punto 3.43.13 y 3.43.14.
- Definir una arquitectura segura para servicio WIFI Oficina
    - Access Point, controlador WIFI, para servicio WIFI oficina.
    - Red de Visitas.
    - Red para trabajo
- Implementar WAF para todos los servicios de Previred, servicios expuestos Internet
- Implementar solución Anti DDOS que permita proteger todos los servicios/segmentos de Previred
- Implementar SIEM para la plataforma de Previred, que permita detectar eventos de forma automática y centralizada, debe considerar equipos de comunicación/seguridad/servidores
- Se debe implementar plataforma IPS para todo el tráfico de Previred en todos sus ambientes

- Previred cuenta con servicios de seguridad Cloud con AKAMAI, los servicios contratados son KONA SITE DEFENDER, PROLEXIC Y FASTDNS, loa cuales deben ser considerados por el oferente.

3.44.2 Servicio de Acceso a Internet

Este servicio hace referencia al acceso Internet para los servicios productivos y ambientes previos de Previred. Previred cuenta con un ASN y 2 segmentos IPv4 Público propios:

- 200.14.111.0/24
- 200.10.158.0/24

Del segmento 200.14.111.0/24 se reserva la subnet **200.14.111.128/25** para comunicaciones privadas, es decir para establecer comunicaciones con otras instituciones y no generar ningún conflicto con redes privadas, actualmente se utiliza en la WAN de AFP, VPNs , Wan de Terceros, no existe ningún servicio publicado a internet con esta subnet.

Actualmente se cuenta con 4 enlaces Internet para negocio:

- Kyndryl San Bernardo, enlaces Activos
    - GTD 1 GB / 200.10.158.0/24
    - Movistar 1GB / 200.14.111.0/24
- Kyndryl Providencia: Secundario, enlaces Standby
    - GTD 1 GB / 200.10.158.0/24
    - Movistar 1GB / 200.14.111.0/24

3.44.3 RED WAN de las AFP Y SUPEN

Este es un servicio que permite la interconexión entre las 7 AFP y Superintendencia de Pensiones hacia los servicios de Previred de forma rápida y segura.

Actualmente cada institución (AFP) cuenta con un enlace principal de 100Mb hacia la red MPLS de GTD, y un enlace de respaldo con CLARO donde nuestros Data Center Principal y Secundario cuentan con troncales de 1GB.

Toda esta comunicación es realizada vía túneles encriptados, generados entre cada institución y Previred, no existe comunicación entre las instituciones, solo existe comunicación bidireccional hacia PREVIRED.

Las características del servicio actual son:

- Este servicio es a través de la Redes MPLS de GTD y CLARO
- El tráfico sólo se genera desde cada institución (AFP) y Previred (Bidireccionalmente)
- Tráfico principalmente HTTP, HTTPS, FTP, SFTP
- No existe tráfico entre AFP por estos enlaces
- El tráfico es encriptado a través de túneles a través de los routers que se instalan en cada institución y un router concentrador de túneles en cada DC de Previred
- Cada AFP cuenta con 2 Routers y 2 enlaces de 100Mb cada uno (principal GTD y respaldo CLARO)
- AFP Capital y Habitat están ubicados en las mismos Data Center, no se utilizan enlaces
- AFP Provida tiene su site Secundario en Kyndryl San Bernardo, por lo que solo hay un enlace
- Los enlaces troncales que llegan a los Data Center son de 1Gb
- Previred utiliza subnet 200.14.111.128/25 con todas las instituciones para este tráfico y se habilitan subnet especificas a las AFP para evitar conflictos de direccionamientos IP.

La siguiente imagen describe la situación actual de las AFP Y SUPEN, en cuandro siguiente, su ubicación.

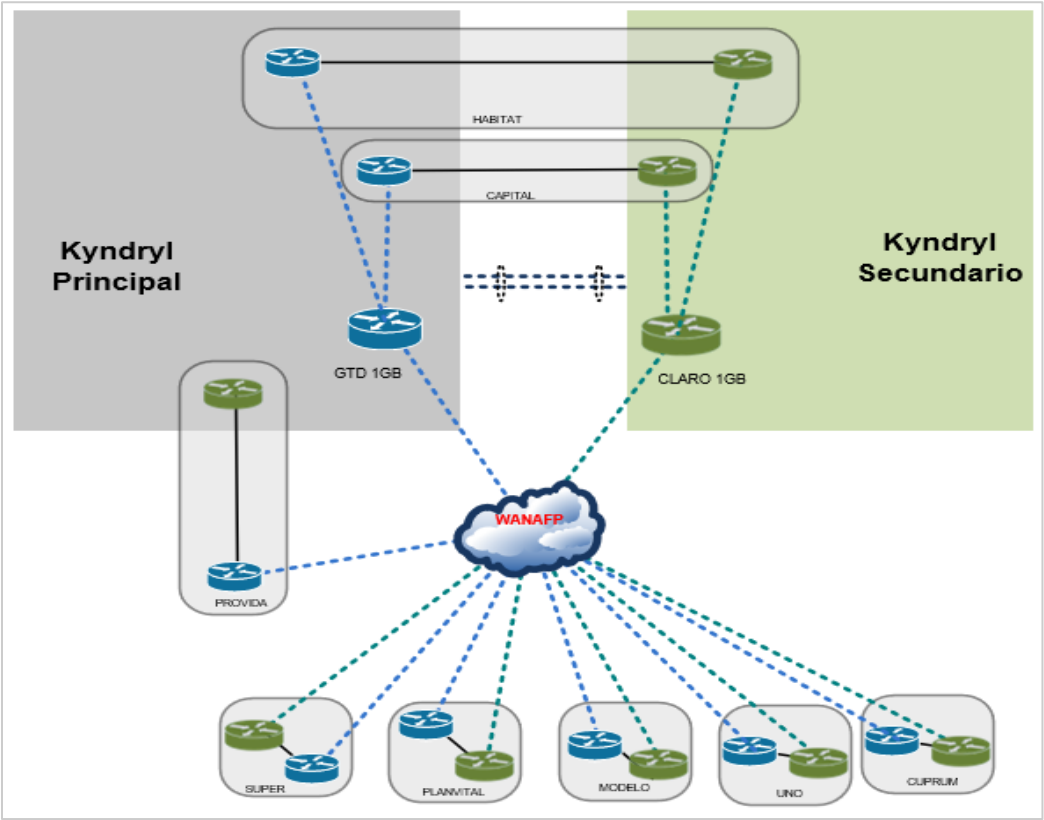


Ilustración 12: WAN AFP: Situación Actual

Institución	Site Principal	Site Secundario
Super	Av. Bernardo O'Higgins 1449	Av. Bernardo O'Higgins 1449
Cuprum	Liray 1120, Colina	Del Valle 928, Huechuraba
UNO	Av Victor Uribe Sur 221, Quilicura	Av Victor Uribe Sur 221, Quilicura
Modelo	Teatinos # 500, Santiago	Av. Víctor Uribe 2211, Quilicura
Planvital	Av. Víctor Uribe 2211, Quilicura	Teatinos # 500, Santiago
Provida	Pedro de Valdivia 100 Piso 5 , Providencia	Av. Puerta Sur 03320, San Bernardo
Habitat	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia
Capital	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia

Por lo descrito, se requiere por parte de oferente:

- Proveer los enlaces necesarios para implementar esta red
- El oferente debe proporcionar todos los equipos de comunicación que se requieran, incluido los equipos de borde en cada institución.
- Se deben implementar diferentes modelos de conexión hacia las AFP (HSRP, enrutados)
- Durante el tiempo de vida del servicio estos modelos de conectividad pueden cambiar a solicitud de las AFP o Previred
- Sera de responsabilidad del oferente implementar, administrar, monitorear estos equipos.
- Administración, configuraciones, monitoreo, entre otros, son parte del servicio solicitado
- Proveer 2 o más enlaces hacia cada institución para garantizar conectividad (esto debido al incremento de corte de enlaces por actos vandálicos/accidentes)

3.44.4 Conexión a Red WAN Terceros

Este servicio está destinado a dar conectividad a otros clientes de Previred que requieran conectarse de forma privada a través de enlaces dedicados Ejemplo: Bancos, Isapres, Retail, Clínicas, Gobierno, entre otros.

El objetivo principal es tener una opción de llegar a los servicios de Previred de una forma única y a través de un solo operador, así evitar la instalación de enlaces por cada tercero que se quiera integrar a Previred.

Actualmente existen las siguientes integraciones:

- Poder Judicial
- AFC
- Banco Falabella
- IPS
- Fonasa
- Equifax

Previred tiene contratados 2 enlaces troncales de 1Gb hacia la red MPLS de GTD, por cada cliente que acceda a este modelo se habilitaran VLAN a través de GTD.

- Previred requiere mantener el esquema actual de manera imperativa, valorando de igual manera aquellos oferentes que presenten alguna solución que cumpla con lo requerido con mejoras sustanciales e innovadoras.

- Los enlaces troncales hacia el DC pueden ser provistos por Previred.
- Administración, configuraciones, monitoreo, adiciones de terceros son parte del servicio solicitado

3.44.5 Monitoreo de Redes

Se requiere una plataforma de monitoreo que abarque todos los equipos de comunicación, seguridad y servicios asociados, esta puede ser una plataforma compartida, pero que solo se pueda visualizar lo que corresponda a cada cliente.

Algunas características mínimas requeridas:

- Contar con un NOC 24x7, cuyas funciones mínimas correspondan a supervisar, prevenir, detectar, investigar y responder sobre la disponibilidad y operación de las redes y enlaces.
- Utilización de enlaces (Consumo ancho de banda)
- Estado de los dispositivos
- Detección de errores/intermitencias/conmutaciones
- Visualización de monitoreo con diagramas vía WEB
- Alerta de errores vía mail / WhatsApp
- Informes Periódicos

3.44.6 Concentrador VPN

Este es un servicio para establecer VPNs punto a punto y VPN Client, actualmente existen 2 equipos CiscoFPR2210 en modo HA Activo-Pasivo, uno en Data Center Principal y otro en el Secundario.

Existen 6 VPNs IPSEC Site to Site activas (a modo de ejemplo)

- 2 DIS
- BANMEDICA
- Oracle OCI
- NeoSecure
- ITAU

El servicio debe contemplar implementar a otros clientes o prestadores de servicio en la medida que se requiera.

Se solicita al oferente prestar un servicio de similares o mejores características.

3.44.7 Capa Balanceadores

Previred cuenta con 2 capas de balanceadores F5, cada capa está configurada en modalidad HA, capa GTM para balanceo accesos internet y terminación SSL y capa LTM para balanceo en granja de servidores. Funciones principales requeridas:

- Terminación SSL para todos los sitios Web de todos los ambientes (mejorar en tiempos de respuesta y mejor custodia de certificados)
- Balanceo de sitios hacia internet
- Configuración de Irules para control de accesos y redirecciones especiales
- Balanceo hacia granjas de servidores

Los equipos actuales son:

- 2 equipos F5 i4800 capa GTM
- 2 equipos F5 i4600 capa LTM

Se requiere mantener prestaciones y capacidades similares o mayores a la actual plataforma F5.

3.44.8 WAF

La plataforma Kona Site Defender es el WAF implementado por Previred, es parte de los servicios entregados por AKAMAI, esta solución se encuentra en modalidad Cloud. Por esta plataforma se trafica alrededor de 10TbB mensuales para todos los servicios productivos que operan en esta capa como:

- www.Previred.com
- www.portalafp.cl
- cotizaciones.Previred.com

- contratistas.Previred.com
- demandas.portalafp.cl
- rhapvc.portalafp.cl

Este servicio adicionalmente integra los "módulos" CAC (Client Access Control) y SiteShield. CAC nos entrega un conjunto de IPs específicas para el servicio, estas no cambian en el tiempo, en caso de requerir actualizaciones estas son programadas.

SiteShield es un conjunto de direcciones ips desde donde llegara el tráfico hacia Previred, cualquier otro tráfico con IPs diferentes debe ser bloqueado en la plataforma para evitar que alguien se pueda saltar la protección AKAMAI.

El monitoreo/configuración/revisión/recomendaciones del WAF y sus reglas es de responsabilidad del SOC.

Se requiere mantener este servicio y sus componentes o de presentar uno de mejores características y prestaciones al actual para todos los servicios productivos y de ambientes previos de Previred. De ser presentado un nuevo producto, éste deberá ser aprobado por Previred.

3.44.9 Anti DDOS / Ataques Volumétricos

Actualmente Previred cuenta con la plataforma ANTI-DDOS Prolexic de AKAMAI, es una protección On-Demand capaz de contener todo el tráfico malicioso y solo dejar pasar tráfico válido hacia la plataforma de Previred, esta solución esta aplicada a toda la infraestructura On Premise para los segmentos públicos de Previred en todos sus ambientes (Producción, QA, Desarrollo, etc.).

Existe un monitoreo activo sobre el tráfico Internet y en caso de identificarse un evento de ataques DDOS o volumétricos el servicio Prolexic protegerá los segmentos 200.14.111.0/24 y 200.10.158.0/24 derivando el tráfico hacia los centros de limpieza ubicados en EEUU.

Esta protección es para todo tipo de tráfico hacia Previred, ya sea HTTP, HTTPS, SSH, ICMP, SMTP, entre otros.

3.44.10 IPS

La plataforma IPS está compuesta por 2 equipos IPS Cisco FP7120, uno instalado en DC principal y otro en el secundario, está orientado a todo el análisis del tráfico externo tanto de entrada como salida. Estos equipos operan en modalidad Activo-Activo y operan bajo la plataforma F5, por lo que todo el tráfico HTTPS es desencriptado en la capa superior y analiza en modo HTTP.

Se requiere implementar equipamiento similar o con mejores prestaciones/características para analizar todos los tráficos externos a Previred, como Internet o integraciones WAN, Redbanc, etc.

3.44.11 DNS Público

Actualmente el servicio es otorgado por la plataforma FastDNS de AKAMAI, los cambios son realizados en plataforma F5 y se replican a AKAMAI. Contamos con varios dominios, entre los principales:

- certificadospreviredcl
- comunicacionprevisional.cl
- controlcontratista.cl
- controlcontratista.com
- controlcontratistas.cl
- controlcontratistas.com
- gestion-previred.cl
- infocotizaciones.cl
- mailprevired.cl
- portalafp.cl
- previred.cl
- previred.com
- rhapvc.cl
- sontuslucas.cl

Se requiere que el oferente proporcione una plataforma DNS en alta disponibilidad y con las prestaciones y tiempos de respuesta similar o mejores a lo que tenemos implementados, puede ser compartida con otros clientes.

3.44.12 Conectividad con Redbanc

Previred está conectado al servicio RBI de Redbanc, esto es a través de 2 enlaces que provee Redbanc, donde el enlace principal llega al Data Center principal y el enlace de respaldo llega al Data Center secundario.

Los enlaces en ambos Data Center son recibidos por equipos de capa 3 y Redbanc propaga rutas de instituciones financieras.

Este servicio está destinado sólo a la recaudación de Previred.com, donde principalmente existe tráfico de mensajería MQ y archivos a través de casillas FTP/SFTP de Redbanc.

Se requiere mantener esta misma arquitectura en el nuevo Data Center, por ser un modelo estándar de Redbanc. El oferente debe proporcionar equipo capa 3 que recibirá los enlaces, se deberá realizar las configuraciones necesarias para establecer las comunicaciones con la RBI (configuración de protocolos, extensión de VLAN, etc.) o cambios que sean requeridos en el futuro.

3.44.13 Red LAN Oficina

Actualmente Previred cuenta con oficinas en Marchant Pereira 10, Piso 18, Providencia. Debido a que Previred está operando en modelo híbrido (algunos días en la oficina y otros desde la casa) los usuarios van esporádicamente hacia las oficinas y es utilizado principalmente para trabajo remoto que se establece a través de VPNs.

Se cuenta con 2 Firewall Fortinet 300E de propiedad de Previred para el control de accesos de usuarios hacia Internet y accesos a los Data Center de Kyndryl (Principal y Secundario).

Los usuarios desde nuestras oficinas navegan a Internet por enlaces independientes de los enlaces Internet dedicados al negocio (Servicios Recaudación, Cotizaciones, entre otros).

La solución ofertada debe considerar el equipamiento necesario para conexión con el Data Center Principal y Secundario en alta disponibilidad, enlaces Internet en el Data Center en alta disponibilidad exclusivos para navegación de usuarios oficina, incorporando los componentes de seguridad adecuados que permitan controlar. (Ejemplo: Filtro de Contenido/Aplicaciones, entre otros).

3.44.14 Servicio Internet Oficina

El objetivo de este servicio es otorgar acceso a Internet a las oficinas de Previred y escritorios virtuales con el fin de no utilizar los enlaces productivos del negocio.

En la actualidad hay 2 enlaces internet (Movistar/GTD) de 100Mb, uno en DC principal y otro en DC Secundario, el control de estos enlaces lo maneja la plataforma F5, en caso de fallar alguno envía todo el tráfico por el enlace operativo.

Adicionalmente se debe considerar un enlace Internet para contingencia y navegación de WIFI de visitas en las oficinas de Previred.

3.44.15 VPN para trabajo Remoto

Previred cuenta una plataforma destinada al acceso para trabajo remoto de sus colaboradores y proveedores que requieran acceder a algún ambiente en Previred (Desarrollo, QA, entre otros) a través de VPN SSL

Este servicio está compuesto por 2 equipos Fortinet Fortigate 200F configurados en modalidad de HA, un equipo en cada DC, hoy entrega accesos remotos para 300 usuarios.

Existe una definición de accesos RBAC para las diferentes áreas de trabajo donde se habilita sólo el acceso requerido por el área de trabajo, permite el acceso a todos los recursos en el DC, oficina o accesos a servicios de terceros que cuentan con restricción de IP de origen.

Se requiere cotizar un servicio/plataforma que realice esta función a través de VPN SSL, ZTNA o similar cumpliendo las principales características:

- Validación de Usuarios en Active Directory
- 300 cuentas VPN habilitadas, soportar hasta 500 usuarios
- Tiene habilitado 2FA para todos los usuarios
- Habilitación por grupos de acceso según requerimiento (tipo RBAC)
- Accesibilidad desde cualquier lugar/ubicación (oficina, casa, etc.)
- Entregue accesos a los recursos en el DC, Oficina, Nubes, etc.

3.44.16 WIFI Oficina

Previred requiere para sus oficinas conexión inalámbrica para diferentes tipos de usuarios, ya sean internos o visitas, que cumplan con las políticas de acceso definidas para cada ambiente.

El objetivo es ofrecer conectividad inalámbrica (administrativos e invitados) con el fin de acceder a servicios y sistemas corporativos, y navegar en Internet haciendo uso de equipos móviles (notebook, tablets, celulares, etc.), manteniendo o mejorando las características actuales de velocidad, estabilidad y disponibilidad.

El servicio debe considerar la cobertura para oficina de Previred ubicada en Marchant Pereira 10, piso 18, donde la zona de cobertura es aproximadamente de 10.000 metros cuadrados

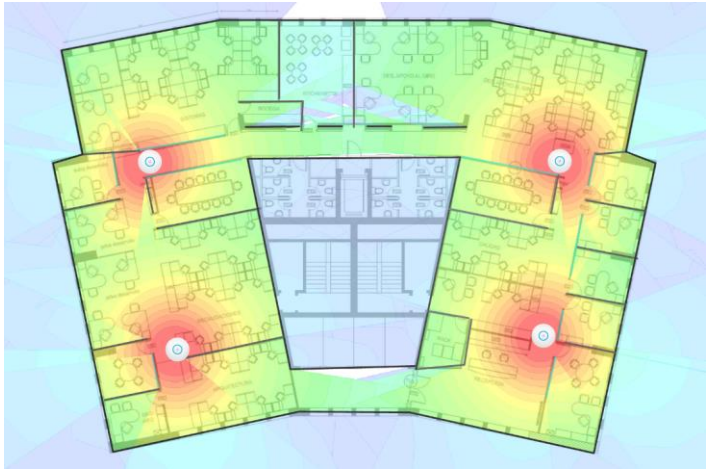


Ilustración 13: Plano oficina PREVIRED y zonas de cobertura WIFI (Referencial)

3.44.17 Seguridad para Acceso Internet usuarios Oficina Previred o Escritorios Virtuales

3.44.17.1 Filtro de Contenido o Tecnología de última generación que permita:

Monitorizar y controlar el acceso a Internet, lo cual nos permita una adecuada administración y control sobre lo que están examinando y descargando los usuarios en tiempo real. Las principales características de la solución requerida son:

- Considerar 100 usuarios concurrentes.
- Alta disponibilidad.
- Acceso a clasificación de URL.
- Monitoreo de ancho de banda por usuario/sitio, el administrador tiene la capacidad de seguir el tráfico de bajada y subida y el número de sitios web visitados, ya sea en base a usuarios o sitio web.
- Excepciones de la directiva de filtro.
- Filtrado por horario.
- Protección contra sitios Phishing

- Capacidad de crear múltiples directivas por usuario/grupo/IP para reflejar las directivas de seguridad de la organización.
- Analizar archivos descargados con motores Anti Virus
- Permite excepciones mediante listas blancas y negras.
- Permitir la navegación para usuarios autenticados y no autenticados
- integración de usuarios con Active Directory
- Permite el acceso a Internet para cualquier tipo de protocolo según se requiera (SSH, RDP, FTP, SMTP, entre otros)

3.45 Enlaces de Datos

Previred cuenta con diferentes enlaces de datos para sus servicios, que son contratados por el Data Center y otros contratados directamente:

3.45.1 Enlaces contratados por Data Center Kyndryl para servicio WAN

Institución	Site Principal	Site Secundario	Ancho de Banda
Super	Av. Bernardo O'Higgins 1449	Av. Bernardo O'Higgins 1449	100MB
Cuprum	Liray 1120, Colina	Del Valle 928, Huechuraba	100MB
UNO	Av Victor Uribe Sur 221, Quilicura	Av Victor Uribe Sur 221, Quilicura	100MB
Modelo	Teatinos # 500, Santiago	Av. Víctor Uribe 2211, Quilicura	100MB
Planvital	Av. Víctor Uribe 2211, Quilicura	Teatinos # 500, Santiago	100MB
Provida	Pedro de Valdivia 100 Piso 5 , Providencia	Av. Puerta Sur 03320, San Bernardo	100MB
Habitat	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia	100MB
Capital	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia	100MB
Kyndryl Troncal GTD	Av. Puerta Sur 03320, San Bernardo		1GB
Kyndryl Troncal CLARO		Av. Providencia 655, Providencia	1GB

3.45.2 Enlaces para interconexión Oficina – Data Center

Institución	Site Principal	Site Secundario	Ancho de Banda
PREVIRED	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia Pereira 10	1GB

3.44.3 Enlaces exclusivos para interconexión Data Center primario y secundario, enlaces de fibra en HA

Interconexión	Cantidad	Site Principal	Site Secundario	Ancho de Banda
Conexión Storage entre Site 1 y Site 2	4	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia Pereira 10	4GB cada Fiber Channel (FC)

Interconexión	Cantidad	Site Principal	Site Secundario	Ancho de Banda
Interconexión de Datos entre DataCenters	2	Av. Puerta Sur 03320, San Bernardo	Av. Providencia 655, Providencia Pereira 10	1GB

3.44.4 Enlaces Internet Negocio contratados por Data Center Kyndryl

Enalce	Oferente	BW Nacional	BW Internacional
Site Principal Negocio	GTD	1Gb	10Mb
Site Secundario Negocio	GTD	1Gb	10Mb
Site Principal Negocio	MOVISTAR	1Gb	10Mb

Site Secundario Negocio	MOVISTAR	1Gb	10Mb
Site Principal Usuarios	GTD	100Mb	10Mb
Site Secundario Usuarios	MOVISTAR	100Mb	10Mb

3.44.5 Enlaces contratados por Previred

Descripción	Dirección	Descripción	Ancho de Banda
WAN Terceros	Av. Puerta Sur 03320, San Bernardo	Enlace Troncal para servicio WAN Terceros, GTD	100Mb
WAN Terceros	Av. Providencia 655, Providencia	Enlace Troncal para servicio WAN Terceros, GTD	100Mb

Se requiere que el oferente provea de todos los enlaces necesarios para establecer todos los modelos de conectividad de Previred hacia las AFP, Internet, oficina, entre otros, todas las comunicaciones deben ser establecidas en modelos de HA para garantizar la continuidad del servicio.

4 Requerimientos de Informes de Gestión

El oferente deberá incluir dentro de los servicios otorgados, personal y mecanismos para efectuar informes de servicios, y antes eventos.

4.1 Informes de Eventos No Programados

Estos eventos se definen como acontecimientos de contingencias en el servicio o los servicios presentados por el Data Center, sean de cualquier índole, en donde, se vean afectados los servicios prestados. Por ejemplo; caída de servidor, servicio detenido, problemas en bases de datos, problemas de seguridad, entre otros.

Periodicidad: Ante Eventos

Plazo de Entrega: 32 horas hábiles después de ocurrido el evento.

Este informe debe contener, al menos, el siguiente detalle:

- Fecha y Hora de inicio del incidente.
- Fecha y Hora de término del incidente.
- Duración del incidente.
- Servicio Afectado.
- Causas del incidente.
- Acción inmediata.
- Acción mitigante.
- Acción correctiva.
- Resumen de situación final.
- Personal que atendió el incidente

4.2 Informes de Eventos Programados

Estos eventos se definen como requerimientos por parte de personal debidamente autorizado y validado por Previred, en donde se afecta un servicio específico. Por ejemplo; detener un servicio por un trabajo requerido programado.

Periodicidad: Ante Eventos

Plazo de Entrega: 12 horas hábiles después de ocurrido el evento.

Este informe debe contener, al menos, el siguiente detalle:

- Fecha y Hora de inicio del trabajo requerido.
- Fecha y Hora de término del trabajo requerido.
- Duración del Evento.
- Personal que atendió el Evento.
- Personal de PREVIRED que requirió la actividad.
- Actividad requerida.
- Acción Realizada.
- Resumen de situación final.
- Hora de validación telefónica o mail dada por la contraparte de Previred.

4.3 Informes de Eventos Acceso al Data Center

Definido como el acceso por parte de personal de Previred o un tercero quien será autorizado debidamente por Previred, para los fines que sean pertinentes. Por ejemplo; auditorías al Data Center, trabajos Data Center secundario, trabajos de parte de personal de Previred en el Site, entre otros.

Periodicidad: Ante Eventos

Plazo de Entrega: mensual al 5to día hábil del mes siguiente.

Este informe debe contener, al menos, el siguiente detalle:

- Fecha y Hora de inicio del acceso.
- Fecha y Hora de término del acceso.
- Duración del acceso al Data Center.
- Nombres de las personas que realizaron el acceso físico al Data Center.
- RUT de las personas que realizaron el acceso físico al Data Center.

4.4 Informes de Respaldos

Se requiere al menos los siguientes informes de Respaldos por parte del oferente

4.4.1 Informe semanal del estado del proceso de respaldo.

Periodicidad: Semanal

Plazo de Entrega: Todos los lunes

El detalle debe contemplar entre otros datos:

- Fecha y Hora de inicio y términos del respaldo.
- Servidor respaldado.
- Objeto respaldado (File System, base de datos, etc.).
- Modalidad del respaldo (full).
- Datos transferidos (MB)
- Condiciones de término del respaldo (OK o Error).
- Acción tomada ante evento (En caso de ser Error la opción anterior).
- Personal que realizó la labor o unidad a cargo de la realización.

4.4.2 Informe con detalle de los backups/restore de las BDs

Periodicidad: Diaria de lunes a sábado

Plazo de Entrega: Todas las mañanas

Detalle que debe contemplar:

Se envía informe de respaldos y restauraciones de Previred, al día 01-07-2013.

Nombre BD	ID	Inicio	Fin	Duración	Orden	ID	Inicio Restauración	Término restauración	Duración Restauración
previred_operacional	65	1:30:05	3:17:36	01:47:31	1	111	04:11:41	4:47:02	00:35:21
goliath	65	1:30:05	3:17:36	01:47:31	2	111	03:39:02	4:09:38	00:30:36
previred_privilegios	71	1:30:13	3:07:28	01:37:15	3	149	05:25:51	05:28:10	00:02:19
previred_privback	97	2:31:14	3:59:57	01:28:43	4	143	05:18:09	05:19:04	00:00:55
previred_backlists	71	1:30:13	3:07:28	01:37:15	5	171	06:01:04	07:42:07	01:41:03
previred_backend	97	2:31:14	3:59:57	01:28:43	6	143	05:04:40	05:18:01	00:13:21
previred_deudas	71	1:30:13	3:07:28	01:37:15	7	149	05:24:14	05:25:51	00:01:37
previred_notificaciones	65	1:30:05	3:17:36	01:47:31	8	111	04:09:38	4:11:37	00:01:59
Gestion	97	2:31:14	3:59:57	01:28:43	9	172	06:08:50	07:30:27	01:21:37

4.4.3 Informe con detalle de todos los Backup realizados en el mes.

Donde se pueda apreciar el cumplimiento de la política de Respaldo.

Periodicidad: mensual

Plazo de Entrega: cada 4to día hábil del mes siguiente.

4.4.4 Informe con tasa de éxito/falla de los respaldos diarios.

Donde se indique la cantidad total de backup realizados y la tasa de éxito, también que muestre el acumulado al mes correspondiente y el total anual.

Periodicidad: mensual

Plazo de Entrega: cada 2do día hábil del mes siguiente.

Detalle que debe contemplar, por ejemplo:

4.5 Informe de Modificación de Ambientes

Este informe está orientado a conocer los elementos alterados, en su configuración o físicamente, durante el transcurso del mes. Las modificaciones de cualquiera de estos elementos deben ser siempre coordinadas y aceptadas por personal de Previred.

1) Dentro de estos se deben considerar a modo de ejemplo:
2) Cambios en la configuración de parámetros; sistemas Operativos o BDD.
3) Reemplazo de equipamiento defectuoso.
4) Retiro o instalación de equipamiento.

Periodicidad: Ante peticiones de cambio

Plazo de Entrega: 12 horas hábiles de ejecutado el requerimiento

Este informe debe contener el siguiente detalle:

1) Fecha y Hora de inicio de la acción.
2) Fecha y Hora de término de la acción.

3) Duración de la acción.
4) Nombre del solicitante de la acción.
5) RUT del solicitante de la acción.
6) Motivo de la acción requerida.

4.5.1 Informe de Versionamiento a nivel de firmware de la plataforma

Este informe está orientado a conocer los elementos y sus actualizaciones, en base a sus mejoras. Las modificaciones de cualquiera de estos elementos deben ser siempre coordinadas y aceptadas por personal de Previred.

4.5.2 Informe de Inventario de Hardware

- Este informe deberá contener la información relacionada con:
- Versionamiento y modelo.
- Calendario de Parchados y/o actualizaciones.
- Eventos de errores.
- Uptime acumulado último año móvil.
- Trabajos en curso y estado de avances.
- Tabla actualizada del ciclo de vida que incluya EOL.
- Matriz de compatibilidad con el software.

4.5.3 Informe de Seguridad

Este informe deberá contener información relacionada a los eventos y trabajos de la plataforma de seguridad, considerando como mínimo lo siguiente:

- Eventos mensuales WAF, IPS, SIEM, Firewall, entre otros
- Comparación con respecto al mes o meses anteriores
- Trabajos en curso relacionados a la plataforma de seguridad

- Mejoras, Recomendaciones a aplicar

4.5.4 Informe de Gestión Mensual

Deberán contener un ítem de análisis y recomendaciones. Los ítems a ser considerados, como mínimo, en el informe de gestión son los siguientes:

- Resumen de Gestión Data Center.
- Detalle SLA y Calidad de Servicio
- Detalle de Incidentes, requerimientos y nivel de cumplimiento
- Hitos relevantes del mes
- Informe de acceso físico y vía red al Data Center, tanto del mismo Data Center como de Previred y otros proveedores, detallando el día, hora, requerimiento, solicitante, autorización respectiva y conclusión final del trabajo. De periodicidad mensual.
- Bitácora control de cambios
- Informes del estado de respaldos., detalle de todos los respaldos del mes.
- Informe de Análisis y recomendaciones (Performance, máquinas, FW, BD`s, cantidad de sesiones por día, entre otros)
- Incidentes de Seguridad
- Informe monitoreo de seguridad
- Informe Filtro de Contenido.
- Informe de Antivirus, estado de actualización en cada una de las máquinas.

5 Niveles de Servicios

Los niveles de servicios contratados son mensuales y serán informados por el oferente a Previred mediante el Informe de Servicio mensual, dentro de los 5 primeros días del mes siguiente, junto con los respectivos estados de Pre-Pago mensuales.

El oferente deberá disponer de herramientas que permitan medir en forma objetiva y demostrable los distintos niveles de servicio.

Para los efectos de cálculo, se define como Uptime como el tiempo total en que un servicio está al 100% de sus capacidades, disponible para su uso y función específica. La medición será mensual. Dado un servicio su Uptime se calcula de la siguiente forma:

Uptime = (Tiempo total – Tiempo inactivo) / Tiempo total * 100

Por ejemplo, estimando para el Data Center en un mes con 720 horas como tiempo total (el tiempo requerido del servicio), y teniendo 24 horas como Tiempo inactivo (el servicio no estuvo disponible para su uso), el Uptime sería de 96.67%, según lo siguiente:

Uptime = (720 – 24) / 720 * 100

Uptime = 96.67%

5.1 Niveles de servicio asociados a Site Productivo

Tiempo Ejecución Requerimientos: Corresponde al tiempo máximo trascurrido entre que PREVIRED coloca un ticket de requerimiento, cumpliendo con los procedimientos acordados, y el momento en que Data Center ejecute el requerimiento.

Los tiempos máximos están establecidos de acuerdo al nivel de urgencia de los requerimientos.

Tiempo de ejecución requerimientos de Networking: Corresponde al tiempo entre que Previred solicita un nuevo requerimiento de Networking y el momento en que Data Center ha ejecutado e informado a PREVIRED de la realización de la tarea. El tiempo establecido será de 8 horas hábiles.

Tiempo de entrega máquinas virtuales: Corresponde al tiempo transcurrido entre que PREVIRED solicita creación de una máquina virtual, cumpliendo los procedimientos acordados, y el momento en

que DATACENTER entrega la máquina creada. Los tiempos de entrega están establecidos de acuerdo al tipo de máquina virtual solicitada.

Los niveles de urgencia y sus tiempos máximos de atención establecidos, así como los tipos de máquinas virtuales y sus tiempos de entrega establecidos son:

Gestión de requerimientos			
Nivel de urgencia	**Tiempo de respuesta de atención**	**Tiempo máximo de resolución**	**Nivel de Servicio**
BAJA	20 minutos	3 días hábiles	Del total de los tickets de requerimientos el 98% atendidos en plazo, según columna "Tiempo máximo de Resolución"
MEDIA	20 minutos	8 horas hábiles	
ALTA	20 minutos	2 horas corridas	
MUY ALTA o "URGENTE"	10 minutos	30 minutos	

Tiempo de creación y entrega de máquinas en plataforma virtual	Tiempo máximo	Nivel de servicio
Máquinas con template	1 día hábil	100% de las máquinas entregadas en los plazos comprometidos
Máquinas sin template (solo sw base, linux o WS)	3 días hábiles	
Máquinas en clúster virtual	4 días hábiles	

Tiempo de ejecución requerimientos de Networking: Corresponde al tiempo entre que Previred solicita un nuevo requerimiento a networking (por ejemplo: nueva regla de firewall, habilitación VPN, habilitación de tráfico, revisión de tráfico o cambio de IP) y el momento en que Data Center ha ejecutado e informado a PREVIRED de la realización de la tarea. El tiempo establecido será de 8 horas hábiles.

Tiempo de atención a incidencias: Corresponde al tiempo transcurrido entre que se produce la incidencia y el momento en que Data Center toma contacto para atenderla e iniciar su solución.

Tiempo de ejecución solicitudes de controles de cambio: Corresponde al tiempo máximo transcurrido entre que Previred solicita un control de cambio, cumpliendo con los procedimientos acordados, y el momento en que Data Center toma contacto para atenderlo y ejecutarlo.

- Quien define la "Urgencia" para los requerimientos es PREVIRED
- Respecto a Peticiones de servidores en equipamiento dedicado, los tiempos se aplican en el entendido que se tiene capacidad física.

5.2 Indicadores niveles de servicio

Las siguientes tablas detallan los niveles de servicio establecidos para las categorías definidas por Previred

Requerimientos:

INDICADOR	ASPECTO	VALOR
Tiempo atención requerimientos (incluye requerimientos de networking)	Gestión de requerimientos según su nivel de urgencia (*)	98% del total de los tickets de requerimientos atendidos en plazo (*)

(*) Los plazos y niveles de urgencia se encuentran descritos en el punto 5.1

Máquinas virtuales:

INDICADOR	ASPECTO	VALOR
Tiempo entrega máquinas virtuales	Creación y entrega de máquinas en plataforma virtual según su tipo (*)	100% de las máquinas entregadas en los plazos comprometidos (*)

(*) Los plazos y tipos de máquinas virtuales se encuentran descritos en el punto 5.1

5.3 Niveles de servicio definidos para servicios asociados a Data Center productivo y para Red de Datos y Comunicaciones

UPTIME

Para que el nivel de servicio sea aceptable el uptime debe estar según las cotas señaladas para cada servicio, de acuerdo a las siguientes tablas.

SERVICIO	CRITICIDAD	VALOR
Previred.com	ALTA	99,80%
Home Público Previred.com		
Plataforma de Pagos y Clientes MQ		
Batch C y Java		
Granja de Pagos		
Granja Notificación		

Granja Servicios		
Granja Integración		
BackOffice Recaudación		
Control Contratistas		
InfoCotizaciones		
Workload - CAWA		
SWING		
WEF		
Traspaso WEB		
TVI		
Bloqueo TWEB		
Servicio Clave Única SACU		
Servicio de Verificación de Identidad (SVI)		
Interposición Demanda		
Cobranza SEGRD		
Fidelización		
Retiro Enfermos Terminales 10%		
Consulta Afiliados 10%		
Consulta Afiliados Extranjeros 10%		
INTCAPJ		
STJ/SEJ		
SICUJ		
SIDEP		
API-AFC		
Administración y gestión de usuarios (AGU)		
Transversal Utilitario		
Servicio STI AGU		
Validador de identidad		
CMH		
CMH Cotizaciones		
GROOT		
Preguntas Previsionales		
SAGCOM		
Portal Prestadores FACM		
Portal Soluto FACM		
STI-Otros / STI-CMH		
Recaudación Externa		
Recaudación Externa New		
Plataforma Openshift (Infraestructura)		
Plataforma de gestión de datos - BI		
SSO		
IPA		

SIDEP		
Consulta Planillas Gravámenes		
SFTP REC		
SFTP AG		
Relay de Correo		
Sendgrid		
NTP		
NEXUS		
Servicio de administración de microservicios transversales en Openshift		
Plataforma de administración de máquinas virtuales (ej. VMWARE).		
Controlador de Dominio .COM		
Controlador de Dominio. NEG		
DNS		99,90%
Enlaces		
Monitoreo Bancos	MEDIA	99,50%
Ejecutor BEST		
Ejecutor de Procesos Cobranza		
Ejecutor Recaudación		
CONPAG/COMPIN		
Pilar Solidario		
RHAPVC		
CAPRI		
Carga y Procesa Archivo		
SCOMP		
SACU AFC		
SACU BackOffice		
WS DT Apoyo al Giro		
Subsidios		
Ciclo Demanda		
Consulta (DNPA) Regularización		
DNPA Cartas		
Firmador Central		
Regulus		
Ventana Demanda		
IDM		
LDAP		
Concentrador de LOGs (CDL)		
Ambiente de Desarrollo y Homologación		
Ambiente de Testing (QA)		
Consulta nuevos afiliados (CNA)		

Servicio NIFI (Notificaciones)		
Notificador		
Ingreso Mínimo Garantizado (IMG)		
SonTusLucas (Rezagos)		
Redis		
Subrogación Fonasa		
SICOP	BAJA	99,00%
SISAC		
SICERT		
Postino		
ePass		
Intranet		
Gestor Documental / ARIS		
Servicios Aranda (Mesa de Ayuda, Metrix, Inventario)		

Todo nuevo servicio no indicado en tabla anterior corresponderá a criticidad alta, salvo indicación expresa de Previred.

Para los otros servicios no aplicativos y propios a brindar el Data Center, éstos vienen definidos en la siguiente tabla:

Servicio	Requerimiento	Niveles de Servicio
Respaldos	Realización de los respaldos definidos en documento "GOTSGS-PC-Procedimiento de respaldo, retención y recuperación de la información DATACENTER-018" en la última versión vigente	Realización del 99,8% Respaldos pactados en un mes calendario
	Entrega de copias de copias de respaldos con sus respectivas guías	Entrega al 8° día hábil del mes siguiente
	Traslado de cintas en transporte especializado	Cumplimiento del servicio de transporte especializado
Entrega de Informes	Plazo de entrega de informe mensual de cumplimiento de niveles de servicios	Tiempo de entrega no superior al 8º dia habil del mes siguiente
	Plazo de entrega de informe incidentes de falla	Entrega máximo 4 días hábiles ==> 32 horas hábiles
	Plazo de entrega de informe de gestión de tickets	Entrega todos los lunes
	Entrega informe con Resultados mantenciones de BD Plazo de entrega de informe con resultados de las mantenciones de BD ejecutadas el fin de semana	Entrega todos los lunes
	Entrega Bitácora Operaciones Plazo de entrega cuaderno o bitácora actualizada (parches, revisiones, mantenciones)	Entrega todos los lunes
	Entrega de informe con Evidencias de Respaldos (aplicativos y BD) Plazo de entrega de informe con evidencias de respaldos	Todos los días, de lunes a sábado
Calidad del Servicio	Servidores sin contagio de Virus de ningún tipo en servidores	Para el 99,8% de los servidores sin virus

	Servidores con sw antivirus y actualizaciones al día.	100% de los servidores actualizados
	Aplicación de Políticas, Normas y Procedimientos de Seguridad de PREVIRED	100% de las normas aplicadas
Continuidad de servicio	Participación en la ejecución de pruebas DRP programadas semestral o anualmente según calendario definido.	100% de las pruebas ejecutadas en tiempo.
	Ejecución de Pruebas de Servicios en Alta disponibilidad de acuerdo a calendario definido	95% de las pruebas ejecutadas en fecha
Respaldos y restauraciones realizados equipos usuarios críticos	Ejecución de todos los respaldos de los equipos de usuarios críticos definidos, pactados en un mes calendario	100% ejecución respaldos
	Ejecución de las restauraciones de data de estaciones de trabajo solicitadas en un mes (por parte del DATACENTER)	100% ejecución restauraciones
Soporte	El tiempo de atención a incidencias máximo de 90 minutos. Es condición que no esté afectado el servicio.	99 % de los casos atendidos en tiempo
Aplicación controles de cambio	Ejecución de solicitudes de controles de cambio planificados. Se considera exitoso un cambio cuando es realizado en su totalidad dentro de la ventana de cambio definida por PREVIRED	95% de la totalidad de los controles de cambio ejecutados en tiempo
	Tiempo de atención solicitudes de controles de cambio por incidentes (urgencia)	
	Tiempo máximo de 1 hora en horario hábil de lunes a viernes.	
	Tiempo máximo de 2 horas fuera de horario y fines de semana o festivos	
Cumplimiento de proyectos	Entrega de planificación tras partida inicial con objetivos y alcances correctamente definidos en tiempo y forma	Entrega al 3er día hábil tras punto de partida (reunión de kickoff)
	Seguimiento y control de la ejecución del proyecto	Debe existir un seguimiento semanal del proyecto en cuestión donde debe ser enviada una minuta correspondiente al 2do día hábil
	Fecha de Implementación del proyecto	Cumplimiento en fecha acordada de puesta en marcha del proyecto y de calidad según lo requerido por Previred
	Medición de impacto y cierre del proyecto	Entrega de informe de revisión y valoración del resultado final al 7mo día hábil a partir de la fecha de implementación del proyecto

5.4 Niveles de servicio centro de procesamiento alterno

Se distinguirán dos condiciones operacionales para el sitio, para efectos de cálculo de SLA.

ACTIVO: Los servicios están funcionando y dando respuesta a los clientes de Previred desde el site secundario, dado que el site primario fue desactivado. Cobertura: durante el periodo que dure la contingencia, SLA: se calculará en base a esta cantidad de días las 24 horas del día.

PASIVO: Sólo se están actualizando las transacciones que se generan en el site primario. Cobertura: todos los días del mes las 24 horas del día, mientras no se encuentre en modalidad ACTIVO. SLA: se calculará en base a esta cantidad de días y horario indicado en la cobertura.

INCIDENTE: Se entenderá por incidentes un requerimiento y/o atención de falla.

Se define como Uptime el tiempo total en que un servicio está al 100% de sus capacidades, disponible para su uso y función específica. La medición será de acuerdo al periodo y horario de la cobertura, distinguiendo de acuerdo a ACTIVO o PASIVO.

Por ejemplo, si el sitio está operativo (activo) 8 días del mes, se considerará el tiempo total en 8*24 = 192 horas. Y se produce dentro de ese periodo una suspensión de los servicios por 1 hora.

Niveles de servicio centro de procesamiento alterno			
Indicador	Descripción	Control	Objetivo
Atención de incidentes	ACTIVO: Porcentaje de incidentes con primera respuesta por parte del DATACENTER antes de 1 hora de la solicitud. Los reportes de incidentes realizadas después de las 20:30 Hrs podrán tener su primera respuesta al dia siguiente hábil	Se utilizará el registro de incidentes provisto por el DATACENTER	99%
	PASIVO: Porcentaje de incidentes con primera respuesta por parte del oferente antes de 2 Hrs de la solicitud. Las peticiones realizadas después de 20:30 Hrs podrán tener su primera respuesta al dia siguiente hábil	Se utilizará el registro de requerimientos (peticiones) utilizados por el Service Desk	97%
Continuidad de servicio	Cumplimiento de calendario prueba de contingencia semestral	Reporte pruebas de contingencia	100%

Indicador	ESTADO	Objetivos
Uptime Datacenter	ACTIVO	99,90%
	PASIVO	98,90%
Uptime comunicaciones (*)	ACTIVO	99,90%
Uptime Servidores	PASIVO	98,50%
	ACTIVO	99%

Uptime Comunicaciones (*) RTO (Tiempo recuperación objetos)	PASIVO	99,90%
	ACTIVO	<= 2 horas
RPO (Punto de recuperación objetivo)	ACTIVO	<= 5 minutos

5.5 Niveles de servicio definidos para servicios adicionales (Servicio de administración de contraseñas y claves maestras, desbloqueo de claves y Escritorios Virtuales):

INDICADOR	ASPECTO	VALOR
Tiempo de respuesta promedio (*)	Tiempo de respuesta promedio: Es el promedio aritmético del tiempo que transcurre desde el momento en que se efectúa el requerimiento por parte de PREVIRED a través de una llamada de servicio y el momento en que el representante de servicios DATACENTER soluciona dicho requerimiento, todo ello contabilizado en un periodo de un mes.	2 horas

(*) indicador correspondiente a mantenimiento

6 Multas

Se establece que las multas, de forma individual o conjunta, estarán limitadas a un valor tope mensual equivalente al 10% del cargo mensual del servicio, del mes en que se aplica la multa. En caso de que en un mes determinado la suma de las multas resulte en un valor superior al 10% del valor mensual del servicio, la multa limitará a dicho tope, clasificándose, al mismo tiempo, dicho mes como de servicio insatisfactorio. En caso de que una misma causa impacte en dos o más niveles de servicios se pagará el cargo más alto.

Se debe considerar que por cada mes a evaluación si ya se poseía en el mes anterior multa, se le debe entonces agregar un porcentaje equivalente a un 1% a la multa final calculada.

6.1 Multas definidas por incumplimiento de servicios asociados a Data Center productivos, red de datos y comunicaciones en Data Center productivo y alterno

A continuación, se definen las multas que se aplicaran, por incumplimiento en los niveles de servicio comprometidos.

6.1.1 UPTIME

SERVICIOS CON UPTIME DE:	RANGO UPTIME	% DE CUOTA MENSUAL
99,90%	Entre 100% y 99,9%	No Aplica
	Entre 99,89% y 99,7%	4%
	Menor o igual a 99,69%	10%
99,80%	Entre 100% y 99,8%	No Aplica
	Entre 99,79% y 99,6%	4%
	Menor o igual a 99,59%	10%
99,70%	Entre 100% y 99,7%	No Aplica
	Entre 99,69% y 99,2%	4%
	Menor o igual a 99,19%	10%
99,00%	Entre 100% y 99%	No Aplica

	Entre 98,99% y 98,6%	4%
	Menor o igual a 98,59%	10%
98,50%	Entre 100% y 98,5%	No Aplica
	Entre 98,49% y 98,2%	4%
	Menor o igual a 98,19%	10%

6.1.2 Requerimientos

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Tiempo de atención requerimientos	Si nivel de cumplimiento promedio mensual es menor a 98%	3%

6.1.3 Máquinas virtuales

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Tiempo Entrega Máquinas Virtuales	Por cada 3 días hábiles de atraso en la entrega de cada servidor virtual	1%

6.1.4 Respaldos

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Realización de respaldos	Por cada respaldo no realizado según Procedimiento de Respaldo de PREVIRED	2,5%
Entrega cintas de seguridad	Por cada set de cintas de respaldo no entregado o no entregado entre los 5 días hábiles siguientes del mes siguiente	5%

6.1.5 Informes

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Entrega Informe Cumplimiento Niveles de Servicios	Por cada 5 días hábiles de retraso en la entrega del informe mensual	1%
Entrega Informe incidentes de falla	Por cada 3 días hábiles de retraso en la entrega de cada informe de incidencia	0,5%

6.1.6 Calidad del Servicio

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Servidores sin contagio de virus	Por cada servidor con virus	5%
Servidores con sw antivirus y actualizaciones al día	Por cada servidor sin antivirus actualizado	2%
Aplicación de Políticas, Normas y Procedimientos de Seguridad de PREVIRED	Por cada incumplimiento en la aplicación de política, normas o procedimientos de seguridad de PREVIRED	5%

6.1.7 Aplicación Controles de Cambio

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Tiempo de ejecución solicitudes de controles de cambio planificados	Si nivel de cumplimiento promedio mensual es menor a 95%	3%
Tiempo de ejecución solicitudes de controles de cambio por incidentes (urgencia)		

6.1.8 Cumplimiento de proyectos

INDICADOR	CONDICIÓN	% DE CUOTA MENSUAL
Implementación de calidad de proyecto en tiempo estipulado	Si el proyecto no se ha implementado según lo requerido por Previred en el tiempo establecido	1%
	Si el proyecto no se ha implementado según lo requerido por Previred, sino hasta un par de semanas después de la fecha establecida	3%
	Si el proyecto no se ha implementado según lo requerido por Previred, sino hasta un mes después	5%

6.2 Multas definidas para incumplimientos centro de procesamiento alterno

Aplicables a servicios de contingencia correspondientes a las distintas líneas de negocio .

INDICADOR	Condición de NO cumplimiento	MULTA
Ejecución de Pruebas DRP	1. Por cada no ejecución de pruebas atribuible al oferente 2. Por no cumplimiento de calendario definido e informado. 3. Por cada prueba fallida en que no fue posible disponibilizar los servicios en site secundario. El no cumplimiento de 1 o más condiciones, aplica multa.	5% de la cuota mensual del contrato
RTO <= 2 horas	Por cada 30 minutos o fracción de atraso, sobre el RTO definido, aplica tanto a la ida a site secundario como vuelta a site principal.	5% de la cuota mensual del contrato por cada 30 minutos o fracción Con tope de 10%

Indisponibilidad de los servicios	1. Caída de 1 o más servicios operando en site secundario, responsabilidad del proveedor. 2. Degradación de 1 o más servicios operando en site secundario, responsabilidad del proveedor. 3. Falla en 1 o más funcionalidades de uno o más servicios, responsabilidad del proveedor. El no cumplimiento de 1 o más condiciones, aplica multa.	5% de la cuota mensual del contrato por cada 30 minutos o fracción Con tope de 10%

7 Tabla de Precios

La tabla de precios a completar deberá presentarse en 3 versiones de posibles plazos de contratación del servicio "operando" a 48 meses, 72 meses y 96 meses.

7.1 Se entiende por Servicio BASE los ítems siguientes:

Todo lo comprendido en la presente documentación se entiende como servicios Base.

7.2 Formato de Entrega Oferta Económica

	Servicios / Plazo Servicio	**a 48 meses**		**a 72 meses**		**a 96 Meses**	
	Moneda (UF / Dólar)	UF	Dólar	UF	Dólar	UF	Dólar
ITEM	**SERVICIOS BASICOS**						
1	**Servicios presentados en la presente documentación**						
2	Infraestructura de Servidores (*)						
2.1	**Grupo 1 (Producción)**						
2.2	**Grupo 2 (Producción)**						
2.3	**Grupo 3 (PreProducción)**						
2.4	**Grupo 4 (Openshift)**						
2.4	**Grupo 5 (Contingencia)**						
	Servicios / Plazo Servicio	**a 48 meses**		**a 72 meses**		**a 96 Meses**	
	Moneda (UF / Dólar)	UF	Dólar	UF	Dólar	UF	Dólar
ITEM	**Ítems a cotizar por separado**						
3	Servicio de monitoreo y observabilidad, detallado en punto 3.43						

4	Escritorios Virtuales, detallado en punto 3.18						
5	Migración Cintas Históricas, detallado en punto 3.12						
6	Licencias de Software Adicionales a las de Previred, detallado en punto 3.39						
7	Servicios Base de Seguridad Descritos, detallado en punto 3.40.2						
8	Servicios Adicionales de Seguridad descritos, detallado en punto 3.40.3						

(*): El detalle de cada grupo de servidores se encuentra especificado en Anexo N° 2, Listado de Servidores.

(*): Los valores deben presentarse en UF y/o dólar sin IVA

PREVIRED SE RESERVA EL DERECHO A CONTRATAR TOTAL O PARCIALMENTE LOS ÍTEMES COTIZADOS.

Para efectos de valorización por grupo de servidores, se solicita que todos los costos de servicios que se asocian directamente a los servidores sean incluidos en los costos de cada grupo.

> Ejemplo: Para los servidores de los Grupos 1, 2 y 4: se deben considerar, Servicios de ingeniería de Sistema, Administración de BD, Respaldos y Monitoreo. En definitiva, con todos sus servicios asociados. Esto para efectos de dividir costos por Unidades de Negocio internas de Previred.

Para los Servidores virtuales solicitados en el Grupos 3: se han solicitado en plataforma cloud para tener la posibilidad de dar de alta o baja servidores cuando el negocio lo requiera.

Los valores a considerar para la baja de servidores son los mismos que el oferente cotizará para altas de servidores. Punto 7.3

7.3 Crecimiento a Demanda

El oferente deberá considerar la valorización de componentes a demanda, para crecimientos futuros de Previred.

El contrato debe tener la flexiblidad de crecimiento o bajas de recursos a demanda. Se espera que los costos de crecimientos sean homólogos a cuando se quieran dar de baja.

COSTOS DE ALTA Y BAJAS SERVICIOS EN CLOUD	UF MES	US$ MES
Hoja exclusiva, equivalente en capacidad a las ofertadas		
Operación básica		
Monitoreo		
Respaldo por cada 150 GB.		
Respaldo por cada 500 GB.		
Restore por cada 150 GB		
Restore por cada 500 GB		
Storage crecimiento 1 TB discos rápidos o SSD		
RAM adicional 1 GB.		
Core adicional 1 Vcore		
Licencia Windows Server SPLA		
Antivirus		
Soporte Linux Redhat		

Licencia SQL STD SPLA (2 core)		
Licencia SQL ENT SPLA (2 core)		
Cloud Vserver A - 2 Vcores, 4 GB. RAM, 100 GB. SSD, RHEL (64 bit), Operación, Respaldo, Monitoreo		
Cloud Vserver B - 4 Vcores, 8 GB. RAM, 100 GB. SSD, RHEL (64 bit), Operación, Respaldo, Monitoreo		
Cloud Vserver C - 8 Vcores, 16 GB. RAM, 100 GB. SSD, RHEL (64 bit), Operación, Respaldo, Monitoreo		
Cloud Vserver D - 2 Vcores, 4 GB. RAM, 100 GB. SSD, Win Server, Operación, Respaldo, Monitoreo		
Cloud Vserver E - 4 Vcores, 8 GB. RAM, 100 GB. SSD, Win Server, Operación, Respaldo, Monitoreo		
Cloud Vserver F - 8 Vcores, 16 GB. RAM, 100 GB. SSD, Win Server, Operación, Respaldo, Monitoreo		
Network - VLAN		
Network - Public IP - 32 Portable Public IP Addresses		

Los valores deben presentarse en UF y/o dólar sin IVA

COSTOS DE ALTA Y BAJAS SERVICIOS ON PREMISE	**UF MES**	**US$ MES**
Hoja exclusiva, equivalente en capacidad a las ofertadas		
Operación básica		
Monitoreo		

Ingeniería de Sistemas		
Administración de BD		
Respaldo por cada 150 GB.		
Respaldo por cada 500 GB.		
Storage crecimiento 1 TB discos rápidos o SSD		
Crecimiento 500 GB. almacenamiento replicado (para servicios con contingencia)		
RAM adicional 1 GB.		
Core adicional 1 Vcore		
Licencia Windows Server SPLA		
Antivirus		
Soporte Linux Redhat		
Licencia SQL STD SPLA (2 core)		
Licencia SQL ENT SPLA (2 core)		
Vserver A - 2 Vcores, 4 GB. RAM, 150 GB. almacenamiento, RHEL (64 bit), Operación, Respaldo, Monitoreo		
Vserver B - 4 Vcores, 8 GB. RAM, 150 GB. almacenamiento, RHEL (64 bit), Operación, Respaldo, Monitoreo		
Vserver C - 8 Vcores, 16 GB. RAM, 150 GB. almacenamiento, RHEL (64 bit), Operación, Respaldo, Monitoreo		
Vserver D - 2 Vcores, 4 GB. RAM, 150 GB. almacenamiento, Win Server, Operación, Respaldo, Monitoreo, Antivirus		

Vserver E - 4 Vcores, 8 GB. RAM, 150 GB. almacenamiento, Win Server, Operación, Respaldo, Monitoreo, Antivirus		
Vserver F - 8 Vcores, 16 GB. RAM, 150 GB. almacenamiento, Win Server, Operación, Respaldo, Monitoreo, Antivirus		

Nota: para los Vserver se deben contemplar todos los componentes que permita a la máquina en cuestión operar de manera correcta y lista para poder ser utilizada. Esto considera: sistema operativo, antivirus si aplica, monitoreo, respaldo, anclamiento a dominio según definición, entre otros.

Los valores deben presentarse en UF y/o dólar sin IVA

7.4 Bajas de Servicios o Máquinas

El oferente deberá descontar a Previred la valorización indicada en punto 7.3 al momento de que Previred proceda a dar de baja algún servicio o máquina(s).

El descuento respectivo será efectivo en la facturación del mes siguiente a la baja del servicio o máquina(s).

8 Anexos

En esta sección se incluye información necesaria para el dimensionamiento del servicio.

8.1 Anexo de requerimientos físicos y ambientales del Data Center

Se adjunta documento Word "Anexo N° 1 Requerimientos Físicos y ambientales del Data Center"

8.2 Anexo de listado de servidores ambientes Producción, Preproducción y Contingencia

Se adjunta documento Word "Anexo N° 2 Listado Servidores"

8.3 Anexo de licencias propiedad de Previred

Se adjunta documento Word "Anexo N° 3 Licencias Propiedad PreviRed"

8.4 Anexo de fichas de diagramas de servicio

Se adjunta documento Word "Anexo N° 4 Fichas Diagramas de Servicio"

8.5 Anexo de procedimientos de respaldo, retención y recuperación de la información

Se adjunta documento Word "Anexo N° 5 Procedimiento de Respaldo, Retención y Recuperación de la Información"

8.6 Anexo de consideraciones para la arquitectura servidores de base de datos

Se adjunta documento Word "Anexo N° 6 Consideraciones para la Arquitectura Servidores de Base de Datos"

8.7 Anexo de templates utilizados para la solicitud de creación de máquinas virtuales

Se adjunta documento Word "Anexo N° 7 Template para máquinas virtuales"

8.8 Anexo del protocolo de aceptación de los servicios

Se adjunta documento Word "Anexo N° 8 Protocolo de Aceptación de Servicios"

8.9 Anexo de grupos de migración según etapas de migración definidos (ETM)

Se adjunta documento Word "Anexo N° 9 Grupos Migración ETM"

8.10 Anexo de Inventario Base, matriz de software

Se adjunta documento Word "Anexo N° 10 Inventario Base - Matriz Software"

8.11 Anexo de Inventario de comunicaciones

Se adjunta documento Word "Anexo N° 11 Inventario Comunicaciones Seguridad".