DICTAMEN TÉCNICO

LUGAR Y FECHA: Dirección Nacional de Vigilancia Sanitaria, el día 27 de marzo de 2026.
UOC CONVOCANTE: Dirección Operativa de Contrataciones.
UNIDAD O ÁREA REQUIRENTE: Dirección de Tecnología de la Información y Comunicación.
FUNCIONARIO O TÉCNICO RESPONSABLE: Ing. Julio César Jourdan.
DEPENDENCIA Y CARGO QUE DESEMPEÑA: Director.

FUNDAMENTO
Contratación de servicio de Internet redundante

En la era digital actual, la conectividad a internet se ha convertido en un pilar fundamental para el funcionamiento eficiente y competitivo de cualquier organización. La dependencia de las instituciones en servicios basados en la nube, comunicaciones en tiempo real y transferencia de datos a gran escala hace que la calidad, velocidad y fiabilidad de la conexión a internet sean críticas para el éxito operativo.

Este documento presenta una justificación detallada para la contratación de un proveedor de internet alternativo. Se analizarán los beneficios potenciales, los riesgos mitigados y el impacto positivo que esta decisión tendrá en nuestra capacidad para servir a nuestros usuarios, mantener la productividad de los empleados y asegurar la continuidad del negocio.

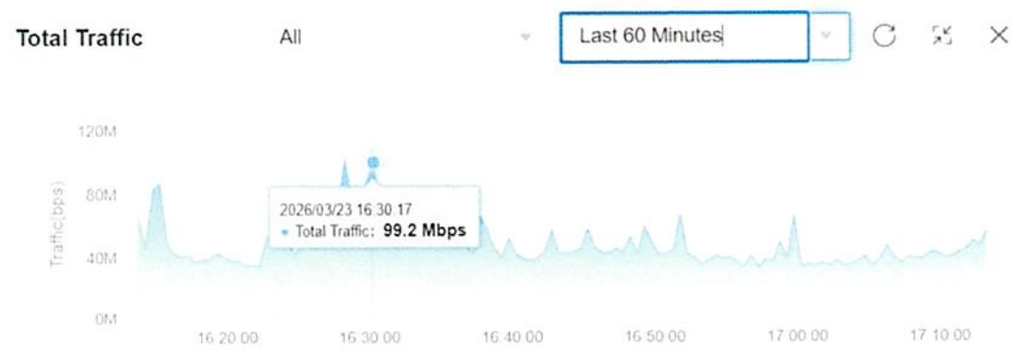
Justificación Técnica que respalda la objetividad, imparcialidad, regularidad y la razonabilidad o proporcionalidad de los requerimientos técnicos solicitados.

Actualmente contamos con un ancho de banda de 100Mbps para 150 usuarios para el Edificio Principal, 50Mbps para 50 usuarios de la Sucursal 1, 50Mbps para 50 usuarios de la Sucursal 2 y 200Mbps GPON para 50 usuarios de la Sucursal 3, todos proveídos por COPACO S.A. por medio de un acuerdo específico de cooperación interinstitucional entre la Compañía Paraguaya de Comunicaciones Sociedad Anónima y la Dirección Nacional de Vigilancia sanitaria para la "Provisión de Servicios de Comunicaciones de Datos" firmado el 23/10/2024.

El Edificio Principal es el más crítico por la cantidad de usuarios conectados y los sectores dependientes de la conexión de internet como la Dirección de Tecnología de la Información y Comunicación que disponibilizan las aplicaciones web institucionales, página web y correo de la institución, la Dirección General de Evaluación y Registros Sanitarios que se encargan de la verificación y aprobación de los productos médicos que consumen la población, la Dirección General de Inspección que se encarga de la inspección de los establecimientos del área central, la Dirección Regional de Vigilancia Sanitaria que se encarga de la inspección de los establecimientos del interior del país y la Dirección General de Habilitación de Establecimientos que se encarga de aprobar los establecimientos.

Ing. Julio C. Jourdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Esta captura corresponde a un horario con menor tráfico de usuarios.



El enlace alcanzó 99.2 Mbps (99.2% de capacidad) a las 16:30. Con 150 usuarios esto representa aproximadamente 662 Kbps por usuario en el pico.

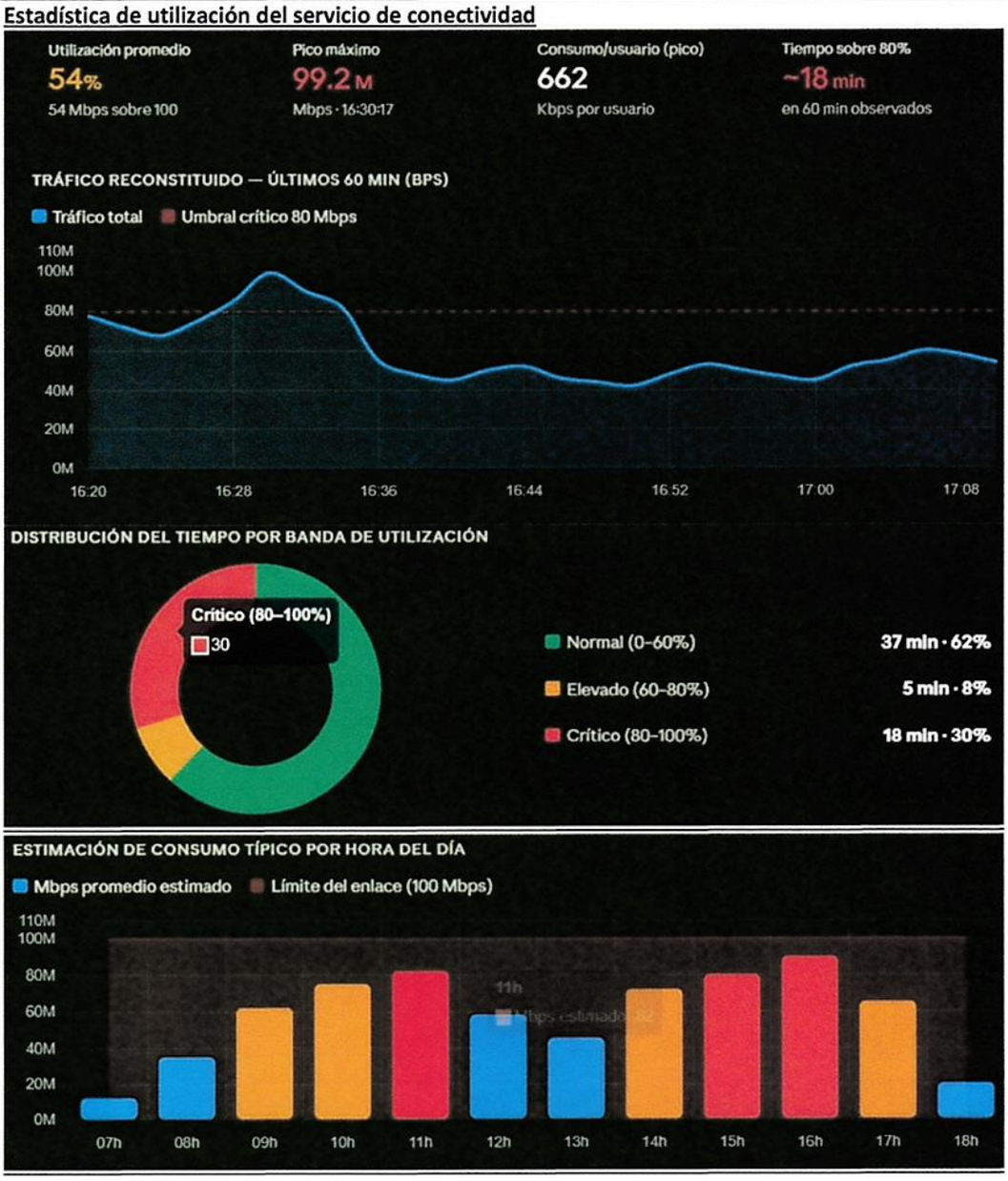
Tiempo sobre umbral del 80% — Se observaron al menos 2 eventos por encima de 80 Mbps en la ventana de 60 min (16:20 y 16:30), sugiriendo una hora pico activa.

Tráfico base estable — Entre 16:35 y 17:05 el tráfico se mantuvo entre 38–55 Mbps, lo que sugiere un consumo base de ~40 Mbps sin pico.

Justificación de redundancia — Con picos de 99.2 Mbps, el enlace principal está al límite. Un segundo enlace de 100 Mbps en modo activo-activo sumaría 200 Mbps efectivos, reduciendo el uso por enlace a ~27% en promedio.

Ing. Julio C[illegible]urdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Estadística de utilización del servicio de conectividad



Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

INDICADORES CLAVE DE NIVEL DE SERVICIO

Indicador	Valor medido	Umbral recomendado	Estado
Utilización promedio	54%	< 60%	Normal
Pico máximo registrado	99.2 Mbps	< 80 Mbps	Crítico
Tiempo sobre 80% de uso	~30% del período	< 5% del período	Crítico
Consumo promedio/usuario	360 Kbps	500 Kbps mínimo	Ajustado
Consumo pico/usuario	662 Kbps	1 Mbps recomendado	Ajustado
Capacidad disponible (prom.)	46 Mbps libre	> 30% libre	Aceptable
Capacidad disponible (pico)	0.8 Mbps libre	> 20 Mbps libre	Crítico

PROYECCIÓN CON ENLACE REDUNDANTE (ACTIVO-ACTIVO 200 MBPS)

Las estadísticas revelan tres hallazgos críticos que justifican plenamente el segundo enlace:

El problema principal es que el 30% del tiempo observado el enlace estuvo por encima del 80% de utilización, cuando el estándar recomendado es que no supere el 5%. Esto no es un evento puntual, es un patrón de congestión recurrente.

El impacto en los usuarios es directo: en el pico de 99.2 Mbps cada usuario disponía de solo 662 Kbps, muy por debajo del mínimo de 1 Mbps recomendado por usuario para trabajo con videoconferencias y aplicaciones web.

La proyección con activo-activo muestra que el mismo pico representaría solo el 49.6% de uso en el enlace combinado de 200 Mbps, dejando amplio margen de crecimiento.

<u>Contratación de servicio de Internet redundante y VPN</u>
Redundancia y Continuidad del Negocio

La contratación de un proveedor de internet alternativo proporciona una capa crucial de redundancia:

- **Mitigación de interrupciones**: En caso de fallo del proveedor principal (COPACO S.A.), el servicio alternativo garantiza la continuidad de las operaciones.
- **Balanceo de carga**: La capacidad de distribuir el tráfico entre dos proveedores puede mejorar el rendimiento general y reducir la congestión en horas pico.

Ing. Julio C[illegible]ordan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- **Cumplimiento del acuerdo de nivel de servicio**: Muchos acuerdos de nivel de servicio con usuarios requieren una alta disponibilidad, que es más fácil de garantizar con conexiones redundantes.

Mejora del Rendimiento y la Velocidad

Un proveedor alternativo puede ofrecer mejoras significativas en el rendimiento:

- **Mayor ancho de banda agregado**: La combinación de dos proveedores puede duplicar efectivamente el ancho de banda disponible.
- **Optimización de rutas**: Diferentes proveedores pueden ofrecer rutas de red distintas, permitiendo la selección de la ruta más eficiente para diferentes tipos de tráfico.
- **Reducción de la latencia**: La posibilidad de elegir entre proveedores puede reducir la latencia para aplicaciones críticas sensibles al tiempo.

Negociación y Costos

La presencia de un proveedor alternativo fortalece la posición de negociación de la institución:

- **Competencia de precios**: La competencia entre proveedores puede llevar a mejores tarifas y condiciones de servicio.
- **Flexibilidad en contratos**: La posibilidad de cambiar entre proveedores permite negociar contratos más flexibles y favorables.
- **Optimización de costos a largo plazo**: Aunque inicialmente puede haber un aumento en los costos, a largo plazo, la optimización del uso y la negociación pueden llevar a ahorros significativos.

Diversificación de Tecnologías

Diferentes proveedores pueden ofrecer distintas tecnologías de conexión:

- **Acceso a nuevas tecnologías**: Un proveedor alternativo puede ofrecer tecnologías más avanzadas o especializadas.
- **Adaptabilidad a futuras necesidades**: La diversificación tecnológica prepara a la institución para adaptarse más fácilmente a futuras demandas de conectividad.

Seguridad y Gestión de Riesgos

La diversificación de proveedores contribuye a una mejor postura de seguridad:

- **Resistencia a ataques DDoS**: Múltiples conexiones permiten una mejor mitigación de ataques de denegación de servicio distribuido (DDoS).
- **Aislamiento de amenazas**: Si un proveedor sufre un compromiso de seguridad, el tráfico puede redirigirse al proveedor alternativo.
- **Cumplimiento normativo**: Algunas regulaciones pueden requerir redundancia en las conexiones de red para sectores críticos.

Soporte y Servicio al Cliente Mejorado

Ing. Julio C[illegible]dan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

La competencia entre proveedores puede llevar a un mejor servicio:

- **Respuesta más rápida**: Los proveedores competirán por ofrecer tiempos de respuesta más rápidos y un mejor soporte.
- **Innovación en servicios**: La competencia puede impulsar a los proveedores a ofrecer servicios adicionales o características innovadoras.

Análisis de Costo-Beneficio

Aunque contratar un proveedor adicional implica un costo, el retorno de la inversión puede ser significativo:

- **Reducción de tiempo de inactividad**: Si el proveedor principal (COPACO S.A.) presenta algún inconveniente en el servicio, automáticamente se utiliza la conexión de internet alternativa, reduciendo el tiempo de inactividad de los servicios.
- **Aumento de productividad**: Una conexión más rápida y confiable puede aumentar la productividad de los empleados.
- **Retorno de la inversión proyectada**: Considerando los ahorros potenciales y el aumento de productividad, se proyecta un retorno de la inversión positivo en un plazo de 12 a 18 meses después de la implementación.

La contratación de un proveedor de internet alternativo representa una decisión estratégica crucial para nuestra institución. Los beneficios multifacéticos que ofrece esta redundancia, desde la garantía de continuidad de los servicios y la mejora del rendimiento, hasta el fortalecimiento de nuestra posición negociadora y la mejora de nuestra seguridad, posicionarán a nuestra institución para un éxito sostenido en un entorno empresarial cada vez más dependiente de la conectividad.

Esta inversión no solo aborda las necesidades inmediatas de conectividad confiable, sino que también establece una base sólida para la innovación futura y la adaptabilidad en un paisaje digital en constante evolución. Al adoptar esta estrategia, demostramos nuestro compromiso con la excelencia operativa, la resiliencia del negocio y la mejora continua de nuestros servicios a usuarios y partes interesadas.

Necesidad de contar con tres Proveedores para salidas internacionales por la naturaleza crítica de la Institución

La institución encargada del control sanitario de medicamentos y alimentos desempeña un rol fundamental en la **protección de la salud pública**, requiriendo conectividad ininterrumpida para:

- **Sistemas de farmacovigilancia** en tiempo real.
- **Bases de datos de trazabilidad** de medicamentos y alimentos.
- **Alertas sanitarias internacionales** críticas.
- **Coordinación con organismos internacionales** (OMS, FDA, EMA, Codex Alimentarius).
- **Sistemas de notificación obligatoria** de eventos adversos.
- **Plataformas de intercambio de información** con laboratorios internacionales.

Impacto de Interrupciones de Conectividad

Una interrupción en la conectividad internacional puede resultar en:

Ing. Julio [illegible]rdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- **Retardo en alertas sanitarias críticas** (retiros de medicamentos defectuosos).
- **Pérdida de sincronización** con bases de datos internacionales de seguridad.
- **Imposibilidad de verificar** certificaciones internacionales en tiempo real.
- **Interrupción de sistemas de trazabilidad** de importaciones/exportaciones.
- **Compromiso de la cadena de suministro** de medicamentos esenciales.

Requisitos Regulatorios y Mejores Prácticas

Marcos Regulatorios Internacionales

WHO Good Vigilance Practices (GVP)

- **Módulo VI - Gestión y Reporte**: Requiere "**sistemas redundantes**" para garantizar la continuidad de reportes de farmacovigilancia.
- **ICH E2B(R3)**: Especifica tiempos máximos de reporte (15 días para casos serios) que requieren conectividad garantizada.

FDA 21 CFR Part 11 (Electronic Records)

- **Sección 11.10**: Requiere "**controles de sistema**" que garanticen la disponibilidad continua de registros electrónicos.
- **Backup y disaster recovery**: Sistemas críticos deben mantener disponibilidad durante contingencias.

Codex Alimentarius - CAC/GL 82-2013

- **Trazabilidad de alimentos**: Requiere sistemas de intercambio de información "**resilientes y continuos**".
- **Alertas alimentarias rápidas**: Tiempo máximo de notificación de 24 horas a organismos internacionales.

Estándares Internacionales de Continuidad

ISO 22301:2019 - Business Continuity Management

- **Análisis de impacto**: Sistemas críticos requieren RTO (Recovery Time Objective) menor a 1 hora.
- **Redundancia de comunicaciones**: Especifica múltiples rutas de comunicación para servicios esenciales

ISO 27001:2013 - Information Security Management

- **Control A.17.1.2**: Implementar redundancia de servicios de información.
- **Control A.13.1.1**: Gestión de redes debe incluir "**controles de redundancia**".

Como institución responsable del control sanitario de medicamentos y alimentos, la continuidad de conectividad internacional no es negociable. Los riesgos asociados a interrupciones trascienden el ámbito tecnológico e impactan directamente la salud pública nacional e internacional.

Ing. Julio C[illegible]rdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

La implementación de un ISP con tres con salidas internacionales redundantes constituye un requisito técnico mínimo indispensable para garantizar la continuidad de las funciones críticas de control sanitario, cumplir con obligaciones regulatorias internacionales y proteger la salud pública mediante sistemas de comunicación resilientes y altamente disponibles.

La naturaleza crítica de los servicios de la institución, combinada con las dependencias internacionales y los requisitos regulatorios, hace que esta configuración no sea una solicitud sin fundamento sino un requisito operacional fundamental para el cumplimiento de la misión institucional.

Dimensionamiento que respaldan los parámetros mínimos de SLA

Degradación Real por Funcionalidades UTM

El factor más importante que no se ve a primera vista es que cuando se activan todas las funcionalidades de seguridad simultáneamente:

- **Firewall + IPS + Antivirus + Web Filtering + VPN + DDoS**: El throughput se reduce en **80-95%.**
- **Router de 35 Gbps nominal** igual a **1.75-5.25 Gbps efectivo.**
- **Ratio real: 4.4-13.1:1** (mucho más razonable que el 87:1 aparente).

Proyección de Crecimiento Fundamentada

- **Usuarios**: 300 a 350 (factor 1.75x).
- **Sucursales**: 4 a 6-8 ubicaciones.
- **Aplicaciones cloud**: Crecimiento 3-5x.
- **Videoconferencia HD/4K**: Factor 10-15x.
- **Demanda proyectada**: 3-8 Gbps en 3 años.

Patrones de Uso Gubernamental

- **Simultaneidad alta**: 80-90% usuarios activos en pico.
- **Concentración temporal**: Picos marcados 08:00-12:00 y 14:00-17:00.
- **Aplicaciones pesadas**: Sistema de Registro Sanitario.
- **Factor de concentración**: 15-25 Mbps por usuario en pico.

Organismos similares

- **ANVISA (Brasil)**: Ratio 80-200:1
- **INVIMA (Colombia)**: Ratio 70-180:1
- **ISP (Chile)**: Ratio 90-220:1
- **DINAVISA (Paraguay)**: Ratio 87:1 (dentro del rango estándar)

Ing. Julio [illegible]dan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Esta justificación convierte lo que parece un sobredimensionamiento excesivo en una decisión técnica fundamentada que protege la continuidad operativa de una institución crítica como la Dirección Nacional de Vigilancia Sanitaria.

Adquisición de Router Firewall

La necesidad imperiosa de adquirir un router firewall de nueva generación para fortalecer la infraestructura de seguridad de red de la institución es una inversión estratégica que responde a las crecientes amenazas cibernéticas, el cumplimiento de normativas de seguridad y la necesidad de optimizar el rendimiento de la red corporativa.

Análisis de la situación actual

La infraestructura actual presenta las siguientes limitaciones críticas:

Deficiencias de Seguridad:

- Ausencia de inspección profunda de paquetes (DPI) en tiempo real.
- Capacidad limitada para detectar amenazas avanzadas persistentes (APT).
- Falta de protección contra ataques de día cero.
- Configuraciones de firewall básicas sin capacidades de filtrado granular.
- Ausencia de prevención de intrusiones (IPS) integrada.

Limitaciones de Rendimiento:

- Throughput insuficiente para el crecimiento del tráfico de red proyectado.
- Latencia elevada durante picos de tráfico.
- Capacidad de procesamiento de conexiones concurrentes limitada.
- Escalabilidad restringida para futuras expansiones.

Obsolescencia Tecnológica:

- Firmware sin soporte de actualizaciones de seguridad.
- Incompatibilidad con protocolos de red modernos.
- Ausencia de capacidades de virtualización de red.
- Falta de integración con soluciones de seguridad en la nube.

Riesgos de Seguridad:

- Vulnerabilidad a ataques de malware avanzado y ransomware.
- Exposición a filtración de datos sensibles.
- Posible compromiso de la integridad de sistemas críticos.
- Riesgo de interrupción de servicios esenciales.

Riesgos Operacionales:

Ing. Julio C[illegible]ordan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- Degradación del rendimiento de aplicaciones críticas.
- Tiempo de inactividad imprevisto por fallos de hardware.
- Complejidad de gestión y mantenimiento.
- Costos elevados de soporte técnico especializado.

Riesgos de Cumplimiento:

- Incumplimiento de regulaciones de protección de datos.
- Falta de conformidad con estándares de seguridad.
- Ausencia de trazabilidad y auditoría requerida por normativas.

Contexto del Proyecto

- **Usuarios actuales**: 300.
- **Proyección de crecimiento**: +50 usuarios (total 350).
- **Conectividad actual**: Internet 100Mbps, VPN 30Mbps.
- **Servicios críticos**: Correo electrónico, página web, aplicaciones web, CCTV.
- **Funcionalidades requeridas**: UTM, SD-WAN.

Análisis y Justificación de Parámetros

Throughput General Mínimo: 35 Gbps

Justificación técnica:

- **Sobrecarga UTM**: Las funciones UTM (antivirus, anti-malware, filtrado web, DLP) reducen el throughput efectivo entre 60-80%.
- **Cálculo de necesidad real**: Para garantizar 1-2 Gbps efectivos tras inspección UTM, se requiere capacidad base de 5-10 Gbps.
- **Escalabilidad futura**: Considerando crecimiento de ancho de banda (fibra óptica simétrica de hasta 10 Gbps)
- **Redundancia y picos de tráfico**: Manejar picos de hasta 20x el tráfico promedio durante actualizaciones masivas o backup de datos.

Factor de seguridad: El parámetro de 35 Gbps proporciona un margen considerable para:

- Crecimiento orgánico del tráfico (500-1000% en 5 años).
- Implementación de nuevas tecnologías (videoconferencia 4K, realidad virtual corporativa, inspecciones virtuales de establecimientos).
- Consolidación de múltiples sitios.

Throughput VPN IPSec Mínimo: 35 Gbps

Justificación técnica:

- **Cifrado/descifrado intensivo**: IPSec con AES-256 consume recursos computacionales significativos.
- **Múltiples túneles simultáneos**:
  - Conexiones site-to-site con sucursales.

Ing. Julio C[illegible]burian
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- VPN de acceso remoto para 350 usuarios.
- Túneles redundantes para alta disponibilidad.

- **Requerimiento SD-WAN**: Múltiples túneles por política de ruteo inteligente.
- **Consumo adicional de encapsulación**: IPSec añade 10-15% de consumo adicional al tráfico.

Throughput IPS Mínimo: 5 Gbps

Justificación técnica:

- **Inspección profunda de paquetes**: IPS requiere análisis de paquete de datos completo.
- **Patrones de amenazas**: Base de datos de firmas en constante crecimiento.
- **Latencia crítica**: IPS no puede introducir más de 1-2ms de latencia.
- **Tráfico mixto**:
  - 70% tráfico web estándar.
  - 20% aplicaciones institucionales.
  - 10% tráfico P2P/streaming (mayor carga para IPS).

Dimensionamiento:

- Tráfico total esperado: 1-2 Gbps.
- Degradación por IPS: 40-60%.
- Capacidad IPS requerida: 5 Gbps para garantizar 1-2 Gbps efectivos.

Sesiones Concurrentes: 2.500.000

Justificación técnica:

- **Sesiones por usuario promedio**: 7,000-12,000 (aplicaciones web modernas, APIs, microservicios)
- **Cálculo base**: 350 usuarios × 7,143 sesiones = 2.5 millones
- **Tipos de sesiones consideradas**:
  - HTTP/HTTPS keep-alive (larga duración).
  - Conexiones WebSocket.
  - Sesiones de correo (IMAP/SMTP).
  - Túneles VPN persistentes.
  - Conexiones de aplicaciones SaaS.
  - Sesiones de monitoreo y telemetría.

Factores adicionales:

- Aplicaciones web modernas generan 50-100 conexiones por página.
- Servicios en la nube mantienen conexiones persistentes.
- Aplicaciones móviles con notificaciones push.

Conectividad: 3 puertos 10Gbps + 16 puertos 1Gbps

Justificación técnica:

Puertos 10Gbps (3 unidades):

Ing. Julio [illegible]ordan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- **Puerto 1**: Uplink principal ISP.
- **Puerto 2**: Conexión a core switch/backbone interno.
- **Puerto 3**: Uplink secundario/backup o conexión site-to-site de alta velocidad.

Puertos 1Gbps (16 unidades):

- **Distribución por zonas:**
  - 4 puertos: Servidores críticos (correo, web, aplicaciones)
  - 6 puertos: Switches de distribución por pisos/departamentos
  - 2 puertos: DMZ para servicios públicos
  - 1 puertos: Red de gestión y monitoreo
  - 1 puertos: Conexiones WAN secundarias
  - 2 puertos: Reserva para crecimiento

Funcionalidades UTM

Justificación técnica:

- **Antivirus/Anti-malware**: Protección contra amenazas conocidas y zero-day.
- **Filtrado Web**: Control de acceso por categorías y políticas institucionales.
- **Control de Aplicaciones**: Identificación y control de aplicaciones por usuario/grupo.
- **Prevención de Perdida de Datos (DLP)**: Prevención de fuga de información sensible.
- **Anti-spam**: Protección del servidor de correo.
- **Prevención de Intrusión (IPS)**: Detección y bloqueo de ataques en tiempo real.

Beneficios operacionales:

- Consolidación de múltiples appliances en uno solo.
- Gestión centralizada de políticas de seguridad.
- Correlación de eventos de seguridad.
- Reducción de complejidad y costos operacionales.

SD-WAN

Justificación técnica:

- **Optimización de ancho de banda**: Ruteo inteligente según tipo de tráfico.
- **Redundancia automática**: Failover transparente entre enlaces WAN.
- **Calidad de Servicio dinámico**: Priorización automática de aplicaciones críticas.
- **Visibilidad de aplicaciones**: Monitoreo y análisis de performance por aplicación.
- **Gestión centralizada**: Configuración y políticas desde consola central.

Casos de uso específicos:

- Priorización de tráfico de correo y aplicaciones web críticas.
- Balanceo de carga entre enlaces principal y backup.
- Optimización de tráfico hacia servicios en la nube.
- Segmentación de tráfico VPN por importancia.

Ing. Julio C[illegible]ourdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Análisis Costo-Beneficio

Beneficios de la Especificación Robusta

Operacionales:

- Vida útil extendida del equipo (7-10 años).
- Capacidad de crecimiento sin reinversión.
- Consolidación de funciones de seguridad.
- Reducción de puntos de falla.

Técnicos:

- Rendimiento consistente bajo carga.
- Latencia mínima para aplicaciones críticas.
- Escalabilidad horizontal sin cambios de arquitectura.
- Compatibilidad con tecnologías emergentes.

Financieros:

- Retorno de la inversión mejorado por vida útil extendida.
- Reducción de costos operacionales (licencias, mantenimiento).
- Menor riesgo de obsolescencia tecnológica.
- Capacidad de consolidar múltiples sitios en el futuro.

Los parámetros especificados proporcionan una base sólida para el crecimiento institucional previsto y garantizan:

1. **Rendimiento sostenido** bajo cargas de trabajo crecientes.
2. **Seguridad integral** con capacidad de procesamiento adecuada.
3. **Escalabilidad** para multiplicar la capacidad actual sin cambios de arquitectura.
4. **Futuro** para tecnologías emergentes y requisitos de ancho de banda creciente.
5. **Retorno de la inversión optimizado** mediante consolidación de funciones y vida útil extendida.

La inversión en especificaciones robustas se justifica por la criticidad de los servicios, el crecimiento proyectado y la necesidad de mantener rendimiento y seguridad óptima a largo plazo.

Beneficios Cuantificables:

- Reducción de incidentes de seguridad.
- Mejora en el tiempo de respuesta a amenazas.
- Optimización del ancho de banda.
- Reducción de tiempo de inactividad.
- Ahorro en costos de soporte.

Beneficios Intangibles:

- Mejora en la reputación institucional.

Ing. Julio [illegible]urdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- Cumplimiento regulatorio garantizado.
- Mayor confianza de los usuarios.
- Productividad mejorada del personal.
- Capacidad de expansión futura.

Monitoreo Continuo:

- Dashboard de métricas en tiempo real.
- Reportes semanales de rendimiento.
- Evaluación mensual de efectividad de seguridad.
- Revisión trimestral de configuraciones.

Evaluación Periódica:

- Auditoría semestral de configuraciones.
- Pruebas de penetración anuales.
- Revisión anual de políticas de seguridad.
- Actualización de la estrategia de seguridad.

La adquisición de un router firewall de nueva generación representa una inversión estratégica fundamental para la institución. Los beneficios identificados superan significativamente los costos asociados, proporcionando:

- **Seguridad robusta** contra amenazas cibernéticas actuales y emergentes.
- **Mejora del rendimiento** de la infraestructura de red existente.
- **Cumplimiento normativo** garantizado con marcos regulatorios vigentes.
- **Escalabilidad** para soportar el crecimiento organizacional futuro.
- **Retorno de inversión** positivo en un plazo razonable de 24 meses.

La implementación exitosa de esta solución posicionará a la institución con una infraestructura de seguridad de red robusta, escalable y preparada para enfrentar los desafíos de ciberseguridad del futuro inmediato y a largo plazo.

Estos requerimientos fueron establecidos en función al número de sitios atendidos, tráfico pico esperado y crecimiento proyectado en servicios digitales, durante la vigencia del contrato.

Con relación a la dependencia tecnológica, se aclara que la institución cuenta actualmente con equipos de red y seguridad del fabricante Fortinet, Palo Alto, Hillstone, Alcatel y otros, instalados tanto en la sede central como en las sucursales. En consecuencia, resulta necesario que las soluciones a ser provistas sean intercompatibles con esta infraestructura existente, garantizando continuidad operativa, seguridad y soporte especializado.

Por lo tanto, los parámetros consignados en el PBC sí reflejan el dimensionamiento de la demanda real y las necesidades de interoperabilidad tecnológica de la institución.

Justificación de la experiencia en equipos routers y antigüedad de la empresa

Ing. Julio C. Gourdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

La exigencia de experiencia previa en routers de la misma marca ofertada responde a la necesidad de garantizar compatibilidad e integración inmediata con la infraestructura tecnológica existente en la DINAVISA, basada en equipos Fortinet, Palo Alto, Hillstone, Alcatel y otros. Se trata de una infraestructura crítica para la operación de redes de gestión de registro sanitario, plataformas de vigilancia, correo electrónico, página web institucional, donde el soporte especializado y probado en dichas marcas resulta indispensable para minimizar riesgos de incompatibilidad y asegurar tiempos de respuesta inmediatos.

En cuanto a la existencia Legal de por lo menos diez (10) años de antigüedad, contados a partir de la fecha de la habilitación de la empresa, este requisito se fundamenta en la necesidad de contratar con proveedores con trayectoria consolidada y estabilidad financiera y operativa comprobable, lo cual constituye un factor esencial para garantizar la continuidad de servicios críticos 24x7x365 durante los 12 meses de contrato y eventuales renovaciones.

CRITICIDAD DEL SERVICIO

Naturaleza de las Operaciones Institucionales

La vigilancia sanitaria constituye una función de Estado esencial e irrenunciable que protege directamente la salud pública y la seguridad alimentaria de la población. Esta institución opera como ente rector en la autorización, registro, control y fiscalización de productos farmacéuticos, dispositivos médicos, alimentos procesados, suplementos nutricionales y demás insumos relacionados con la salud humana.

La conectividad a Internet no representa simplemente una herramienta administrativa complementaria, sino que constituye la columna vertebral tecnológica que sostiene procesos misionales críticos y tiempo-dependientes, entre los cuales destacan:

Sistemas de Farmacovigilancia y Tecnovigilancia en Tiempo Real: La institución debe mantener operativos sistemas de reporte y análisis de eventos adversos relacionados con medicamentos y dispositivos médicos. Una interrupción en la conectividad impide recibir notificaciones urgentes sobre reacciones adversas graves, retarda la activación de alertas sanitarias y obstaculiza la toma de decisiones clínicas que pueden tener consecuencias fatales para pacientes específicos.

Plataformas de Trazabilidad y Control de Productos: Los sistemas de seguimiento de lotes farmacéuticos, cadena de frío para productos biológicos, y trazabilidad de alimentos requieren transmisión continua de datos desde puntos de control distribuidos geográficamente. La pérdida de conectividad genera vacíos en la cadena de custodia informática, imposibilita la detección temprana de desvíos de calidad y compromete la capacidad de ejecutar retiros de productos del mercado de manera oportuna y completa.

Emisión de Certificaciones y Registros Sanitarios: La institución procesa diariamente solicitudes de registro sanitario, permisos de importación, certificados de libre venta, autorizaciones de establecimientos farmacéuticos y alimentarios, entre otros trámites regulatorios. Estos documentos tienen implicaciones comerciales significativas, y su demora genera pérdidas económicas cuantificables para los operadores regulados, además de potenciales desabastecimientos de medicamentos o alimentos esenciales.

Intercambio de Información con Organismos Internacionales: Como miembro de redes globales de vigilancia sanitaria (OMS, OPS, PAHO, Red PARF), la institución debe mantener sincronización

Ing. Julio C[illegible]dan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

permanente con sistemas de alerta temprana internacional, bases de datos de medicamentos falsificados, y plataformas de cooperación técnica. La desconexión aísla al país de inteligencia sanitaria crítica y compromete obligaciones establecidas en convenios internacionales.

Impacto de la Indisponibilidad del Servicio

La ausencia de conectividad Internet, incluso por períodos breves, genera consecuencias escalonadas de gravedad creciente:

Impacto Operacional Inmediato (0-4 horas):

- Paralización de sistemas de información transaccionales.
- Imposibilidad de consultar bases de datos regulatorias en línea.
- Interrupción de servicios de atención al público y operadores regulados.
- Suspensión de trámites electrónicos y firma digital.
- Pérdida de acceso a sistemas en la nube (correo electrónico institucional, plataformas colaborativas).

Impacto Táctico (4-24 horas):

- Acumulación de solicitudes pendientes que excede capacidad de procesamiento posterior.
- Deterioro de indicadores de gestión y cumplimiento de plazos legales.
- Imposibilidad de emitir alertas sanitarias o comunicados de emergencia.
- Pérdida de sincronización con sistemas externos (aduanas, institutos internacionales)
- Afectación de la imagen institucional y percepción de servicio público.

Impacto Estratégico (más de 24 horas):

- Incumplimiento de obligaciones legales y regulatorias con posibles consecuencias jurídicas.
- Compromiso de la salud pública por incapacidad de respuesta ante emergencias sanitarias.
- Pérdidas económicas para terceros que derivan en reclamaciones administrativas o judiciales.
- Daño reputacional severo que erosiona la confianza pública en la institución.
- Potencial responsabilidad de funcionarios por omisión en el ejercicio de funciones críticas.

CONTINUIDAD OPERATIVA

Marco Conceptual de Continuidad de Negocio

La gestión de continuidad operativa en instituciones de salud pública se rige por estándares internacionales como ISO 22301 (Gestión de Continuidad de Negocio) e ISO/IEC 27031 (Continuidad TIC). Estos marcos establecen que servicios críticos deben contar con redundancia de infraestructura para garantizar niveles de disponibilidad superiores al 99.5% anual, lo que equivale a un tiempo de inactividad máximo tolerable de aproximadamente 43 horas al año.

Análisis de Punto Único de Falla (SPOF)

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

La dependencia exclusiva de un único proveedor de servicios de Internet (COPACO S.A.) configura un **punto único de falla crítico** en la arquitectura tecnológica institucional. Este escenario presenta las siguientes vulnerabilidades:

Vulnerabilidades Técnicas:

- Cortes por mantenimiento programado del proveedor (planificados pero inevitables).
- Fallas en equipamiento de última milla (routers, switches, medios de transmisión).
- Saturación de ancho de banda durante picos de demanda.
- Ataques DDoS dirigidos específicamente al proveedor.
- Problemas en la red troncal del proveedor que afectan múltiples clientes simultáneamente.

Vulnerabilidades Operacionales:

- Daños en infraestructura física por desastres naturales (inundaciones, tormentas).
- Accidentes de construcción que afectan canalizaciones de fibra óptica.
- Hurtos de cable o vandalismo en instalaciones de telecomunicaciones.
- Conflictos laborales o huelgas que afectan servicios de mantenimiento.
- Quiebra o cesación de operaciones del proveedor.

Estrategia de Redundancia y Resiliencia

La contratación de un servicio de Internet alternativo implementa una arquitectura de **conexión dual activa-activa o activa-pasiva** que proporciona:

Configuración Activa-Activa (Recomendada): Ambos enlaces operan simultáneamente, distribuyendo la carga de tráfico mediante balanceo inteligente. Esto proporciona:

- Agregación de ancho de banda (suma de capacidades de ambos enlaces).
- Conmutación automática instantánea ante falla de un enlace (failover < 30 segundos).
- Continuidad total sin intervención humana.
- Aprovechamiento óptimo de la inversión en ambos servicios.

Configuración Activa-Pasiva: El enlace primario maneja todo el tráfico, mientras el secundario permanece en espera (standby). Ante falla del primario, se activa automáticamente el secundario. Ofrece:

- Menor complejidad de configuración.
- Menor costo operativo (el enlace secundario puede ser de menor capacidad).
- Tiempo de conmutación ligeramente mayor (30-60 segundos).

Diversificación Tecnológica

Para maximizar la resiliencia, el servicio alternativo debe utilizar tecnología y rutas físicas diferentes al servicio principal:

Si el servicio principal es fibra óptica terrestre:

- El alternativo podría ser fibra por ruta diferente, enlaces de microondas, o conexión satelital.

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Si el servicio principal utiliza proveedor con infraestructura nacional:

- El alternativo debería ser proveedor con backbone internacional independiente.

Esta diversificación garantiza que eventos que afecten a un proveedor (cortes de fibra en ruta específica, problemas con carrier upstream) no comprometan ambos enlaces simultáneamente.

Cumplimiento Normativo

La implementación de planes de continuidad operativa no es meramente una buena práctica técnica, sino una obligación legal en muchos sectores. Las instituciones de salud pública están sujetas a:

- Leyes de gobierno electrónico que exigen disponibilidad de servicios digitales.
- Normativas de protección de datos que requieren medidas de disponibilidad.
- Estándares de gestión de calidad ISO 9001 que demandan prevención de interrupciones.
- Regulaciones específicas de salud pública sobre tiempos de respuesta.

El incumplimiento de estas obligaciones puede derivar en responsabilidades administrativas, civiles e incluso penales para autoridades institucionales.

Beneficios Operativos Adicionales

Más allá de la función de respaldo, el servicio alternativo aporta:

Mejora en Calidad de Servicio:

- Reducción de latencia mediante enrutamiento inteligente.
- Mayor ancho de banda agregado para aplicaciones intensivas.
- Separación de tráfico crítico y no crítico por enlaces diferenciados.

Flexibilidad Operativa:

- Capacidad de realizar mantenimientos preventivos sin afectar operaciones.
- Posibilidad de migración gradual entre proveedores sin riesgo.
- Opciones de negociación mejoradas con proveedores al no tener dependencia absoluta.

ESCALAMIENTO CON FABRICANTE/PROVEEDOR

Modelo de Soporte Técnico Estructurado

La contratación formal de servicios de Internet empresariales incluye obligatoriamente esquemas de soporte técnico escalonado que garantizan resolución eficiente de incidencias. Este modelo, conocido como **Service Level Agreement (SLA)**, establece:

Niveles de Escalamiento:

Nivel 1 - Mesa de Ayuda (Helpdesk):

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- Atención 24/7/365 vía telefónica, correo electrónico y chat.
- Personal capacitado para diagnóstico inicial de problemas.
- Resolución de incidencias básicas (reinicio de equipos, verificación de configuraciones).
- Tiempo de primera respuesta: < 15 minutos.
- Tasa de resolución en primera llamada: objetivo 40-60%.

Nivel 2 - Soporte Técnico Especializado:

- Ingenieros de campo con capacidad de desplazamiento a sitio.
- Diagnóstico avanzado mediante herramientas de monitoreo remoto.
- Resolución de problemas de configuración, calidad de señal, interferencias.
- Tiempo de escalamiento desde Nivel 1: < 30 minutos.
- Tiempo de llegada a sitio: < 4 horas (según SLA contratado).

Nivel 3 - Ingeniería de Red y NOC:

- Equipo de ingenieros senior con acceso a infraestructura troncal del proveedor.
- Capacidad de reconfiguración de enrutamiento, asignación de recursos de red.
- Coordinación con proveedores upstream para problemas de conectividad internacional.
- Involucramiento en incidencias complejas o no resueltas en Nivel 2.
- Disponibilidad 24/7 con tiempos de respuesta crítica.

Nivel 4 - Gerencia y Relación Comercial:

- Ejecutivo de cuentas asignado como punto de contacto único.
- Escalamiento ejecutivo para incidencias con impacto crítico al negocio.
- Coordinación de visitas técnicas preventivas y auditorías de servicio.
- Gestión de cambios, actualizaciones y proyectos de mejora.

Acuerdos de Nivel de Servicio (SLA) Garantizados

Los contratos empresariales de Internet establecen compromisos medibles y penalizables:

Disponibilidad del Servicio:

- SLA estándar: 99.5% de disponibilidad mensual (tiempo de inactividad máximo: ~3.6 horas/mes).
- SLA premium: 99.9% de disponibilidad mensual (tiempo de inactividad máximo: ~43 minutos/mes).
- SLA crítico: 99.95% o superior (tiempo de inactividad máximo: ~22 minutos/mes).

Tiempos de Respuesta y Resolución:

- Tiempo de respuesta inicial a reporte de incidencia: 15-30 minutos.
- Tiempo de resolución para incidencias críticas (servicio totalmente caído): 4-8 horas.
- Tiempo de resolución para incidencias de degradación: 12-24 horas.

Penalizaciones por Incumplimiento: Los SLA incluyen cláusulas de compensación económica (créditos en facturación) cuando el proveedor no cumple los niveles garantizados, típicamente:

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- 10-25% de crédito por incumplimiento leve.
- 50-100% de crédito por incumplimientos graves o reiterados.
- Derecho a terminación anticipada sin penalidad por incumplimientos sistemáticos.

Gestión Proactiva vs. Reactiva

El modelo de escalamiento profesional permite transitar de una postura reactiva (resolver problemas cuando ocurren) a una gestión proactiva:

Monitoreo Continuo:

- El proveedor implementa sistemas de monitoreo 24/7 sobre el enlace institucional.
- Alertas automáticas ante degradación de parámetros (latencia, pérdida de paquetes, fluctuación).
- Detección y corrección de problemas antes de que impacten operaciones.

Mantenimientos Preventivos:

- Actualizaciones de firmware en equipos de cliente programadas en ventanas de bajo impacto.
- Inspecciones periódicas de infraestructura física (cables, conectores, equipos).
- Pruebas de respaldo y conmutación automática de enlaces.

Reportes y Analítica:

- Informes mensuales de desempeño del servicio con estadísticas de disponibilidad, latencia, throughput.
- Análisis de tendencias de consumo de ancho de banda para planificación de capacidad.
- Documentación de incidencias con tiempos de respuesta y resolución.

Ventajas del Modelo Contractual Formal

Contratar servicios empresariales versus soluciones residenciales proporciona:

Respaldo Legal y Contractual:

- Contrato formal que establece derechos, obligaciones y recursos legales.
- Garantías comerciales exigibles jurídicamente.
- Protección ante incumplimientos mediante cláusulas penales.

Priorización de Servicio:

- Los clientes empresariales reciben prioridad sobre residenciales en asignación de recursos técnicos.
- Acceso directo a ingeniería sin colas de espera extensas.
- Compromiso de atención preferente en situaciones de múltiples incidencias simultáneas.

Comunicación Institucional:

Ing. Julio C[illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- Canal directo con gerencia comercial del proveedor.
- Posibilidad de coordinar necesidades especiales (incrementos temporales de ancho de banda, configuraciones específicas).
- Participación en programas de clientes corporativos con beneficios adicionales.

Escalamiento para el Servicio Alternativo

Contar con un servicio alternativo NO duplica los problemas de gestión, sino que FORTALECE la capacidad de escalamiento:

- **Diversificación de opciones:** Ante problemas críticos con un proveedor, se mantiene la operación por el otro mientras se resuelve.
- **Presión competitiva:** La existencia de un proveedor alternativo incentiva mejor calidad de servicio de ambos.
- **Comparación de desempeño:** Métricas paralelas permiten identificar objetivamente cuál proveedor ofrece mejor calidad.
- **Redundancia en soporte:** Equipos técnicos independientes multiplicando capacidad de respuesta institucional.

GESTIÓN DE RIESGOS

Marco Metodológico de Gestión de Riesgos

La gestión de riesgos tecnológicos en instituciones públicas se fundamenta en estándares como ISO 31000 (Gestión de Riesgos) e ISO/IEC 27005 (Gestión de Riesgos de Seguridad de la Información). El proceso sistemático incluye:

Identificación → Análisis → Evaluación → Tratamiento → Monitoreo

Para servicios de conectividad críticos, esta metodología identifica amenazas específicas que la contratación de un servicio alternativo mitiga eficazmente.

Matriz de Riesgos Identificados

RIESGO 1: Interrupción Prolongada del Servicio Principal

- **Probabilidad:** MEDIA-ALTA (1-3 eventos por año en promedio nacional).
- **Impacto:** CRÍTICO (paralización operativa total).
- **Exposición sin control:** Pérdidas elevadas por evento + impacto en salud pública.
- **Mitigación con servicio alternativo:** Conmutación automática, continuidad del 95-100% de operaciones.
- **Reducción de riesgo:** 90-95%.

RIESGO 2: Degradación de Calidad del Servicio (Latencia, Pérdida de Paquetes)

- **Probabilidad:** ALTA (múltiples episodios mensuales).
- **Impacto:** MODERADO-ALTO (lentitud operativa, timeouts de aplicaciones).
- **Exposición sin control:** Pérdida de productividad 10-30%, frustración de usuarios.
- **Mitigación:** Balanceo de carga, enrutamiento por enlace de mejor desempeño.

Ing. Julio Caballero
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- **Reducción de riesgo:** 70-80%.

RIESGO 3: Ataques de Ciberseguridad (DDoS, Intrusiones)

- **Probabilidad:** MEDIA (instituciones públicas son objetivos frecuentes).
- **Impacto:** CRÍTICO (indisponibilidad de servicios, comprometimiento de datos).
- **Exposición sin control:** Caída de servicios públicos, filtración de información sensible.
- **Mitigación:** Diversificación de puntos de ingreso, segregación de tráfico, filtrado distribuido.
- **Reducción de riesgo:** 50-60%.

RIESGO 4: Desastres Naturales o Daños de Infraestructura

- **Probabilidad:** BAJA-MEDIA (dependiendo de ubicación geográfica).
- **Impacto:** CATASTRÓFICO (interrupción por días o semanas).
- **Exposición sin control:** Paralización institucional completa, costos millonarios.
- **Mitigación:** Rutas físicas diversificadas, tecnologías alternativas (terrestre/inalámbrica).
- **Reducción de riesgo:** 85-95%.

RIESGO 5: Obsolescencia o Fin de Vida del Servicio Actual

- **Probabilidad:** MEDIA (cambios tecnológicos, reestructuraciones empresariales).
- **Impacto:** ALTO (necesidad de migración urgente sin preparación).
- **Exposición sin control:** Interrupción durante migración, costos elevados por urgencia.
- **Mitigación:** Servicio alternativo operativo permite migración planificada y sin prisa.
- **Reducción de riesgo:** 100%.

RIESGO 6: Incumplimiento de SLA por Parte del Proveedor

- **Probabilidad:** MEDIA (estadísticas sectoriales indican 15-30% de incumplimientos anuales).
- **Impacto:** MODERADO (afectación de operaciones, sin compensación suficiente).
- **Exposición sin control:** Dependencia absoluta, capacidad de negociación nula.
- **Mitigación:** Competencia entre proveedores, opción de cambio inmediato.
- **Reducción de riesgo:** 60-70%.

Retorno de Inversión (ROI): Incluso en el escenario más conservador, evitar una sola interrupción crítica por año justifica completamente la inversión del servicio alternativo, con ROI superior al 300-1000%.

Gestión de Riesgos de Seguridad de la Información

La conexión dual proporciona beneficios adicionales de ciberseguridad:

Segregación de Tráfico:

- Tráfico crítico (sistemas transaccionales, bases de datos) por enlace dedicado.
- Tráfico general (navegación, correo) por enlace separado.
- Reducción de superficie de ataque y contención de amenazas.

Ing. Julio [illegible]rdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Redundancia de Controles de Seguridad:

- Firewalls y sistemas IPS en ambos enlaces.
- Detección de anomalías comparando patrones de tráfico entre enlaces.
- Capacidad de cerrar un enlace comprometido sin perder conectividad.

Cumplimiento Normativo de Seguridad:

- Requisitos de redundancia en normativas de protección de datos personales.
- Estándares de seguridad de información (ISO 27001) que exigen controles de disponibilidad.
- Auditorías de seguridad valoran positivamente arquitecturas resilientes.

Estrategia de Respuesta a Incidentes

El servicio alternativo debe generar un **Plan de Respuesta a Incidentes de TI** institucional:

Fase de Detección:

- Monitoreo automatizado detecta falla en enlace primario.
- Alertas inmediatas al equipo técnico y sistemas de gestión.

Fase de Contención:

- Conmutación automática a enlace alternativo (< 1 minuto).
- Comunicación interna sobre el incidente y estado de contingencia.

Fase de Erradicación:

- Trabajo con proveedor afectado para diagnóstico y reparación.
- Operación normal continúa por enlace alternativo sin presión de tiempo.

Fase de Recuperación:

- Pruebas de restauración del enlace primario.
- Retorno a configuración normal una vez verificada estabilidad.
- Documentación del incidente y lecciones aprendidas.

Fase de Post-Incidente:

- Análisis de causa raíz y medidas correctivas.
- Actualización de procedimientos y documentación.
- Evaluación de desempeño de proveedores.

Riesgos de NO Implementar Servicio Alternativo

La ausencia de redundancia configura en sí misma un riesgo inaceptable:

Riesgo Operacional:

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- Exposición total a fallas de proveedor único.
- Incapacidad de respuesta ante emergencias sanitarias durante cortes.

Riesgo Reputacional:

- Percepción pública negativa por servicios no disponibles.
- Pérdida de confianza de operadores regulados.

Riesgo Legal:

- Incumplimiento de normativas de continuidad operativa.
- Responsabilidad por daños derivados de interrupciones prevenibles.

Riesgo Financiero:

- Pérdidas económicas directas e indirectas.
- Costos de recuperación ante interrupciones prolongadas.

POSVENTA Y SOPORTE CONTINUO

Concepto de Servicio Posventa en Telecomunicaciones

A diferencia de productos tangibles donde la posventa se limita a garantías y reparaciones puntuales, en servicios de telecomunicaciones el **soporte posventa es la esencia misma del servicio contratado**. El verdadero valor no radica en la instalación inicial, sino en la gestión continua, optimización y soporte durante toda la vigencia contractual.

Componentes del Servicio Posventa Integral

A) Gestión de Cuenta Dedicada

Los proveedores empresariales asignan un **Gerente de Cuenta (Account Manager)** como punto de contacto único institucional:

- **Relación personalizada:** Conocimiento profundo de necesidades, configuración y particularidades del cliente.
- **Visitas periódicas:** Reuniones trimestrales de revisión de servicio, identificación de oportunidades de mejora.
- **Coordinación ejecutiva:** Facilita escalamientos urgentes, gestiona solicitudes especiales, actúa como vocero institucional ante áreas técnicas del proveedor.
- **Planificación estratégica:** Asesora sobre evolución tecnológica, migraciones, ampliaciones de capacidad.

B) Centro de Operaciones de Red (NOC) 24/7/365

El NOC constituye el cerebro operativo que garantiza funcionamiento ininterrumpido:

- **Monitoreo proactivo:** Supervisión continua de parámetros de desempeño (latencia, jitter, pérdida de paquetes, utilización de ancho de banda).

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- **Alertas tempranas:** Notificación automática ante anomalías o degradaciones antes de que impacten usuarios.
- **Intervención preventiva:** Ajustes de configuración, balanceo de carga, optimización de enrutamiento sin intervención del cliente.
- **Reportería detallada:** Dashboards en tiempo real, reportes mensuales de disponibilidad, análisis de incidencias.

C) Soporte Técnico Especializado

Equipo de ingenieros con alto nivel de conocimiento en:

- **Diagnóstico avanzado:** Herramientas de análisis de tráfico, medición de calidad de enlaces, identificación de cuellos de botella.
- **Resolución remota:** 80-90% de problemas se resuelven sin necesidad de visita a sitio mediante acceso remoto seguro.
- **Soporte en sitio:** Cuando se requiere, ingeniero de campo se desplaza con equipamiento de reemplazo y herramientas de medición.
- **Capacitación continua:** Sesiones de training para personal técnico institucional sobre mejores prácticas, nuevas funcionalidades, troubleshooting.

D) Mantenimiento Preventivo Programado

A diferencia de la actitud reactiva, el mantenimiento preventivo profesional incluye:

- **Inspecciones físicas periódicas:** Revisión de cableado, conectores, equipos terminales, condiciones ambientales (temperatura, humedad).
- **Actualizaciones de software/firmware:** Parches de seguridad, nuevas funcionalidades, correcciones de bugs en equipos de cliente.
- **Pruebas de failover:** Verificación trimestral de que mecanismos de conmutación automática funcionan correctamente.
- **Limpieza y optimización:** Depuración de configuraciones, eliminación de reglas obsoletas en firewalls, optimización de tablas de enrutamiento.

E) Garantía de Equipamiento

Los equipos proporcionados por el proveedor (routers, modems, switches) incluyen:

- **Garantía de fábrica extendida:** Cobertura total durante vigencia contractual.
- **Reemplazo inmediato:** Inventario de equipos de respaldo para sustitución en < 4 horas.
- **Actualización tecnológica:** Cuando equipos quedan obsoletos, el proveedor los actualiza sin costo adicional.
- **Propiedad según modelo:** Algunos contratos transfieren propiedad al cliente al finalizar, otros mantienen propiedad del proveedor.

Valor del Soporte Continuo para Servicios Duales

Cuando se opera con dos proveedores de Internet simultáneamente, la posventa adquiere dimensiones adicionales:

Ing. Julio C[illegible]dan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

Coordinación entre Proveedores: Aunque cada proveedor opera independientemente, situaciones complejas requieren coordinación:

- **Problemas de enrutamiento BGP:** Cuando se implementa enrutamiento avanzado con ambos proveedores.
- **Optimización de balanceo:** Ajustes finos de distribución de tráfico según patrones de uso.
- **Resolución de incompatibilidades:** Configuraciones que funcionan individualmente pero generan conflictos al operar simultáneamente.

El personal técnico institucional actúa como orquestador, pero cuenta con soporte especializado de ambos proveedores.

Benchmarking y Mejora Continua: La existencia de dos servicios permite comparación objetiva:

- **Métricas de disponibilidad:** ¿Cuál proveedor tiene menos interrupciones?
- **Calidad de servicio:** ¿Cuál ofrece mejor latencia, menor jitter?
- **Eficiencia de soporte:** ¿Cuál responde más rápido y resuelve mejor?

Esta información empodera decisiones estratégicas (renovaciones, renegociaciones, cambios de proveedor).

Servicios de Valor Agregado Incluidos

Los contratos empresariales suelen incluir servicios complementarios sin costo adicional:

Seguridad Gestionada:

- **Protección DDoS básica:** Mitigación de ataques de denegación de servicio distribuido a nivel de red del proveedor.
- **Filtrado de contenido:** Bloqueo de sitios maliciosos, phishing, malware mediante DNS seguro.
- **Reportes de amenazas:** Alertas sobre intentos de intrusión, escaneos de puertos, tráfico anómalo.

Optimización de Aplicaciones:

- **Priorización de tráfico (QoS):** Garantía de ancho de banda para aplicaciones críticas (videoconferencia, VoIP, sistemas transaccionales).
- **Aceleración de contenido:** Cacheo de contenido frecuente, compresión de datos, optimización de protocolos.
- **Monitoreo de aplicaciones:** Visibilidad sobre desempeño de aplicaciones específicas (Office 365, etc.)

Consultoría Técnica:

- **Asesoría en arquitectura:** Recomendaciones sobre mejores configuraciones, implementación de nuevas tecnologías.
- **Planificación de capacidad:** Análisis de crecimiento de tráfico, proyecciones de necesidades futuras.

Ing. Julio C. [illegible]rdan
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

- **Estudios de caso:** Acceso a mejores prácticas de otros clientes similares (con anonimización).

Ciclo de Vida del Servicio y Renovaciones

La relación posventa se extiende a lo largo de múltiples ciclos contractuales:

Evaluación Anual de Desempeño:

- Revisión formal de cumplimiento de SLA.
- Análisis de incidencias y tiempo promedio de resolución.
- Satisfacción del cliente y áreas de mejora.
- Decisiones sobre renovación, renegociación o cambio de proveedor.

Actualización Tecnológica Proactiva:

- Notificación sobre nuevas tecnologías disponibles (fibra simétrica, SD-WAN, 5G).
- Migración asistida a planes superiores o nuevas plataformas.
- Ventanas de oportunidad para upgrades sin costo durante renovaciones.

Flexibilidad Contractual:

- Cláusulas de ajuste de capacidad (aumentos temporales o permanentes).
- Opciones de agregar servicios complementarios (VPN, hosting, telefonía IP).
- Términos justos de finalización anticipada si las necesidades cambian radicalmente.

Medición de Calidad del Soporte Posventa

Para garantizar valor continuo, se establecen KPIs de gestión posventa:

- **MTTR (Mean Time To Repair):** Tiempo promedio de reparación < 4 horas para incidencias críticas.
- **First Contact Resolution:** Resolución en primer contacto > 50%.
- **Customer Satisfaction (CSAT):** Satisfacción post-soporte > 85%.
- **Disponibilidad real:** Cumplimiento de SLA > 99.5%.
- **Proactividad:** Ratio de problemas detectados por el proveedor vs. reportados por el cliente > 60%.

Síntesis de Justificación

La contratación de un servicio de Internet alternativo para la Dirección Nacional de Vigilancia Sanitaria no constituye un gasto discrecional ni una redundancia superflua, sino una **inversión estratégica esencial** fundamentada en:

1. **Criticidad Absoluta:** Las operaciones de vigilancia sanitaria son funciones de Estado irrenunciables que protegen directamente la salud y la vida de la población. La conectividad Internet es infraestructura crítica que sostiene procesos misionales tiempo-dependientes.

Ing. Julio [illegible]
Director
Dirección de Tecnología de la Información y Comunicación
DINAVISA

2. **Imperativo de Continuidad:** Los estándares internacionales, obligaciones legales y mejores prácticas exigen redundancia en servicios críticos. Un punto único de falla es inaceptable en instituciones de esta naturaleza.
3. **Respaldo Técnico Robusto:** Los servicios empresariales proveen mecanismos de escalamiento, soporte profesional y gestión proactiva que multiplican la capacidad de respuesta institucional ante incidencias.
4. **Mitigación Efectiva de Riesgos:** La inversión anual en redundancia es marginal comparada con el costo potencial de una sola interrupción crítica, logrando un retorno de la inversión superior al 300-1000%.
5. **Valor Continuo del Soporte:** La posventa profesional transforma la conectividad de un servicio básico en un servicio gestionado que evoluciona con las necesidades institucionales.

En consecuencia, la experiencia y la antigüedad exigidas no restringen la competencia de manera arbitraria, sino que constituyen condiciones técnicas directamente vinculadas al nivel de riesgo del servicio y la naturaleza estratégica de los sistemas sanitarios bajo responsabilidad de DINAVISA.

Indicar si la compra es periódica/sucesiva o responde a una necesidad temporal.

El servicio responde a una necesidad sucesiva de la Dirección de Tecnología de la Información y Comunicación.

Identificar y justificar de forma expresa si algún requerimiento podría limitar la participación de potenciales oferentes.

Las Bases y Condiciones del llamado a Licitación son participativas y abiertas para todos los potenciales oferentes.

Si en las bases licitatorias se indican una marca específica u otro derecho intelectual exclusivo, mencionar la justificación que respalda lo solicitado o que no existe otro modo de identificarlo. Se aclara que, en caso de incluirlos, los mismos tendrán carácter referencial.

No Aplica.

Obs.:
-En caso de citar o remitirse al análisis o argumentos contenidos en otra documentación, se debe adjuntar la misma al presente dictamen.
-Podrán formar parte de los argumentos técnicos de este dictamen, el análisis previo citado en el artículo 25 de la Ley N° 7021/22, los resultados de dicho análisis o los documentos que lo integran.

Ing. Julio [illegible]
Dirección de Tecnología de la Información y Comunicación
DINAVISA